SKI Report 2004:04

Research

Dependency Defence and Dependency Analysis Guidance

Volume 2: Appendix 3-8

How to analyse and protect against dependent failures. Summary report of the Nordic Working group on Common Cause Failure Analysis

Gunnar Johanson
Per Hellström
Tuomas Makamo
Jean-Pierre Bento
Michael Knochenhauer
Kurt Pörn

October 2003

ISSN 1104–1374
ISRN SKI-R-04/04-SE

SKI

SKI PERSPEKTIV

Bakgrund
SKI ställer krav på PSA-studier och PSA-verksamhet i SKIFS 1998:1. Uppföljning av denna verksamhet ingår därför i SKI:s tillsynsverksamhet. Enligt krav i SKIFS 1998:1 skall säkerhetsanalyserna vara grundade på en systematisk inventering av sådana händelser, händelseförlopp och förhållanden vilka kan leda till en radiologisk olycka.

Forskningsrapporten *Vägledning för försvar och analys av beroenden* har utvecklats på uppdrag av Nordiska PSA-gruppen (NPSAG), med syftet att skapa en gemensam erfarenhetsbas för försvar och analys av beroende fel, s.k. Common Cause Failures (CCF).

SKI:s och rapportens syfte
Ordet Vägledning i rapporttiteln används för att tydliggöra en gemensam metodologisk och av NPSAG accepterad vägledning som baserar sig på den allra senaste kunskapen om analys av beroende fel och anpassade till förhållanden som anses gälla för nordiska kärnkraftverk. Detta kommer att göra det möjligt för tillståndshavarna att genomföra kostnadseffektiva förbättringar och analyser.

Resultat
Rapporten *Vägledning för försvar och analys av beroenden* presenterar ett gemensamt försök, mellan myndighet och tillståndshavare, att skapa en metodologi och erfarenhetsbas för försvar och analys av beronde fel.

Eventuell fortsatt verksamhet inom området
Erfarenheter från tillämpningen av rapportens vägledningar skall inväntas, eventuella större ändringar och tillägg i vägledningsdokumentet beslutas om vid senare tillfälle. Utveckling av metoder och förfining av sådana pågår dock, vartefter det ställs högre krav på nya analysförutsättningar och -djup.

Effekt på SKI:s verksamhet
SKI Rapport 04:04 - *Vägledning för försvar och analys av beroenden* bedöms även vara ett bra stöd för myndigheterna i sin granskning av olika tillståndshavares verksamhetsprocesser, analysmetoder förknippade med analyser av beroende fel.

Projektinformation
SKI:s projekthandläggare: Ralph Nyman
Projektnummer: 01031
Dossié-diarienummer: 14.2-010001

SKI PERSPECTIVE

Background
The Swedish Nuclear Inspectorate (SKI) Regulatory Code SKIFS 1998:1 includes requirements regarding the performce of probabilistic safety assessments (PSA), as well as PSA activities in general. Therefore, the follow-up of these activities is part of the inspection tasks of SKI. According to SKIFS 1998:1, the safety analyses shall be based on a systematic identification and evaluation of such events, event sequences and other conditions which may lead to a radiological accident.

The research report *"Dependency Defence and Dependency Analysis Guidance"* has been developed under a contract with the Nordic PSA Group (NPSAG), with the aim to create a common experience base for defence and analysis of dependent failures i.e., Common Cause Failures, CCF.

The Aim of SKI and of the Report
The word *Guidance* in the report title is used in order to indicate a common methodological guidance accepted by the NPSAG, based on current state of the art concerning the analysis of dependent failures and adapted to conditions relevant for the Nordic Nuclear Power Plants. This will make it possible for the utilities to perform cost effective improvements and analyses.

Results
The report *"Dependency Defence and Dependency Analysis Guidance"* presents a common attempt by the authorites and the utilities to create a methodology and experience base for defence and analysis of dependet failures.

Possible Continued Activities within the Area
Experiences from the application of the Guidance shall be awaited for, i.e., major changes or extensions to the document shall be decided at a later stage. However, the development of methods is an on-going process which is guided by changes in analysis assumptions or increased level of detailed of the analysis.

Effect on SKI Activities
The SKI Report 04:04 *"Dependency Defence and Dependency Analysis Guidance"* is judged to be useful in supporting the authority's review of procedural and organizational processes at utilities, methodology for the analysis of dependent failures.

Project Information
Project responsible at SKI: Ralph Nyman
Project number: 01031
Dossier Number: 14.2-010001

SKI Report 2004:04

Research

Dependency Defence and Dependency Analysis Guidance

Volume 2: Appendix 3-8

How to analyse and protect against dependent failures. Summary report of the Nordic Working group on common Cause Failure Analysis

Gunnar Johanson
ES-konsult AB, Svetsarvägen 7, SE-171 41 Solna, Sweden

Per Hellström
Relcon AB, Box 1288, SE-172 25 Sundbyberg, Sweden

Tuomas Mankamo
Avaplan Oy, Itainen rantatie 17B, FIN-0223

Jean-Pierre Bento
JPB Consulting AB, Box 68, SE-611 23 Nyköping, Sweden

Michael Knochenhauer
Impera-K AB, Kyrkvägen 20, SE-196 30 Kungsängen, Sweden

Kurt Pörn
Pörn Consulting AB, Skivlingvägen 24, SE-611 63 Nyköping, Sweden

October 2003

Outline of project reporting

	Title	Report No
SKI REPORT 04:04 Volume 1		
Summary	Summary report of the Nordic Working group on Common Cause Failure Analysis	PR21
Appendix 1	Dependency Defence Guidance	PR12
Appendix 2	Dependency Analysis Guidance	PR13
	150 pages	
SKI REPORT 04:04 Volume 2		
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures	PR05
Appendix 3.2	Defence Assessment in Data	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey	PR04
Appendix 4.2	Impact Vector Method	PR03
Appendix 4.3	Impact Vector Construction Procedure	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels	PR10
Appendix 5.6	Impact Vector Application to Pumps	PR18
Appendix 5.7	Impact Vector Application to MOV	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties	PR15
Appendix 6	Literature survey	PR06
Appendix 7	Terms and definitions	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme	PR01
	540 pages	

Project Report list: SKI REPORT 04:04

No	Title	Appendix
PR01	Nordisk Arbetsgrupp för CCF Studier, Project Programme	Appendix 8
PR02	Data Survey and Review	Appendix 5.1
PR03	Impact Vector Method	Appendix 4.2
PR04	Model Survey	Appendix 4.1
PR05	Survey of defences against dependent failures	Appendix 3.1
PR06	Literature survey	Appendix 6
PR08	Qualitative analysis of the ICDE database for Swedish emergency diesel generators	Appendix 5.3
PR09	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs	Appendix 5.4
PR10	Impact Vector Application to Diesels	Appendix 5.5
PR11	Data survey and review of the ICDE-database for Swedish emergency diesel generators	Appendix 5.2
PR12	Dependency Defence Guidance	Appendix 1
PR13	Dependency Analysis Guidance	Appendix 2
PR14	Terms and definitions	Appendix 7
PR15	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties	Appendix 5.8
PR17	Impact Vector Construction Procedure	Appendix 4.3
PR18	Impact Vector Application to Pumps	Appendix 5.6
PR19	Impact Vector Application to MOV	Appendix 5.7
PR20	Defence Assessment in Data	Appendix 3.2
PR21	Summary report	

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
App3.1	**Survey of defences against dependent failures PR05**	**PR05**
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title:	Survey on Defences against Dependent Failures
Author(s):	Per Hellström, RELCON AB
Issued By:	Per Hellström, RELCON AB
Reviewed By:	Michael Knochenhauer, Impera-K, Tuomas Mankamo, Avaplan OY
Approved By:	Gunnar Johansson
Abstract:	This report presents a plant and regulatory survey on defences against dependent failures. The survey is carried out as part of the qualitative work performed within the Nordiska arbetsgruppen för CCF studier (NAFCS). The survey investigates current plant and regulatory strategies for defence against dependent failures, and especially common cause failures. Examples on defences in use are presented.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public??

Revision control:	Version	Date	Initial
Created	A1	2001-10-24	PH
For presentation at SKI CCF seminar	A2	2002-03-11	PH
For internal review	A3	2002-03-18	PH
Consideration of MK and TM comments: New title,	A4	2002-09-09	PH
Final update	F1 rev 0	2003-08-31	PH

List of Content

List of tables

Appendices

A) Questionnaire and items for discussion for Plant Survey Meetings
B) Agenda for Plant Survey Visits
C) Notes from STUK Visit[1]
D) Notes from SKI Visit[1]
E) Notes from OKG Visit[1]
F) Notes from BKAB Visit[1]
G) Notes from TVO Visit[1]
H) Notes from Forsmark Visit[1]

Terms and Abbreviations

BKAB	Barsebäck Kraft AB
BWR	Boiling Water Reactor
Bicycle	Tool for accessing TUD database with failure records
CCF	Common Cause Failure
CFR	Code of Federal Regulation
CRDA	Control Rod Drive Assembly
DKV	Driftklarhetsverifiering (operational readiness control)
FKA	Forsmarks Kraftgrupp AB
GDC	General Design Criteria
IAEA	International Atomic Energy Agency
ICDE	International Common Cause Data Exchange

[1] The notes from the visits are stored in a separate Worknote and are not published

INPO	International Nuclear Power Organisation
KFB	Konstruktionsförutsättningar för byggnader
KFE	Konstruktionsförutsättningar för elektriska komponenter
KFM	Konstruktionsförutsättningar för mekaniska komponenter
KSU AB	Kärnkraftsäkerhet och utbildning AB (Nuclear Safety and Training Center)
NAFCS	Nordisk Arbetsgrupp för CCF-studier
NOG	Nuclear Owners Group
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OKG	Oskarhamns Kraftgrupp
PSA	Probabilistic Safety Assessment
PSG	Primär Säkerhetsgranskning (Primary Safety Review)
RO	Rapporterbar omständighet (LER/Licensee Event Report)
SAR	Safety Analysis Report
SKI	Statens Kärnkraftinspektion (Swedish Nuclear Authority)
SKIFS	SKI författningssamling (SKI statute books)
STF	Säkerhetstekniska förutsättningar (Technical Specifications)
STUK	Radiation and Nuclear Safety Authority of Finland
TBE	Tekniska bestämmelser för elkomponenter (Technical rules for Electrical Components)
TBM	Tekniska bestämmelser för mekaniska komponenter (Technical rules for Mechanical Components)
TUD	Tillförlitlighet Underhåll Drift (Department at Swedpower responsible for collecting and distribution of reliability related information
TVO	Teollisuuden Voima Oy
WANO	World Association for Nuclear Operation

Survey on Defence against Dependent Failures

1 Introduction

1.1 Background

Defence in depth is a basic safety precaution in a NPP, and it is realised by redundancy and separation/diversity. It is important that redundant equipment have as little as possible in common in order to decrease the risk for dependent failures.

It is obvious that functional dependencies, like two redundancies being dependent on the same signal or power supply, is a bad solution in cases where high reliability and safety is needed. There has to be a complete separation on functional level to avoid that a single failure interrupts a function.

Spatial dependencies may also be critical, due to the potential for so called area events like fires, flood and also the same normal environment affecting components in the same location. Separation of redundancies in different locations or at least by distance is therefore also an important defence against dependent failures.

Both functional and area dependencies can in a safety analysis be treated with explicit modelling and the defences are quite obvious. A PSA model can be used to verify that the single failure criterion is fulfilled, and also to find cases of violation in functional separation. Identification of weaknesses in spatial separation can also be checked, e g by special use of the PSA model.

Still, there are so called subtle interactions due to commonalities on a very low level of detail that can decrease the efficiency of redundancies. These kinds of dependencies are in probabilistic safety analysis treated as so called common causes and their impact on the reliability is calculated with common cause failure analysis methods.

The basic CCF formula for a system with 2*100% redundancy is (beta factor):

$$P_{system} = ((1-\beta) * P_{train})^2 + \beta * P_{train}$$

P_{system} Total system failure probability

P_{train} Train failure probability

β CCF factor, indicating the share of independent failure probability that affects both trains.

The formula shows that there are two ways to increase the system reliability performance.

1. High reliability of individual trains, i e low P_{train}
2. Low dependency between the trains, i e low CCF contribution (low β).

Many factors contribute to a high reliability, and they may also contribute to keep the risk for common cause failures on a low level. There are in addition factors that are targeted against CCF. The survey described below concentrated on the latter factors of defence, but several factors effective to consider other dependencies in general are also included.

1.2 Objectives

The objectives for the survey as presented in the NAFCS project programme [1] were to provide a background to the NAFCS project based on the needs and experience from the plant owners and from authorities:

1. Survey of plant objectives in relation to CCF defences
2. Survey of plant operations/events in relation to CCF
3. Survey of plant modifications in relation to CCF
4. Survey of plant organisation/rules (extension compared to project programme)
5. Survey of authority requirements, guidance and activities (extension compared to project programme)

Important elements of the survey were also to carry out a dialog with the organisations to engage them in the issues related to the programme and to market the outcome and use of the project.

The survey should reach a wide spectrum of personnel from operation, design engineering, safety committees and risk assessment groups

The final survey result considers several CCF defence areas as can be seen in the result section.

The survey focussed on the way that the plants and authorities provide a defence against dependent failures (standards, quality assurance system, internal guidelines and work descriptions and practices in use) with special attention for common cause failure defences.

The results of the survey are to be used for further processing within the project for the following purposes:

1. Creation of a Qualitative CCF defence model
2. Discussion on potential benefit of existing defences in quantitative CCF analysis
3. Input to a defence guidance document.

1.3 Scope of Dependency Defences Survey

The scope is (implicitly) restricted to CCF type dependencies (component failure dependencies, pre-initiator error dependencies).

It became evident during the visits that it is difficult to completely separate common cause failure defences from other dependency defences, e g defences with regard to area dependencies and functional dependencies. Certain defences will be effective against several types of dependencies.

The defences that are looked at are in principal restricted to defences that decrease the probability for common cause failures.

Section 2 presents the survey activity, section 3 presents the results and section 4 the conclusions of the survey.

2 Survey Organisation

2.1 Survey Meetings

The organisations listed in Table 1 are included in the survey.

Table 1: Organisations Covered by the Survey Activity.

	Date and duration of visit	Meeting participants[2]
OKG	2001-09-18 (1 day, whole group together)	Frithiof Schwartz, TR, Michael Landelius, TR, John Svensson, D2Q-D, Johan Melkersson, D3D, Mats Gustafsson, D1F.
Barsebäck	2001-09-19 (1 day, whole group together)	Ingemar Ingemarsson, PSA/FoU, André Strömberg, SP (maintenance/planning), Ulf Hansson, BTS (Control room, BOKA, SAR/PSA)
SKI	2001-11-07 (2 hours, whole group together)	Ralph Nyman, Anders Hallman, Bo Liwång, Kjell Olsson
STUK	2001-11-21 (2 hours, whole group together)	Reino Virolainen, Ilkka Niemelä
TVO	2001-11-30 (1 day, separate small meetings and summary meeting)	Jari Pesonen and Risto Himanen (PSA group), Ingvald Lilja (Operation), Markku Friberg and O Luhta (Safety committee), J Tanhua (Maintenance), Sami Jakonen (Enginering).
Forsmark	2001-12-03 (4 hours, whole group together)	Jan-Erik Stenmarck, Bjarne Grönqvist (cFTE)

Ringhals could not participate in the survey visits.

The following material was used as a basis for the discussions and was sent to the organisations before the meetings[3]:

1. A questionnaire (see appendix A). The questionnaire contains questions, statements and explanations in rather raw form. The discussions were structured against this questionnaire).
2. A copy of the report “Defences Against Common Cause Failures.. “ [2]
3. A PowerPoint presentation of the project
4. Site specific example CCF data reports from the ICDE database.

The agenda at each meeting had the structure as presented in appendix B.

[2] Per Hellström, RELCON, was on all meetings
[3] A separate questionnaire, developed by Mr Tuomas Mankamo in support of a Nordic PSA project on control rod CCF was also discussed during the meetings. The results of the control rod investigation is reported separately.

The length of the meetings varied between two hours and up to a full working day. Limits on resources allocated for the survey activity mean that the survey itself is limited. There are differences also between the number of personnel involved from each organisation, that together with the length of the meetings, make a comparison of information from each meeting difficult.

It has to be stressed that the survey not is an inspection or attempt to compare the organisations with each other. The information collected during the visits are summarised in the result section as different principles, approaches, good practices and rules that have an impact on the dependent failure defence.

The individual meeting notes are documented separately and are not published.

3 Survey Results

3.1 Results from Regulatory Visits and Communication

Both STUK and SKI are involved in the safety work as regulators meaning that requirements are stated in regulatory documents and the organisations form part of the reporting of abnormal events (Licensee Event Reports) and follow-up and analysis of these.

The regulators also have an inspection role to review that current regulatory requirements are fulfilled.

Some aspects related to CCF defence in relation to the authorities STUK and SKI are presented below: It has to be stressed that the visits and discussions with both SKI and STUK were very short, and this report therefore, can not provide the full picture of CCF defence activities.

3.1.1 STUK

A State Council Decision requires systems to be safe with good redundancy, separation and diversity.

STUK has several Regulatory guides (YVL series) indicating requirements related to CCF defence. Examples are:

YVL	Title	Date of current version
1.0[3]	Safety criteria for design of nuclear power plants	12 Jan 1996
1.5[4]	Reporting nuclear power plant operation to the Finnish Centre for radiation and Nuclear Safety	1 Jan 1995
2.7[5]	Ensuring a Nuclear Power plant´s safety functions in provision for failures	20 May7 1996
2.8[6]	Probabilistic Safety Analyses (PSA)	20 Dec 1996

It is required to have data collection and data processing systems (1.5).

It is required to have statistical trend analyses (1.5).

One should be able to identify CCF events.

Training in CCF identification is performed.

Below is an excerpt from STUK regulatory guide YVL 1.0 (Safety criteria for design of nuclear power plants, 12 Jan. 1996).

If inherent safety features cannot be made use of in ensuring a safety function, priority shall be given to systems and components which do not require an off-site power supply or which, in consequence of a loss of power supply, will settle in a state preferable from the safety point of view.
Systems which perform the most important safety functions shall be able to carry out their functions even though an individual component in any system would fail to operate and, additionally, any component affecting the safety function would be out of operation simultaneously due to repairs or maintenance (redundancy principle).
Safety systems which back up each other as well as parallel parts of safety systems shall be separated from each other so that their failure due to an external common cause failure is unlikely (separation principle).
In ensuring the most important safety functions, systems based on diverse principles of operation shall be used to the extent possible (diversity principle).
Detailed requirements for the application of failure criteria and the diversity principle can be found in Guide YVL 2.7.

And excerpt from YVL 2.8 (Probabilistic safety analyses (PSA), 20 Dec. 1996)

According to the Nuclear Energy Decree, section 36, the applicant for a licence has to submit the PSA to the Finnish Centre for Radiation and Nuclear Safety (STUK) while applying for an operating licence. According to the Council of State Decision (395/91), second paragraph, section 6, *nuclear power plant safety and the design of its safety systems shall be substantiated by accident analyses and probabilistic safety analyses. Analyses shall be maintained and revised if necessary, taking into account operating experience, the results of experimental research and the advancement in calculating methods*

Activities discussed during the STUK visit as being part of the defence against CCF are:

1. The requirement for in-house PSA analysis (since 1984). There is a practice to send the latest PSA model to STUK twice a year.
2. Operating experience is collected and reported.
3. Use of PSA to identify design errors. This has resulted in changes.
4. PSA reviews. Weak design points have been identified by these reviews.
5. Requirement for Living PSA.
6. Low threshold for reporting (judgement by STUK).
7. Inspections.
8. Replacement principles are important to identify and defend against ageing problems. A special potential CCF event concerning TVO isolation valves led to exchange from Bakelite gears to brass gears, and discussion about replacement principles.

9. Compilation of the report "Human based Common Cause Failures in Finnish plants". The report presents 10-15 events during the last 10-15 years. Many events are related to distraction during work, e g due to delays.
10. The production of two recent reports (excerpts from draft versions received during the visit) in a EU project on the Harmonisation in the field of safety of nuclear installations, Survey of PSA from both TVO and IVO "R Virolainen, "Major Risk Informed Plant and Procedural Changes at Loviisa 1 and 2" [7], STUK 15/6 2000. and R Virolainen et al, "Use of Living PSA in Regulatory Decision-Making" [8].

3.1.2 SKI:

SKI has one main document SKIFS 1998:1 [9] with requirements on nuclear power plant safety analysis and reporting. The following is an excerpt from SKIFS 1998:1.

1 § Grundläggande säkerhetsbestämmelser finns i 4 § första stycket lagen (1984:3) om kärnteknisk verksamhet. Förebyggandet av radiologiska olyckor skall ske med hjälp av dels en till varje anläggning anpassad grundkonstruktion i vilken skall ingå flerfaldiga barriärer, dels ett till varje anläggning anpassat djupförsvar. Djupförsvaret skall uppnås genom att

- konstruktionen, uppförandet, driften, övervakningen och underhållet av en anläggning är sådana att driftstörningar och haverier förebyggs,
- det finns flerfaldiga anordningar och förberedda åtgärder som skall skydda barriärerna mot genombrott, och om ett sådant genombrott skulle ske, begränsa konsekvenserna därav,
- – utsläpp av radioaktiva ämnen, som ändå kan ske till följd av driftstörningar och haverier, förhindras eller, om detta inte är möjligt, kontrolleras och begränsas genom anordningar och förberedda åtgärder.

1 § requires defence in depth to be achieved by design, construction, operation, inspection and maintenance.

SKIFS 1998:1, chapter 4 presents requirements on performing safety analysis:

Säkerhetsanalys
1 § Analyser av förhållanden som har betydelse för säkerheten i en anläggning skall göras innan anläggningen uppförs och tas i drift. Analyserna skall därefter hållas aktuella. Säkerhetsanalyserna skall vara grundade på en systematisk inventering av sådana händelser, händelseförlopp och förhållanden vilka kan leda till en radiologisk olycka.

The advice section to the above paragraph states that a safety analysis should cover, as far as possible, scenarios and circumstances, potentially affecting the defence in depth defence.

För att analysera en anläggnings funktionsförmåga från säkerhetssynpunkt behövs en god kunskap om anläggningens konstruktion, möjliga felmekanismer och om de processer och förlopp som kan äga rum. Till detta kommer behovet av modeller som beskriver de processer, förlopp och felmekanismer som bör analyseras. Både deterministiska och probabilistiska analyser bör användas eftersom de kompletterar varandra och på så sätt ger en så allsidig bild som möjligt av risk och säkerhet.
En säkerhetsanalys bör omfatta en uppsättning händelser eller scenarier som så långt det är möjligt täcker in de händelseförlopp och förhållanden som kan påverka djupförsvarets funktion och därmed ytterst leda till en påverkan på omgivningen. Med utgångspunkter från en analys av sannolikheten för olika händelser eller scenarier bör de indelas i olika kategorier.

R2000 (document still in development) contain explanations and guidance on how to interpret and apply SKIFS 1998:1. R2000 draft (2001) [10] states:

> "*Diversifiering*
>
> *Vid konstruktion, tillverkning, installation, idrifttagning, drift och underhåll av utrustning av betydelse för säkerheten bör, utifrån det säkerhetsmässiga behovet, rimliga åtgärder vidtas för att minimera införande och förhindra uppkomst av fel med gemensam orsak (CCF).*
>
> *Diversifiering bör dels utformas så att identifierade möjligheter till CCF mellan redundanta utrustningar förebyggs, dels så att sannolikheten för oförutsedda CCF minskas så långt som är rimligt och möjligt. För att uppnå diversifiering av funktionen kan, utöver säkerhetssystemen, även övrig utrustning som är klassad som utrustning av betydelse för säkerheten tillgodoräknas. Diversifiering bör som minimum tillämpas till och med ej förväntade händelser och för säkerhetsfunktionerna reaktoravställning, härdkylning, resteffektkylning och tryckavsäkring.*
>
> *Diversifiering och dess avsedda effekt på CCF bör i säkerhetsredovisningen beskrivas för varje säkerhetsfunktion med dess stödfunktioner.*
>
> *Reaktorskyddssystemet bör vara konstruerat så att det för alla händelser till och med osannolik händelse finns minst två olika sätt att via processparametrar detektera händelsen, identifiera behov och initiera skyddsåtgärder. Ett exempel på detta är att vid yttre rörbrott i kokvattenreaktorer kan skyddsåtgärder initieras både via rumsövervakningssystemet och via låg vattennivå i reaktortanken. De olika sätten att detektera en händelse bör vara funktionellt separerade."*

This mean that diversity shall be applied as afar as reasonable possible in order to minimise introduction of CCF (translated from Swedish).

The following activities are also seen by SKI as important contributors to a good defence against CCF:

1. SKI requirements on MTO activities and feedback of experience.
2. Certain inspection- and maintenance principles that are generally adopted, e g no maintenance of two redundant subs at the same time. Tech. Spec´s. requires that other redundancies are tested in case failure is identified for one redundancy.
3. The requirement to perform a PSA and to consider the results (according to SKIFS 1998:1).
4. Requirements for operational readiness verification (DKV)

5. Requirements for two stage safety review (An internal SKI document control the safety review)
6. Different disciplines at SKI co-operates in inspection and review activities, leading to a high efficiency in identification of any missing dependency barriers is achieved.
7. Requirement for SAR including single failure criteria. A group is formed for re-assessing the SAR content.
8. Regular reporting, e g yearly and 10-year reporting (ASAR) with defined content, and RO reported immediately and checked by SKI.
9. Inspection activities used for follow-up of plant safety issues together with review of reporting from the plants

Some areas with potential for strengthening the CCF defence were also discussed:

1. Increase awareness about common cause failure issue and defence by introduction of specific CCF education.
2. Improve reporting of near misses.

It is the opinion of SKI (meeting participants) that programmable systems are a challenge with regard to CCF. This is supported by the event at Ringhals during summer 2001 when a software update for a breaker was introduced simultaneously in more than 40 breakers. The CCF potential was identified in the project. The test was designed to make sure the breaker opened in case of overcurrent (more than 120%). However, the breaker opened already at 80%, making the attached components unavailable also during normal conditions. Normal operation was not tested. The event show the importance of test design, and to include also normal operation in a test.

SKI has assigned personnel responsible for this specific area, which follows the development, and in summer 2001, one activity is the follow-up of Ringhals REPAC project concerning change of control system from an analogue to a digital system. One of the important aspects in this project is to consider CCF protection in the planning.

3.2 Observations and Discussion of Regulatory involvement in CCF defence

This limited investigation has identified the following similarities and differences:

Both SKI and STUK requires certain safety principles to be applied to assure defence in depth and maximum reasonable CCF protection. The organisations have an exchange of ideas and the basic CCF defence as imposed by regulations and advice are similar.

STUK have many regulatory guides (YVL) for different areas. The number of guides is 70 (2001), including radiation guides. Radiation guides are in Sweden covered by SSI (the radiation protection Institute).

Swedish requirements are less detailed than the corresponding set of STUK requirements.

It is not possible to judge the preferred approach with organisation of requirements and way of regulation with regard to CCF.

A general observation is that key words like dependency, defence in depth, redundancy and diversity are missing in most headings in the regulatory documents, both Swedish and Finnish.

One question related to this fact is if CCF and dependent failure defence awareness and thus CCF defence itself can be improved by the introduction of more clear requirements on CCF, by changes in current guides or a separate guide with requirements on CCF defences including reporting, routines, analysis of events, and education.

3.3 Plant Aspects

The survey collected many aspects on defence against dependent failures and especially common cause failures. This section summarises these aspects as a whole without differentiating between different plants/organisations).

The following phases are important parts of the life of equipment/systems at a nuclear power plant:

- Design
- Implementation
- Operation
- Test and maintenance

The defence against dependencies during design, implementation and test and maintenance is discussed below. Operation is not discussed separately. However, failure reporting, the plant information system and feedback of experience are other very important part of the defence and they are also discussed below.

3.3.1 Design

Redundancy is required to meet the single failure criteria and redundancy is implemented on function and system level.

The basic protection against dependent failures in redundancies is the use of separation, where separation is used in three principal ways:

- Functional separation
- Spatial separation
- Diversity (different design principles for different redundant systems or functions and different software for the same purpose)

There are also other types of separation that can be used, like separation in organisation.

The need for functional separation is quite obvious, two redundant trains dependent on the same power bus mean that failure of the power bus will fail both trains.

Never the less, it can be difficult to prove that functional separation exists. Methods used to do this include:

1. Design process with requirements on dependency assessment for dependencies within a change project and impact on current design.
2. Use of PSA(detailed modelling of build-up and functional interaction of safety systems and support systems).
3. Use of simulator for testing

The design process itself is secured by having adequate project management instructions where dependency evaluation is explicitly required. Using different teams and methods to develop diverse designs can also help to secure redundancies.

Another example is to have this requirement in the standard contract template.

The design process also includes requirements on internal review and preliminary safety review (PSG). All these are administrative barriers to identify and remove weaknesses in the process. Finally, authorities will review the process.

Separation cost money, and especially diversity in design and spatial separation can be resource consuming. The validation and verification cost can be substantial. Therefore, there will in the final design be many similar components that are placed in the same location. Separation by distance is used instead of closed compartments.

3.3.2 Implementation

Time separation by the use of stepwise implementation is a method to discover and correct design weaknesses before they can affect redundancies. Stepwise implementation will also help in identifying ageing effects. Full effectiveness of time separation is achieved if the plant information system contains enough detailed information on change time points, as well as time points for tests and maintenance activities.

Important aspects with regard to stepwise implementation are:

- Stepwise implementation is not always possible
- How long should the step be?
- How is CCF to be detected between steps?
- What are the requirements on systematic evaluation of experiences?

An effective failure reporting system and high quality in safety culture is also needed to allow credit for time separation in dependency protection.

3.3.3 Maintenance and Testing

Time separation in maintenance and testing will lead to an increased probability to detect potential common cause failures before they happen. This is a common approach.

Separation of staff may decrease the probability of dependent failures, but also has a potential to increase the independent failure rate because of less training of the staff on each activity.

Other defences related to maintenance and testing include:

- Test of redundant trains in case one train is failed, with or without judgement on potential CCF.

- Checking of calibration and tool settings before use, after use, regular intervals.
- Work on one sub at a time
- Limited access to redundant trains, only part of redundancies. Realised e g by use of key system. Work order for one redundancy first, then finish and go for next work order.
- Key locking of valve positions.
- DKV (operational readiness control)
- Monitoring of equipment depending on its importance, individual component, no follow-up or batch follow-up.
- Maintenance activities divided in four groups:
  1 STF related (safety)
  2 Operation (money)
  3 Important but not necessary
  4 Less important (are allowed to fail)
  Group 1 are repaired according to STF. Group 4 has no repair priority, the work is done when time is available.

There are also some other practices in the use of procedures:

1. Page numbering and checking of that all pages are included in a copy.
2. Extra verification and signing of the state of manual valves that have changed position during testing and maintenance activities.
3. Regular review of procedures e g every four year.

3.3.4 Failure Reporting

Failure reporting practices are in principal as follows:

Failure report is made and judgement is made if it is a potential dependency or not. Judgement is verified in steps.

It is observed that a special check mark shall be made on the form only if CCF is suspected. This mean that there will be no evidence that the judgement/decision on CCF is made, if the check mark is missing. It is proposed to change the form either to check mark if no CCF is suspected, or to have two choices: CCF and no CCF.

Important for reporting is to have a low treshold for reporting, where also near misses shall be reported.

3.3.5 Plant Information system

A plant information system[4] is essential in the defence against dependencies.

The plant information system need to have information on all factors of importance for plant safety on an enough level of detail to allow follow-up on failure of critical parts of components whose failure will be critical for the component in consideration.

[4] The plant information system refer to all databases carrying information on the plants systems, structures and components such as component types, history, test intervals, real test times, location of components, work orders etc.

Again, the focus shall be on the risk important components. Less risk important can be given less attention, and resources can be focussed on the high contributors. This kind of grouping can be used in maintenance, testing and plant information system.

3.3.6 Exchange of Experience

Exchange of experience in addition to failure reporting is made in many different ways. Examples of practices in place are:

- The plants have special persons assigned as component and system responsible.
- It is required to produce yearly a written report on performance of components and systems according to a separate instruction and templates.
- Internal meetings are held for exchange of experience.
- External meetings are held for exchange of experience between systems and component responsible from different plants.
- Participation in owners group (meetings and information exchange).
- Participation in other groups meeting and work as ERFATOM, INPO and WANO.

3.4 Most Important Contributors and Defences

Questions concerning the judgement on dominating dependency contributors and best defences were asked during the meetings. The following answers were noted without priority:

Table 2: Opinion on Dominating Contributors to CCF.
Money savings resulting in a slim organisation and movement from preventive to corrective maintenance
Staff turnover (has an impact on knowledge and experience).
Ageing
Human factors- planning errors and organisational factors
Design (Changes, ageing)

Table 3: Opinion on Important Defences Against Dependencies.
Awareness (increased)
Simple solutions
Knowledge and experience
Good safety culture

Table 3: Opinion on Important Defences Against Dependencies.
Effective feedback of experience.
Review in several steps.
Tests, use of information system

4 Conclusions

The basic mechanism to avoid failure of redundant equipment due to a common cause is to use separation. Separation can be introduced in many ways. The most important types of separation used are:

- Functional separation
- Spatial separation
- Design separation (diversity)
- Time separation

Functional, spatial and design separation are mainly technical defences.

Different types of time separation are administrative defences. Time separation by stepwise introduction of new equipment, staggered testing etc. need to be combined with efficient systems for testing, failure reporting and plant information. The plant information system needs to have enough level of detail that common parts can be traced. Efficient reporting is dependent on skilled and motivated personnel supported by good procedures.

A collection of defences collected during the plant visits are presented in Table 4.

Even if defences are applied, there will always be a risk that something is overlooked.

It is not possible to create total separation in all aspects between redundant equipment.

There is also a money issue involved in CCF defence. Introduction of diverse equipment requires extra equipment qualification with related costs. This mean that diverse equipment will be very expensive. Same equipment introduced stepwise saves money, but it is important with quality control and exchange of experience and take advantage of stepwise introduction and other types of time separation. To be able to do this it is necessary with a detailed follow-up and reporting. It has to be noted that stepwise implementation not always is possible and also may cost extra compared to introduction in all redundancies at the same time.

Depending on the level of detail, there might be dependencies on a level below pump and valve, e g use of same oil for lubrication, or some small common parts. To prove diversity may therefore also be difficult. Who is delivering the small parts used by all suppliers/designers?

An important part of the defence is a high level of awareness about the dependency and CCF issue. The work within the NAFCS group contributes to an increased awareness. The plant visits indicate differences in the level of awareness of the CCF issue. The discussions have been good and there seem to be an interest for a continued communication in this area.

One idea is to produce education material based on the information collected during the plant visits and from the ICDE database, and complemented with other material.

The continued work may also involve a comparison between different actors. Such a comparison can be seen in relation to differences in reported CCF events, reported failures, reported availability etc. Is it possible to see any differences in the fractions of common cause failures in different countries, plants, owners? The same question can also be asked concerning the independent failure rates and plant availability. Is high availability a factor that can be given credit when assessing common cause parameters?

Table 4: Dependency Defence Factors Noted during Survey Meetings

Design
Instruction for introducing changes: 1) Proposal 2) Meeting every month (operation, safety, maintenance) 3) Indicate need for PSA analysis 4) Change/modification proposal with PSA plan.
Contract with supplier requires that CCF is considered.
Require consideration of dependence impact in contracts with suppliers
Require PSA (mainly for evaluation of functional and spatial dependencies, but also for checking of other types of common characteristics)
Include CCF requirements in Project management model.
Validate procedures in simulator
Defence in depth in design by combination of Independent review and primary safety review (PSG)
Functional separation
Spatial separation
Diversity in design
Review system functions by using simulators to identify dependent failure risk
Single failure analysis.
Fire PSA to identify spatial separation deficiencies
Use PSA for subtle interaction checking
Choose components with high quality and lot of experience.
Requirement on dependencies, failure rates and CCF rate in purchasing. It is required to show that the requirements are met.
Requirements on FMEA, FTA and HRA in purchasing.
Consideration of ageing in case of purchasing.
Test of new design in simulator before installation.
Several meetings to present a modification: technical meeting and plant meeting.
Equipment qualification
Use PSA for CCI analysis
Use simulator for CCI analysis

Table 4: Dependency Defence Factors Noted during Survey Meetings
Feedback of experience
Reporting of LERs
Participation in ICDE
Participation in NAFCS
Risk follow-up activities
Meetings with different plants system responsible
Meetings with different plants component responsible
ERFATOM
System responsible
Component responsible prepares yearly report that shall take a position concerning CCF.
Procedure for work by system/component responsible.
Group SAMDOK with TVO, FKG, OKG and BKAB (before also RAB). The group exchanges technical planning information. Meeting report is distributed.
NOG – Nuclear Owners Group
Implementation
Test after installation.
Stepwise introduction of new equipment (to achieve experience before full introduction)
Stepwise introduction of new equipment Different age of different redundancies
Operation
Have CCF on the agenda for shift meetings (other meetings)
Have as a policy to use instructions
Make sure to have page numbering of procedures and instructions
Check of page numbering of copies
Competent personnel.
Weekly (friday) meetings to inform personnel about changes (shift supervisors).
Limited access to redundancies (administrative)
Limited access to redundancies (by different keys for accessing AC and BD subs respectively.
Awareness of CCF
Safety culture
Crosslists (krysslistor) for new instructions (each operator shall acknowledge a new instruction)
Safety Committee
Recurring review of procedures every 3rd year (operation, maintenance and emergency).

Table 4: Dependency Defence Factors Noted during Survey Meetings
Reporting
Check for possible dependency impact in case of failure
Check marking on failure reporting form to make check of dependency potential traceable.
Next step is primary review meeting + new evaluation of affected components and mitigating actions.
Reporting of instances of miscalibrated equipment
Reporting of instances of miscalibrated tools (e g calibration instruments and torque keys)
Low reporting threshold
PSA investigation for deviation from STF.
Perform root cause analysis after LER and report lessons learned.
Morning meeting with review of failure reports and check for CCF and systematic failures
Follow-up on reported CCF failure report cases
Extra monitoring of especially important components, e g control rod drives, according to a special instruction.
Trend analysis on components and systems to identify ageing effects

Table 4: Dependency Defence Factors Noted during Survey Meetings
Test and maintenance
All maintenance activities should be recorded in the work order system.
Time separation between tests
Time separation between maintenance
One redundancy is tested while the other is kept available
One redundancy is maintained while the other is kept available
Judgement if other redundancies can be affected by test.
Judgement if other redundancies can be affected by maintenance activity
Exchange practices to make sure that a state of different ages for different redundant equipment is maintained
Different testing times (operation of diesel 1 only short time period and diesel 2 longer time, and next time shift)
Independent analysis of quality of delivered oil to diesels.
Test of redundant equipment in case of unavailable component (independent if CCF or not?)
Driftklarhetsverifiering (DKV)
Staggered testing
Staff separation in test and maintenance Not necessarily good defence. Observe the risk for too little training if test occasions are few. The risk of too little training has to be related to the risk of trained personnel making the same mistake in several redundant trains.
Check of calibration instrument before calibration
Check of calibration instrument after calibration
Regular calibration checking
Marking of calibrated equipment
Bicycle used for maintenance optimisation.
Motivate Maintenance intervals changes
Logging of maintenance/test interval changes in the plant information system.
Provide information on possible dependency/CCF risks on work permits. Judgement by skiftingenjör and approval by driftledning (morgonbön).
Several persons involved in activity, e g electrical permission: one writes and another reviews and approves.
Have an extra operator to verify the position of manual valves that have changed position during the test.
Model work (mockups).
Other
Existence and use of SKIFS 1998:1
Existence and use of applicable IAEA guidelines
Existence and use of 10CFR50, and especially appendix J concerning test and maintenance in support for dependency protection.
CCF policy?
Guides with dependency defence principles
Education/safety culture for shift ingenieurs.
Encourage personnel to propose improvements of any kind.
Have CCF check in check lists

5 References

1. Gunnar Johansson, NORDISK ARBETSGRUPP FÖR CCF STUDIER: PROJECT PROGRAMMME, ES-konsult, 2000-12-19.
2. A.J. Bourne G.T. Edwards D.M.Hunns, D.R.Poulter I.A.Watson, ” Defences against Common mode failures in redundancy systems, A guide for management, designers and operators”, SRD R 196, SRD, January 1981.
3. YVL 1.0, Safety criteria for design of nuclear power plants, 12 Jan 1996.
4. YVL 1.5, Reporting nuclear power plant operation to the Finnish Centre for radiation and Nuclear Safety, 1 Jan 1995.
5. YVL 2.7, Ensuring a Nuclear Power plant´s safety functions in provision for failures, 20 May7 1996.
6. YVL 2.8, Probabilistic Safety Analyses (PSA), 20 Dec 1996.
7. “R Virolainen, “Major Risk Informed Plant and Procedural Changes at Loviisa 1 and 2”, STUK 15/6 2000.
8. R Virolainen et al, “Use of Living PSA in Regulatory Decision-Making”.
9. SKIFS 1998:1, Statens kärnkraftinspektions föreskrifter om säkerhet i vissa kärntekniska anläggningar, 22 september 1998.
10. R2000, draft 2001.

Appendix A: Questionnaire and items for discussion for Plant Survey Meetings

1 Introduction

The Questions are intended to support the discussion. Some background and example defences and indicators are listed after the questions.

2 Questions

Describe, exemplify and/or give references to plant document.

1. Exist a CCF-problem policy, education or/and information programme. Which plant staff is included in the programme. Describe and exemplify
2. How is system reliability demands and CCF problem expressed by the design phase of plant modifications for example:
    a. Identification
    b. Minimised
    c. Defences
    d. Review
    e. Guides
2. Example of the plant policy, for operation, test and maintenance activities, to prevent CCFs by
    a. Faulty procedures
    b. Human errors
    c. Design errors
3. Is there a check list or procedure to identify potential CCF from a single failure? After a potential CCF is detected rules of action? Is there a special records for failures, potential CCF and CCFs and actions taken to prevent reoccurrence.
4. Basic engineering principles used in plant design and plant modification guidelines or other recommendations used?
5. Strategy for repair of degraded safety important equipment in time pressure (STF repair criteria) and with a thorough fault analysis not yet available?
6. How is the test mix of a system optimised within the desired safety level?
7. Which (method, tool) is used optimise safety and resources of preventive maintenance actions to minimise downtime and costs?
8. Is there a potential in developing STF towards online maintenance? (To optimise the amount and more flexible planned maintenance during operation)
9. How are maintenance (conditioning) intervals for check valves decided?

10. Action taken by a pump failure?
11. Action taken when a DG fails?

Shorter questions more yes / no

1. Is system functions reviewed to identify CCF risks ?
2. After a identified CCF or potential CCF is possible defences analysed?
3. Is the risk of possible CCF events notified on work permits?
4. Is procedures reviewed of potential CCFs
5. Original design principles and modification principles includes:
    a. Diversity
    b. Fail safe design
    c. Separation
    d. Derating
    e. Simplicity
6. Is separation in time used by:
    a. Construction
    b. Test
    c. Maintenance
7. Is separation of staff used in
    a. Construction
    b. Test
    c. Maintenance
8. Which is last actions in a maintenance procedure?
9. Is the maintenance equipment verified before use?
10. Is all maintenance activities recorded?
11. Is test procedures aimed to reveal any CCF in redundancy systems?
12. Is test procedures checked to not introduce CCFs?
13. Is operational access limited to any system?
14. Is access to all redundancy systems governed by detailed procedures?

3 Background

Difference of consequence

- Single failure
- Common cause failure

The plants are designed for single failure “single failure criteria” to handle a single failure.

To achieve desired system reliability and single failure the design includes redundancy and diversity.

The plant reacts to single failure management/operator/maintenance have to act to handle CCF.

For single failure T-book data can be used directly in PSA. The data is a direct measurement of plant equipment performance.

For CCF parameters for PSA is dependent on human performance to a higher degree compared to single failure parameters.

4 Example Defense

1. Separation
- Physical
- Design
- Construction
- Maintenance
- Time
2. Management
- Knowledge
- Actions
- Monitoring
3. Procedures
- Maintenance
- Test
- Operation

5 Indicators

Time and means of detection can be used as an indicator of plant CCF awareness. In the ICDE database the detection codes can be graded from god CCF response to less god

1. God response
- Test during operation
- Monitoring in control room
- Monitoring on walkdown
- Unscheduled test (second failure)

2. Acceptable response
- Test in laboratory
- Test during annual overhaul
- Maintenance / test
- Unscheduled test (first failure)

3. Bad response
- Demand event

Time interval between first and second failure can be used as a second indicator and the operators' identification of a failure as a potential CCF event. Immediate test of other equipment in a CFF group is good response. If the second and further failures are detected at normal operation, tests or maintenance with a time span giving the possibility to analyse an act after the first failure in the CCF group, indicate as less god response to CCF events.

6 Some General Questions

1. What protection against dependencies is built into the design?
2. What protection against dependencies is used in operation?
3. What protection against dependencies is used in maintenance?
4. How is experience concerning dependent failures collected, analysed and used as feedback?
5. Has failure experience led to changes in dependent failure defence.
6. Has PSA or other types of analyses identified deficiencies in dependent failure protection?
7. If yes, have changes been introduced?
8. Has the PSA been used to actively check for subtle interactions?
9. What IAEA guidelines, if any are used in dependent failure protection?
10. What SKI guidelines have been or are used regarding dependent failure protection?
11. What NRC guidelines have been or are used regarding dependent failure protection?
12. What other guidelines have been or are used regarding dependent failure protection?
13. How is the single failure criteria applied?
14. Which lacks of defence have been identified at the plant during the years?
15. What is your opinion on the most important improvement areas with regard to dependency defences?
16. What is your opinion on the dominating factor resulting in dependent failures?

Appendix B: Agenda for Plant Survey Visits

Meeting opening
Presentation of meeting participants
Presentation of NAFCS work plan – Objectives, scope, tasks, time schedule
Presentation of ”Plant Survey” planning and list of questions/statements for discussion.
Planning of day for individual discussions with plant representatives from different departments.
Discussions in full group individually following list of questions.
Summing up the day in the whole group.

NAFCS

Nordisk Arbetsgrupp för CCF studier **Work Notes to NAFCS-PR05**

Title:	PR05 Work Notes- Survey Meeting Notes (Appendix C-H to report NAFCS PR05)
Author(s):	Per Hellström, RELCON AB
Issued By:	Per Hellström, RELCON AB
Reviewed By:	N/A
Approved By:	N/A
Abstract:	These work notes are the meeting notes from the visits to plants and authorities performed as part of the plant and regulatory survey on defences against dependent failures. The meeting notes are part of the NAFCS report PR05, but are not published.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Restricted

Revision control:	Version	Date	Initial
Final	U1	2003-08-31	PH

List of Content

Appendix C: Notes from STUK Visit

STUK	2001-11-21 (2 hours, whole group together)	Reino Virolainen, Ilkka Niemelä

Policies

State Council Decision requires systems to be safe with good redundancy, separation and diversity.

Requirement for in-house PSA since 1984.

Guiding Documents

Several Regulatory guides (YVL series) indicate requirements related to CCF defence. Examples are:

YVL	Title	Date of current version
1.0	Safety criteria for design of nuclear power plants	12 Jan 1996
1.5	Reporting nuclear power plant operation to the Finnish Centre for radiation and Nuclear Safety	1 Jan 1995
2.7	Ensuring a Nuclear Power plant´s safety functions in provision for failures	20 May7 1996
2.8	Probabilistic Safety Analyses (PSA)	20 Dec 1996

It is required to have data collection and data processing systems (1.5).

It is required to have statistical trend analyses (1.5).

One should be able to identify CCF events.

Training in CCF identification is performed.

Routines

3-step inspection system:

A Management inspection on top level and less detailed

B Process inspection: Purpose is to inspect different work processes dependent with each other, e g maintenance and connected processes. This level usede for review of modernisation projects.

C Detailed inspection on function and system level. Until 2-3 years ago (1998) this was the only inspection type. PSA is at this level.

Reporting

Operating experience is collected and reported.

PSA is used to identify design errors and has resulted in backfitting.

PSA reviews has identified weak points.

Practice to send the latest PSA model to STUK twice a year.

Living PSA required.

The treshold for reporting is judged as low (Virolainen). This mean that it is felt likely that CCF events really are reported.

A report "Human based Common Cause Failures in Finnish plants" presents 10-15 events during the last 10-15 years. Many events are related to distraction during work, e g due to delays.

Testing efficiency in identifying CCF too low.

Measures taken

Received during meeting:

Draft of reports from EU project on the Harmonisation in the field of safety of nuclear installations, Survey of PSA from both TVO and IVO.

R Virolainen, "Major Risk Informed Plant and Procedural Changes at Loviisa 1 and 2", STUK 15/6 2000.

R Virolainen et al, "Use of Living PSA in Regulatory Decision-Making".

Special potential CCF event: TVO isolation valves. Led to exchange from bakelite gears to brass gears. Replacement principles are important to identify ageing problems.

APPENDIX D: Notes from SKI Visit

SKI	2001-11-07 (2 hours, whole group together)	Ralph Nyman, Anders Hallman, Bo Liwång, Kjell Olsson

SKI requires certain activities, through the document SKIFS 1998:1, that contain the basic requirements on safety assessment and reporting to SKI.

Input from SKI (R Nyman via mail):

SKIFS 98:1 talar om robusthet, om diversifiering och redundans. I R2000 talas om CCF i samband med diversifiering.

Vissa inspektions- och underhållsprinciper finns anammade och är allmänt vedertagna, tex underhåll inte två subbar samtidigt. STF kräver vid fel, att övriga redundanser testas.

Ett viktigt försvar mot CCF är bl.a. följande; Jag tycker att kravet på tillståndsinnehavaren att genomföra PSA och att även beakta resultaten av PSA (vilket framgår av 98:1) är ett väsentligt krav vad gäller CCF. Vi pratar ju även om diversitet vad gäller programerbara system.

Det som styr eller ställer krav på tillräckliga DKV-rutiner kan ju sägas vara krav som skall förhindra CCF.

Ytterligare en sak är våra krav på granskning i två led, där syftet med granskning av t.ex en anläggningsändring är att undvika konstruktionsfel som bl.a. skulle kunna orsaka en CCF. Många av våra krav och verksamheter syftar på ett eller annat sätt till att undvika CCF.

R2000 text (received working draft in Swedish dated 2001-08-22. requirements on both single failure strength, diversity, separation and independence, dynamic effects related to pipe breaks, external events, design with regard to corrective and preventive maintenance, environmental durability, etc.

Diversifiering

Vid konstruktion, tillverkning, installation, idrifttagning, drift och underhåll av utrustning av betydelse för säkerheten bör, utifrån det säkerhetsmässiga behovet, rimliga åtgärder vidtas för att minimera införande och förhindra uppkomst av fel med gemensam orsak (CCF).

Diversifiering bör dels utformas så att identifierade möjligheter till CCF mellan redundanta utrustningar förebyggs, dels så att sannolikheten för oförutsedda CCF minskas så långt som är rimligt och möjligt. För att uppnå diversifiering av funktionen kan, utöver säkerhetssystemen, även övrig utrustning som är klassad som utrustning av betydelse för säkerheten tillgodoräknas. Diversifiering bör som minimum tillämpas till och med ej förväntade händelser och för säkerhetsfunktionerna reaktoravställning, härdkylning, resteffektkylning och tryckavsäkring.

Diversifiering och dess avsedda effekt på CCF bör i säkerhetsredovisningen beskrivas för varje säkerhetsfunktion med dess stödfunktioner.

Reaktorskyddssystemet bör vara konstruerat så att det för alla händelser till och med osannolik händelse finns minst två olika sätt att via processparametrar detektera

händelsen, identifiera behov och initiera skyddsåtgärder. Ett exempel på detta är att vid yttre rörbrott i kokvattenreaktorer kan skyddsåtgärder initieras både via rumsövervakningssystemet och via låg vattennivå i reaktortanken. De olika sätten att detektera en händelse bör vara funktionellt separerade.

Requirements on MTO activities and feedback of experience.

Requirement for SAR including single failure criteria. A group is formed for re-assessing the SAR content.

Education in PSA should lead to a high degree of awareness of the important safety issues including CCF defences.

Clear and traceable reporting to TUD.

Near misses to be reported. This is an area where improvements can be made.

Recent event at Ringhals shows the importance of the design of tests. A software update for a breaker was introduced in more than 40 breakers. The CCF potential was identified. The test was designed to make sure the breaker opened in case of overcurrent (more than 120%). However, the breaker opened already at 80%, making the attached components unavailable also during normal conditions. Lesson: Normal operation has to be tested.

An internal SKI document control the safety review.

Inspection activities are used for follow-up of plant safety issues together with review of reporting from the plants.

Yearly reporting and 10-year reporting (ASAR) with defined content.

RO reported immediately and checked by SKI.

Special activity at the moment is Ringhals REPAC concerning change of control system from analog to digital system. Planning with regard to CCF protection.

Is CCF included in peer review of modifications?

Different disciplines co-operates in the inspection and in reviews. Thus, a high efficiency in identification of any missing dependency barriers is achieved.

Reporting:

Deviations from requirements – Action plan. Review and commenting.

RO also to ERFATOM – Review by SKI.

KSU monthly reports

International reports from IAEA.

Knowledge base.

Programmable systems a new challenge!

Appendix E: Notes from OKG Visit

OKG	2001-09-18 (1 day, whole group together)	Frithiof Schwartz, TR, Michael Landelius, TR, John Svensson, D2Q-D, Johan Melkersson, D3D, Mats Gustafsson, D1F.

Contract with supplier requires that CCF is considered.

Judgement if other redundancies can be affected. Test after installation.

Time separation between:

Test and preventive maintenance occurrences

Different operational times (can be achieved by introducing new equipment stepwise, requires detailed plant information system to be in operation).

Different testing times?

I-7260 Riktlinjer för konstruktion av system innehållande programmerbar elektronik (PE) – hjälpinstruktion till I-0103. Excerpts concerning CCF (supplement to OKG notes) provide a CCF definition and design defences as diversity in function, equipment, software, software development process. Appropriate level shall be chosen depending on the application. Then stepwise installation, e g, one sub or a channel in a system. This gives experience of the new equipment and the CCF contribution is kept on a limited and controlled level.

Form for failure reporting has a box for check marking if CCF is suspected.

OKG is member of the ICDE project.

10 CFR50 appendix J has guidance on CCF defences.

Q1: Driftssammanträden has one item on the agenda about CCF.

Part of templates for purchasing in new projects. Also part of certain check lists.

Q2a. Purchasing template contain requirements on CCF assessment.

Evaluation of design with PSA (including CCF).

Stepwise installations.

Project management model include CCF requirements.

Q3. Procedures are validated in simulator.

Policy to use instructions.

Instructions have numbered pages. Checks are made that all pages are included.

Competent personnel.

Weekly (friday) meetings to inform personnel about changes (shift supervisors).

Independent analysis of quality of delivered oil to diesels.

Q4. Failures are evaluated regarding CCF. This is noted on a failure reporting form. (PH comment: need to change form to increase probability that CCF or not CCF is actively decided. Current form shall be check marked if CCF is suspected. Change to checkmark if no CCF or allow the choice to be visible by having two boxes, one if

CCF, and another if not CCF). Next step is primary review meeting + new evaluation of affected components and mitigating actions (motåtgärder).

Q5. TBE, TBM, KFM describes the basic engineering principles in plant design and modifications.

Q6. Test of redundant equipment in case of unavailable component (independent if CCF or not?)

Q7. Optimisation of test mix is under way.

Q10. Maintenance (conditioning) is made according to manufacturer recommendations. Changes according to experience of equipment. Also Technical Specifications.

Q11, Q12. No difference between actions in case of component malfunction.

Short questions (S-1)

SQ-1. System functions are reviewed to identify CCF riks (PSM-Projektstyrningsmodell)

SQ-2. CCF defences are analysed (see SQ-1).

SQ-3. Work order has nothing about possible CCF risk during work. This is controlled by the planning. A strict review against STF is performed. Driftklarhetsverifiering of one system at a time.

SQ-5. CCF defence design principles applied include diversity, separation. Noted that some other defences not are for CCF defence, but are general defences against malfunction of an intended function, e g fail safe princíple.

SQ-6. Separation in time is used in construction, test (but not strictly) and maintenance.

SQ-7. Separation of staff is not used in design. However, internal review and independent review (PSG) is made. SKI is also reviewing, though mainly the process.

Separation of test staff is not scheduled, but this is achieved any way (not controlled).

Separation of maintenance: Same personell, same calibration instrument, Calibration checked before. Question if it is checked after calibration?May be it should be?

SQ-8. Last action in maintenance activity is to test if this is possible.

SQ-9. Similar as for calibration. (Question if there is a complete coverage of this type of activities).

SQ-10. All maintenance activities should be recorded in the work order system. (how is the effectiveness checked? Can there be activities that not are recorded?)

SQ-11. Test procedures are designed to reveal CCF in redundancy systems, e g staggered testing and check of redundant train if failure is identified. Is this complete?

SQ-12. Test procedures are designed to avoid introduction of CCFs. PSM (projektstyrningsmodellen) The Project management model should secure this.

SQ-13. Operational access is limited to systems and redundancies (Are there any differences between plants?)

Answers to general questions:

G1. Separation and diversity are used as protection against dependencies in design.

G2. Testing combined with reporting system is a protection during operation together with access control, etc, many different administrative rules.

G3. Similar as G2 for maintenance. Testing after completed maintenance, planning of maintenance according to PSM.

G4. Collection of experience about failures (CCF) is done via the work order system, RO, ICDE, NAFCS, Risk follow up is done, but there is no requirement. O1 is doing risk follow up, O2 has done limited risk follow up.

G5. Failure experience has resulted in dependent failure protection. Examples?

G6. PSA and other analysis results have identified deficiencies in dependent failure protection (mainly functional dependencies and spatial dependencies).

G7. G6 has resulted in plant changes.

G8. The PSA has been used to actively check for subtle interactions. (PH comment. In general, probably more can be done).

G9. many different IAEA guides are used as a basis for different types of analyses, e g PSA.

G10. SKI guides 98:1, 2000:1 etc are used.

G11. 10CFR50, and especially appendix J concerning test and maintenance is used in support for dependency protection.

G12. Other guides used are: Check lists, failure reporting forms, lazy dogs.

G13. The single failure criteria is applied in accordance with STF.

G14. Among defence deficiencies identified are several cases of unknown functional dependencies. (ICDE data base to be checked for examples).

G15. The OKG participants opinion on the most important improvement area with regard to dependency defences are related to redundant instruments, awareness (increased), knowledge and experience, good safety culture (openness and dialogue).

G16. The OKG participants opinion on the dominating factor behind dependent failures are money savings resulting in tight organisation and movement from preventive to corrective maintenance (PH comment - STUK principle can be applied), and staff turnover (has an impact on knowledge and experience).

Appendix F: Notes from BKAB Visit

Barsebäck	2001-09-19 (1 day, whole group together)	Ingemar Ingemarsson, PSA/FoU, André Strömberg, SP (maintenance/planning), Ulf Hansson, BTS (Control room, BOKA, SAR/PSA)

NOG – Nuclear Owners Group?

To easy to create CCF groups in Riskspectrum.

Need to clean up in the terms and definitions.

Ageing.

Primary safety review and independent review.

Need for better guidance on how to use (work with) deterministic and probabilistic analyses.

Basic questions:

Q1. No CCF policy exist? May be in design.

Q2. PME (Projekt modell ?) contain a heading “effect on nearby systems”.

Q3. Procedures: Pages shall be controlled, instruction shall always be used, crosslists (krysslistor) for new instructions (each operator shall acknowledge a new instruction), safety culture - kontrollrumsmannaskap.

Q4. Check mark if CCF.

Q5. Engineering principles: KFB, KFM, PSG meeting, TBE, TBM etc. Many of these are common for all NPPs and are updated in accordance with SKIFS.

Q6 Strategy for repair of imported components is guided by STF. PSA investigation for deviation from STF.

Q7-8. Bicycle used for maintenance optimisation. Not optimised with regard to risk. Attempts with PSA a long time ago. All NPPs have access to bicycle via TUD.

Q9. –

Q10. Maintenance intervals (conditioning) are based on initial + experience + bicycle. STF Change has to be motivated. Contact with SKI. Change is logged in the maintenance information system.

Q11-12. Depends on STF. Failure report, check mark if CCF.

Short questions:

QS1. System functions are reviewed to identify dependent failure risk by using simulators, PSA analysis, single failure analysis.

QS2. Defences are analysed. After RO, root cause analysis is required and lessons learned shall be reported.

QS3. Work permits do not contain information on possible dependency risk.

QS4. ?

QS5. Original design include several cases of diversity, e g 532/354, 312/TB, 323-327-312, inner and outer containment isolation valves. Gas turbines and diesels. Fail safe design - egenmediestyrda ventiler. Separation - EB1 noted that in case of area event there is a potential problem with flooding/steam.

QS6. Separation in time used in design (similar to OKG), test diesels tested at different time points and also gas turbines. Pumps are tested sequentially. 516 växelvis. Maintenance förskjutet.

QS7. Separation of staff in construction similar to OKG. Test, different persons, but no real control/schedule. Observe the risk for too little training if test occasions are few. The risk of too little training has to be related to the risk of trained personnel making the same mistake in several redundant trains. Maintenance: Electrical permission: one writes and another review and approval. Similar with Work orders. DNV independent review.

QS8.The last action in maintenance is DKV and test.

QS9. Maintenance equipment is verified before use: e g torque key (momentdragare) and calibration equipment. Idea: check also after use to identify if something has happened.

QS10. Work order system shall contain all.

QS11. Test procedures aimed at identifying CCF (those cases with staggered testing).

QS12. Test procedure has requirement that another person verifies the position of manual valves that have changed position during the test.

QS13. Operational access limited.

QS14. Förväxling har inträffat. Work order has information on which unit that should be worked on. Access card is the same for both units.

Marking important.

Some general questions:

QG1-3. Skipped.

QG4. Similar as for OKG, but no risk follow-up.

QG5. Failure experience has led to changes in dependent failure protection.

QG6-7. PSA and other analyses has identified deficiencies in dependent failure protection and extensive changes have been introduced because of this.

QG8. PSA not used to check for subtle interactions.

QG9. Access to all IAEA guides. Guide for PSA used. This area is not fully covered.

QG10. SuperASAR results and SKIFS 1998:1 guides dependent failure protection.

QG11. NRC guidance in GDC 10CFR50 is a basic document.

QG12. No answer

QG13. Single failure criteria seen as well implemented. Active single failure direct and passive after 12 hours.

QG14. Skipped.

QG15. Most important improvement area with regard to dependency protection is awareness about the problem area, good competence, use simple solutions and avoid complex if not needed.

QG16. The dominating factor resulting in dependent failures are the human factor and organisational factors.

Appendix G: Notes from TVO Visit

TVO	2001-11-30 (1 day, separate small meetings and summary meeting)	Jari Pesonen and Risto Himanen (PSA group), Ingvald Lilja (Operation), Markku Friberg and O Luhta (Safety committee), J Tanhua (Maintenance), Sami Jakonen (Enginering).

Q7. PSA is used (Living PSA). In a number of ways, e g test interval optimisation.

QS1. Risk for CCF is not noted on work permits.

QS5. Original design include diversity, separation.

QS6. Separation in time is used in construction and maintenance (packages).

QS7. Independent check is made of actions, e g spänningssättning.

QS10. All maintenance activities are recorded.

QS11. If failures identified during testing judged as CCF, then redundancy is checked.

QS13. Different keys for accessing AC and BD subs respectively.

The general questions:

QG6. Fire PSA identified deficiencies in sub separation. PSA used in modernisation for test of alternative solutions. Shutdown PSA results have led to changes that have reduced therisk.

QG7. Changes have been introduced

QG8. The PSA has not actively been used to check subtle interactions, but in some cases of plant changes.

QG10. STUK YVL guides are guiding dependent failure protection.

QG16. The most dominating factor resulting in dependent failures. Ageing: Can be reduced by reporting, feedback of experience, classification etc. Human factors-planning errors: Can be reduced by applying review in several steps.

Maintenance instructions are checked every 4 year.

Jari Pesonen and Ingvald Lilja (driftchef OL1).

Morning meeting. Review of failure reports (felanmälan), CCF check and systematic failures.

Operation and maintenance shall detect any risk for CCF.

CCF is listed as an item in the failure report which has to be checked if CCF (similar as in Sweden/PH). Co-ordinator shall make a follow-up on CCF cases (5-6 per year for unit 1 and 2 together).

Also maintenance can find failures.

Meeting TVO and Forsmark 2 times per year. Other units once a year.

Exchange of experience:

Representative from operation in ERFATOM, + more.

Education/safety culture for shift ingenieurs.

All are encouraged to propose improvements of any kind.

Maintenance during operation 5-6 work orders for each unit.

Maintenance activities divided in four groups

1 STF related (safety)

2 Operation

3 Important but not necessary

4 Less important (are allowed to fail)

PSA calculation in case of disturbance.

Safety Committee (Markku Friberg and O Luhta)

Safety group with 9 members + one from tekniska högskolan). Members are experts (sakkunniga) in different areas, e g radiation protection.

Meetings 6-8 times per year (Forsmark every second week).

No high level CCF policy exist.

STUK guide YVL 1.0.

There are also plant meetings (once per month or more often during revision period), that discusses similar items as the safety committee meetings.

Component responsible prepares yearly report that shall take a position concerning CCF.

Received a copy of safety committee tasks. Noted that nothing is explicitly mentioned about dependency defence.

Maintenance (J Tanhua)

Policy with stepwise changes.

Choose components with high quality and lot of experience.

Judgement on systematic impact (CCF).

Component responsible.

System responsible: failures, ageing, Need for modifications. (procedure for work by system responsibles).

Classification of maintenance is made (see above).

Awareness about the risk for too much testing.

One sub is tested first with one form and the other using another form. Contact with control room in between.

Optimisation of maintenance:

All work at one occasion (package).

Marking.

Standard routines for maintenance. Model work (mockups).

Failure report example: check mark if suspected CCF, then follow-up to get a Yes/No. Depending on the importance of the system. If yes, report.

Enginering (Sami jakonen).

Introduction of changes in one sub at a time.

Similar for components.

In case of purchase of new equipment:

Requirement on dependencies, failure rates and CCF rate. It is required to show that the requirements are met. Also requirements on FMEA, FTA and HRA.

Diversity policy in preparation.

Extra monitoring of especially important components, e g control rod drives, according to a special instruction.

Large modification - PSA is made.

Small modifications - no PSA.

Several meetings to present a modification: technical meeting and plant meeting.

Analysis are presented for STUK.

Received copy of requirements document that is part of purchasing. This document include requirements on:

Dependability - Failure probability of common cause failures shall be less than xxx (individual failure rates are also specified). Functional dependencies on systems or equipment outside deliverers responsibility shall be assessed. addition to individual failure rates. Requirement for PSA modelling.

PSA group (Risto Himanen and Jari Pesonen).

CCF between (active) similar components in the same system. Not monitored. No CCF if short latent exponeringstid or if very low probability.

Mechanical design (Henry Rönndahl, mananger for mechanical planning group)

Instruction for introducing changes:

1) Proposal
2) Meeting every month (operation, safety, maintenance)
3) Indicate need for PSA analysis
4) Change/modification proposal with PSA plan.

System for change message has a position for decision on PSA analysis.

TBE, TBM or corresponding as in Sweden.

Group SAMDOK with TVO, FKG, OKG and BKAB (before also RAB).

The group exchanges technical planning information. Meeting report is distributed.

Routin for monthly meetings.

Also function groups, valve groups etc.

Monthly meeting makes judgement on reviewer. Then internal TVO review.

Ageing is considered in case of purchasing.

Components full service every 4 year. Rubber life time is 10 years.

Reserv is thrown away after 6 years.

Levels of follow-up.

1 Individual components

2 No follow-up

3 Partiuppföljning

Large changes are not introduced at the same time in all trains.

Appendix H: Notes from Forsmark Visit

Forsmark	2001-12-03 (4 hours, whole group together)	Jan-Erik Stenmarck, Bjarne Grönqvist (cFTE)

Examples of dependency barrier practices:

15 days/operational per sub and year used for preventive maintenance work. One sub at a time. Work perfomed according to Technical Specifications.

Design Process:

Plant specification from purchaser.

System design is based on FSAR.

Impact on existing plant is investigated and considered. Design based on TBE (Tekniska bestämmelser för elektriska komponenter), TBM (Tekniska bestämmelser för mekaniska komponenter) and KB (Konstruktionsbok).

Before installation, testing of new design in simulator.

Independent review is performed and preliminary safety review (PSG).

Qualifictaion of equipment.

Complete testing of new equipment.

New equipment/modification is introduced stepwise. First one sub.

It is of interest to save money by sharing costs for equipment qualification. This mean that requirements on separation and especially diverse equipment can be expensive. Same equipment introduced stepwise saves money, but it is important with quality control and exchange of experience and take advantage of the stepwise introduction. To be able to do this it is necessary with a detailed follow-up and reporting.

Certain very critical function are designed to be diverse. To prove diversity may also be difficult. Who is delivering the small parts used by all suppliers/designers? (own question)

Replacement approval.

Staggered testing.

PH note: Reasons to avoid CCF:

Safety: redundant equipment may fail simultaneously.

Availability: Unavailable equipment cost money and resources.

Failure itself may be more expensive than exchange before failure.

Therefore, lessons learned must be considered.

Very important with a good failure and availability reporting and follow-up. Requires good reporting system (plant information system on the level of detail needed and PSA model on the level of detail needed), motivated personnell, good procedures.

Trend analysis on components and systems.

PSA used for CCI analysis. Test with F1 simulator.

Changes → underlag till FSAR (7-8 months delay)

Similar failure reporting as all NPPs.

Test of all other redundancies in case of failure in one redundancy. No judgement if test is needed.

TBE used for purchase definitions.

AKF, EKF basis for design.

Staggered testing.

Transient analyses (FSAR chapter 9) part of defence against CCF.

Analysis on site with standard format. RO + disturbance report + MTO investigation (approximately 10/year).

Calibration via individual cards.

Instruments have calibration frequency. Individuals are registered. Torque Momentnycklar kalibrerade.

Qusetion: What happens if a miscalibrated calibration instrument is identified? Rules for this have to be in place.

There is no CCF problem policy or specific education and information.

System reliability and CCF defence requirements during design changes:

No explicit reliability requirements in FSAR or other document. Emergency core cooling requirement for availability of more than one train. Similar for diesels.

New projects have sometimes explicit reliability requirements, but there is no policy.

There is no explicit policy to prevent CCFs.

Identified faults are treated similar to other plant procedures, i e failure reporting, judgement of any CCF implication etc (an improvement in the reporting form was identified during the visit to OKG/BKAB).

System functions are reviewed using CCI testing (PSA and plant simulator).

Possible CCF impact is noted on work permits. Judgement of shift ingenjör and approval by driftledning (morgonbön).

Procedures are reviewed (quality review) every 3rd year (operation, maintenence and emergency).

Different principles are in place, e g Diversity, fail safe, separation.

Separation in time is used in design, test and maintenence. This together with effective reporting and plant information system is maybe one of the most important defences (Pers comment).

Maintenance/calibration equipment is verified with regular intervals.

Operational access is limited by a key system where different keys are needed for access to the different trains.

Different trains are maintained during different weeks.

All maintenance activities are recorded.

The general questions:

Protection against dependencies is built into the design, operation and maintenance.

The reporting system has a checkmark which should be check marked if dependencies are suspected.

Failure experience has lead to changes in defence against dependent failures (functional, spatial and CCF type). One example is fire protected power supply.

PSA has identified deficiencies in dependency defence and changes have been introduced.

The PSA probably has not been actively used for checking of subtle interactions (CCF). It has been used together with simulator to check effect of CCIs (thereby covering certain functional dependencies.

Guidelines from SKI, IAEA, NRC or other, have not directly been used or are used for dependent failure protection. Chapter 4 in FSAR makes a reference to GDC.

Single failure criteria is applied.

The FKG teams opinion on the most important improvement for dependency defence is to have carefully designed tests.

The opinion on the dominating factor behind CCF. Design related.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
App3.2	**Defence Assessment in Data PR20**	**PR20**
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title: Defence Assessment in Data
Author(s): *Jean-Pierre Bento, JPB Consulting AB*
Issued By: *Jean-Pierre Bento, JPB Consulting AB*
Reviewed By: Gunnar Johanson, ES-konsult, Per Hellström, Relcon and Pekka Pyy, OECD/NEA
Approved By: Gunnar Johanson

Abstract: This report presents proposals for defences against MTO-related CCF events. The proposals build upon results from the study of the MTO-database relating to the LERs reported by the Swedish nuclear power plants during the years 1994 – 2002.

The study indicates that five defences against MTO-related CCF events have to be strengthened. These are in order of importance:

- Self-checking (individual and collective).
- Work planning and preparation.
- Procedure content.
- Operability readiness control (DKV).
- Respect of procedure.

Proposals for the improvement of these partly intertwined defences against CCF events are presented.

Defences against hardware CCF events have not been assessed in the frame of the present study.

This report has several interfaces with NAFCS-PR08 "Qualitative analysis of the ICDE-database for Swedish emergency diesel generators" [Ref.1], and with NAFCS-PR12 "Redundancy Protection Guidance" [Ref. 4].

Doc.ref: Project reports
Distribution WG, Project WebSite, Project archive
Confidentiality control: Public

Revision control:

Version	Date	Initial
A1	2003-03-13	JPB
A2	2003-03-26 (includes comments by G Johanson, P Pyy and P Hellström)	JPB
Final	2003-03-26	GJ

List of Content

List of Figures

1. Introduction

Within the NAFCS framework, a quality control of the ICDE-database was performed in year 2002 as a comparative review of data points contained in the ICDE-database and in the MTO-database (Man – Technology – Organisation) for the Swedish emergency diesel generators. This earlier study was reported in "Qualitative analysis of the ICDE-database for Swedish emergency diesel generators", NAFCS-PR08, [Ref. 1].

Insights gained during the above mentioned review were utilised as ground for the formulation of proposals for remedial actions with the potential of minimising both hardware and MTO-related CCF events in the Swedish emergency diesel generators.

The general defences against CCF presented in this report are based solely on the study of the MTO-database for the Licensee Event Reports (LERs) reported by the Swedish nuclear plants during the years 1994 – 2002. Considering the high number of LERs contained in the database, and also those reviewed earlier during the MTO assessment process, this study represents an exhaustive review well in line with the analysis reported in [Ref. 1].

The study is based on the assessment of the causal categories and of the dominating root causes contributing to MTO-related CCF events. The word event is used in the present report to denote a LER, except where otherwise stated.

The study objectives and limitations are found in section 2.

Section 3 presents shortly the specificities of the event data studied.

Section 4 presents results of the qualitative assessment of the CCF events and their causes.

Section 5 discusses proposals for general defences against MTO-related CCF.

Section 6 discusses general defences against hardware related CCF and further work.

Section 7 presents overall conclusions.

2. Study objectives and limitations

The original intention behind the present report was to extend the proposals relating to the diesel generators to general defences against CCF events suitable for all component categories contained in the ICDE-database. The intention was furthermore to encompass both hardware and MTO-related CCF. However, such an exhaustive exercise was outside the scope of the NAFCS project.

These limitations mostly impact the thorough treatment of hardware related CCF and the proposals of robust defences against these.

Another limitation is that all components and systems in the MTO-database have been considered as one population, the focus being on the assessment of the dominating

root causes behind MTO-related CCF events, as ground for the proposal of general defences against these.

Even with these limitations, the achievement of the objectives connected to the MTO-related CCF events for all components categories still represents a noticeable contribution to overall defences against CCF. This achievement also allows well-grounded recommendations for future work within the NAFCS project.

As mentioned, the detailed review of hardware CCF events for other component categories has not been performed. Such a comprehensive review is proposed to be performed in a future work.

3. Event data

The ICDE-database is thoroughly described in "Data Survey and Review", NAFCS-PR02, [Ref. 2].

One of the insights gained earlier during the course of the comparative assessment of the ICDE-database and the MTO-database was that the MTO-related data points contained in the former represented a sub-ensemble of the data points contained in the latter. This insight underlined the applicability and credibility of using the data points in the MTO-database as ground for the identification of the root causes behind MTO-related CCF and the proposals of defences against them.

For informative purposes the MTO-database[1] is shortly presented below.

All LERs reported to the Swedish Nuclear Power Inspectorate (SKI) are since many years reviewed from an MTO-perspective. One specific feature of the review is that the events are also assessed from a CCF point of view.

After review the events caused by weaknesses in the interaction MTO are classified and entered into the MTO-database. The event reports entered into this database pertain only to events within the plant and its organisation, including contractors.

The structure of the MTO-database is built on a classification at two levels of the event contributing factors. The first level is defined as the overall causal category level, exemplified by "Plant management & organisation", "Work organisation", "Work practice", etc. The second level is defined as the root cause level, exemplified for "Work organisation" by "Deficient planning", "Staffing with deficient training/ competence", "Deficient operability readiness control", etc. The MTO-database structure has 11 MTO causal categories and about 70 MTO root cause categories.

The structure of the MTO-database encompasses also the event consequences for the involved components/systems, etc. This allows for the classification of CCF related to MTO-deficiencies.

[1] The so called MTO-database is maintained by JPB Consulting AB.

The content and classification of the MTO-database is quality assured, except for year 2002, trough yearly discussions with plant representatives. The database for year 2002 is not yet quality assured, waiting the reporting of the final version of some LERs.

For the years 1994 – 2002 representing the time frame of the present study, the MTO-database contains more than 1200 MTO-related LERs out of more than 3000 LERs reported to SKI during the same period. Slightly less than 450 of the MTO-related LERs exhibit a CCF character. For the sake of clarity, the definition of a CCF in the MTO-database is somewhat wider than the ICDE definition, and it includes recurring events due to a shared cause, even if the time span between the events is longer than the time span specified in the ICDE-database coding guidelines [Ref. 3]. The time span defined in [Ref. 3] is "…two pertinent inspection periods or, if unknown, a scheduled outage period".

4. Data survey and review

As reminder according to the study limitations, hardware CCF events are not part of the analysis presented below.

In order to be able to propose pertinent defences against the occurrence of MTO-related CCF events, it has been judged necessary to identify the dominating causal categories and root causes having contributed to these events.

The contribution from the causal categories and root causes to the events contained in the database for the years 1994 – 2002 is presented as facts in section 4.1 and 4.2. These causes are discussed in chapter 5 in relation with the proposal of barriers against the occurrence of CCF events.

When considering the content of figures 1 – 3, it should be remembered that several root causes often contribute to each one of the events in general, and of each one of the MTO-related CCF events in particular.

4.1 Causes of MTO-related CCF events (LERs)

About 40% of the LERS reported to the SKI during the years 1994 – 2002 exhibit MTO aspects. Furthermore, 37% of the MTO-related LERs have a CCF character.

The causal categories contributing to these MTO-related CCF events (slightly less than 450 events) are presented in figure 1.

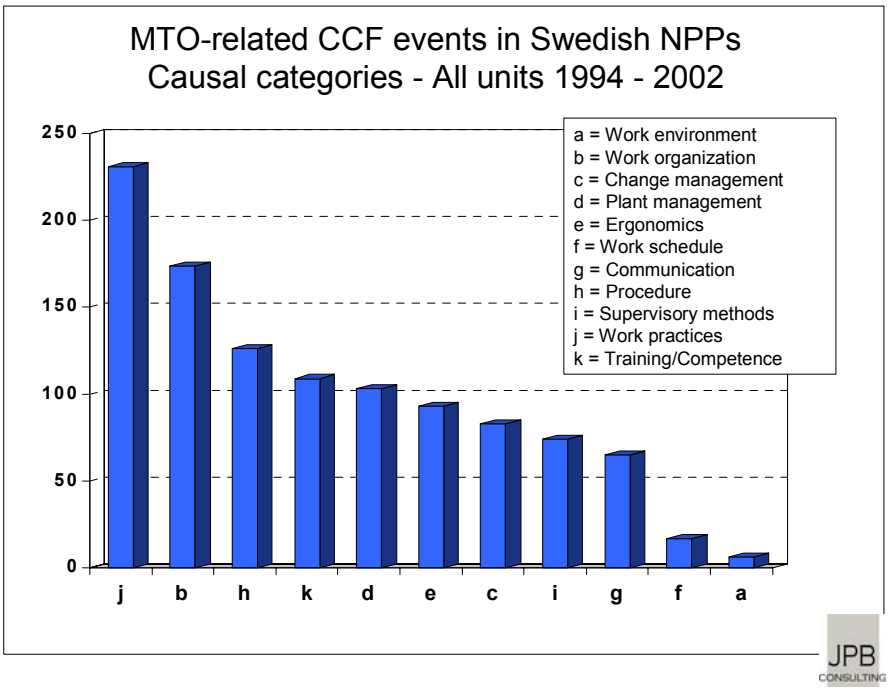


Figure 1: Causal categories to MTO-related CCF events in Swedish LERs.

The repartition of the causal categories as depicted in figure 1 is, for the dominating contributors, well in line with the similar repartition illustrated in figure 2 for the diesel generators.

Figure 1 indicates clearly the dominating contribution from weaknesses in "Work practices" to the occurrence of MTO-related CCF events. Such weaknesses contribute to slightly more than 50% of all occurred MTO-related CCF events in the Swedish nuclear plants during the period studied.

Weaknesses in "Work organisation" represent the second dominating contributor and such weaknesses are involved in about 40% of the studied MTO-related CCF events.

Deficiencies in "Procedures" represent the third dominating causal category involved in about 30% of the studied events.

Three other causal categories are also noteworthy contributors to CCF. Deficiencies in "Plant management", "Training/Competence" and "Ergonomics/Design" contribute each to between 20 and 25% of the MTO-related CCF LERs.

For completeness and comparison, the causes contributing to CCF events in the Swedish emergency diesel generators are shortly summarised below.

MTO-aspects of CCF events in the Swedish emergency diesel generators
The CCF events described in [Ref. 1] covered the years 1994 - 2001. The causal categories contributing to the 27 studied MTO-related CCF events in the emergency

diesel generators are presented in figure 2 for the most frequent work types performed on the diesel generators.

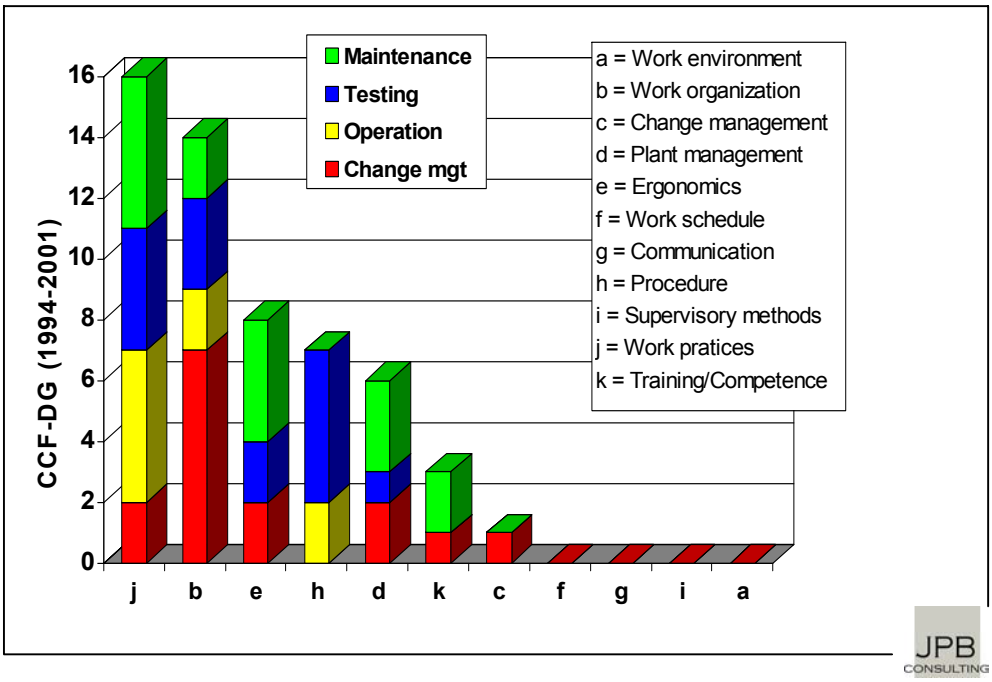


Figure 2: Causal categories contributing to MTO-related CCF events in the Swedish emergency diesel generators

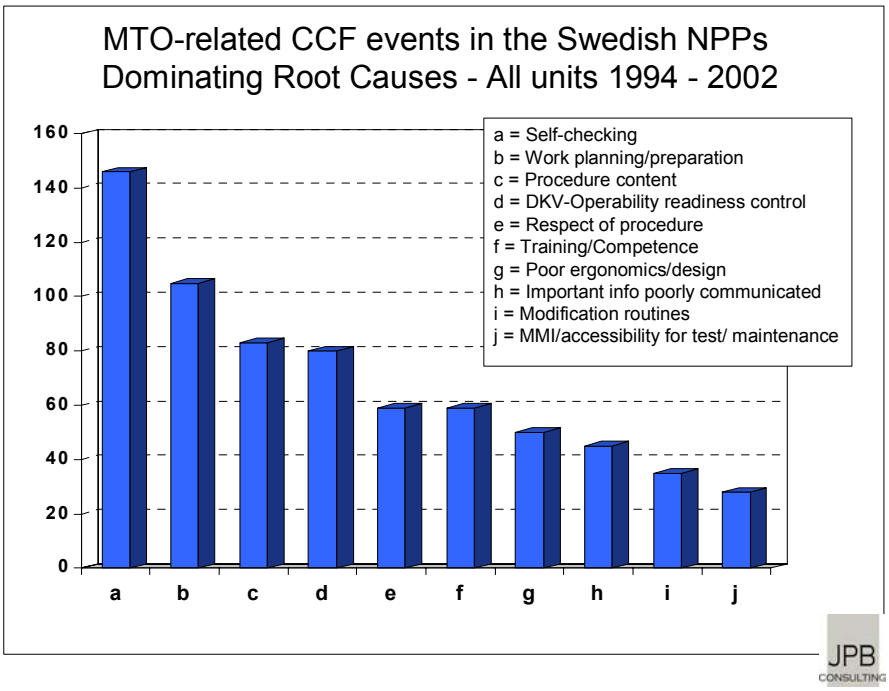
This figure shows that deficient "Work practices" and deficient "Work organisation" are the clearly dominating contributors to the MTO-related CCF events for the Swedish diesel generators.

The dominating root causes contributing to these events represent deficiencies in:

- Self-checking (was involved in about 50% of the events).
- Work preparation (25%).
- Operability readiness control (DKV) (25%).
- Procedure content (ca 25%).

4.2 Dominating root causes to MTO-related CCF events

The 77 root causes constituting one part of the MTO-database have been studied with the aim to identify the 10 dominating root causes for CCF events, irrespective of the work type and component and/or systems involved. These dominating root causes are presented in figure 3.



*MMI = Man-Machine Interface

Figure 3: Root causes to MTO-related CCF events in Swedish LERs.

The results in figure 3 indicate that two of the five dominating root causes contributing to MTO-related CCF events, belong to the causal category “Work practices” and two belong to “Work organisation”. These results are well in line with the ones presented in the previous section.

Weaknesses in individual and/or collective “Self-checking” during the planning, decision, performance, reporting and control of the work tasks thus contribute to about 33% of the MTO-related CCF events. Similarly, “Non-respect of procedure” contributes to about 13% of these events.

The second and fourth dominating root causes both relate to weaknesses in the “Work organisation”. Deficient “Work planning/preparation” is involved in 24% of the MTO-related CCF events in the Swedish nuclear power plants, and deficient “Operability readiness control” in 18% of the events.

Finally deficient “Procedure content” has contributed to about 19% of the studied events.

The above identification of the dominating causes and root causes behind MTO-related CCF events makes possible the proposal of barriers against such events. These proposals are presented and discussed in the next chapter.

5 Defences against MTO-related CCF - Proposals and discussion

This chapter can be considered as a complement to NAFCS-PR12 "Redundancy Protection Guidance" [Ref. 4]. However and as mentioned earlier, the present report does not assess "pure" hardware/ component failures.

The review of the MTO-database, focussing on CCF events, has provided several insights deemed of broad applicability for the proposal of barriers against this type of events. In the subsequent sections, proposals for defences against CCF are made, based on the results presented in chapter 4.

5.1 Improvement of the defence "Work practices"

"Work practices" viewed as a defence against the occurrence of plant events in general and CCF events in particular, represent the methods and routines that each individual utilises when performing his/her work tasks. The notion of work practices thus encompasses both the planning and preparation phases of the own tasks, gathering of documentation and tools, accomplishment and reporting of the work tasks. The notion of work practices concerns all individuals in the plant and in the company.

Preconditions must be established by the utility to enable individuals to exhibit good work practices:

a) Each individual should have been clearly informed – through policy document, supervisor, etc - about the expectations that the organisation has on him/her.
b) The company management has established functioning programmes for quality assurance, training, experience feedback, etc. The frames of these programmes are well documented in updated policy documents.
c) The staffing of the company/plant is commensurate with the work assignments and commitments.
d) The work organisation takes due consideration to the time needed for the preparation, planning and performance of work tasks. This is equally valid for limited and/or routine tasks as for larger modification projects.
e) The tools, components and systems - that are to be operated, tested and maintained - have a technically good standard.

The study of the Swedish LERs indicates that these preconditions are sometimes deficiently fulfilled and that, symptomatically, less than adequate work practices at different organisational levels are one of the underlying causes behind this deficiency.

The dominating contribution to MTO-related CCF events from weaknesses in the barrier "Work practices" indicates that a significant reduction in the number of such events could be obtained by strengthening and improving the following barrier elements (defences):

- Self-checking (Swedish acronym STARK).
- Respect of procedure.

5.1.1 Improvement of "self-checking"

In a plant/company with high safety culture it is expected that each individual – notwithstanding his/her organisational level – exhibits the following behaviours:

- Individuals demonstrate a strong sense of personal ownership by developing their knowledge, skills and attitudes necessary for their success on the job.
- Individuals focus on the task at hand. They take the time to think about the task at hand with a questioning attitude. They are alert to the potential impact of distractions during work.
- Individuals, and especially planners and supervisors, expect success but anticipate failure, What-if?
- Individuals self-check and expect to be checked by others. They locate and verify the correct procedure, tools and components. They control that the component and/or system response to their actions is as expected.
- Individuals take the time needed to do the task correctly.
- When faced with uncertain conditions, individuals take conservative decisions.
- Individuals communicate often for safe planning, performance and reporting of works tasks. Three-way communication with repeat-back is practiced rigorously.

A widespread belief is that weaknesses in the defence "Self-checking" are most often related to the action phase of the work tasks. Experiences, supported by the study of the MTO-database, indicate however that the weaknesses as well and as often relate to the planning, preparation and verification phases of the tasks. In such cases potential failures are already embedded in the tasks to be performed.

Efficient remedies for the improvement of the individual and collective work practices, and especially of the self-checking, exist based on what characterises a high professionalism:

- A questioning attitude.
- A cautious work practice.
- Correct communication.

The improvement of the individual work practices in general and self-checking in particular, requires both immediate and long-term actions. It also requires that necessary preconditions (points a – e in section 5.1) be established.

A short-term action is to make each individual conscious that the expectations concerning good individual self-checking will be more tightly enforced. This action should be part of a broader campaign where the plant management clearly informs all individuals about the necessity and requirement to exhibit a questioning attitude during the different phases of the work.

The company/plant management has hereby to realise that higher management expectations on the organisation's members will naturally result in increased expectations from the individuals on the management that the preconditions for good work practices a) – e) listed above, are well established.

The plant management has also to ensure an environment where each individual is confident and does not start a work task when the organisational or operational

conditions are not in accordance with procedure, requirement or management expectations.

The management must similarly declare that each individual has the possibility to stop an activity when the preconditions have reached outside prevailing rules and requirements, or when the individual judges that he/she has not full control over the on-going activity.

A further efficient action is to establish a programme for self-assessment within the organisation. Such a programme means that all members of the organisation assess themselves, individually or collectively, with a given periodicity. The assessment includes each individual's approach to safety issues and safety culture. Such a programme is particularly efficient for the identification of weaknesses and proposals of corrective actions, when a team of individuals has been involved in several events.

Finally, improvement of the individual work practices in general, and of self-checking in particular, is judged to be less a question of economy than a clearly – in wording and in action – emphasis on the expectations on each individual, and also a sustained and visible management involvement.

5.1.2 Improvement of "Respect of procedure"

"Procedure" is defined as all written documentation used for the planning, performance, control and reporting of the tasks necessary for the operation and maintenance of the plants. Accordingly, "Procedure" represents both operating, testing and maintenance instructions/procedures, work orders, system documentation including flow charts and logic diagrams, etc.

Non-respect of a procedure is obviously one aspect of deficient work practice, and in some cases a sign of deficient safety culture. Non-respect of procedure is relatively often coupled to weaknesses in the work organisation, supervisory methods and communication.

A differentiation has to be made between individual and collective non-respect of a procedure. In the first case, the involved person is more or less unconscious of the deviation. One step in a procedure is for example not correctly followed due to distraction or tiredness. Cases exist however, when the individual was conscious that a non-respect of the procedure steps was made.

A collective non-respect of a procedure is also, often the consequence that the involved team was not aware that a deviation from intended procedure(s) was committed. Sometimes yet, the non-respect of a procedure is the consequence of an unspoken agreement between the members of a work team, or that no individual dares to point out the non-compliance. The latter cases are however judged infrequent in the Swedish plants.

The non-respect – individually or collectively – of a procedure can also depend from the fact that the procedure content is unclear or otherwise deficient, or that the work task cannot be performed correctly if the procedure steps are closely followed. When such a situation occurs, the involved personnel still try to do the best of it, for example in order to not stop the plant operation or delay a plant shutdown. The consequence is

however that the task is performed, despite every involved individual is well conscious of the non-respect, and of potential risks.

Concerning proposals for improvement of the defence "Respect of procedure", it is judged that the core part of the proposals made for "Self-checking", if well addressed, also represents an efficient mean for minimising the occurrence of CCF events due to the non-respect – individually or collectively – of procedure.

In addition, a general rule against the non-respect of procedure should be to not start or to stop a work task if it cannot be performed without violating an existing procedure. The possibility for each individual to exhibit such a conservative attitude has hereby to be clearly supported by both the management and direct supervisor. The individuals should also have received proper information and guidance for this line of conduct. For specific cases a possibility has to exist to depart from the above main rule. The work practice must then include a formal assessment, with managerial and/or supervisory involvement, of potential risks.

5.2 Improvement of the defence "Work organisation"

"Work organisation" viewed as a defence against the occurrence of plant events in general, and CCF events in particular, includes the planning, preparation, performance and control of a work task. "Work organisation" also includes staffing and repartition of responsibility within the team of individuals that perform a task.

The dominating contribution to MTO-related CCF events from weaknesses in the barrier "Work organisation" indicates that a significant reduction in the number of such events can be obtained by strengthening and improving the following barrier elements (defences):

- Work preparation and planning.
- Operability readiness control (Swedish acronym DKV).

5.2.1 Improvement of "Work planning and preparation"

The study of the MTO-database with focus on CCF events indicates that latent failures, or failure potentialities, are relatively often introduced already at the planning and preparation stages of the work task(s), due to insufficient focus from the involved individuals on technical, organisational or safety aspects. The risk potential then increases significantly if additional technical problems arise or if subsequent human performance problems occur, irrespective of their eventual relationship with the work organisation.

The improvement of "Work planning and preparation" presupposes an increased awareness among planners and other individuals involved in the preparation - and its control - of different work tasks, of their responsibility to ensure a work package/preparation free from latent failures. Such awareness is strongly coupled to basic safety values, and to the understanding and respect of colleagues work conditions.

In light of the large number of tasks performed at a plant, each individual involved in the planning and preparation of these tasks has to fully recognise that a well

planned/prepared work represents one of the most efficient defences against plant events.

Another important aspect is that the individuals involved in the planning and preparation of different work tasks have to realise that the loyalty of colleagues or of co-workers, or the complacency of a contractor, cannot be expected as compensatory measures for a less than adequate work planning. Clear information to the staff about this aspect has to be given by the company/plant management.

5.2.2 Improvement of "Operability readiness control"

Deficiencies in the defence "Operability readiness control" are potentially insidious because control room operators and other personnel (I&C, maintenance, electrician, etc) may base their action(s) upon the false premise(s) that components and systems are available on demand, or aligned according to procedures. Operating experiences show that this is apparently not always the case.

Deficiencies in this defence mean furthermore that a work task is finished and a component/system "returned" to the operation department without the final and fully exhaustive verification of the adequate component and/or system function. Such deficiencies can result in long lasting latent component unavailability or partly defeated system function, without annunciation in the main control room.

Some CCF events occurred during the nineties in safety systems at some of the Swedish plants demonstrated the value, necessity and also difficulty to perform a full covering operability readiness control of the plants systems.

Significant efforts have been made since then by the plant organisations to improve the defence against such (CCF) events. These efforts seem to have been substantially successful since only 12 out of the 80 MTO-related CCF events due to deficient "operability readiness control" identified in the study, occurred during the three latest years.

Considering that "Operability readiness control" is the latest physical step of the overall "Work organisation" it is finally assessed that further improvement of the defence "Operability readiness control" can be achieved through the proposals for improvement mentioned above for "Work planning and preparation".

5.3 Improvement of the defence "Procedure content"

The study of the MTO-database indicates that deficient "Procedure" is involved in slightly more than 25% of all MTO-related LERs. Noticeable is the fact that about 40% of these procedure related events – two thirds of them being related to deficient procedure content - exhibits a CCF character.

Based on a limited trend analysis of the MTO-database, a slightly declining trend concerning the yearly number of procedure related CCF events has been observed. On an average this number is 11 for the three latest years, and 14 for the years 1994 – 2002. A similar but not as robust trend is identified for CCF events related to "Procedure content".

Consequently, to formulate proposals for strengthening the defences "Procedure" and "Procedure content" is judged here somewhat over-ambitious in light of the focussed, sustained and very significant efforts spent during decennials by the industry for improving the quality of "Procedure".

Finally, recent events concerning software deficiencies that affected tens of objects demonstrate that the improvement of the quality of "Procedure content" is most probably a never-ending process.

6 Defences against hardware related CCF – Further work

The Swedish operating experiences for the latest decennium indicate that slightly more than 50% of the LERs relate to hardware/component failures. No figure exists about the overall repartition of CCF between hardware and MTO-related events, at least presently, for the Swedish LERs.

A general overview of the data points contained in the ICDE-database indicates that the fraction of hardware related CCF events is lower than the corresponding value for MTO-related events. Furthermore, the battery database indicates that 95% of the CCF events are MTO-related. These two facts mitigate somewhat the consequences of the limitations of this study. It has still to be underlined that whether or not the repartition of the ICDE-database is representative of the overall Swedish experiences has not been analysed here.

Results from [Ref. 1] indicated that ageing and experience feedback were the two most important issues which could, well managed, reduce the occurrence of hardware CCF events, at least as far as diesel generators were concerned.

Based on these facts, and in view of the limitations of the present study as to the assessment of hardware related CCF events, it is recommended that NAFCS should support a data review and analysis of different component types, as the one reported in [Ref. 1].

Finally, it is reasonable to envisage that specific insights - gained during the course of the above proposed future works - about defences against both hardware and MTO-related CCF could be integrated in an updated version of [Ref.4] and [Ref. 5].

7 Conclusions

The assessment made of all MTO-related CCF LERs reported during years 1994 – 2002 indicates that weaknesses in the following causal categories are dominating contributors to these events:

- Work practices
- Work organisation
- Procedures
- Training/Competence
- Company management & plant organisation.

Similarly, the five most dominating root causes contributing to the MTO-related CCF events in the Swedish LERs represent weaknesses in:

- Individual and collective self-checking
- Work planning & preparation
- Procedure content
- Operability readiness control (DKV).
- Respect of procedure.

It is tempting to believe that the proposals formulated in the previous section represent, if implemented, generally efficient defences against the occurrence of new MTO-related CCF events, notwithstanding the component category involved.

Such a state of fact is most probably true, based on the concordance of the results and proposals formulated herein and the ones presented in [Ref. 1] for the Swedish emergency diesel generators. However, having in mind the specificity of different component categories, it is judged that some particularities of significant importance for the minimisation of CCF events can only be identified through a thorough analysis of these categories.

It is consequently recommended to assess the potential benefits of such analyses, before deciding on their eventual accomplishment. A decision could be based on the results from the analysis of one or two other component categories, and on the assessment of the new results compared with the insights gained during the diesel generator study.

The benefits of a further defence assessment in data as proposed here are rather evident for plant safety, not only as a mean to prevent insidious multiple failures due to a shared cause, but also for increased knowledge for the better modelling and quantification of the often dominating CCF contributions in the PSA.

8 References

1. J-P Bento, JPB Consulting, “Qualitative analysis of the ICDE-database for Swedish emergency diesel generators”, NAFCS-PR08, March 2002.
2. T. Mankamo, Avaplan Oy, “Data Survey and Review”, NAFCS-PR02, January 2002.
3. G. Johanson et al, ES-konsult, “ICDE General Coding Guidelines”, ICDECG00 Rev.4, October 2000.
4. J-P Bento, JPB Consulting, and P. Hellström, Relcon, “Redundancy Protection Guidance”, NAFCS-PR12, April 2003.
5. M. Knochenhauer, Impera, and T. Mankamo, Avaplan Oy, “Dependency Analysis Guidelines“, NAFCS-PR13, April 2003.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
App4.1	**Model Survey PR04**	**PR04**
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR04**

Title:	**Model Survey and Review**
Author(s):	Tuomas Mankamo
Issued By:	Tuomas Mankamo
Reviewed By:	Michael Knochenhauer
Approved By:	Gunnar Johanson 2003-10-17

Abstract: This report presents the survey and review of the CCF models that are being used in the Nordic PSA studies. The relationships of the models are described. The parameter transformations are presented and illustrated by a practical example. The parameter estimation for the models is generally described by the maximum likelihood estimators and connection to the impact vector presentation. The aim is to provide neutral basis for linking the outcome of quantitative classifications to any of the defined qualified CCF model. A fundamental aim of this task is to harmonize the definitions and terminology on the subject area to constitute a solid basis for the later tasks in the workgroup.

Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2001-05-22	TM
Draft 1	2001-06-05	TM
Draft 2	2001-09-21	TM
Draft 3	2001-10-24	TM
Draft for Peer Review	2002-01-12	TM
Issue 1	2003-10-10	TM

This report was closed declaring Draft for Peer Review as final for this phase with small editorial changes only. See concluding remarks for the discussion of needed further work.

Contents

Model Survey and Review

1. Introduction

This topical report documents the survey and general description of the CCF models that are being used in the Nordic PSA studies.

1.1 Objectives

The emphasis is on collecting the model definitions in a consistent way for the later uses in the NAFCS. The aim of this survey is not to rank the models, as they can be regarded generally equally applicable. Instead, the aim is to provide neutral basis for linking the outcome of quantitative classifications to any of the defined qualified CCF model.

The relationships (similarities and differences) of the models are generally described. The parameter transformations are presented and illustrated by a practical example.

The estimation procedure for the models is generally characterized regarding the maximum likelihood estimators and coupling to the impact vector presentation. The more developed estimation techniques, including uncertainty analysis will be subject of a separate later task.

One of the fundamental aims of this task is to harmonize the definitions and terminology on the subject area to constitute a solid basis for the later tasks in the workgroup. The ICDE terminology will be followed whenever applicable.

1.2 Scope

The survey covers the definitions and features of the following CCF models (terms “model” and “method” are used interchangeable in this context, preferring the convention of the original source):

- Alpha Factor Method
- Beta Factor Method
- Common Load Model
- Direct Estimation Method (called also as Basic Parameter Model)
- Multiple Greek Letter Method

The model descriptions are collected into Section 2, which starts with laying out the common features of parametric CCF models. The models are basically discussed as applicable to demand failure probability. Connection to failure rate based modeling is shown.

The basic estimation procedures for the considered models are presented in Section 3 which first introduces the general frame and common aspects.

Section 4 will summarize the model survey discussing specific regimes of the reviewed models.

2. Model descriptions

This section gathers the basic descriptions of the considered CCF models. The presentation order is chosen for the convenience of definition, starting from the most basic Direct Estimation Method.

2.1 Introduction to parametric CCF models

The parametric CCF models are aimed at presenting the dependence in multiple failure probabilities by using conveniently defined parameters, called as CCF parameters or dependence parameters. The Direct Estimation Method works directly with the probability entities.

A part of the CCF models are defined using the concept of Common Cause Basic Events (CCBEs) and corresponding probabilities:

$$Q(m|n) = P\{\text{Specific m components fail due to CCF, other n-m not affected in a CCCG of size n}\} \quad (2.1)$$

Another part of the CCF models are defined using the probabilities for multiple failure within CCCG, so called Subgroup Failure Probability (SGFP) entities. Compare to the definitions in Annex 1. One of the SGFP entities is close to CCBE probabilities, namely:

$$Peg(m|n) = P\{\text{Specific m components fail while other n-m not affected in a CCCG of size n}\} \quad (2.2)$$

The difference between these two entities is that Peg(m|n) covers any multiple failure of order m, also due to combination of different causes, while Q(m|n) is restricted to actual CCFs of order m, exactly, and due to a clear shared cause. In practice the two entities are numerically close, i.e.

$$Q(m|n) \cong Peg(m|n), \quad (2.3)$$

and the difference is more a theoretical issue. This issue is relevant also in the event analysis and impact vector construction for the cases of multiple failures due to combination of causes, including so called coincidental multiple failures. Compare to further discussion in [NAFCS-PR03].

The most common way of modelling CCFs (and dependences more generally) in PSA is based on the definition of CCCGs and use of CCBEs in fault tree modeling. Compare to more detailed presentation in [RS-ThM].

Usually CCCGs are assumed internally homogeneous, which means also internal symmetry – so also in this report. Thus the probability of a CCBE is not dependent of the specific combination of components, only the multiplicity affects, i.e. same Q(m|n) or Peg(m|n) applies to all CCBEs of order m (the count equals to the number of different choices of m components out of n). But it must be emphasized that the size of CCCG matters: $Q(m|n_A) \neq Q(m|n_B)$ and $Peg(m|n_A) \neq Peg(m|n_B)$ when $n_A \neq n_B$ in the range of $m \leq \min(n_A, n_B)$ – except some coincidence – even for two mutually homogeneous CCCGs.

In this respect Psg entity has a special property as it is *subgroup invariant*, see Annex 1 for the definition of this concept. This means that among two mutually homogeneous CCCGs of different size $Psg(m|n_A) = Psg(m|n_B)$ in the range of $m \le \min(n_A, n_B)$. Especially, that is valid always for a subgroup (group A) within a CCCG (group B) – assuming internal homogeneity, of course. The subgroup invariance of Psg entity is very helpful in practice. It is advisable to perform data comparisons and pooling in terms of Psg entity. This applies also to mapping and pooling of impact vectors, see further discussion in [NAFCS-PR03].

2.2 Direct Estimation Method

In the Direct Estimation Method, called also as Basic Parameter Model, no special parametric model is concerned, but the multiple failure probabilities are directly estimated (to be discussed in Section 3.2). Mostly, CCBE probabilities Q(m|n) are considered because they are typically used in fault tree modeling. Alternatively some of the SGFP entities can be estimated directly and used in the system modeling: this approach is typical in highly redundant groups.

2.3 Alpha Factor Method

Alpha Factor Method is basically defined by using CCBE probabilities, see e.g. [NUREG/CR-5485]:

$$\alpha(m|n) = \frac{\binom{n}{m}.Q(m|n)}{\sum_{k=1}^{n}\binom{n}{k}.Q(k|n)} \tag{2.4}$$

Using the practical approximation $Q(m|n) \cong Peg(m|n)$, and using another SGFP entity

$$Pes(m|n) = \binom{n}{m}.Peg(m|n), \tag{2.5}$$

we may also express the Alpha Factors in the following way:

$$\alpha(m|n) = \frac{Pes(m|n)}{\sum_{k=1}^{n}Pes(k|n)} = \frac{Pes(m|n)}{Pts(1|n)}, \tag{2.6}$$

where Pts(m|n) is one more of the SGFP entities, see Annex 1. It is thus seen that the Alpha Factors represent the fraction of multiple failure probability of order m with respect to the total failure probability of at least one failure.

It is essential to notice that the Alpha Factors are not subgroup invariant. Hence the size of the concerned CCCG should always be explicitly indicated. As a consequence of lacking subgroup invariance the Alpha Factors cannot be directly compared or pooled across CCCGs of different size. A drawback of Alpha Factors is also that they do not have an intuitively simple connection to the dependence level.

In the reverse direction Q(m|n) can be calculated in terms of Alpha Factors and total single failure probability Q_T by using the following expression:

$$Q(m|n) = \frac{m}{\binom{n-1}{m-1}} \cdot \frac{\alpha(m|n)}{\alpha_T} \cdot Q_T \qquad (2.7)$$

where

$$\alpha_T = \sum_{m=1}^{n} m \cdot \alpha(m|n)$$

Basically this expression applies to the standby components, failure the start of demand and in the nominal situation of sequential testing. For staggered test case the CCBE probability of order m should be reduced by factor m, i.e.

$$Q(m|n) = \frac{1}{\binom{n-1}{m-1}} \cdot \frac{\alpha(m|n)}{\alpha_T} \cdot Q_T \text{ for evenly staggered testing} \qquad (2.8)$$

The detailed reasoning behind this is presented in [NUREG/CR-5485].

It is quite a common practice to take Alpha Factors from an international source and connect those with the plant specific estimate of total single failure probability. The negative side effects of this procedure will be discussed in Section 4.

2.4 Multiple Greek Letter Method

Multiple Greek Letter Method is the predecessor of Alpha Factor Method. It is defined in terms of CCBE probabilities in the following way:

$$g(m|n) = \frac{R(m,n)}{R(m-1,n)} \text{ for } m \geq 2 \qquad (2.9)$$

where

$$R(m,n) = \sum_{k=m}^{n} \binom{n-1}{k-1} \cdot Q(k|n)$$

It should be noticed that in the Rare Event Approximation

$$R(1,n) = Q_T \qquad (2.10)$$

Usually MGLM parameters are denoted by Greek alphabets which is the background to the method's name:

$$g(2|n) = \beta^{(n)} \qquad (2.11)$$
$$g(3|n) = \gamma^{(n)}$$
$$g(4|n) = \delta^{(n)}$$
...

The interpretation of MGLM parameter g(m|n) is "the conditional probability that the cause of a component failure that is shared by m-1 or more components will be shared

by m or or more additional components, given that m-1 specific components have failed". It is essential to keep in mind that the MGL parameters, similarly as Alpha Factors, are not subgroup invariant. Hence the size of the concerned CCCG should always be explicitly indicated. The MGL parameters across different size of groups are not directly comparable.

The CCBE probabilities can be inversely solved in terms of MGL parameters:

$$Q(m|n) = \frac{1}{\binom{n-1}{m-1}} . \prod_{k=1}^{m} g(k|n).(1-g(m+1|n)).Q_T \qquad (2.12)$$

with the following defaults

$g(1|n) = 1$

$g(n+1|n) = 0$

In practical uses MGLM is being replaced by AFM due to the reason that the latter method bas better properties for estimation aims. For point estimates (maximum likelihood estimates) these two models are largely equivalent. The parameters can be transformed from one to another, most conveniently through the CCBE probabilities:

$$\alpha(m|n) \leftrightarrow Q(m|n) \leftrightarrow g(m|n) \qquad (2.13)$$

Ref.[NUREG/CR-5485] presents the transformation equations for low order groups. The MGL parameters are more intuitively connected to the dependence level than Alpha Factors. Usually the MGL parameters saturate towards one for increasing order, i.e. g(m|n) > g(m-1|n). This aspect is not, however, generally valid. Especially in highly redundant systems the MGL parameters use to behave in a different non-intuitive way. Besides, increasing dependence can imply that the MGL parameters increase at high multiplicity as expected but decrease at the intermediate multiplicity: this can happen already in low order CCCGs.

2.5 Beta Factor Method

Beta Factor Method is in turn a predecessor of Multiple Greek Letter Method, being initially defined for two components:

$$\begin{aligned} Q(1|2) &= (1-\beta).Q_T \\ Q(2|2) &= \beta.Q_T \end{aligned} \qquad (2.14)$$

Inversely (in the Rare Event Approximation for two components $Q_T = Q(1|2)+Q(2|2)$:

$$\beta = \frac{Q(2|2)}{Q_T} = \frac{Q(2|2)}{Q(1|2)+Q(2|2)} \qquad (2.15)$$

Beta Factor Method has been in later connections extended to CCCGs above size 2 in the fashion of a cut-off model, a useful simple model for a screening analysis:

$$\begin{aligned} Q(1|n) &= (1-\beta).Q_T \\ Q(m|n) &= 0 \ \text{ for } 1<m<n \\ Q(n|n) &= \beta.Q_T \end{aligned} \qquad (2.16)$$

2.6 Common Load Model

In the Common Load Model (CLM), the failure condition is expressed by stress-resistance analogy: at the demand, the components are loaded by a common stress S, and their failure is described by component resistances (strengths) R_k. Multiple failure of order m occurs when the common load exceeds the resistances of the components in the considered group:

$S > R_k$ for each component k in a specific group of m components (2.17)

Both the common stress and component resistances are assumed stochastic, distributed variables. The failure condition corresponds to the following probability expression

$$Psg(m|n) = \int_{x=-\infty}^{+\infty} dx . f_S(x) . [F_R(x)]^m \quad (2.18)$$

where

$f_S(x)$ = Probability density function of the common stress

$F_R(x)$ = Cumulative probability distribution of the component resistances

In the practical implementation of this concept [HiDep] the normal distributions (or equivalently log-normal distributions) are used for the stress and resistance variables. The common load is extended to be composed of two parts: a base load part that determines the failure probability and dependence at low order and an extreme load part that determines the failure probability and dependence at high order. Four model parameters are defined, see Table 2.1. The parametrization is made with the aim to obtain such parameters that are intuitively simply connected to the probability level and dependence. As being defined through Psg entities CLM is a subgroup invariant model. Consequently, the parameters of CCCGs with different size are directly comparable. For a detailed mathematical description, see [ECLM_Pub].

Table 2.1 Parameters of the extended Common Load Model.

Parameter	Description	Range	Typical value
p_tot	Total single failure probability	[0, 1]	10^{-4} - 10^{-2}
p_xtr	Extreme load part as contribution to the single failure probability	[0, p_tot]	p_tot/p_xtr ≅ 1% – 5% and p_tot >10^{-5}
c_co	Correlation coefficient of the base load part	[0, 1]	0.1 - 0.5
c_cx	Correlation coefficient of the extreme load part	[c_co, 1]	0.6 - 0.9

2.7 Failure rate based models

In the failure rate based modeling the component failures and multiple failures are described by (usually constant) event rates:

$L(m|n)$ = Rate of events where specific m components fail, while other n-m not affected in a CCCG of size n} (2.19)

The multiple events are assumed to be strictly simultaneous, which is a simplification. It is readily noticed that L(m|n) are closely similar to Q(m|n) or Peg(m|n) in the demand failure probability modelling. In the case of standby components and failure to operate at the initial demand the following connection applies:

$$Q(m|n) \cong \tfrac{1}{2} \cdot L(m|n) \cdot T_s(m|n) \quad (2.20)$$

where

$T_s(m|n)$ = Mean time in the standby state over the combinations for m out of n components

The two approaches are via this connection largely compatible. The failure rate based modelling offers a more convenient way to consider test arrangements. It is the obvious choice in the case of time-dependent modelling of standby components and systems. In case of mission time failures and repairable (monitored) components the failure rate based modelling is the more natural way and mostly used approach. Compare to the discussion of this issue in the connection of impact vector method [NAFCS-PR03].

The failure rate based modelling has been used in Loviisa PSA, see the summary description in seminar paper [ICDE-S-Vaurio] and the methodological publications referred to in the seminar paper.

The failure rate based modelling can be used in the manner of Direct Estimation Method (Basic Parameter Model), i.e. L(m|n) are estimated and used as such. Further details of estimation procedures will be discussed in Section 3.7. Alternatively, a parametric model can be applied, e.g. Alpha Factor Method through substituting Q(m|n) by L(m|n) in the parameter definitions, compare to Eq.(2.4) etc.

3. Basic estimation procedures

This section discusses the basic estimation procedures for the considered models and the relationship to impact vector presentation of event statistics.

3.1 Introduction to the estimation of CCF model parameters

The estimation for all of the considered CCF models is based on the presentation of failure statistics by using impact vector method [NAFCS-PR03]. The common statistical input has a very important bearing: the quantitative results obtained by the considered CCF models are generally equivalent (compatible). Only in special cases the specific properties of some model can provide benefits over the others. (It should be kept in mind that the Beta Factor Method is limited to the groups of two components except regarding its use as a crude cut-off model in larger groups.)

The following notation is used for the sum impact vector representing the observed failure statistics:

$V(m|n)$ = 'm+1'th element of sum impact vector in a CCCG of size n (3.1)

The total number of tests/demands in the observation period, i.e. the number of so called Test/Demand Cycles (TDCs) is

ND = Number of demands on the whole CCCG

$$= \sum_{m=0}^{n} V(m|n) \tag{3.2}$$

It should be emphasized that the number of component demands is 'n*ND'. For the failure rate based estimation the observation period is denoted by

E = Exposure time of the CCCG (3.3)

Generally the exposure time need not be a single continuous period of calendar time but it can be constituted of a sum of observed exposure periods, e.g. standby or operation periods. The total component exposure time is 'n*E'.

3.2 Direct Estimation Method

The point (maximum likelihood) estimates for the multiple failure probabilities are obtained most straightforwardly in the following way:

$$\langle Q(m|n)\rangle \cong \langle Peg(m|n)\rangle = \frac{V(m|n)}{\binom{n}{m}.ND}, \tag{3.4}$$

$$\langle pes(m|n)\rangle = \frac{V(m|n)}{ND} \tag{3.5}$$

The brackets <> indicate maximum likelihood estimation. The point estimates for the other SGFPs can be obtained from <Peg(m|n)> by using the SGFP transformations, Annex 1, owing to the linearity of the equations. But, for completeness, the expressions are given explicitly here:

$$\langle Pts(m|n)\rangle = \frac{S(m|n)}{ND} \tag{3.6}$$

where

$$S(m|n) = \sum_{k=m}^{n} V(k|n) \tag{3.7}$$

The direct estimation equation for Psg entity is somewhat more complicated:

$$\langle Psg(m|n)\rangle = \sum_{k=m}^{n} \frac{1}{ND.\binom{n}{k}}.\binom{n-m}{k-m}.V(k|n) \tag{3.8}$$

The point estimate of single failure probability can be reduced from the above equation in case of m = 1:

$$\langle Psg(1)\rangle = \sum_{m=1}^{n} \frac{m.V(m|n)}{n.ND} \tag{3.9}$$

Psg entity is subgroup invariant. Thus for two mutually homogeneous CCCGs of different size the following is valid:

$$Psg(m|n_A) = Psg(m|n_B) \text{ , for } m \le \min(n_A, n_B) \tag{3.10}$$

This aspect can be utilized to present a way of data pooling that uses direct estimation approach to combine statistics from CCCGs of different size, as is discussed in more detail in [NAFCS-PR03].

3.3 Alpha Factor Method

The point (maximum likelihood) estimates for the Alpha Factors are following:

$$\langle \alpha(m|n)\rangle = \frac{V(m|n)}{\sum_{k=1}^{n} V(k|n)} \tag{3.11}$$

Equivalently, the CCBEs could first be estimated, Eq.(3.4) and Alpha Factors derived then by using Eq.(2.4).

3.4 Multiple Greek Letter Method

The point (maximum likelihood) estimates for the MGL parameters are following:

$$\langle g(m|n)\rangle = \frac{\sum_{k=m}^{n} k.V(k|n)}{\sum_{k=m-1}^{n} k.V(k|n)} \tag{3.12}$$

Equivalently, the CCBEs could first be estimated, Eq.(3.4) and MGL parameters derived then by using Eq.(2.9).

3.5 Beta Factor Method

The point (maximum likelihood) estimate for the Beta Factor is same as for MGL parameter of order two (as a cut-off model for n>2):

$$\langle \beta \rangle = \langle g(2 \mid n) \rangle \tag{3.13}$$

This estimation procedure is taken from [NUREG/CR-5485]. In particular, it makes Beta Factor estimate as dependent of the group size, while the basic definition seems to imply subgroup invariance, compare to Eq.(2.16). Due to the extension for n>2 by neglecting the intermediate order CCBEs, there is no coherent unique way to generally estimate the Beta Factor for larger groups. An alternative might be to map impact vector down to CCCG of size 2 for estimation. The presented procedure can, however, be regarded as acceptable taking into account the nature of Beta Factor Method as a crude cut-off model in CCCGs of size above two.

3.6 Common Load Model

It is not possible to present simple point estimation expressions for CLM parameters (Table 2.1) except for the total single failure probability. Of course, it would be possible develop crude point estimation equations, but that may not make sense because the established developed estimation techniques such as maximum likelihood estimation and Bayesian estimation suit very well for CLM. These techniques are based on the use impact vector method. For details see [ECLM_Pub].

3.7 Estimation of failure rate based models

The point (maximum likelihood) estimates for the multiple failure rates are:

$$\langle L(m \mid n) \rangle = \frac{V(m \mid n)}{\binom{n}{m}.E} \tag{3.14}$$

Notice the analogy with the estimation of CCBE probabilities, Eq.(3.4). It has to be emphasized the 0'th element of the sum impact vector does not have direct bearing in the failure rate based modeling. Similarly, TDCs do not have such a central role as in the demand failure probability based modelling. Still the TDCs can be defined in an equal way to aid the consideration of simultaneity aspect in the event analysis and interpretation. This issue is discussed in more detail in [NAFCS-PR03].

The implementation of Bayesian estimation method to failure rate based modelling of CCFs and the uses in Loviisa PSA are described in seminar paper [ICDE-S-Vaurio].

4. Model regimes

This section will summarize the specific practical regimes of the models, including the current uses in the Nordic PSA studies.

The CCF models considered here use impact vector method for the presentation of failure statistics. Owing to the same statistical input the methods will produce compatible results. Still the specific properties of some model can provide practical benefits over the others in certain respects and/or in special application cases.

Alpha Factor Method can be regarded as a generally applicable model. Especially lot of development work is made and published for this method about the Bayesian estimation and uncertainty analysis.

Multiple Greek Letter Method is similar to Alpha Factor Method but does not lend equally well to developed estimation techniques. This can be bypassed by first estimating Alpha Factors, converting then the parameters into Multiple Greek Letters.

The Beta Factor Method is limited to the groups of two components except regarding its use as a crude cut-off model in larger groups.

Common Load Model is especially suitable to highly redundant systems as it has a fixed number of parameters and is subgroup invariant – in contast to Alpha Factor Method and Multiple Greek Letter Method which add a further parameter for each order of multiplicity and are not subgroup invariant.

The Direct Estimation Method is close to AFM (or vice versa, in fact): the difference is in the normalization of Alpha Factors. It might be advisable to primarily use the Direct Estimation Method and to convert the obtained SGFPs then into form of CCF parameters (Alpha Factors, Multiple Greek Letters) for the presentation of relative dependence level or for comparison purpose. It has to be noticed that for these aims there are also other suitable parametric CCF models (Annex 2).

Annex 3 presents a practical example to illustrate the CCF models discussed here.

In practical uses of the parametric CCF models, such as AFM, MGLM and Beta Factor Method, it is usual in case of lacking specific CCF data to use internationally published CCF parameter values in conjunction with plant specific single failure probability. This means that the multiple failure probabilities are directly dependent of the single failure probability although only part of the CCF mechanisms contain such a connection, while the other part can be largely not at all correlated to the single failure probability. One way to control this aspect is to check the level of single failure probability in the source data if possible. The Direct Estimation Method (Basic Parameter Method) does not have this problem. But on the other hand, there are rather little published data to support this approach and hence it is mainly viable only in case of sufficient amount of specific data input. For CLM one guideline to assess the extreme load part (see Table 2.1) is to keep it in the range of a few percent relative to single failure probability. It is, however, advised also to consider other factors that can influence on the probability level of high order CCFs.

5. Concluding remarks

An important notion related to the connection of dependence level with single failure probability is the substantial impact that the test interval and staggering can have. It is highly recommended to control this influence when transferring data, e.g. by an adequate mapping procedure. A coherent treatment of test interval and staggering influence needs to be taken care of in the continuation across event analysis, impact vector construction, estimation and use of CCF parameters.Compare to the further discussion of this subject in [NAFCS-PR03].

The correlation of single failure and multiple probability levels is also discussed in connection to so called Generic Dependence Classes in [NAFCS-PR02].

This survey was closed by declaring Draft for Peer Review as final for this phase with small editorial changes only, due to resource limitations. No comments were gained from the peer review, except a question raised about the treatment of single failures (so called independent failures) in the event data collection. This question is related to the coupling issue of the single failure probability and CCF probability, which was discussed in the previous section. See separate further notes on the subject in [NAFCS-WN-TM12].

There are many areas and issues of the CCF models which would need further elaboration. Hopefully, the work in this direction can be continued in the next phases of NAFCS. It is especially proposed that the current uses of the CCF models in the Nordic PSA studies will be more systematically summarized in the next issue of this report, based on the information gathered in the utility survey [NAFCS-PR05]. The consideration of further CCF models used in the other countries, especially in the ICDE member countries as outlined in Annex 2, is desired to facilitate future comparison aims. One more important issue for the further work concerns CCF models for time-dependent modelling of standby components and systems.

Acknowledgements

The NAFCS members have given valuable contribution in conducting this task through the discussions and comments. Especially the comments by Kurt Pörn on the last working draft are acknowledged.

References

NAFCS-Programme-R1
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR02
Data Survey and Review. Topical Report NAFCS-PR02, prepared by Tuomas Mankamo, Issue 1, 10 October 2003.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2, 31 August 2003.

NAFCS-PR05
”Survey on Defence against Dependent Failures”- Compilation and Results of Plant Survey. Per Hellström.

NAFCS-WN-TM12
Coupling of the single failure probability and CCF probability. Work notes by T. Mankamo, 07 April 2003.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

ICDE-S-Vaurio
From Failure Rate to CCF-Rates and Basic Event Probabilities. Presentation by J.K. Vaurio, ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, Stockholm, 12 – 13 June 2001.

NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

NUREG/CR-5497 CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998

SKI TR-91:6 Mankamo, T., Björe, S. & Olsson, L., CCF analysis of high redundancy systems, SRV data analysis and reference BWR application. Technical report SKI TR-91:6, Swedish Nuclear Power Inspectorate, 1991.

HR_CCFRe High redundancy structures, CCF models review. Work report prepared by Mankamo, T., Avaplan Oy, 31 December 1990. (Work report companion to SKI TR-91:6)

SKI R-96:77 Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Summary report, prepared by T. Mankamo. SKI Report 96:77, December 1996.

SKI/RA-26/96
CCF Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Work reports, prepared by T. Mankamo. SKI/RA-26/96, December 1996.

CA_HRedI Instructions for CCF analysis of high redundancy systems. 2nd Version, T. Mankamo, Avaplan Oy, 22 November 1995. (Part of SKI/RA-26/96)

ECLM_Pub Mankamo, T., Extended Common Load Model, A tool for dependent failure modeling in highly redundant structures. Manuscript, 15 February 1995, 10 February 2001.

RS-ThM Risk Spectrum Theory Manual. Ulf Berg, Relcon AB, Version 2.1, April 1994.

HiDep HiDep, CCF Analysis Toolbox, Version 2.4. Avaplan Oy, 2001.

SHACAM Mankamo, T., SHACAM, Shared Cause Model of Dependences - A review of the Multiple Greek Letter Method and a modified extension of the Beta-factor Method. Avaplan Oy, 28 March 1985.

TC_PASDG Mankamo, T., A timedependent model of dependent failures, application to a pairwise symmetric structure of four components. Manuscript NKS/SIK-1(92)13, 31 December 1993.

Abbreviations

Acronym	Description
CCBE	Common Cause Basic Event
CCCG	Common Cause Component Group
CCF	Common Cause Failure
TDC	Test/Demand Cycles
SGFP	Subgroup Failure Probability
AFM	Alpha Factor Method
CLM	Common Load Model
MGLM	Multiple Greek Letter Method
CRDA	Control Rod and Drive Assembly
HPSI	High Pressure Safety Injection
MOV	Motor Operated Valve
ICDE	International CCF Data Exchange
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate

Annex 1: Terminology, Probability Entities

The terminology defined in ICDE is used whenever applicable. This annex collects definitions of special additional terminology and probability entities.

Special terminology

Homogeneity

- *of a CCCG:* the probability entities in the subgroups of any given size are mutually identical, i.e. homogeneity means also symmetry
- *across two CCCGs of same size:* both CCCGs are internally homogeneous and the probability entities of the CCCGs are mutually identical
- *across two CCCGs of different size:* both CCCGs are internally homogeneous and the probability entities of the smaller CCCG are mutually identical with any subgroup of the same size in the larger CCCG
- *a CCCG population:* the CCCGs of the population are internally and mutually homogeneous.

Subgroup invariance:

The probability entity or parameter is same in a subgroup as in the whole CCCG. As a corollary, a subgroup invariant probability entity or parameter is same in mutually homogeneous CCCGs of different size.

Mapping up/down:

In order to transfer an impact vector (or CCF parameters of a model or SGFP entities which are not subgroup invariant) from a 'source' group A to 'target' group B the following procedures are required:

- mapping down if the target group is smaller
- mapping up if the target group is bigger

See further details in [NAFCS-PR03, Section 6].

Single failure probability

This entity is also called as "total single failure probability" in order to emphasize that the probability contains all the instances where the specific considered component fails either alone or as part of a multiple failure (that is most likely an actual CCF, but can be also a coincidental multiple failure with differing failures causes). In the mathematical expressions the single failure probability is denoted by Q_T or Psg(1). In the connection to CCF analysis the concept "independent failure" is used to characterize instances where the specific considered component fails alone and not due to a CCF mechanism that happens to affect only one component that time (so called non-lethal shock with one component failure event). This concept is practically convenient but it must be emphasized that a clear distinction for independent failure cannot be done. The CCF models which do not require such a distinction have a certain advantage.

Special probability entities

Subgroup Failure Probability (SGFP) entities represent different ways to express multiple failure probabilities in a CCCG. The definitions of four entities are presented in the attached diagram. Here it is assumed that the CCCG is internally homogeneous, which means also internal symmetry. Thus the SGFP entities are connected to failure multiplicity but not to the specific combination of failing components. The SGFP entities are connected to the group size with the exception that Psg entity is subgroup invariant (but the other three defined SGFP entities are not).

The SGFP entities can be transformed within each other. The attached diagram shows a practically convenient transformation scheme.

The background to the naming convention is composed by the following key words:

Psg denotes failure Probability of a Specific Group of components (typically a subgroup of a CCCG)

Peg denotes failure Probability of an Exclusive and specific Group of components

Pes denotes failure Probability of an Exclusive groups of components Summed over given multiplicity

Pts denotes failure Probability of Total System for a given failure criterion

The three letter syntax was initially adopted when defining variable names for programming the transformation equations.

The different SGFP entities can be exemplified in the case of four components, n=4 and failure multiplicity m=3:

$$Psg(3\,|\,4) = P\{X_1 X_2 X_3\} = \ldots = P\{X_2 X_3 X_4\}$$

$$Peg(3\,|\,4) = P\{X_1 X_2 X_3 \overline{X_4}\} = \ldots = P\{\overline{X_1} X_2 X_3 X_4\}$$

$$\begin{aligned} Pes(3\,|\,4) &= P\{X_1 X_2 X_3 \overline{X_4} + \ldots + \overline{X_1} X_2 X_3 X_4\} \\ &= P\{X_1 X_2 X_3 \overline{X_4}\} + \ldots + P\{\overline{X_1} X_2 X_3 X_4\} \end{aligned}$$

$$Pts(3\,|\,4) = P\{X_1 X_2 X_3 + \ldots + X_2 X_3 X_4\}$$

where X_k = Failure event of component k

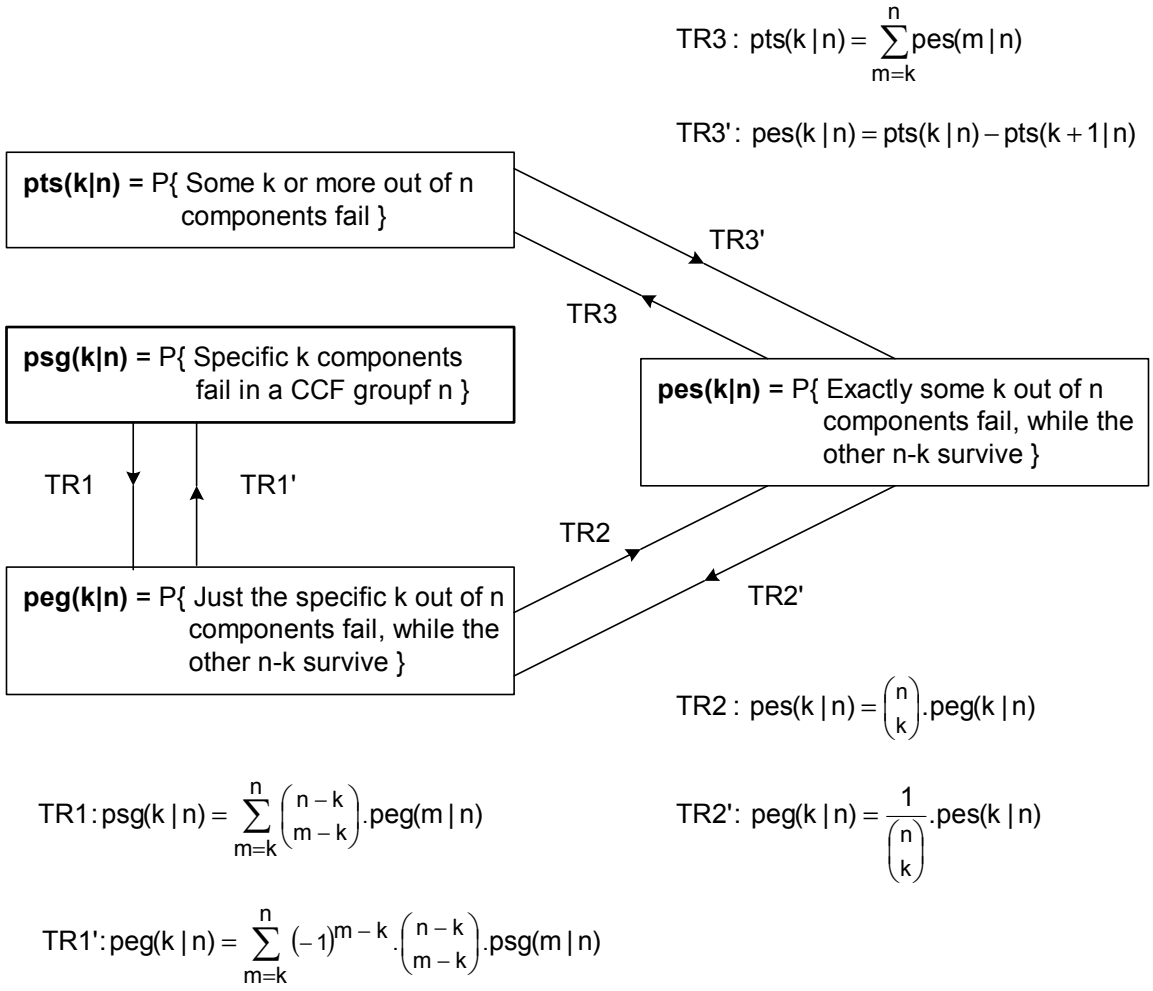
These probability expressions form the background to the transformation equations. Then, if the subgroup of the first three components is considered:

$$Psg(3\,|\,3) = Peg(3\,|\,3) = Pes(3\,|\,3) = Pts(3\,|\,3) = P\{X_1 X_2 X_3\}$$

The comparison with the entities of the whole group, and same failure multiplicity m=3 illustrates the subgroup invariance of Psg, and lack of that property by the other three entities. Further discussion of SGFP entities can be found in [ECLM_Pub, CA_HredI].

Transformation scheme

of subgroup failure probability entities



SGFP-Transf.vsd

Annex 2: CCF Models Used in Other ICDE Member Countries

The survey is proposed to be extended to generally describe the CCF models used in the other ICDE countries in addition to those primarily covered in this report. One purpose is to allow principal comparisons.

Table A2 The following scope is suggested:

CCF model	ICDE member country used in
General Shock Model	…
Binomial Failure Rate Model	…
Extended Binomial Failure Rate Model	Germany
…	
Primitive Parameters	Finland
SHACAM Parameters	Finland
…	

…

Primitive Parameters

Primitive Parameters are defined as step-wise relative reduction of Psg entity for increasing failure multiplicity:

$$z_m = \frac{Psg(m)}{Psg(m-1)} \qquad \text{(A2.1)}$$

The practical interpretation of z_m is that it represents the conditional failure probability of the next specific component given that a subset of m-1 components fails. The subgroup invariance property of Psg entity means that the Primitive Parameters are also subgroup invariant.

In TVO/PSA the Primitive Parameters are used for the data presentation, because they are easy to understand and facilitate the comparison of relative dependence level. Due to subgroup invariance property the Primitive Parameters are comparable even between CCCGs of different size. The estimation of CCF data is, however, done by using direct estimation, or CLM depending on the case, to primarily derive SGFP entities. When using internationally published CCF data that is first transformed into SGFP entities for the considered CCCG, including eventual mapping and data pooling. As said the Primitive Parameters are an auxiliary tool for a convenient presentation of the relative dependence level. The limitation of the Primitive Parameters is that they should not be directly modified without an aid of an ordinary CCF model due to the risk of causing contradiction with the inherent connections between the failure probabilities of different multiplicity.

SHACAM Parameters

The dependence parameters can defined as the conditional probability of specific m components failing due to CCF given that a subset of m-1 components fails due to CCF, in mathematical terms:

$$y(m \mid n) = P\left\{Y^{(n)}_{1...m} \middle| Y^{(n)}_{1...m-1}\right\} = \frac{P\left\{Y^{(n)}_{1...m}\right\}}{P\left\{Y^{(n)}_{1...m-1}\right\}} \qquad \text{(A2.2)}$$

where

$Y^{(n)}_{1...m}$ = Failure of a set of specific m components due to CCF
(for convenience of presentation, the components are indexed by 1, …, m)

with the following defaults

$Y^{(n)}_{1...1}$ = Failure of one specific component due to any cause

$P\left\{Y^{(n)}_{1...1}\right\}$ = Psg(1|n) = Q_T

It is noticeable that for one component failure cause there is not made distinction for "independent causes" and "CCF mechanisms"; this well-known dilemma was discussed already in the main body of the survey report, and is a feature of MGLM and AFM as well. See for details of the definition and comparisons in [SHACAM].

In the Rare Event Approximation:

$$P\left\{Y^{(n)}_{1...m}\right\} = \sum_{k=m}^{n} \binom{n-m}{k-m} . Q(k \mid n) \qquad \text{(A2.2)}$$

Notice the similarity with respect to the derivation of Psg(m|n) in terms of Peg(m|n), see Annex 1. In fact SHACAM parameters are close counterparts to the Primitive Parameters with the difference that in SHACAM multiple failures due to CCF are counted while the Primitive Parameters consider multiple failures due to any causes. Compare the definitions in Eq.(A2.1) and (A2.2).

SHACAM parametrization is similar to MGLM and AFM but it has the benefit that the parameters are subgroup-invariant in practical approximations. This property can be seen in the example cases presented in Annex 3. The SHACAM parameters have also the following intuitive property, that is valid practical cases:

$$0 < y(1|n) < y(2|n) < \ldots < y(n-1|n) < y(n|n) < 1 \qquad \text{(A2.3)}$$

The basic definition in terms of escalating CCF probability makes SHACAM parameters particularly convenient for the use in the quantitative analysis of CCF defence factors. These parameters have been used in the analysis of test arrangements [TC_PASDG].

Annex 3: Example Case of CCF Parameters

The CCF models are exemplified here with a numeric example taken from the US sources (one reason is to reuse a recent example prepared in connection to Kola 2 PSA) . In the continuation it is recommended to change to an example with local specific data, where the input is better known and controlled.

Data

The example data is from Ref.[NUREG/5497] for Motor Operated Valves (MOVs) of High Pressure Safety Injection (HPSI) systems in PWRs; failure mode is 'Failure to Open'. The impact vectors and average Alpha Factors are quoted in Table A3.1. The source presents so called adjusted independent events separately, but here it is combined to 1st element of impact vector. The source lacks information about the 0th element of impact vector similarly as the number of TDCs (not directly needed to merely estimate Alpha Factors). For CCCG=6 those missing variables are derived using the assumed single failure probability and a procedure to be explained in connection to CLM example in the later section.

As for the MOV reliability data in order to derive probability entities, the generic US IPE data will be used for the demand failure probability. According to [NUREG/CR-

Table A3.1 CCF data for HPSI MOVs and failure mode 'Failure to Open' [NUREG/5497, Section 31].

Multiplicity k		Impact Vectors for CCCGs of Size 2...6				
		CCCG=2	CCCG=3	CCCG=4	CCCG=5	CCCG=6
0	V_0					15215.1
1	V_1	78.9599	116.3994	152.6964	188.5346	224.2402
2	V_2	6.7393	1.9575	3.7738	4.5094	5.2865
3	V_3		6.0569	0.2089	1.2016	1.6735
4	V_4			6.0045	0.0612	0.5533
5	V_5				6.0006	0.0210
6	V_6					6.0000

Km

Multiplicity k		Alpha Factors for CCCGs of Size 2...6				
		CCCG=2	CCCG=3	CCCG=4	CCCG=5	CCCG=6
1	α_1	0.9213610	0.9355827	0.9386097	0.9412263	0.9430793
2	α_2	7.86E-2	1.57E-2	2.32E-2	2.25E-2	2.22E-2
3	α_3		4.87E-2	1.28E-3	6.00E-3	7.04E-3
4	α_4			3.69E-2	3.06E-4	2.33E-3
5	α_5				3.00E-2	8.83E-5
6	α_6					2.52E-2

Notes for CCCG=6:			
	Assumed single failure probability	p_tot	3.00E-3
	Sum of $k*V_k$	VfSum	278.15
	Total number of group demands	ND	15452.9

4550] Q_t = p_tot = 3E-3 for MOV and failure mode 'Failure to Open'. It is believed that this single failure probability is reasonably compatible with the CCF data.

Comparing CCF parameters for CCCG of size 2 ... 4

The CCF parameters and corresponding SGFP entities are compared in Fig.A3.1 for CCCG sizes of 2 through 4. The derivation is based on Alpha Factors from Table A3.1 and assumed single failure probability P1 = Psg(1) = 3E-3, that is needed in deriving the probability entities. Primitive parameters z_m are explained in Annex 2. Parameters y_m are defined as the conditional probability of specific m components failing due to CCF given that a subset of m-1 components failed due to CCF; these so called SHACAM parameters are described in Annex 2.

The example case shows rather high dependence. This is related to the large portion of impact vector element of order 6, corresponding to a fraction of about 3% relative to single failure count, i.e. a CCF ratio that is in general typical for double failures.

CLM parameters

Using the presented impact vector of CCCG=6 as statistical input a Maximum Likelihood fit to CLM is presented in Fig.A3.2, including calculation of the SGFPs. The number of group demands ND is obtained from the following equality:

$$p\_tot = \frac{1}{ND} \cdot \sum_{k=1}^{n} k \cdot V_k = \frac{1}{ND} \cdot VfSum \qquad (A3.1)$$

As p_tot must be taken from a separate source than impact vector there is certain implied uncertainty (unfortunately, it is the standard practice in the USA to collect and estimate component reliability data and CCF data separately). It shall be further noticed that impact vector element V_0 can be derived from the equality

$$ND = \sum_{k=0}^{n} V_k \qquad (A3.2)$$

once ND is known in conjunction to $V_1, \ldots, V_n$. Element V_0 is a necessary part of the Maximum Likelihood estimation for dependence parameters.

The obtained CLM parameters from Maximum Likelihood fit show strong dependence at high multiplicity (relatively large p_xtr and c_cx) in accordance with the conclusion from the look at the parameters of other CCF models in Fig.A3.1.

HiDep/Version 2.3
CCF Parameter Scale Down, 22 Sep 00

This execution sheet is used to calculate for given Alpha Factors and P1 the corresponding SGFP entities and dependence parameters, in each CCCG size 4..2

P1 3.00E-3 is given — HPSI MOV Alpha Factors from NUREG/CR-5497

	P1 Q(1|n) peg(1|n) pes(1|n) pts(1|n)	P2 Q(2|n) peg(2|n) pes(2|n) pts(2|n)	P3 Q(3|n) peg(3|n) pes(3|n) pts(3|n)	P4 Q(4|n) peg(4|n) pes(4|n) pts(4|n)	 alpha1 alphat	z2 beta y2 alpha2	z3 gamma y3 alpha3	z4 delta y4 alpha4
CCCG4	3.00E-3	4.46E-4	3.93E-4	3.90E-4		0.149	0.882	0.990
	2.48E-3	4.08E-5	3.38E-6	3.90E-4		0.174	0.765	0.975
	2.45E-3	4.90E-5	3.76E-6	3.90E-4		0.146	0.899	0.991
	9.81E-3	2.94E-4	1.50E-5	3.90E-4	0.939	2.32E-2	1.28E-3	3.69E-2
	1.05E-2	6.99E-4	4.05E-4	3.90E-4	1.136			
CCCG3	3.00E-3	4.45E-4	3.94E-4			0.148	0.886	
	2.52E-3	4.23E-5	3.94E-4			0.159	0.823	
	2.50E-3	5.09E-5	3.94E-4			0.145	0.903	
	7.51E-3	1.53E-4	3.94E-4		0.936	1.57E-2	4.87E-2	
	8.06E-3	5.47E-4	3.94E-4		1.113			
CCCG2	3.00E-3	4.46E-4				0.149		
	2.56E-3	4.37E-4				0.146		
	2.55E-3	4.46E-4				0.146		
	5.11E-3	4.46E-4			0.921	7.86E-2		
	5.55E-3	4.46E-4			1.079			

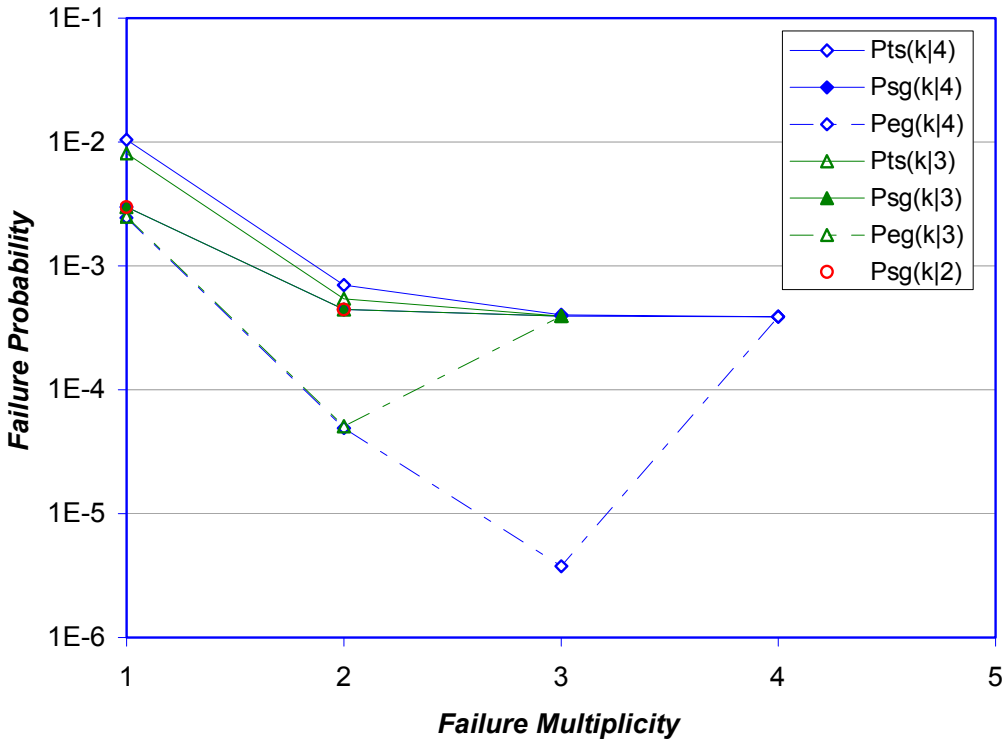


Figure A3.1 Comparison of CCF parameters and SGFP entities in case of the Alpha Factors for HPSI MOVs, failure mode 'Failure to Open' [NUREG/5497, Section 31] .

HiDep Version 2.4
Extended Common Load Model
Avaplan Oy, April 2001

BE **HPSI MOVs, Failure to Open, Best Estimate**
2

CCF group size
KmMax 6

CLM parameters

p_tot	3.0E-3	c_co	0.15
p_xtr	5.0E-4	c_cx	0.90

Point estimate

ND	15452.9
VfSum	278.152
p_est	3.00E-3

Km	Psg_b	Psg_x	Psg	Zk	Peg	Pes	Pts	Vk	Sk/ND
0	0.999	1.27E-3	1.000	-	0.985	0.985	1.000	15215.1	1.000
1	2.50E-3	4.99E-4	3.00E-3	0.003	2.41E-3	1.44E-2	1.54E-2	224.24	1.54E-2
2	2.25E-5	4.09E-4	4.31E-4	0.144	2.57E-5	3.85E-4	9.21E-4	5.29	8.76E-4
3	4.82E-7	3.66E-4	3.66E-4	0.849	3.76E-6	7.51E-5	5.36E-4	1.67	5.34E-4
4	1.92E-8	3.39E-4	3.39E-4	0.925	4.57E-6	6.86E-5	4.60E-4	0.55	4.25E-4
5	1.22E-9	3.20E-4	3.20E-4	0.944	1.44E-5	8.64E-5	3.92E-4	0.02	3.90E-4
6	1.11E-10	3.05E-4	3.05E-4	0.955	3.05E-4	3.05E-4	3.05E-4	6.00	3.88E-4

LogLikeL -747.379
DeltaLL 0.222

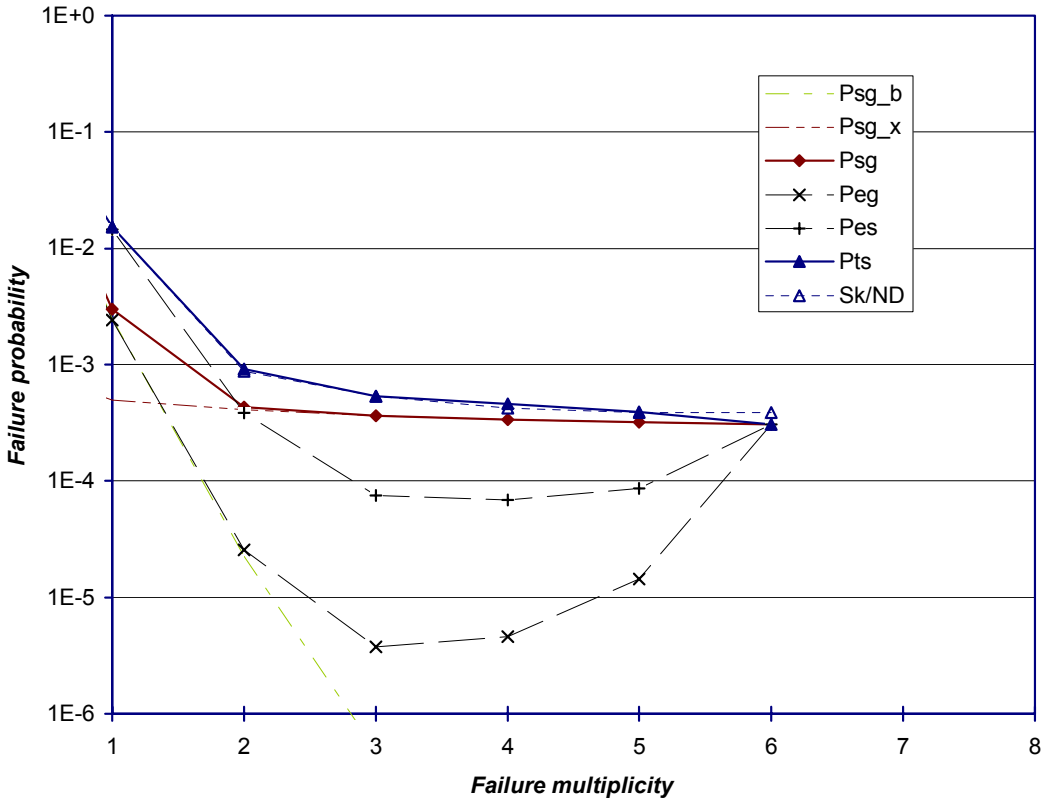


Figure A3.2 CLM fit to the impact vector data for HPSI MOVs, failure mode 'Failure to Open' [NUREG/5497, Section 31] .

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
App4.2	**Impact Vector Method PR03**	**PR03**
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR03**

Title:	**Impact Vector Method**
Author(s):	*Tuomas Mankamo*
Issued By:	
Reviewed By:	*Michael Knochenhauer, 2002-10-29*
Approved By:	Gunnar Johans0n
Abstract:	This topical report presents the definition, theoretical background and methodological aspects of Impact Vectors to support the practical instructions that are presented in a separate report NAFCS-PR17 (from Issue 2 on). The current issue is begun with a synopsis introducing the concept of Impact Vector and its role in the CCF data analysis.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2001-05-18	TM
Draft 1	2001-06-04	TM
Draft 2	2001-09-18	TM
Draft 3	2001-10-18	TM
Draft for Peer Review	2002-01-12	TM
Issue 2, outline … partially upgraded	2002-10-10 … 2002-10-21	TM
Issue 2, Draft 1	2002-11-27	TM
Issue 2	2003-08-31	TM
Final	2003-08-31	GJ

Contents

Synopsis

Impact Vector expresses the conditional failure probability, given an observed Common Cause Failure (CCF), that different number of components would fail if an actual demand should occur during the presence of CCF impact. In the group of 'n' components, which is exposed to CCF, Impact Vector contains 'n+1' elements, one for each order of failure 'm', including the outcome 'no failure' (m = 0) and 'all failed' (m = n). The elements describe the probability distribution for the outcome states of a postulated demand.

Impact Vector is a generalized presentation of the demand outcome. It is especially needed in such situations where the outcome is not perfectly known to be one certain failure state, chances existing for different states. Such a situation typically arises when CCF is detected in a periodic test and testing does not completely represent actual demand conditions. For example, when a fuel leak is detected in testing a diesel generator the test run will be promptly stopped to avoid fire risk. Furthermore, the redundant diesel generators with eventually degraded fuel piping are neither experimented by extensive load running test to verify if they would survive or burn into inoperable state. It is left to the analyst to interpret the existing information from the test and the failure mechanism in overall, including observations from the past similar events, and to make assessment for the outcome in the case that an actual demand had been imposed on the components (group of the redundant diesel generators in the example).

Impact Vector provides to the analyst the necessary way to express the spectrum of chances (or equivalently the uncertainty) by a distribution of the possible demand outcome over different failure states. The principal method for Impact Vector assessment is the use of alternative scenarios (hypotheses) about the CCF impact. Impact Vector constitutes an interface from the CCF event analysis to the statistical treatment and quantitative assessment of CCF probability.

1. Introduction

1.1 Objectives

One of the basic tasks of NAFCS is the preparation of a guideline for Impact Vector construction, starting from the method description and including examples of different types of cases [NAFCS-PR01]. The current issue of this report contains the methodological part, while the practical instructions are moved to a separate report [NAFCS-PR17].

The method description and construction guide will support the quantitative classification and evaluation of CCF events. A pilot application has been conducted for the diesel generators (DGs), see [NAFCS-PR10]. The more recent applications for the centrifugal pumps and motor operated valves [NAFCS-PR18, NAFCS-PR19] follow much the same procedure. It is expected that both the method description and construction guide will be supplemented in the course of coming assessment work with different types of components to cover more comprehensively special issues. Also the spectrum of practical examples will be extended according to the cumulating insights. The needed continued work will be summarized in Section 7.

Besides of the recent applications within NAFCS, this method description is based on the experiences that have been cumulated in several earlier CCF analyses [SKI TR-91:6, SKI R-96:77, T314_TrC], including EdF pilot study for the Control Rod and Drive Assemblies (CRDAs) [ICDE-S-EdF]. The early work on this task was presented in the ICDE seminar in June 2001 [ICDE-S-ImpVe].

1.2 Scope

The construction of Impact Vector is basically developed as applicable to demand failure probability. Application to failure rate based modeling will be generally discussed and simplified approach presented. However, this issue still requires further development, similarly as the treatment of time-dependence more generally.

The initial data collection of CCF event information is not handled here. This part of the CCF analysis is well covered by the ICDE guideline [ICDECG00]. For an integral description of various CCF analysis parts, see [NUREG/CR-5485].

1.3 Report structure

Chapters 1-5 are made parallel in this method description (PR03) and construction guide (PR17) in order to facilitate finding the additional background and explanations from PR03 when working in practice following the guide PR17. For this aim the headings of the parallel sections are identical or similar. Some very basic definitions are repeated in both reports. One argument behind this is to make the reports possible to understand sufficiently well as stand-alone. Another argument is that the similarity of key parts will support the linkage between the texts. The reader, for whom the subject is new, is recommended to explore first the guideline [NAFCS-PR17] as a concise tutorial. The annex of the guideline contains type examples of Impact Vector construction.

2. Impact Vector concept

This section presents the definition and theoretical background for the Impact Vector concept. Connection to the probability entities of Common Cause Component Group (CCCG) is pointed out.

A large number of special terms are defined during the course of presentation. The definitions are not collected anywhere. Such an annex for definitions is planned to be contained in the future version of this method description and/or in the guideline. For the time being the reader is recommended to use the 'Find' command to locate the definition or introduction to a special term within the electronic document. A basic definition of terms, mainly related to CCF event analysis, is presented in the ICDE guideline [ICDECG00], and more comprehensively in [NUREG/CR-5485].

2.1 Basic definition and assumptions

The Impact Vector describes the outcome of a demand placed on a group of components, which constitute a CCCG. In a CCCG of size 'n' the Impact Vector has 'n+1' elements:

$$\mathbf{v} = [\, v_0, v_1, v_2, \ldots, v_n \,] \qquad (2.1)$$

In the basic case, where the functioning of each component at the demand is perfectly known either successful or failed, the number of failures is exactly determined: the Impact Vector elements are then zero, except $v_m = 1$ given that 'm' components failed, e.g.

$$\mathbf{v} = [\, 1, 0, 0, \ldots, 0 \,] \text{ , when all components functioned} \qquad (2.2)$$
$$\mathbf{v} = [\, 0, 1, 0, \ldots, 0 \,] \text{ , when one component failed, n-1 survived}$$
$$\mathbf{v} = [\, 0, 0, 1, 0, \ldots, 0 \,] \text{ , when two components failed, n-2 survived}$$
$$\mathbf{v} = [\, 0, 0, \ldots, 0, 1 \,] \text{ , when all components failed}$$

The majority of the demands are represented in practice by failure-free Impact Vectors [1, 0, 0, … , 0].

In order to be more precise in certain formulas it is important to show the total number of components. The elements are then denoted by $v_m = v(m|n)$. The Impact Vector entity alone, without showing elements, is denoted by bold letter.

Symmetry assumption

The normal assumption of CCF analysis is used also here as starting point: the considered CCCG is assumed internally symmetric and homogeneous. This means that the component combination of certain order are equal with respect to CCF impact. Consequently, they are not normally separated in Impact Vector. For example, Impact Vector [0, 0, 1, 0, … , 0] represents all n*(n-1)/2 combinations where some 2 out of n components fail, while the other n-2 survive. In order to follow this line the assumption of internally symmetry and homogeneity has to be met in sufficient degree, or it has to be postulated as a simplification. The parametric CCF models also normally use this assumption.

If there exists a significant asymmetry in the considered component group it is possible to generalize Impact Vector definition (and CCF models as well) to handle component combinations specifically. For example, in the case of four safety trains (ABCD) the pairs (e.g. AC and BD) can be in the same room and share process environment, while the physical and process separation is more efficient between the pairs. In such a situation the train combination in a pair (AC or BD) are more vulnerable to CCF that other combinations (AB, AD, BC, CD). The generalization of Impact Vector to this kind of pair-wise symmetric case is straightforward, see analogous generalization of a CCF model in [TC_PASDG].

Intact, degraded and failed state

When a failure (CCF) mechanism is present the conditional failure probability is increased above the normal:

$$P\{X\} << P\{X|E\} \leq 1 \qquad (2.3)$$

where

E denotes the evidence about the failure mechanism present at a given time point or during a given time period

In the above formula P{X} denotes the normal failure probability, i.e. long-term mean, and X denotes the component failure at demand. For the conceptual introduction the failure probability is considered here according to the time-independent simplification except that the present failure mechanism implies a temporary increase (the more developed time-dependent approach will be discussed later). The above conditional failure probability is called as component degradation value (or impairment value):

$$d = P\{X|E\} \qquad (2.4)$$

The component degradation value can range between the low bound of normal failure probability, which is called as intact state, and high bound of value one, i.e. completely failed state. There is similar connection between Impact Vector and conditional multiple failure probability as will be discussed in the following sections. Besides, for practical convenience the normal (bottom line) failure probability will be renormalized away as will be presented in Section 2.2.

The term ‘intact’ means in practical context that the present failure mechanism has no or only negligible effect on the operability of the component.

The treatment of degraded component states is very central in the Impact Vector construction, and will be discussed further in the following sections.

Independent or single failure

The single failure outcome [0, 1, 0, … , 0] is traditionally called as “independent” failure, and the number of such observations as ‘independent count’. The attribute “independent” is, however, misleading because it may be just a coincidence for many cases that only one component failed and other components remained intact. Therefore, the term ‘single failure’ is preferred in this report in order to not confuse ‘dependence’ directly with observed failure multiplicity.

It is also essential to understand the group context. Namely, the considered CCCG can be broken up into one-component subgroups and disregard the connection information when gathering the failure observations (as done in a data analysis for plain component reliability). For example, when considering the observation that component with index k = 1 fails and other n – 1 are operable, the Impact Vector for the whole group 'G' and the subgroup 'A' composed of the first component are two different entities:

$$\mathbf{v}_G = [\,0, 1, 0, \ldots, 0\,] \neq \mathbf{v}_A = [\,0, 1\,]$$

The former entity carries the information what happens with the other components while the latter disregards that information. In practical sense, the 'single failure' event in a CCCG (size two or more) excludes multiple failure event.

Connection to failure mode

The Impact Vector presentation is bound to failure mode similarly as component and CCF models. The different functional failure modes require each a specific way of treatment. Especially, latent and monitored failure modes should be kept strictly separate because they differ significantly both regarding qualitative analysis and quantitative treatment. The experiences show that the dependence characteristics can be much different between the various failure modes of the component type.

Surveillance test versus actual demand

In some cases the surveillance test for a particular component and failure mode can be regarded as complete as an actual demand in the meaning that the test outcome perfectly tells what had been the outcome of an actual demand at that time point. However, more often the tests are less complete. The observed degradation of the component(s) at the test is then left for the interpretation and judgment regarding the operability in actual demand conditions. One typical reason to this situation is that testing of pumps, diesel generators and other kinds of rotating machines are stopped once symptoms of degradation are detected in order to avoid catastrophic failure, i.e. the operability is not completely verified by forcing the test to the end such as running the component over required mission time under full load.

Another type of situation, where judgment is needed, is connected to staggered testing without strict rule to test the redundant components always directly when one component is found degraded or failed. In such a situation the observations of the redundant components' status will be spread over disjoint time points, and a crucial question is, whether several components had failed, if an actual demand had occurred during that period of time. Impact Vector method provides a systematic procedure to handle the needed judgment.

The actual demands are relatively rare, and consequently the "hard" evidence cumulating from them is sparse. The information from surveillance tests is much more abundant, but mostly imperfect evidence, so the analyst is facing the "hard" work of interpretation and judgment to benefit from test-based information. These questions will be treated further in the next section.

2.2 Degraded component states and Impact Vector

The Impact Vector method is really needed to consider such failure situations where the operability of the components is observed degraded but not perfectly known to be either completely failed or practically taken intact. Such a situation is typically connected to the incompleteness of testing, compare to the discussion in the previous section. The affected component is then called degraded, i.e. being in a state between clearly operable and clearly inoperable state. Correspondingly, the elements of Impact Vector will then attain values in the range (0,1) with the following interpretation:

v_m = Conditional probability that some 'm' components fail and other 'n-m' survive given that an actual demand should occur in the observed condition (2.5)

Similarly, component degradation value (also called impairment value) can be defined in the following way

d_k = Conditional probability that a specific component, indexed by 'k', fails given that an actual demand should occur in the observed condition (2.6)

It has to pointed out that the Impact Vector definition means that following equality has to be met:

$$\sum_{m=0}^{n} v_m = 1 \quad (2.7)$$

It can thus be said that the Impact Vector elements describe how the demand outcome probability is distributed over different order of failure states.

There is no universal one-to-one correspondence between the Impact Vector and component degradation values, see a more thorough discussion in [CR_ImpVe, CR_ImpV2]. (Those work notes are available at the ICDE web site.) However, they are fundamentally connected. The assessment of component degradation values is easier, and they can be useful in the Impact Vector construction as will be discussed later on, e.g. constructing upper and lower bound Impact Vector, see Section 5. An obvious connection is that the highest order of non-zero elements in Impact Vector equals to the number of components having non-zero degradation value. In mathematical terms, if 'm' components are completely failed and 'j' degraded, then the highest order of non-zero elements in Impact Vector equals to 'm+j'.

In practical analysis a somewhat different interpretation is used for Impact Vector and component degradation values, deviating from the strict definition as conditional probability, Eqs.(2.4-6). Only the impact of the present (observed) CCF mechanism is taken into account while the contribution of other failure mechanisms is neglected, mathematically formulated:

$$v(m|n) \approx P\left\{ \bigcup_{o(S)=m} \prod_{k \in S} X_k | E \right\} - Pes_{Nom}(m|n) \qquad (2.8)$$

$$d_k \approx P\{X_k | E\} - Psg_{Nom}(1)$$

where

$Pes_{Nom}(m\|n)$	=	Probability that some 'm out of n' components fail and other 'n-m' survive in the average (nominal condition)
$Psg(1)$	=	Total component failure probability in the average (nominal condition)
$o(S)$	=	Order of subset S
E		denotes the evidence about the failure mechanism present at a given time point or during a given time period

The entities Pes, Psg and other Subgroup Failure Probability (SGFP) entities are handled in more detail in [NAFCS-PR04].

The approximation sign is used in the renormalization equation, because in the case of strong evidence about that the number 'm' of the components is completely failed with certainty and the other 'n-m' are intact with certainty, Impact Vector is per definition $v(m|n) = 1$ and $v(j|n) = 0$ for $j \neq m$, compare to Section 2.1. The nominal probabilities are in practice small in comparison to value one. Similarly the component degradation value is per definition equal to one for a component known with certainty completely failed, while assigned to value zero for an intact component. The presented renormalization is practically convenient, and will be followed in this report. It has been followed – often, however, implicitly – also in the other applications and literature. It has to be emphasized that the above approximations in the numeric values are negligible in comparison to the uncertainties connected in practice to Impact Vectors and component degradation values.

The practical meaning of the above renormalization is that the Impact Vector and component degradation values are intended to describe the temporary impact of an observed CCF mechanism. The active time period for the impact is from the observation to the removal of the root cause(s), including the possible latent time for standby components. The latent time is counted from the previous test time point where no degradation was not yet observed. In the case of staggered testing it can be different for different components in the CCF group. As already said, Impact Vector method contains procedures to handle such situations.

2.3 Test and demand cycles

The test cycles constitute renewal periods of the CCF mechanisms for standby components (other types of components will be discussed later). Random actual demands add renewal points, but are usually relatively infrequent in comparison to tests. The Impact Vector will be used to express the group state, similarly as the component degradation values to express the disjoint component states for each renewal period, called as test and demand cycle (TDC). The coverage of all TDCs (majority failure-free cycles) is not only needed for pure completeness but due to the reason that certain CCF models and estimation methods require the complete statistical information including the number of "successes".

The number of TDCs is denoted as 'ND', and is obtained from the random actual demands and periodic tests basically as a simple sum:

$$ND = N_{AD} + N_{ST} \quad (2.9)$$

where

N_{AD} = Number of actual demands (on whole group)

N_{ST} = Number of surveillance tests (on whole group)

It should be emphasized that the number of component demands is 'n*ND'. When the observed population contains several CCCGs (assumed identical and homogeneous), the number of TDCs for the pooled data is derived as the sum over the tests and demands in the considered component groups.

The precise treatment of TDCs and latent time of degraded or failed states is complicated in the case of staggered testing. There are principal differences in these regards when using failure rate based modeling as will be discussed in Section 2.7. Furthermore, in some cases a part of the tests or demands may concern only a subgroup of the components. The Impact Vector construction for the non-symmetric and other complicated cases will be discussed in Chapter 4.

2.4 Sum Impact Vector

Summing up the Impact Vectors over the TDCs of the observed population produces a Sum Impact Vector (also called observation vector):

$$\mathbf{V} = \sum_{i=1}^{ND} \mathbf{v}_{TDC(i)} \quad (2.10)$$

A capital letter will be used for the Sum Impact Vector in order to make distinction to the basic Impact Vector that is connected to an individual TDC. It has to be emphasized that the Sum Impact Vector is not anymore a conditional probability entity. Instead, it represents the number of events for different multiplicities. Because the sum of the elements of the basic Impact Vector is equal to one per definition, the following applies to the Sum Impact Vector:

$$\sum_{m=0}^{n} V_m = ND \quad (2.11)$$

The practical interpretation of the Sum Impact Vector is very straightforward:

V_0 = Number of failure free TDCs
V_1 = Number of single failure TDCs (2.12)
…
V_m = Number of TDCs with failure of multiplicity m
…
V_n = Number of TDCs with failure of all components

I.e., the Sum Impact Vector merely represents the failure statistics arranged according to failure multiplicity. The real power of Impact Vector method is, however, connected to the generalization, where the elements need not be integer numbers, but the statistical mass can be distributed as was discussed in Section 2.2. The elements of a Sum Impact Vector can generally fall anywhere between [0, ND] but must satisfy the normalization equation (2.11).

2.5 Impact vector for pooled population

If there are CCCGs of identical or closely similar components, and the groups have the same size, the statistics can simply be pooled together. A typical situation of pooling concerns same component groups at twin plant units. In more precise terms pooling requires mutual homogeneity of the observed CCCGs, or postulation of that for a specific analysis purpose. In practice pooling means that the number of TDCs is added together and the Sum Impact Vector for the whole population is built as the sum of all observed Impact Vectors.

It must be strongly emphasized at this point that the Impact Vector is always connected to the size of CCCG, even though this is not necessarily indicated in the shorthand notation. The Impact Vectors over CCCGs of different size cannot be directly summed together. Combining statistics in these regards requires special mapping up/down procedure, to be discussed in Chapter 6 (and of course, also mutual homogeneity or postulation of that).

2.6 Connection to SGFP entities and parametric CCF models

As pointed out the Sum Impact Vector represents the failure statistics arranged according to failure multiplicity. The expected number of events of different multiplicity can be expressed as ND*Pes(m|n) using one of the basic Subgroup Failure Probability (SGFP) entities, see [NAFCS-PR04]. Those in turn are connected to the elements of the Sum Impact Vector in the following way:

$$ND.\langle Pes(m\,|\,n)\rangle = V(m\,|\,n) = V_m \tag{2.13}$$

Here the brackets <> indicate so called maximum likelihood estimation, i.e.

$$\langle Pes(m\,|\,n)\rangle = \frac{V(m\,|\,n)}{ND} \tag{2.14}$$

This represents in fact so called Direct Estimation Method which is a basic alternative to quantify CCFs. Similarly, the Impact Vector constitutes a general way of representing failure statistics to many parametric CCF models as is discussed in more

details in [NAFCS-PR04]. Compare also to the interpretation of the event-specific Impact Vector as conditional probability of the various failure multiplicity as discussed in the previous sections.

The other types of conditional probability entities are connected to Impact Vector similarly as to Pes entity by the transformation rules of SGFP entities [NAFCS-PR04]. In some cases this connection can be very useful for the Impact Vector construction. Furthermore, it provides a very logical route to define mapping up/down procedures as will be discussed in Chapter 6.

2.7 Coincident multiple failures

A multiple failure is in most cases due to a clear shared cause or an identical combination of causes, i.e. an ordinary CCF in its defined meaning. However, also other types of multiple failures can coincidentally occur, i.e. components can have different failure causes. A larger event statistics usually contains so called "independent" double failures. The wording "independent" is, however, idealized. Namely, there can be underlying shared causes such as decreased quality of maintenance even to failures which seem to be different (e.g. different parts in the components can be affected).

Due to possible non-visible dependence (which is strictly taken never possible to be declared excluded) the "coincident" multiple failures are not recommended to be excluded from the CCF event analysis. In a qualitative CCF analysis the emphasis can, of course, be focused on ordinary CCFs. The Impact Vector can be constructed following the same rules for any multiple failure or multiple degradation event. These instructions follow consistently this approach: speaking of actual or potential CCF events should be understood to generally cover all multiple events.

In the literature, e.g. in the basic reference [NUREG/CR-5485], a difference is often made between the coincident multiple failures and CCFs with clear identical cause(s). 'Shared Cause Factor' is used to code the distinction, assigning value one to "clear" CCFs and zero to multiple failures with evidently different causes, and intermediate value to uncertain cases. This practice has migrated also to ICDE Coding Guide [ICDECG00]. This controversial issue will be discussed more comprehensively in Annex 1.

It is thus recommended that coincident multiple failures are likewise covered in the construction of Impact Vectors in a quantitative CCF analysis. This should be done at least in a situation where complete non-screened event statistics is available. Often the amount of coincident multiple failures is relatively small. Thus in practice the discussed dilemma use to have only a small influence to the data analysis results.

The weak degradation cases (to be defined and discussed in Chapter 4) in where the components are affected by different failure mechanisms, can often be neglected in practice as the possible dependence is in those cases is insignificant.

2.8 Implications of failure rate based modeling

Standby components, time-dependent model

In the failure rate based modeling (of a standby component) the principal difference – in comparison to demand failure probability based modeling – is considering the occurrence of failure as distributed in time. Basically the failure rate is assumed constant, i.e. the likelihood of failure is same during any time interval of same duration. The tests and demands constitute (for a standby component) time points of failure detection or operability verification. It is still valid to think that the Impact Vector represents the group state for the standby period based on the observation at the test or demand ending the period. An alternative, more dedicated interpretation is to regard Impact Vector as an outcome of a failure mechanism affecting the components during the considered period. When using this interpretation the Impact Vector can itself be considered as time-dependent entity, which can be a useful generalization of the concept [T314_TrC].

The construction procedure is much the same irrespective of the modeling approach. But the quantitative estimation is different as will be discussed in Section 3.4.

One more generalization is to divide the failure probability (of a standby component at a demand) into demand and standby time related parts, i.e. so called $q + \lambda t$ model. This generalization also affects the quantitative estimation step, and can be regarded as recommended option for specific applications such as the optimization of test arrangements. The basic construction procedure of Impact Vectors still applies.

Monitored failure mode

The above discussion was concerned with standby components and failure modes connected to startup or change of state at a demand. Regarding failures of normally operating components, or more generally so called monitored failures, the situation is fundamentally different. The likelihood of CCFs uses to be relatively small for the monitored failures but can be nevertheless considerable in certain cases. For the monitored failures it is natural to interpret the Impact Vector to represent the outcome of a failure mechanism affecting the components during a specific time period. The basic construction procedure of Impact Vectors still applies but the time spread of failures has to be considered with respect to a defined critical time window, e.g. required mission time in accident condition. These aspects will be discussed further in Section 4.3.

Mixed cases

Finally, components can be intermittently operated or are started from standby for operation over a mission time. In these cases it is advisable to treat startup and operation period failures separately, which has been a standard approach for single failures. It has to be emphasized that part of the failures during mission time, of components that are normally in standby, should be considered in the same way as start-up connected failures, i.e. not as ordinary monitored failures, because they can develop in criticality during the standby time and are only detected in connection to a demand or a test of sufficient operation time.

3. Elements of Impact Vector construction and integration

This chapter discusses the procedure of the Impact Vector construction. The methodological aspects for the basic steps are first considered in Section 3.1. It is assumed that the reader is familiar with the more practically oriented instructions in [NAFC-PR17, Chapter 3]. The other sections in this chapter deal with the integration of Impact Vectors in data pooling, and describe the interface to the estimation of failure probabilities and CCF model parameters.

The requirements for the input information such as the use of ICDE database and need for supplementary plant information are discussed in the guideline [NAFCS-PR17], and will not be duplicated here.

3.1 Basic steps

A flow diagram of the Impact Vector construction is shown in Fig.3.1. The following subsections are devoted to the methodological specialties in the basic steps 1-5.

Definition of test and demand cycles

The meaning of test and demand cycles (TDCs) was already discussed in Section 2.3. When the Impact Vector construction is done as a part of integral CCF analysis, it may possible to precisely record all test and demand events. For example, see the analysis of Safety and Relief Valves (SRVs) of Olkiluoto 1 and 2 in [SKI TR-91:6]. More usually such details are too laborious or even practically impossible to gather. The accurate timing information is, however, vital only in the vicinity of occurred CCFs in order to infer the observations at the preceding tests and remedial post-CCF actions. For the CCFs with time-spread component events the time period of interest can extend over several TDCs. For the time periods without CCFs it is sufficient to just to count the number of tests that are efficient for the considered failure mode (using the test interval defined in the Technical Specifications), actual demands (recorded in plant transient log) and single component events (plant component database). See further discussion in the connection of steps 2 and 4, concerning failure-free TDCs and single-failure TDCs.

Some special failure (CCF) mechanisms may not be detectable in the periodic tests during power operation but only in functional system tests and actual demands. Such failure (CCF) mechanisms should be handled as a separate failure mode, or equivalently by using virtual component and CCCG definition for this purpose. Specific TDCs should be defined to correspond to effective detection points for the failure mode (virtual component). The derived Sum Impact Vector has to be treated separately still in the basic quantification, i.e. up to and including Step 7 in Fig.3.1. The results can either be handled explicitly in the PSA model and applications or added together with the contributions of other failure modes in proper way (the final result will be same). This kind of separation can be needed also if various kinds of complementary periodic tests with different coverage and efficiency are in use, e.g. start tests, load tests and annual functional tests of diesel generators (DGs). For a practical example, how to handle different types of tests and failure modes, see [DGTS_B92].

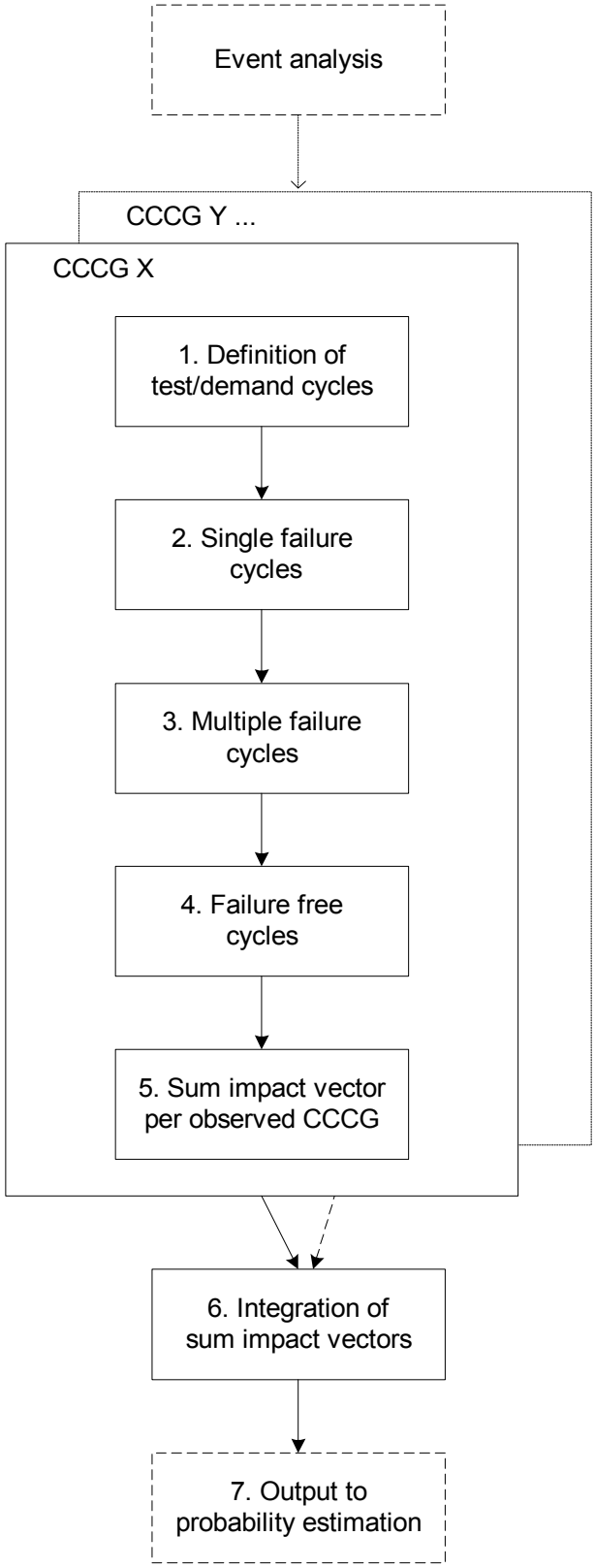


Figure 3.1 Steps and flow of Impact Vector construction.

The component group is asymmetric with respect to tests and demands, if only part of the components are covered in certain tests, or if actual demands may be imposed to a subgroup of the components. For example, the number of SRVs actuated by the plant protection system in a BWR depends on the type of the transient. The asymmetric test and demand patterns will be discussed in Chapter 4.

The above discussion of the TDCs applies to the latent failures of standby components. For the monitored failures the situation is different. Besides, the failure-rate based modeling (used for monitored failures) does not require the definition of TDCs because failure-free periods are not a direct part of the model and estimation, see further discussion in Section 3.4. On the other hand, the TDCs can nevertheless be defined based on renewal points for the component condition. The primary option is to assign the renewal cycles to time-based maintenance scheme. This can be both informative for qualitative purposes and also facilitate a structured consideration of time coupling of the component events. The component events that are on the same cycle can basically be coupled (dependent), while if separated by one or more renewal points the coupling is weak or negligible.

The standby components can have both latent failure modes (detected in tests and actual demands) and monitored failure modes (detected by instrumentation directly or by personnel that are frequently at the place). It is then natural to use the TDCs of latent failures to the monitored failures as well.

Single-failure cycles

The meaning of plain single component events was discussed in Section 2.1, and the input information to obtain their number 'N_{Single}' in connection to the number of TDCs.

Many parametric CCF models, e.g. Alpha Factor Method, require the complete failure statistics including singles as input to the parameter estimation. Besides, the singles carry also qualitatively important information. For example, the relative share of the root causes among singles in comparison to multiples (CCFs) can provide useful insights about the efficient CCF defenses.

Weak CCF cases, where one component is failed and the same root cause is present in the redundant components but at a very incipient state, can be effectively reduced to single failure cycles. For qualitative analysis aims they can still be left among CCFs but represented with Impact Vector of single failure cycle, i.e. [0, 1, 0, … , 0]. The weak CCFs (weak degradation cases) will be discussed in more detail in Chapter 4. The construction guideline presents suggestions for practical screening criteria in these regards [NAFCS-PR17, Section 3.6].

Multiple failure cycles

The most difficult part of the CCF analysis is the interpretation and assessment of the multiple component events, which typically represent more or less fuzzy cases – except those rare clear-cut cases, where certain components are observed to be completely failed at the same time and the other components of the group are known to be intact. As stated earlier, the main difficulty is connected to the need to make the operability assessment with respect to actual demand conditions and typically based on incomplete information from test observations. The following methods can be used:

- Scenario method (earlier called mostly as hypothesis method; the "scenario" is preferred here as the primary term in the connection to practical work, being type of engineering assessment; the "hypothesis" carries the flavor of theoretical exercise; however, the inbuilt subjectivity of the assessment work is not to be undermined)
- Specific causal model, including time-dependent modeling
- Parametric CCF models to support the assessment of conditional dependent failure probability

The scenario method is the principal one and most practicable in general use. It will be discussed here, while the other more specialized techniques in Chapter 4.

The scenario method uses alternate scenarios about the possible status of the component group at the observed condition given that an actual demand should occur, taking into account the preceding operational history and other pertinent information. Compare to the earlier discussion of the degraded states and surveillance tests in Chapter 2.

The scenario method (hypothesis method) is described comprehensively in [NUREG/CR-5485, Section 5.5.2]. Table 3.1 presents a simple example, which has been discussed in [CR_ImpV2]. (There are versatile examples based on the Nordic experience in [NAFCS-PR10]).

Table 3.1 Example construction of Impact Vector using scenario method for a CCF event in a group of three centrifugal pumps: pump A was regarded completely failed by bearing damage, bearings of pump B were detected also degraded in an additional inspection while pump C was largely unaffected.

Scenario	Weight	Impact vector elements				Element sum
		0	1	2	3	
1. Only pump A would fail given actual demand mission	0.9	0	1	0	0	1
2. Pumps A and B would fail …, while C would survive the mission	0.1	0	0	1	0	1
Net Impact Vector		0	0.9	0.1	0	1

The scenarios constitute alternative interpretations of the event. The weights represent analyst's prediction or belief about the chances of the different scenarios to be true. The net Impact Vector for the event is obtained as weighted average over the scenario-specific Impact Vectors $\mathbf{v}_i$:

$$\mathbf{v}_{net} = \sum_{i=1}^{N} w_i \cdot \mathbf{v}_i \qquad (3.2)$$

or equivalently for the elements

$$v_{net}(m \mid n) = \sum_{i=1}^{N} w_i \cdot v_i(m \mid n)$$

where the weights of the N scenarios shall fulfill the following normalization

$$\sum_{i=1}^{N} w_i = 1$$

At the simplest the scenario-specific Impact Vectors represent multiple failures of various order, within the possible range that is indicated by the observations. If the number of completely failed components is denoted by 'm', and additional degraded components by 'j', there will be a scenario for each multiplicity from 'm' up to 'm+j'. Thus the number of scenario equals to 'j+1', i.e. we see here the fact that the assessment work is indeed connected to the observation of degraded states. If the number of degraded states is large (in a highly redundant group), it may be advisable to lay out scenarios only for selected principal multiplicities, because the information can be vague for a finer distribution of the assessment. An example can be seen in Table 3.2 (event OL2/85), see further discussion of the specific aspects for the highly redundant groups in Chapter 4.

Generally, the scenarios need not be restricted to be represented only by multiple failures (each of different order). The elements of the Impact Vector for a specific scenario can also constitute a distribution over failure multiplicities. For example, one possible scenario is the high bound Impact Vector and another the low bound Impact Vector obtained by using maximum and minimum dependence between degraded component states, see Chapter 5 for details. In some cases it is convenient to make a shortcut by a joined scenario. For example, in a group of four components, when two are detected completely failed and the other two degraded in testing, one scenario could state that the degraded components would survive, Impact Vector equal to [0, 0, 1, 0, 0]; the other scenario could consider the possibility of higher order failure with fifty-fifty chances between only one more and both two, which can be expressed by (joined) Impact Vector [0, 0, 0.5, 0.5].

The weights for the scenarios need to be based on engineering judgment. The construction guideline presents advices to enhance consistent and systematic judgments. The above mentioned low and high bounds provide valuable backup to event-specific assessment, see Chapter 5 for details.

It is generally recommended to use scenario method by keeping to the actual available evidence. Extrapolation to failure chances of those components, which were not affected according to the evidence, is not recommended. That would be a kind of extrapolation which is not meaning with the scenario method in the context of Impact Vector construction and CCF data analysis (such activity belongs to modeling). Furthermore, scenarios with small chances to higher order failure (very weak degradation) should be disregarded. The possible statistical evidence is anyway so small in such cases that it is useless for an ordinary estimation purpose but can on the other hand give a misleading picture of the pertinent dependence level. Compare to the further discussion of the weak degradation cases in Chapter 4.

Failure-free cycles

Beside of completeness the number of failure-free cycles 'N_{Zero}' is needed for the estimation of certain parametric CCF models, especially when the estimation uses Likelihood Function, to be discussed in more detail in Section 3.3. When exact records are not available the total number of TDCs 'ND' can first be approximately derived from the observation period, test interval and number of actual demands, and then the number of failure-free cycles can be obtained backwards in the following way:

$$N_{Zero} = ND - N_{Single} - N_{CCF} \quad (3.3)$$

No high accuracy is needed for 'N_{Zero}'. (The same applies also to 'ND'.) Compare to the discussion of TDCs in Section 2.3.

Sum Impact Vector

The Impact Vectors for all TDCs are added together to derive the Sum Impact Vector for the considered CCCG, failure mode and observation period, see illustration in Table 3.2. For simplicity the single failure TDCs and failure free TDCs are lumped together, respectively. The derivation of the Net Impact Vector for event 'OL1/85' will be discussed in more detail in Section 4.2. For checking purpose it is recommended to add a column for the sum of Impact Vector elements on each row:

- for an individual Impact Vector the element sum shall equal to one
- for the joint Impact Vector of a time-spread CCF the element sum shall equal to the number of covered TDCs

Table 3.2 Example derivation of Sum Impact Vector: electromagnetic pilot valves of BWR safety/relief valves, failure to open, during 1981-88 [RESS_HiD]. Regarding the derivation of the Net Impact Vector for event 'OL1/85' see Table 4.3

Event	Scen-ario	Weight	Impact vector 0	1	2	3	4	5	6	7	8	9	10	Element sum
OL1/85	1	0.5			2									2
2xFO + 2xFO	2	0.5	1				1							2
	Net		0.5		1		0.5							2
OL2/85	1	0.8				1								1
3xFO + 7xNO	2	0.15								1				1
	3	0.05											1	1
	Net					0.8				0.15			0.05	1
Single FO				5										5
Success			26											26
Sum Impact Vector			26.5	5	1	0.8	0.5	0	0	0.15	0	0	0.05	34

- for the lumped Impact Vector of a failure category the element sum shall equal to the number of contained TDCs (this option is typically used for the single failure TDCs and failure-free TDCs)
- for the Sum Impact Vector the sum shall equal to the total number of TDCs

3.2 Integration of Sum Impact Vectors

The integration of Sum Impact Vectors, i.e. pooling of data for different CCCGs will depend on the degree of homogeneity and group sizes. Pooling is in any cases usually feasible only for one certain component type and one specific failure mode.

Basic case - pooling over CCCGs with same group size

The Sum Impact Vectors of different CCCGs are directly additive only if the group size is same and the groups are mutually homogeneous. In such a case the event data could be simply pooled together, i.e. separate integration is not necessarily needed. In practice it is often nevertheless wanted to keep CCCGs separately visible in the pooled data, e.g. to facilitate transparency regarding the history of different plant units.

Consideration of differences in group size

Pooling event data from CCCGs of different size requires so called mapping up/down procedures to transfer data to a defined size of group. These procedures will be discussed in more detail in Section 6, which concludes that

- mapping down is well founded, based on combinatorial analysis
- mapping up is controversial, includes necessarily also extrapolation of probabilities into higher order

It is hence recommended not to use mapping up. Combining event data should be done by mapping down the Impact Vectors of the larger group to the size of smaller group for pooling aims. This effectively means that the combined statistical basis is sufficient only up to the order of the smaller group, while for the higher order only the statistics of the larger group is available. For certain CCF models, e.g. when using CLM, the data pooling can be carried out by using a joint likelihood function for parameter estimation, no size-related mapping is needed. Also direct estimation can be performed without size-related mapping. These pooling aspects will be discussed in more detail in Section 6.3.

Consideration of differences in design and/or CCF defense factors

Besides size-related mapping an adjustment may be needed to take into account differences in design and/or CCF defense factors from source to target conditions. Preferably such an adjustment should be based on some model. For example, CLM or BFR model can be used for this purpose because the dependence parameters can be adjusted in order to consider specific aspects but this requires experience about how the parameters reflect various conditions.

A typical difference is concerned with the test arrangements, e.g. test interval. Mapping of difference can be based on the fact that the failure probability (mean unavailability) is crudely linear as the function of test interval.

3.3 Output to the estimation of single failure probability and dependence parameters

The Sum Impact Vector (or integrated Sum Impact Vector) constitutes an input to the estimation of parameters for the CCF models. This subject is handled more comprehensively for selected CCF models in [NAFCS-PR04]. Below is given a brief introduction to Direct Estimation Method.

The point estimate of single failure probability is

$$\langle \mathrm{Psg}(1) \rangle = \sum_{m=1}^{n} \frac{m.V(m|n)}{n.ND} \tag{3.4}$$

The point estimate expression for Pes(m|n) entities was already presented in Section 2.4, Eq.(2.8). Equivalently, one can estimate Pts(m|n) entities in the following way:

$$\langle \mathrm{Pts}(m|n) \rangle = \frac{s(m|n)}{ND} \tag{3.5}$$

where

$$s(m|n) = \sum_{k=m}^{n} V(k|n) \tag{3.6}$$

V(m|n) = Sum Impact Vector, CCCG size being explicitly denoted

For completeness the point estimate expression for Psg entity is following (as can be derived by the SGFP transformations from the expression for Pes entity, Eq.(2.8)):

$$\langle \mathrm{Psg}(m|n) \rangle = \sum_{k=m}^{n} \frac{1}{ND.\binom{n}{k}}.\binom{n-m}{k-m}.V(k|n) \tag{3.7}$$

This reduces to Eq.(3.8) in case of m = 1. Notice that Psg entity is subgroup invariant. Thus for two mutually homogeneous CCCGs of different size the following is valid:

$$\mathrm{Psg}(m|n_A) = \mathrm{Psg}(m|n_B) \text{ , for } m \le \min(n_A, n_B) \tag{3.8}$$

This aspect can be utilized to present a way of data pooling that uses direct estimation approach to combine statistics from CCCGs of different size, see Section 6.3 for more details.

3.4 Failure rate based estimation

When estimating failure rates (single and multiple component events) the number of TDCs, i.e. ND, is effectively replaced by the relevant observation time. The estimation scheme is in other respects similar. Compare to the estimation procedure used in Loviisa PSA implementing failure rate based modeling of CCFs [ICDE-S-Vaurio].

Even though TDCs are not used in the (probabilistic) estimation for failure rate based modeling, the concept can nevertheless be very useful, e.g. for screening purpose and considering time-spread component events. For periodically tested standby components the definition of TDC is identical irrespective of the estimation approach. For intermittently operated components and failure mode in the operational state, TDC is naturally associated with each operation period. For normally running components TDC can be associated with the maintenance interval. Handling of pure mission time failure modes is somewhat controversial but the basic assumption is to handle each test and actual demand mission as one TDC. Compare to the general discussion of these issues in Section 2.8.

4. Special techniques

This chapter considers how to construct Impact Vectors for the various kinds of complex event scenarios.

4.1 Time-spread events

It is quite usual that a failure mechanism contains time-dependent growing degradation. Basic schemes are linear, saturating and accelerating growth. At the simplest, acknowledging such a scheme can support the engineering judgment for the Impact Vector construction. For a more systematic and transparent approach a mathematical growth model can be used, see further discussion in Section 4.6.

Beside of growing degradation mechanisms there can be other stochastic phenomena which produce variation in failure timing between components, i.e. deviation from a simple shock-type CCF where a trigger event strongly synchronizes the failure times of the components. The observation instances can furthermore be spread at time-separated test points in staggered testing in the absence of rule-based additional test of the remaining components given failure.

The basic advice is to consider the impact of time-spread CCF mechanisms jointly for the consecutive test cycles, during which the influence exists. Effectively, the Impact Vectors for the considered TDCs will be bundled. This allows more effective reasoning, e.g. the alternative scenarios can allocate the failure chances in different ways over the TDCs. A basic example is presented in Table 4.1, where two components are observed failed at separate time points of consecutive TDCs. Weight 'q' represents the chance that the mechanism had led to a double failure in the same TDC. The example is typical in the sense that the influence is divided over two TDCs, and described by the bundled (sum) Impact Vector for those two TDCs, which are numbered in the table for simplicity as TDC1 and TDC2. Correspondingly, the element sum equals to 2.

Table 4.1 Example construction of Impact Vector for two failures detected in separate TDCs (denoted as TDC1 and TDC2) in CCCG of size 3. The variability in failure timing suggest that there is a chance of 'q' that the components had failed in the same cycle (TDC1 or TDC2).

Event	Scenario	Weight	TDC	Impact vector elements				Element sum
				0	1	2	3	
One component failed at TDC1, another at TDC2	1. Both components fail in TDC1	q/2	1 2	0 1	0 0	1 0	0 0	1 1
	2. Both components fail in TDC2	q/2	1 2	1 0	0 0	0 1	0 0	1 1
	3. As detected	1-q	1 2	0 0	1 1	0 0	0 0	1 1
Net Impact Vectors			1 2	q/2 q/2	1-q 1-q	q/2 q/2	0 0	1 1
Bundled Impact Vector over TDC1 and TDC2				q	2(1-q)	q	0	2

The comparison of similar cases can give guidance about the strength of time-coupling, or its opposite, the randomness of failure timing. In the ICDE coding and classification 'Time Factor' is used to describe the degree of simultaneity, see [ICDECG00]. Time Factor originates from the American practice, which uses a formula driven approach to consider time-spread events. This approach is generally feasible as a simple procedure (will be commented in more detail in Annex), reflecting the situation that is typical to a CCF data analyst in the USA as he (she) may not know the details of test, operation, maintenance and inspection arrangements of the components. However, if that kind of basic knowledge and detailed event timing are available to the analyst, the dependence among distributed events can be evaluated in a more specific way.

For any more complicated time-spread scenarios it is useful to draw a time chart showing the component events, i.e. test observations and outcome of eventual actual demands. An example is shown in Table 4.2 for the CCF affecting electromagnetic pilot valves (EPVs) at the Olkiluoto plant in 1985 [RESS_HiD]. Initially, two EPVs were detected failed and two more degraded by a transient demand at Olkiluoto 1 in September 1985. The additional tests with one months interval revealed more failures before the root problem could be eliminated, see Table 4.2. The Impact Vectors are assessed jointly for the two TDCs with double failure at each, see Table 4.3. The general procedure, which is described in Table 4.1, is followed. The last observed failure of one component was handled as a plain single failure. See further discussion of this case and the use of more developed causal, time-dependent modeling in Section 4.6.

4.2 Non-symmetric testing

The requirement of internal homogeneity applies especially to the test arrangements in case of standby components. The test frequency and method (efficiency) affect substantially both the component reliability and defense against CCFs. Staggering of the tests across redundant components facilitates detection of CCFs and is an additional feature to be taken into. Test staggering is connected to the possibility of time-spread events as discussed in Section 4.1.

An example of non-symmetric testing is constituted by the safety/relief valves (SRVs), which can be of two functional types at the BWRs: one type relieves steam into suppression pool while the other type blows directly into containment atmosphere. The first type can be tested in power operation state. The second type is feasible to be tested only in overhaul outage. The SRVs blowing to the suppression pool are typically tested once at the mid of power cycle, in addition to the tests when shutting down to overhaul outage and starting up. Effectively, they have a test interval of half year while the direct blowing SRVs have one year. Further examples of non-symmetry can be found in auxiliary feedwater systems of BWRs, where only the part of the trains connected to main feedwater lines can be fully tested in power operation state. Typically, the test arrangements of otherwise identical containment isolation valves can be different. Testing non-symmetry can be particularly relevant for so called global CCF groups constituted of components in different systems.

Table 4.2 Example case of CCF event affecting electromagnetic pilot valves at the Olkiluoto Unit 1 in 1985 (a snapshot of operational history, CCCG size = 10).

Component		Test/demand cycles						
			1985-06-24	1985-09-11	1985-10-10	1985-11-17		
1	V179							
2	V180				F	F		
3	V181			D	F			
4	V182			F				
5	V183							
6	V184							
7	V185			F				
8	V186							
9	V187			D				
10	V188							
		...	Startup tests	Transient	Additional test	Additional test	...	

Syntax:

F = Failed

D = Degraded

Blank = Intact

Table 4.3 Construction of Impact Vector for the example case of CCF event affecting electromagnetic pilot valves at the Olkiluoto Unit 1 in 1985.

Scenario	Weight	TDC	Impact vector 0	1	2	3	4	5	6	7	8	9	10	Element sum
1. As occurred	0.5	1			1									1
		2			1									1
2. Four components	0.5	1	1											1
fail at later demand		2					1							1
Net impact vectors		1	0.5		0.5									1
		2			0.5		0.5							1
Bundled Impact Vector over TDC1 andTDC2			0.5		1		0.5							2

The component group can be asymmetric with respect to tests and demands also, if actual demands may be imposed to a subgroup of the components. For example, the number of SRVs actuated by the plant protection system in a BWR depends on the type of the transient.

The basic approach to handle asymmetric testing is to break the considered group (otherwise identical or closely similar) components into subgroups that are internally symmetric for the test arrangements. The CCF data are processed separately for the subgroup CCCGs. If there are reasonable statistics, this separation can provide valuable insights about the influence of test arrangements through the comparison of differences. For combining the data over the whole group the general instructions of data pooling apply as handled in Section 3.2 and Section 6.

As an approximation the non-symmetry of the test arrangements may be neglected and the considered group postulated as homogeneous. The implications of such an approximation shall be clearly acknowledged and any such assumption documented as part of the produced CCF data.

If failure rate based modeling is followed, the test interval and staggering is modeled explicitly. The component failure rates and CCF rates can usually be assumed to be independent of the test interval and staggering. Thus a break-up with respect to non-symmetric testing may not be needed but nevertheless has to be considered when classifying the events with respect to simultaneity (screening time window) and considering time-spread events. In analogy to failure rate based modeling the demand failure probability can be assumed linear as the function of test interval, which can be used as mapping aid when pooling data (from subgroups with different test intervals).

4.3 Mission time CCFs

The treatment of mission time failures and CCFs in particular divide up into different situations depending on if the components are considered as repairable (recoverable) during the mission time. Compare also to the general discussion of failure rate based modeling in Section 2.8.

If the repair (recovery) is not possible (not credited) during the mission time, the treatment is similar to the failures at the start of demand. TDCs are associated to test mission periods and actual demand mission periods. Often the test mission is less demanding than actual mission, e.g. operation time in test may be short and/or component is not fully loaded. Such differences have to be taken into account when interpreting the criticality of the failure events. Some failure mechanisms that affect mission time of components that are normally in standby can develop in criticality during the standby time and are only detected in connection to a demand or a test. They should thus be considered in the same way as failures connected to the start of demand, e.g. regarding growing degradation and time spread.

If the repair (recovery) is possible (and credited) during the mission time, the situation for the CCF treatment is analogous to monitored failures in general. CCF risk use to be small in these cases and mainly connected to extrinsic hazards (causes outside the

component). It is advisable to use failure rate based modeling in these cases. The Impact Vector will be constructed for each failure event (single or multiple) following the general instructions. The basic construction procedure of Impact Vectors still applies but the time spread of failures has to be considered with respect to a defined critical time window, e.g. required mission time in accident condition. A definition of TDCs is not necessary and the 0^{th} element of Impact Vector can be regarded as a dummy variable (not used in the estimation). Although TDCs do not have direct bearing they can nevertheless be defined for the sake of completeness and consistency, e.g. as time periods (operating cycles) between maintenance and repair time points.

4.4 Use of causal and time-dependent model

In complicated cases with several contributing factors the construction of a specific causal model may be advisable. This approach can be especially desired in the cases where time-dependence of the CCF mechanism is important. A practical example is presented in [T314_TrC], which uses a state model (Markov model) to describe the stochastic process of CCF detection and root cause elimination. The example develops further the assessment for the CCFs of EPVs at the Olkiluoto plant in 1985, which was initially treated (in simplified way) by the scenario method, compare to Tables 3.2 and 4.3. A more recent example is the CCF of seawater pumps at Olkiluoto 2 in 1996, see case SF12 in [NAFCS-PR18]. The Event Tree method was used to layout the scenarios in this case.

Constructing a dedicated case-specific model can be laborious. Fortunately, such an effort is needed only in a small part of the CCFs. On the other hand, many of the complicated CCF mechanisms are desired to be explicitly modeled, i.e. not adapted to be covered by the data of parametric CCF models. For example, the recent pump application contains such cases, see [NAFCS-PR18].

4.5 Use of parametric CCF models to support Impact Vector construction

In the complicated cases with incomplete knowledge about the contributing factors a parametric CCF model can be used to support the assessment of the conditional dependent failure probabilities for the considered CCF event [CR_ImpVe]. Compare to the cases SF11-12 in the DG Pilot [NAFCS-PR10].

4.6 Highly redundant groups

The basic instructions of Impact Vector construction apply irrespective of the group size. However, all difficulties of the assessment increase in higher order situations. The amount of highly redundant component groups is small, and they use to be highly reliable, which means that cumulating overall observations and insights about CCFs are sparse.

One particular problem is that the number of degraded component states per event can be large in a highly redundant group. It is then advisable to lay out the scenarios only for selected principal multiplicities, because the information can be vague for creating a meaningful fine distribution of the chances for every possible multiplicity.

For the end uses such very detailed assessment is effectively not needed. Typically only the probability of system function corresponding to a failure criterion, that 'm out of n' fail, is of principal interest. The assessment should focus to this need. An example can be seen in Table 4.3, event OL2/85: in addition to three completely failed EPVs, all other seven EPVs were observed to be degraded. The Impact Vector assessment was made considering chances of higher order failure at intermediate multiplicity 3+4=7 and total failure of the group. Event though the Impact Vector remains rather "discontinuous", the other (conditional) SGFP entities behave rather smoothly.

4.7 Lack of precise knowledge

It is often the case that the information for the analyzed event is limited and it is impossible to reach more information due to resource and time constraints of the analysis. Besides, for older events it may be impossible to find more information than given in the records. In these cases it is advisable to define different scenarios (scenarios) to cover all principal possibilities, and if there is too little evidence to a specific assessment of the weights, a uniform distribution can be used across the defined scenarios. The last resort is using bounding calculations that will be discussed in Chapter 6, e.g. the defined scenarios could be

- conservative one (high bound) and
- optimistic one (low bound).

Weights can be assumed fifty-fifty if no specific information is at hand, i.e. uniform (non-informative) distribution can be used.

4.8 Weak dependence cases

The situations with weak dependence fall in the following two categories:

- recurring component events (time coupling negligible) or
- component degradations that are detected early at incipient state

It is generally advised to skip these situations, i.e. neglect the possible small chance of CCF because of the assessment difficulties in comparison to the uncertainties and marginal statistical gain. The qualitative analysis aims may justify to carry with the weak dependence cases, but preferably then in distinct categories. The construction guide presents suggestions for practical screening criteria in these regards [NAFCS-PR17, Section 3.6]. The recent applications provide practical examples of screening.

In certain special cases the impact of a CCF mechanism may have been present over large number of test cycles related to non-perfect extent of periodic tests, e.g. during the time between consecutive overhaul outages or from an overhaul outage up to a random actual demand. In these kinds of cases already relatively weak influence to conditional failure probability can cumulate as significant. For these cases a joint sum Impact Vector shall be constructed to cover all affected TDCs. A particular additional feature for the CCF mechanisms that can stay latent for a longer time can be increasing degradation as the function of time. For the treatment of such a case, see [T314_TrC].

5. Upper and lower bounds, uncertainties

The uncertainty analysis of CCF data is outside the scope of these instructions. It is a separate task within NAFCS, compare to [PCM01_4]. In this context it is just emphasized the vital need to document the principal assumptions and judgments during the course of the Impact Vector construction in sufficient detail to facilitate the uncertainty analysis. Especially, when using the scenario method, the scenario vectors and weights shall be documented, e.g. using a table format such as in Tables 3.1, 3.2 and 4.3. Detailed documentation is also needed for sensitivity analysis purposes.

5.1 Bounding considerations

In complicated cases it may help to make bounding considerations with pessimistic versus optimistic assumptions. Because it is usually easier to assess component degradation values than Impact Vectors, high and low bounds can be derived in the following relatively simple way from them. The bounds are obtained as the range allowed for multiple failure probability by the component degradation values when they are interpreted as conditional failure probability of the individual components. These bounds are determined by the basic laws of probability, and therefore useful to know as backup to the specific assessment of Impact Vector, which should stay within the bounds (assuming the assessed component degradation values are thrust on). Compare to the further discussion of the use of the bounds in the Impact Vector construction in Chapter 5. Compare also to the general discussion of the connection between Impact Vector and component degradation values in Section 2.2.

In the earlier connections it was assumed that ‘m’ components are failed and additional ‘j’ degraded, while the remaining ‘n-m-j’ intact, compare to Eq.(3.5). Compare to the discussion of failed, degraded and intact states in Section 2.1. Here the generalized form of the calculation algorithms are used covering all components, by setting the degradation value equal to zero for the intact components. Correspondingly, the degradation value is set equal to one for the completely failed components.

5.2 Low bound

The low bound is handled first as being simpler to define by the assumption that the component degradation values are treated as independent conditional failure probabilities. This means that for example in a subgroup of components 1, 2, ..., m the following is valid, and similarly for the other subgroups:

$$P\{X_1 X_2 .. X_m | E\} \geq P\{X_1 | E\}.P\{X_2 | E\}...P\{X_m | E\} = d_1 . d_2 ... d_m \qquad (5.1)$$

where

E = Considered CCF instance

d_k = Degradation value of component ’k’

This inequality gives a valid lower bound if the existing dependence is positive as it is in practical cases except some very special circumstances that must deserve a special treatment if included in the event analysis.

The calculation algorithms for Impact Vector elements (that correspond to Pes entity in the interpretation of conditional failure probability) can be derived by standard probability calculus, which is not presented in detail here. The obvious expressions are given in Table 5.1, compare also to Table 5-8 of NUREG/CR-5485.

Table 5.1 Expressions for the low bound Impact Vector derived from the component degradation values d_k, assuming them as independent conditional probability of component failure.

Group size	Impact Vector Element $v_{Min}(m\|n)$				
	m = 0	m = 1	m = 2	m = 3	m = 4
n = 2	$(1-d_1).(1-d_2)$	$d_1.(1-d_2).$ $d_2.(1-d_1)$	$d_1.d_2$		
n = 3	$(1-d_1).(1-d_2).(1-d_3)$	$d_1.(1-d_2).(1-d_3)$ + $d_2.(1-d_1).(1-d_3)$ + $d_3.(1-d_1).(1-d_2)$	$d_1.d_2.(1-d_3)$+ $d_1.d_3.(1-d_2)$+ $d_2.d_3.(1-d_1)$	$d_1.d_2.d_3$	
n = 4	$(1-d_1).(1-d_2).(1-d_3).(1-d_4)$	$d_1.(1-d_2).(1-d_3).(1-d_4)$+ $d_2.(1-d_1).(1-d_3).(1-d_4)$+ $d_3.(1-d_1).(1-d_2).(1-d_4)$+ $d_4.(1-d_1).(1-d_2).(1-d_3)$	$d_1.d_2.(1-d_3).(1-d_4)$+ $d_1.d_3.(1-d_2).(1-d_4)$+ $d_1.d_4.(1-d_2).(1-d_3)$+ $d_2.d_3.(1-d_1).(1-d_4)$+ $d_2.d_4.(1-d_1).(1-d_3)$+ $d_3.d_4.(1-d_1).(1-d_2)$	$d_1.d_2.d_3.(1-d_4)$+ $d_1.d_2.d_4.(1-d_3)$+ $d_1.d_3.d_4.(1-d_2)$+ $d_2.d_3.d_4.(1-d_1)$	$d_1.d_2.d_3.d_4$

5.3 High bound

An upper bound can be derived from the following fact based on the laws of probability, when considering a subgroup of components S:

$$P\left\{\prod_{k\in S} X_k \,|E\right\} \le P\{X_k\,|E\} = d_k \quad \text{for every } k \in S \tag{5.2}$$

thus

$$P\left\{\prod_{k\in S} X_k \,|E\right\} \le \underset{k\in S}{\text{Min}}\{d_k\}$$

I.e., an upper bound is constituted by setting the chances of the failure of the whole subgroup equal to the failure probability of the least degraded component. This corresponds to the assumption of maximum dependence between the degraded components. For the derivation procedure it is convenient to arrange the degraded components into descending order of degradation value, which gives a straightforward way to express the high bound, i.e.:

$$d_1 \ge d_2 \ge ... \ge d_k ... \ge d_n \tag{5.3a}$$

then for the high bound

$$P\{X_1 X_2 .. X_m | E\} = d_m \text{ , for } 1 \le m \le n \tag{5.3b}$$

With the above sorting arrangement the high bound is obtained through

$$v_{Max}(n|n) = d_n \qquad (5.4)$$
$$v_{Max}(m|n) = d_m - d_{m+1} \text{ for } 1 \le m \le n - 1$$
$$v_{Max}(0|n) = d_0$$

This result can be derived by using the corollary, that the assumption of Eq.(5.3b) implies that if a specific component 'k' fails, then all more degraded components (index $j < k$ and $d_j \ge d_k$) fail also. (The mathematics of the high/low bound derivation could be described in more detail in a future task.)

This upper bound is guaranteed to give higher Impact Vector elements for the high multiplicity (at or close to the total number of failed plus degraded components) than the earlier discussed low bound. But it may not be so for intermediate multiplicity, because weight is effectively placed towards high order failure. The exclusion aspect and large number of component combinations for the intermediate multiplicity contributes to this anomaly.

The discussed anomaly is illustrated in Table 5.2 with a typical case of four components where one component is completely failed, one degraded and two others in incipient state. For further illustration, the high bound probability of sorted subgroups for the most degraded components is also presented, compare to Eq.(5.3). For additional comparison interest, the other SGFP entities are derived from the Impact Vector (considering it as Pes entity, for the transformations see NAFCS-PR04). It can

Table 5.2 High and low bounds for an example case of CCCG size 4.

Component Degradation Values	k	d_k
Components are sorted in the order of descending degradation	1	1
	2	0.5
	3	0.1
	4	0.1

High Bound	Multiplicity					
	0	1	2	3	4	Notes
Impact Vector	0	0.5	0.4	0	0.1	Element sum = 1
$P_{Max}\{X_1 \dots X_m\}$	1	1	0.5	0.1	0.1	/* 1 */
Pts(m|n)	1	1	0.5	0.1	0.1	
Peg(m|n)	0	0.125	0.0667	0	0.1	
Psg(m|n)	1	0.425	0.1667	0.1	0.1	/* 2 */

Low Bound	Multiplicity					
	0	1	2	3	4	Notes
Impact Vector	0	0.405	0.495	0.095	0.005	Element sum = 1
Pts(m|n)	1	1	0.595	0.1	0.005	
Peg(m|n)	0	0.101	0.0825	0.0238	0.005	
Psg(m|n)	1	0.425	0.135	0.0288	0.005	

Notes:
* 1 * For the most degraded m components
* 2 * In the mean for a subgroup of m components

be shown, that in terms of Psg entity the high and low bounds stay in intuitively correct order, see the example case, Table 5.2. The basic reason is that Psg entity is not affected by combinatorics and exclusion aspect which "disturb" the other SGFP entities. Due to this feature, that Psg entity describes the profile of probability dependence in an intuitive way, it might be advisable to make the impact assessment for certain complicated CCF cases with respect to Psg entity.

The recent applications provide additional information about the behavior of the high and low bounds in varying cases, and about the practical uses of the bounds, see especially DG Pilot [NAFCS-PR10].

5.4 Bounds for the general case of time-spread events

The procedure presented in [NUREG/CR-5485] contains a simple way to handle time-spread events by using the Time Factor. The procedure covers also the Shared Cause Factor. These two factors are included in the ICDE code classifications [ICDECG00].

This procedure will be adapted here for the purpose of bounding calculations. The low bound will be discussed first. The following mutually exclusive hypotheses are made regarding the time spreading of degraded - failed states connected to a CCF event (the number of affected components is denoted by 'j'):

L1) Component events happen simultaneously with overlapping effective unavailability. In this scenario the component events concentrate on one TDC.

L2) Component events are evenly distributed with no overlapping effective unavailability. In this scenario the component events divide up onto 'j' separate TDCs.

The underlying assumptions behind the above hypotheses are basically optimistic as they reflect the conditions of evenly staggered testing and do not consider the scenarios where the unavailability states of a part of the affected components is overlapping, or further combinations. Anyway, the assumptions form a suitable basis for the simple low bound assessment.

The following probability is set for the hypotheses:

$$P\{L1\} = q \cdot c \qquad (5.5)$$

$$P\{L2\} = 1 - P\{L1\} = 1 - q \cdot c$$

where

q = Time Factor

c = Shared Cause Factor

The Shared Cause Factor is controversial in the sense that so called coincidental multiple failures can contain non-visible dependence and should not thus be excluded. Therefore it is recommended to set c = 1. Compare to the more detailed discussion of this issue in Section 2.7.

Next, the Sum Impact Vector over j TDCs shall be constructed for the two hypotheses. For Hypothesis L1 it constitutes of $\mathbf{v}_{Min}$ for one TDC (see Table 5.1) and $\mathbf{v}_{Zero} = (1, 0, \ldots, 0)$ for the other j-1 failure-free cycles. For Hypothesis L2 the Sum Impact Vector is made up of $\mathbf{v}_{Single} = (0, 1, 0, \ldots, 0)$ for all j TDCs. The weighted Sum Impact Vector is thus:

$$\mathbf{V}_{Low} = q \,.\, c \,.\, \mathbf{v}_{Min} + q \,.\, c \,.\, (j - 1) \,.\, \mathbf{v}_{Zero} + (1 - q \,.\, c) \,.\, j \,.\, \mathbf{v}_{Single} \qquad (5.5)$$

The construction of the high bound for the time-spread events follows the same scheme. Firstly, $\mathbf{v}_{Min}$ is replaced by $\mathbf{v}_{Max}$, see Eq.(5.4). Secondly, the Time Factor should reflect the high bound situation. As a first approximation the high bound value for the Time Factor can be obtained by increasing the code class by one step, see Table 5.3. The Shared Cause Factor is again forced equal to one. The mathematical expression for the weighted Sum Impact Vector is thus:

$$\mathbf{V}_{High} = q' \,.\, c' \,.\, \mathbf{v}_{Max} + q' \,.\, c' \,.\, (j - 1) \,.\, \mathbf{v}_{Zero} + (1 - q' \,.\, c') \,.\, j \,.\, \mathbf{v}_{Single} \qquad (5.6)$$

Table 5.3 Numeric values for the code classes of Time Factor.

ICDE code	Description	Low bound q	High bound q´
H	High	1	1
M	Medium	0.5	1
L	Low	0.1	0.5
N	Null	0	0.1

It has to be emphasized that the presented bounds build up of the component degradation values, which are based on assessments. It is often much easier to assess the component degradation values than Impact Vector because in the latter the dimension of multiplicity and dependence between degraded states are added, and makes the assessment more difficult. Anyway, the component degradation values contain also uncertainty, which should be taken into account in a comprehensive uncertainty analysis.

6. Mapping up/down

As pointed out in the introductory sections the Impact Vectors of CCCGs cannot be directly combined together, or statistics transferred between them, if the groups have different size. In order to transfer an Impact Vector from a 'source' group A to 'target' group B the following procedures are required:

- mapping down if the target group is smaller, i.e. if $n_A > n_B$
- mapping up if the target group is bigger, i.e. if $n_A < n_B$

Transferring failure event data requires also (sufficient) mutual homogeneity or a postulation of that for a specific purpose, e.g. comparison aim. A basic option for combining event data for the CCCGs of different size requires that a target group size is defined, usually equalling to one of the considered groups.

The following subsections discuss the procedures starting from mapping down because it is conceptually simpler.

6.1 Procedure for mapping down

Mapping down is theoretically equivalent to considering a subgroup (target group) within a CCCG (source group). The assumption of mutual homogeneity between the source and target groups corresponds to the internal homogeneity in the subgroup analogy. The homogeneity in turn means that Psg entity is subgroup invariant, i.e.:

$$Pgs(m|n_B) = Psg(m|n_A) \text{ for } 0 \le m \le n_B < n_A \qquad (6.1)$$

The concept of subgroup invariance is discussed in more detail in [NAFCS-PR04]. It offers the following very logical way to define the mapping down procedure using the connection of Impact Vector to Pes entity, see Section 2.6:

$$v_E(m|n_A) = Pes(m|n_A|E) \rightarrow Psg(m|n_A|E) \qquad (6.2.a)$$
$$= Psg(m|n_B|E') \rightarrow Pes(m|n_B|E') = v_{E'}(m|n_B)$$

where

E	denotes the source event with Impact Vector $v_E(m\|n_A)$
E′	denotes the event as mapped into target B
→	denotes SGFP transformation

In this procedure the total number of TDCs is preserved, i.e.

$$ND_B = ND_A \qquad (6.2.b)$$

But there is also an alternative procedure, where the source event is mapped into each subgroup of size n_B in the source group of size n_A. The source Impact Vector is mapped into subgroup Impact Vectors which then are summed together:

$$v_E(m|n_A) = Pes(m|n_A|E) \rightarrow Psg(m|n_A|E) \qquad (6.3.a)$$
$$= Psg(m|n_B|E') \rightarrow Pes(m|n_B|E')$$
$$\text{then } V_{E'}(m|n_B) = Cmb(n_B|n_A) \cdot Pes(m|n_B|E')$$

where

$$Cmb(n_B|n_A) = \binom{n_A}{n_B}$$

= Binomial coefficient, i.e. number of different choices of n_B components among a group of size n_A

In this procedure also the TDCs are mapped into subgroups, thus

$$ND_B = Cmb(n_B|n_A) \cdot ND_A \qquad (6.3.b)$$

The above two procedures are equivalent in the respect that the point (maximum likelihood) estimates for multiple failure probability are same. The second procedure produces more statistical mass into the target which can impact the statistical uncertainty (… to be discussed further in the next stage). The practical interpretations of the two ways are different:

- In the first procedure the Impact Vector is regarded as outcome of a CCF mechanism for the given TDC. Consequently, it is natural to transfer only statistics of one TDC to the target group
- In the second procedure the impact of the CCF mechanism is considered from the point of each subgroup of the target size within the source group. Thus the statistics of one TDC is mapped effectively into many target TDCs.

The first procedure is generally preferred in order to retain the statistical mass. Especially in highly redundant systems the second procedure would yield to an unreasonable amount of target TDCs.

Table 6.1 gives an example where the event OL2/85 in Table 3.2 is mapped from $n_A = 10$ down to $n_B = 8$ using the first procedure. As a check the point estimate of single failure probability is calculated using the estimation equation

$$\langle Psg(1|n|E)\rangle = \frac{1}{ND}.\sum_{m=1}^{n} m.V_E(m|n) \qquad (6.4)$$

Because of considering a single source Impact Vector and mapping it to one target TDC (in Procedure 1), ND = 1 in this case both for the source and target. Of course this estimate equals to the value of Psg(1|n) as presented for the corresponding calculation step in Table 6.1. It is interesting to notice that the statistical mass of source element

- m = 10 is mapped to target m = 8,
- m = 7 is mapped to target m = 7…5
- m = 3 is mapped to target m = 3…1

The logic behind this could be understood by following Procedure 2 but that is omitted here for its complexity.

Table 6.1 Mapping down, an example of highly redundant case.

Size n=	10		8
m	Source impact vector Pes(m|10)	Psg	Target impact vector Pes(m|8)
0		1	
1		3.95E-1	5.33E-2
2		1.73E-1	3.73E-1
3	0.8	1.00E-1	3.73E-1
4		7.50E-2	
5		6.25E-2	7.00E-2
6		5.50E-2	7.00E-2
7	0.15	5.13E-2	1.00E-2
8		5.00E-2	5.00E-2
9		5.00E-2	
10	0.05	5.00E-2	
<Psg(1|n)>	0.395		0.395

The impact vector elements less than 1E-10 are truncated to zero to compensate for the inaccuracy in the numerical calculations

Zero elements are blank

Table 6.2 gives another example where a double failure of four components is mapped into a target group of three or two components using the two procedures in parallel for comparison purpose. Again the point estimate of single failure probability is checked in the different cases. When using Procedure 2 ND = 4 and 6 (equal to Cmb) for the target groups of $n_B = 3$ and 2, respectively.

It is again of interest to notice that in mapping from size 4 down to 3 the statistical mass of source element of order two is distributed downwards over two orders and in mapping from size 4 down to 2 it is distributed downwards over three orders. Compare also to the discussion of this behavior in connection to Table 6.1. It is generally valid that the statistical mass of element m is distributed downwards over orders $[m, m + n_A - n_B + 1]$.

It has to be pointed out that the single failure count is affected also in the mapping down. The same procedure shall be followed for single failure TDCs as for other Impact Vectors in general. This applies also to failure-free TDCs. It is peculiar to notice that in the first procedure the number of failure-free TDCs is preserved but in the second procedure it is increased by factor of $Cmb(n_B|n_A)$.

Table 6.2 Mapping down, an example of low redundant case.

Size n=	4		3	*Cmb=4*
	Source impact vector		Target impact vector	
			Proc.1	Proc.2
m	Pes(m|4)	Psg	Pes(m|3)	V(m|3)
0		1	-	-
1		5.00E-1	5.00E-1	2.00E+0
2	1	1.67E-1	5.00E-1	2.00E+0
3				
4				
<Psg(1|n)>	0.5		0.5	0.5

The impact vector elements less than 1E-10 are truncated to zero to compensate for the inaccuracy in the numerical calculations

Zero elements are blank

Size n=	4		2	*Cmb=6*
	Source impact vector		Target impact vector	
			Proc.1	Proc.2
m	Pes(m|4)	Psg	Pes(m|2)	V(m|2)
0		1	1.67E-1	1.00E+0
1		5.00E-1	6.67E-1	4.00E+0
2	1	1.67E-1	1.67E-1	1.00E+0
3				
4				
<Psg(1|n)>	0.5		0.5	0.5

Owing to the linearity of SGFP transformations in particular, and the mapping down procedures as a whole, mapping down can be applied to the Sum Impact Vector (whole statistics) at once and need not be performed individually for each Impact Vector and then summing them together for the target group. Separation can, however, be motivated to show the contribution of individual events or event types.

The procedure presented here for mapping down is equivalent to the formulas presented in [NUREG/CR-5485]. The presented procedure based on the use of SGFP transformations is, however, considered preferable because of its general nature, and because the transformation are relatively simple to program (for example by using VBA for Excel) in comparison to the tedious direct formulas.

6.2 Procedure for mapping up

Unlike mapping down the upwards mapping is not simple scaling for combinatorial aspects. Knowing a failure history in a smaller source group does usually not provide direct nor sufficient evidence what had been the impact in a larger group. Namely, owing to the larger number of components it is generally expected an increase in the failure multiplicity for a given CCF mechanism. The situations can be divided into three types

- The failure mechanism caused a single failure in the source group and does not indicate CCF aspect. Then it is reasonable to assume that the failure mechanism will cause also single failures in the larger target group
- All components failed in the source group and the failure mechanism shows characteristics of a complete dependence (so called complete CCF or lethal shock). In this kind of situation the failure mechanism can be assumed to result in a total failure of the larger target group as well
- In the remaining cases the dependence falls between negligible and complete. Additional judgment (extrapolation) is needed to support upwards mapping

These different situations will be discussed separately in the following subsections. In upwards mapping it is logical to preserve the number of TDCs.

Single failure with negligible dependence

These kinds of failure mechanisms are expected to cause only single failures irrespective of the group size. The expected number of single failures is, however, proportional to the number of components in the observed group (assuming the same number of TDCs). Consequently, the following rationale can be followed in mapping upwards:

$$(0, 1, 0, \dots , 0) \rightarrow (1-n_B/n_A, n_B/n_A, 0, \dots , 0)$$

Doing it in this way means that the negative zero element of the target Impact Vector takes care about decreasing the number of failure-free TDCs by the same amount as the number of single failure TDCs is increased. (Notice that in upwards mapping $n_B/n_A > 1$.

Complete CCFs

As said in case of complete CCFs it is reasonable to assume the total failure of the target group as well. Thus the highest order element of the target Impact Vector is set equal to one and other elements to zero.

Intermediate dependence case

The crucial question in this kind of observed failure mechanism is how likely more components could be affected in a larger group. [NUREG/CR-5485] uses a rationale based on the concept of non-lethal shock in the Binomial Failure Rate (BFR) model. The conditional probability of component failure is described by parameter ρ. Each element of the source Impact Vector is mapped upwards by using this conditional probability. The combinatorial factors are derived from the analogy with corresponding downwards mapping. Nevertheless, the procedure is not reversible, i.e. mapping back downwards the Impact Vector, which is derived by mapping upwards, does not result in the original Impact Vector started from. The problem is even more complicated because generally for a given source Impact Vector there may not exist at all an Impact Vector in the larger group that would produce the source Impact Vector by mapping downwards. Surprisingly, this dilemma has not been discussed in the basic references, e.g. in [NUREG/CR-5485]. Some good examples could be presented in a future task to illustrate the discrepancies.

It is also questionable to use same parameter value of ρ irrespective of the failure multiplicity. All experiences show that generally the conditional probability of additional failure in a CCF increases as the function of failure multiplicity.

One developed and robust way for mapping up is to use a subgroup invariant CCF model, e.g. BFR model (in full, not restricted to non-lethal shock part) or CLM. The dependence (model) parameters are estimated based on a given source Impact Vector, i.e. for a statistics of one observed failure history (for one TDC) in the source group. The obtained model parameters are then used to generate the corresponding Impact Vector in the target group for one TDC. In fact, CLM has been used in some occasions for this purpose, compare to [CR_ImpVe].

Because of the conceptual complexity and also due to uncertainty in the extrapolation to higher multiplicity it is recommended not to use upwards mapping. The next subsection will discuss the practical ways to handle data from CCCGs of different size without using size-related mapping. The upwards mapping is a topic for further elaboration. For the time being it is not meaningful to present the formulas for mapping up in this report.

6.3 Practical aspects

So it is recommended that mapping up is not used due its controversial features and also due to the uncertainties in the extrapolation that is a necessary part of upwards mapping. Mapping up can be avoided in comparisons or pooling of data from CCCGs of different size by mapping only downwards from the larger groups to the smallest CCCG.

It is worth to notice that for certain CCF models the data pooling does not require any mapping at all. For example, the estimation of CLM parameters can be done for a pooled statistics from CCCGs of different size by composing the joint likelihood function (product of the likelihood functions for each CCCG). This provides a mathematically rigorous solution to avoid size-related mapping.

It is possible to make direct estimation (of SGFPs) without mapping in case of data pooling from CCCGs of different size. In short the direct estimation pooling uses the following expression (note homogeneity assumption and sub-group invariance property of Psg entity)

$$\langle Psg(m \mid n) \rangle = \frac{ND_A \cdot \langle Psg(m \mid n_A) \rangle + ND_B \cdot \langle Psg(m \mid n_B) \rangle}{ND_A + ND_B} \qquad (6.5)$$

$$\text{for } m \le n = \min(n_A, n_B)$$

where $< Psg(m|n_A) >$ and $< Psg(m|n_B) >$ are group-specific estimates, compare to Eq.(3.11)

The estimates of higher order elements $m > \min(n_A, n_B)$ can be based only on the statistics of the larger group!

Of course, the best solution is to use CCF data from a given size of CCCG only for that group size.

It must be understood that the homogeneity assumption is in the practical cases at the best only a good approximation when transferring data from one plant to another or when combining data. The difference in the size of CCCG itself can imply differences in the physical separation, in test/maintenance arrangements and in other coupling and defense factors. In addition there can be other differences in the actual conditions. Indeed, the DG Pilot revealed significant difference in the CCF event rate and general dependence level between group sizes 2 and 4, see [NAFCS-PR10, Section 2.1].

Pooling approximations must, however, often be accepted due to sparse data about CCFs. Besides, there are many other uncertainties connected to the interpretation of the CCF events and probabilistic estimation.

The topic of data pooling in different circumstances is also one of the subjects for further work.

7. Concluding remarks

This report has been directed to the methodology of plain Impact Vector construction. The interface with the event analysis, CCF parameter estimation, uncertainty analysis and data storage (still pending task areas within NAFCS) can require supplements and refinements in the future version of this report, construction guide [NAFCS-PR17] and/or other NAFCS documentation.

At this point the need for a detailed documentation of Impact Vector construction has to be emphasized once more, for the following needs especially:

- review and understanding of data origin, e.g. in connection to update needs
- transferring data to another target group, e.g. to another plant with specific differences
- performing uncertainty analysis requires the knowledge about the principal assumptions and judgments, e.g. documentation of the cases analyzed by scenario method should include the scenario vectors and weights

The instructions in these regards belongs more to the construction guide but are not fully covered in its current version.

The tools for Impact Vector construction, pooling and integration should be collected in a toolbox to facilitate practical work. Seamless integration of the tools with other CCF database tools (event analysis, estimation, uncertainty analysis) is needed.

It is suggested that further examples are elaborated to cover more comprehensively different situations for constructing Impact Vectors. Most efficiently this will be accomplished in parallel to cumulating expertise from continued quantitative analysis tasks of NAFCS, as started with the DG Pilot [NAFCS-PR10]. It would be optimal to create a practical case to be used throughout the method description and construction guide as the main example (or rather a series of examples) to illustrate the basic aspects of various steps in a consistent manner.

There are also several specific methodological topics that would require further elaboration:

- Transferring CCF data (Impact Vectors) to different target conditions
- Data pooling in general
- Controversial mapping up, possibility to define a reversible procedure
- Enhanced coverage of Impact Vector construction from the perspective of failure rate-based modeling, which is split in the current version. Especially, the special aspects of the CCFs with time-spread component events should be looked regarding any implications for the analysis

Acknowledgements

The NAFCS members have given valuable contribution in conducting this task through the discussions and comments. Especially the valuable comments and suggestions by Michael Knochenhauer, Impera-K AB, about the latest draft are acknowledged. A part of the many useful suggestions are still pending for an elaboration in the next version.

References

NAFCS-PR01
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR02
Data Survey and Review. Topical Report NAFCS-PR02, prepared by Tuomas Mankamo, Draft for Peer Review, 12 January 2002.

NAFCS-PR04
Model Survey and Review. Topical Report NAFCS-PR04, prepared by Tuomas Mankamo, Draft for Peer Review, 12 January 2002.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 31 October 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Issue 1, 29 August 2003.

NAFCS-PR19
Impact Vector Construction to the MOVs. Topical Report NAFCS-PR19, Issue 1, 30 August 2003.

NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

NUREG/CR-5497 CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998

SKI TR-91:6 Mankamo, T., Björe, S. & Olsson, L., CCF analysis of high redundancy systems, SRV data analysis and reference BWR application. Technical report SKI TR-91:6, Swedish Nuclear Power Inspectorate, 1991.

HR_CCFRe High redundancy structures, CCF models review. Work report prepared by Mankamo, T., Avaplan Oy, 31 December 1990. (Work report companion to SKI TR-91:6)

SKI R-96:77 Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Summary report, prepared by T. Mankamo. SKI Report 96:77, December 1996.

SKI/RA-26/96
CCF Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Work reports, prepared by T. Mankamo. SKI/RA-26/96, December 1996.

CA_HRedI Instructions for CCF analysis of high redundancy systems. 2nd Version, T. Mankamo, Avaplan Oy, 22 November 1995. (Part of SKI/RA-26/96)

ECLM_Pub Mankamo, T., Extended Common Load Model, A tool for dependent failure modeling in highly redundant structures. Manuscript, 15 February 1995, 10 February 2001.

RESS_HiD Mankamo, T. & Kosonen, M., Dependent failure modeling in highly redundant structures - application to BWR safety valves. SRE-Symposium 1988, Västerås, October 10-12, 1988. Enhanced manuscript published in Rel. Eng. and System Safety 35(1992)235-244.

CR_ImpVe Expressing the impact of a CCF mechanism. Work notes, Tuomas Mankamo, Avaplan Oy, 17 September 1996.

CR_ImpV2 Examples on the Relationships between Impact Vector and Component Degradation Values. Work notes, Tuomas Mankamo, Avaplan Oy, 19 November 1996.

DGTS_B92 Test strategies for standby diesel generators. IAEA Technical Committee Meeting on Advances in Reliability Analysis and PSA, Budapest, 7-11 September 1992. Proceedings.

T314_TrC Mankamo, T., A pressure relief transient with pilot valve function affected by a latent CCF mechanism. Work report NKS/SIK-1(92)35, Avaplan Oy, 31 January 1994.

TC_PASDG Mankamo, T., A timedependent model of dependent failures, application to a pairwise symmetric structure of four components. Report NKS/SIK-1(92)13, 31 December 1993.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

ICDE-S-ImpVe Mankamo, T., Impact Vectors–Construction and Linkage of CCF Data to Quantification. ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, 12-13 Stockholm, 2001.

ICDE-S-EdF Vasseur D., Voicu A., Mankamo T., Bonnet C and Dewailly J., CCF Analysis in Progress at EdF. Overview of EdF Involvement in CCF Analysis, e.g. Control Rod Application. ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, Stockholm, 12-13 June 2001.

ICDE-S-Vaurio From Failure Rate to CCF-Rates and Basic Event Probabilities. Presentation by J.K. Vaurio, ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, Stockholm, 12–13 June 2001.

PCM01_4 Some Comments on the Report NAFCS-PR03: Impact Vector Method (Draft 2). Prepared by K.Pörn, 12 October 2001.

Abbreviations

Acronym	Description
BFR	Binomial Failure Rate (Model)
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CLM	Common Load Model
CRDA	Control Rod and Drive Assembly
EPV	Electromagnetic Pilot Valve
DG	Diesel Generator
SGFP	Subgroup Failure Probability
SRV	Safety/Relief Valve
TDC	Test/Demand Cycle
ICDE	International CCF Data Exchange
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate

Annex 1: Comparison and discussion of the inconsistencies for Impact Vector definition in literature

This annex collects more comprehensive critical discussion about certain details in the definition of Impact Vector and construction procedure. In the current version the focus is on the US reference [NUREG/CR-5485] which can be regarded as a basic source. Despite of the criticism on some details the value of this source is acknowledged as an important cornerstone on the subject field.

Singles and multiples

Elaboration of the broader versus narrower definition of the following concepts:

- Dependent multiple failure versus CCF
- Single failure versus independent failure

Compare to Section 2.7.

For example, strictly following the narrow definition for CCF (related to 'Shared Cause Factor') leads to inconsistent handling of probability mass in the case considered in the lower part of page 60 in NUREG/CR-5485. Assuming that both two components failed simultaneously, the Impact Vector should straightly be (0,0,1) irrespective of the causes. The plain counting of multiple failures has the advantage that all underlying dependencies are covered, not only the visible ones, besides of simplifying the event analysis. The pointed problem in the US approach is related to the incomplete coverage of single component failures and success events, due to the history that component reliability data collection and CCF data collection have been separated activities (in the USA).

Time-spread events

The instructions given in Section 5.5.2.2 of NUREG/CR-5485, using Time Factor to describe the coupling, can be used as a simple procedure when handling the time-spread dependent events. It should, however, be noticed that those instructions reflect the situation that is typical to a CCF data analyst in the USA as he (she) may not know the test, operation, maintenance and inspection arrangements of the components. If that kind of basic knowledge and detailed event descriptions are available to the analyst, the dependence among distributed events can be evaluated in a more specific way.

There is also a shortcoming in Section 5.5.2.2 of NUREG/CR-5485 when handling separated events, namely inconsistency in counting single failures and TDCs (already mentioned in the preceding section). For example, in case of two failures at separate time points (consecutive TDCs) and weight of 'q' for the chance that the mechanism had led to a double failure in the same TDC, the Impact Vector construction should follow the scheme of Table 4.1. Compare to 'Average Impact Vector Calculation' in Section 5.5.2.2 and Case 2 of NUREG/CR-5485, where the corresponding result is [0, 2(1-q), q, 0, …, 0], i.e. normalization with respect to pertinent TDCs is missing. It is

advisable to construct a joint (sum) Impact Vector to cover all affected TDCs for a time-spread CCF mechanism. Compare to Section 4.1.

Quantification procedures skipping Impact Vector construction

Some quantification procedures do not use the Impact Vector as (explicit) presentation step of observed failure statistics. The count of failures and degraded component events are “directly” entered into estimation formulas. Further review and comparison with the references (German, UK) using these kinds of estimation procedures could be an interesting future task.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
App4.3	**Impact Vector Construction Procedure PR17**	**PR17**
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR17**

Title:	**Impact Vector Construction**
Author(s):	Tuomas Mankamo
Issued By:	Tuomas Mankamo
Reviewed By:	Michael Knochenhauer, 2002-10-29
Approved By:	Gunnar Johanson 2003-10-17
Abstract:	This report presents step-wise instructions for the construction of impact vectors. The scenario method (hypothesis method) is used as a basic tool. Advices are given for, how to apply the method in different type cases such as time spread component events. A number of fully elaborated example cases are included in the annex of this guide. In-depth description of the methodological details is contained in another report [NAFCS-PR03].
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2002-10-12	TM
Draft 1	2002-10-31	TM
Issue 1	2003-10-10	TM

This report was closed declaring Working Draft 1 as final for this phase with small editorial changes only. See concluding remarks for the discussion of status achieved and prediction of the needed further work.

Contents

Impact Vector Construction

1. Introduction

This section presents the objectives and scope of the instructions, and the regime of implementation. The last subsection describes the document structure.

1.1 Objectives

One of the basic tasks of NAFCS is the preparation of a guideline for impact vector construction, starting from the method description and including examples of different types of cases [NAFCS-PR01]. This report contains the practical instructions, while the methodological part is contained in a separate report [NAFCS-PR03].

The method description and construction guide will support the quantitative classification and evaluation of CCF events, being started by a pilot work for the diesel generators [NAFCS-PR10]. It is expected that both the method description and construction guide will be supplemented in the course of coming assessment work to more comprehensively cover special issues. Also the spectrum of practical examples will be extended according to the cumulating insights.

1.2 Scope

The construction of impact vector is basically developed as applicable to demand failure probability but the instructions presented in this guide apply also to the use of impact vectors to failure rate based modelling. The actual difference is related to estimation stage as discussed in more detail in [NAFCS-PR03]. The presented instructions apply to component groups of both low and high redundancy, but is basically assumed that the group is internally homogeneous, or a postulation of that is reasonable, which is a standard assumption in CCF analysis. It has to be pointed out that the complexity of phenomena and difficulty of assessment increase as the function of redundancy level.

These instructions assume that the event information is gathered, classified and documented according to ICDE frame [ICDECG00], or to another comparable extent. Especially, it is assumed that the CCF events are identified as input information to the impact vector construction, i.e. the CCF identification and screening steps are not discussed here.

1.3 Report structure

Chapters 1-5 are made parallel in the method description (PR03) and this construction guide (PR17) in order to facilitate finding the additional background and explanations from PR03 when working in practice following the guide PR17. For this aim the headings of the parallel sections are identical or similar. Some basic definitions are repeated in both reports. One argument behind this is to make the reports possible to understand sufficiently well as stand-alone. Another argument is that the similarity of key parts will support the linkage between the texts.

2. Impact vector concept

This section presents the definition and theoretical background for the impact vector concept, which forms a link from CCF event data to the estimation of dependent probabilities for a Common Cause Component Group (CCCG). It is assumed that the reader and user of this guideline is well familiar with the ICDE coding guideline [ICDECG00], and with the definitions presented there. The key terms that are highly relevant for the impact vector construction are Component Impairment Value, Time Factor and Shared Cause Factor.

This guideline uses a large number of special terms which are defined during the course of presentation. The definitions are not collected anywhere. Such an annex for definitions is planned to be contained in the future version of this guideline and/or in the method description. For the time being the reader is recommended to use the 'Find' command to locate the definition or introduction to a special term within the electronic document.

2.1 Basic definition

The impact vector describes the outcome of a demand placed on a group of components, which constitute a CCCG. In a CCCG of size 'n' the impact vector has 'n+1' elements:

$$\mathbf{v} = [\, v_0, v_1, v_2, \ldots, v_n \,] \tag{2.1}$$

In the basic case, where the functioning of each component at the demand is perfectly known either successful or failed, the number of failures is exactly determined: the impact vector elements are then zero, except $v_m = 1$ given that 'm' components failed, e.g.

$$\begin{aligned}
\mathbf{v} &= [\, 1, 0, 0, \ldots, 0 \,] \text{ , when all components functioned} \\
\mathbf{v} &= [\, 0, 1, 0, \ldots, 0 \,] \text{ , when one component failed} \\
\mathbf{v} &= [\, 0, 0, 1, 0, \ldots, 0 \,] \text{ , when two components failed} \\
\mathbf{v} &= [\, 0, 0, \ldots, 0, 1 \,] \text{ , when all components failed}
\end{aligned} \tag{2.2}$$

If it is important to show the total number of components, the elements can be denoted by $v_m = v(m|n)$. The impact vector entity alone is denoted by bold letter.

In the context of CCF event analysis the impact vector is used to describe all historical demands covering both actual demands and test demands. The majority of the demands are in practice failure free impact vectors [1, 0, 0, … , 0]. The practical aspects what is meant by the demand will be discussed in Section 2.5.

2.2 Connection to component impairment values

The impact vectors are really needed to describe the more general outcome conditions from such cases where the functioning of every component is not perfectly known, i.e. component state index - called as component impairment or degradation value d - can fall in the range (0,1). Correspondingly, the elements of impact vector will then attain values in the range (0,1) with the following interpretation:

v_m = Conditional probability that some 'm' components fail and other 'n-m' survive in the conditions at a given demand and preceding operational history (2.3)

Similarly, component degradation value can be defined in the following way

d_k = Conditional probability that a specific component, indexed by 'k', fails in the conditions at a given demand and preceding operational history (2.4)

There is no universal one-to-one correspondence between the impact vector and component degradation values. The assessment of component degradation values is easier, and they can be useful in the impact vector construction as will be discussed later on, e.g. constructing upper and lower bound impact vector, see Chapter 5. An obvious connection is that the highest order of non-zero elements in impact vector equals to the number of components having non-zero degradation value.

It has to pointed out that the definition means that following equality has to be met:

$$\sum_{m=0}^{n} v_m = 1 \tag{2.5}$$

It can thus be said that the impact vector elements describe how the demand outcome probability is distributed over different order of failure states.

2.3 Test and demand cycles

An impact vector represents the outcome of each test or demand. The number of tests/demands is denoted as 'ND' and correspondingly the observation period is divided into same number of test/demand cycles (TDCs). When the observed population contains several CCCGs (assumed identical and homogeneous), the number of demands is derived as sum over the tests and demands in the considered component groups. It should be emphasized that the number of component demands is 'n*ND'.

2.4 Sum impact vector

Summing up the impact vectors over the TDCs of the observed population produces a sum impact vector (also called as observation vector):

$$\mathbf{V} = \sum_{i=1}^{ND} \mathbf{v}_{TDC(i)} \tag{2.6}$$

A capital letter will be used for the sum impact vector in order to make distinction to the basic impact vector that is connected to an individual TDC. It has to be

emphasized that the sum impact vector is not anymore a conditional probability entity. Instead, it represents the number of events for different multiplicities. Because the sum of the elements of the basic impact vector is equal to one per definition, the following applies to the sum impact vector:

$$\sum_{m=0}^{n} V_m = ND \tag{2.7}$$

The interpretation of the elements in sum impact vector is very straightforward:

V_0 = Number of failure free TDCs
V_1 = Number of single failure TDCs (2.8)
…
V_m = Number of TDCs with failure of multiplicity m
…
V_n = Number of TDCs with failure of all components

I.e., the sum impact vector merely represents the failure statistics arranged according to failure multiplicity. The real power of impact vector method is, however, connected to the generalization, where the elements need not be integer numbers, but the statistical mass can be distributed as was discussed in Section 2.2. The elements of a sum impact vector can generally fall anywhere between [0, ND] but must satisfy the normalization equation (2.7).

2.5 Practical interpretations

There are following important aspects to be taken into account in the impact vector construction:

- The most part of the event information comes through periodic tests which do often not perfectly represent an actual demand. For example, it is usual that during a load running test of a DG it will be promptly stopped after observing operational anomaly. The test will not be forced to continue over the length for a needed actual mission time to really verify whether the DG would fail or survive, in order to prevent additional often extensive damages. Another example is the exercise test of a closing valves in the standby condition of a train without actual pressure difference and flow conditions that can influence on the vulnerability to jamming. It is these kinds of situations, where the impact vector assessment is basically needed, to evaluate what would be the influence of the CCF mechanism if an actual demand should occur during the presence of the degraded-failed state. The assessment should take into account the pertinent evidence based on the observations from the tests, measurements, findings of any undertaken inspections or investigations, observations from the repair actions etc. – incorporating also other historical information and all engineering knowledge
- The impact vector presents the influence of the occurred CCF mechanism (a particular instance) in terms of increased conditional probability of multiple failure during a certain time period when the degraded-failed state is present, typically during one test cycle
- Cases worth to cover in quantitative analysis shall have significant conditional probability of multiple failure from the presence of a CCF mechanism. The weak

influence can in certain special cases cumulate as significant if the degraded-failed component states are present (latent) for a longer time period.

The last two aspects can be illustrated by an example for a group of two DGs. A total single failure probability 0.02 and Beta Factor 5% means Pes = {0.96, 3.9E-2, 1.0E-3} for the probability of no failure, single failure and double failure, respectively. For a potential CCF the impact vector element of order two should be clearly higher, i.e. v(2|2) >> 1E-3 for a significant case. With "weak" cases the statistical gain is small but the connected uncertainty large and assessment work difficult. A practical justification to cover also "weak" CCF cases may be qualitative and completeness aims, but preferably in separate baskets, e.g. as distinct category for 'recurring failures' and another for 'latent degradation cases'. The screening in these respects will be discussed further in the coming sections, especially in Sections 3.6 and 4.2-3.

Handling of the cases with a long latent time of presence will be discussed in more detail in Section 4.4.

3. Instructions to construct impact vectors

This section presents step-by-step instructions to construct impact vectors. The basic construction procedure uses alternative hypotheses about the failure impact.

The general flow of the impact vector construction is presented in Fig.3.1. Steps 1-5 are concerned with the basic construction for the failure history of a given CCCG and for a defined component failure mode and observation period. In practice often the data of identical or closely similar groups of the same size are pooled together. In a general case the analysis may be concerned, for example, with CCCGs of varying size from different systems and/or plants. Steps 6-7 integrate the impact vectors for the estimation of reliability and dependence parameters. These last steps constitute the interface to the statistical estimation and are handled in the method description [NAFC-PR03].

The classified information including event descriptions such as contained in the ICDE data are in most cases sufficient for the impact vector construction. In more complex cases, and even generally where the analyst feels uncertainty, it is necessary to get hold of plant event reports, eventual incident reports or special investigation reports as well as to contact plant specialist to verify correct understanding and interpretation of what happened. This was a main lesson learnt in the DG pilot [NAFCS-PR10]. It would be optimal to construct impact vectors in parallel to the ICDE data collection.

3.1 Definition of test/demand cycles

In the basic case TDCs are related to actual demands and periodic tests, which challenge all components in equal way. The number of TDCs will be then:

$$ND = N_{AD} + N_{ST} \quad (3.1)$$

where

N_{AD} = Number of actual demands (on whole group)

N_{ST} = Number of surveillance tests (on whole group)

Often the number of actual demands is relatively small, and may be difficult to obtain. In such cases it is reasonable to (conservatively) approximate the number of TDCs by the number of tests, which can be calculated from the observation period by dividing with the test interval. In more complicated cases some of the tests or demands may concern only part of the components. Such non-symmetric cases are discussed in the method description [NAFCS-PR03].

Time between consecutive test/demand events is considered in standard way as the standby period for the components, representing normally the maximum latent time of a failed condition (for the considered failure mode). Additional test after failure will be combined with the initial test. If the additional test is more efficient bringing up additional evidence, that should be taken into account depending on the case.

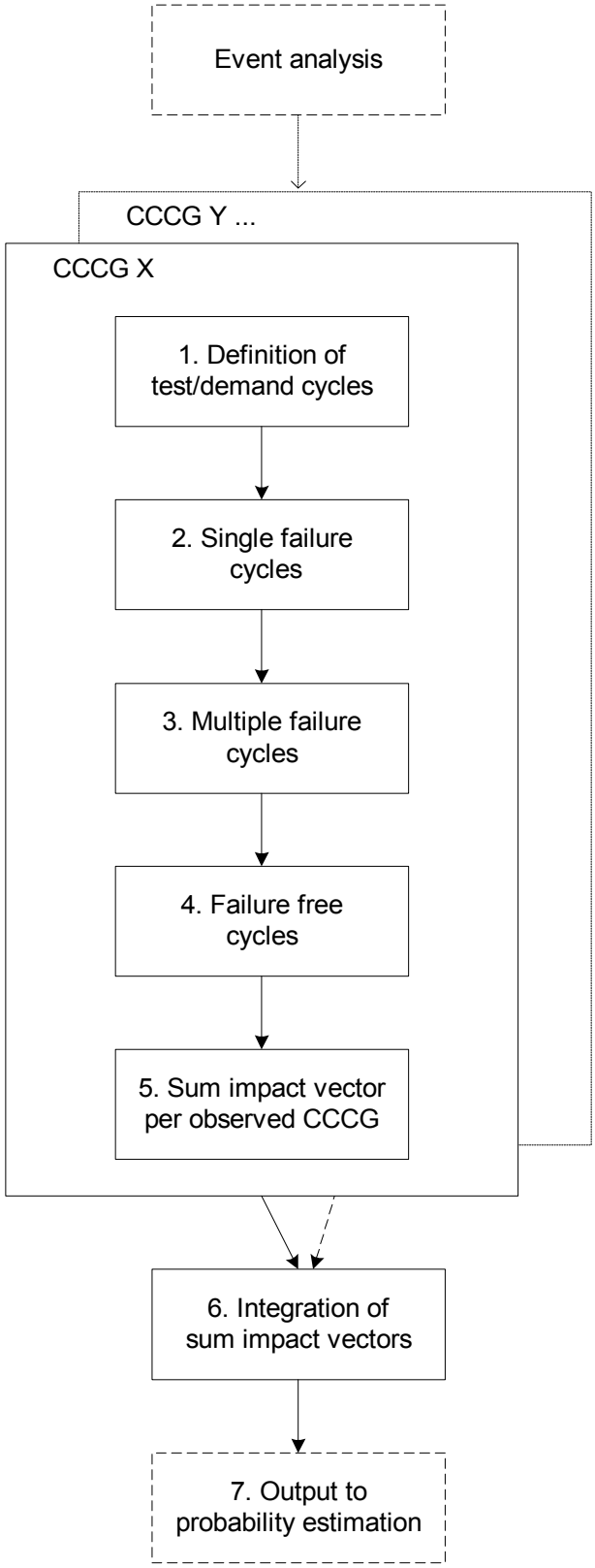


Figure 3.1 Steps and flow of impact vector construction.

3.2 Single failure cycles

TDCs with single failure are represented by the basic impact vector:

$$\mathbf{v} = [\,0, 1, 0, \ldots, 0\,] \quad (3.2)$$

Often in CCF analysis the number of mere single failures (single failure cycles) – also called as independent count – has to be obtained separately. When using ICDE data, the independent count is available from the CCCGs statistical record (field S5).

3.3 Multiple failure cycles

A TDC with actual failure of multiplicity 'm' and other 'n-m' components known to be intact is represented by impact vector:

$$v_m = 1 \quad (3.4)$$
$$v_k = 0, \text{ when } k \neq m$$

In case of a multiple event with 'm' failed and additional 'j' degraded components, the general form of the impact vector is:

$$0 < v_k < 1, \text{ when } m \leq k \leq m + j \quad (3.5)$$
$$v_k = 0, \text{ when } k < m \text{ or } k > m + j$$

The assessment of impact vector elements in the degradation cases is the most difficult part of CCF analysis. The basic methods are the use of alternative hypothesis, specific causal model and using parametric dependence model. These methods will be discussed in the following subsections. Irrespective of the construction method, following general rules should be followed:

- The chances for the failure of various degree have to be assessed with respect to the real demand condition, which may be more challenging than the periodic test condition
- It is generally recommended to keep to the actual available evidence. Extrapolation to failure chances of those components, which were not affected according to the evidence, is not recommended. Exceptions are such cases where a clear random factor is present and could lead to the failure of the components (in an actual demand), which by chance were unaffected (in the observed condition).
- The detection of the recorded situation may have been coincidental in contrast to guaranteed detection at a scheduled test. The chances of a delayed detection could have increased the criticality of component states. The hypothesis method is mostly well suited for such a situation. For a more complicated cases a time-dependent causal model can be used.
- The speed of the failure development can be systematic or varying among the components. In order to get an integral picture, the pertinent history of the components prior to the observed event should be tracked, including the observations in adjacent tests and any similar failures close in time. These aspects will be discussed in more detail in Sections 4.2-3.
- The component impairment values (as well as Shared Cause Factor and Time factor) give background to the impact vector assessment. Firstly, the analyst should check the sensibility of those values as presented in ICDE data. Secondly, the impact vector should be coherent with the verified codes. For this aim it is useful to derive low and high bounds to know the possible range of impact vector

determined by the component impairment values, Shared Cause Factor and Time Factor, and use that information to back up the specific assessment. The derivation of the low and high bounds is discussed in Section 5.

Often in practical cases there can be available more information in addition to the standard failure records, e.g. from a plant incident report or through interviewing the system specialist, to support the proper interpretation of what happened and the implications regarding the operability of the components. As already said, this advice was strongly reinforced in the DG Pilot [NAFCS-PR10].

Hypothesis method[1]

The basic method for impact vector construction uses alternate hypotheses about the possible status of the components at a given demand condition, taking into account the preceding operational history and other relevant information. Table 3.1 presents an example from the DG Pilot material.

Table 3.1 Example construction of impact vector using hypothesis method for a CCF event in a group of four DGs using Case SF25 of DG Pilot [NAFCS-PR10]. In addition to the evident complete failure of two DGs the chance of higher order failure is estimated to be 20% and is divided in equal shares between triple and total failure state.

Hypothesis	Weight	Impact vector elements					Element sum
		0	1	2	3	4	
1. DG A and DG B would fail in an actual demand but the two other degraded DGs would survive	0.8			1			1
2. In addition to DG A and DG B one of the two other degraded DGs would fail in an actual demand	0.1				1		1
3. All four DGs would fail in an actual demand	0.1					1	1
Net impact vector		0	0	0.8	0.1	0.1	1

The hypotheses constitute alternative interpretations of the event. The weights represent analyst's prediction or belief about the chances of the different hypotheses to be true. The net impact vector for the event is obtained as weighted average over

[1] Currently the term "scenario method" is used instead of the earlier common "hypothesis method". The "scenario" is preferred as more descriptive for practical work, being type of engineering assessment, while the "hypothesis" carries the flavour of theoretical exercise. However, the inbuilt subjectivity of the assessment work is not to be undermined. The newer terminology is followed in Issue 2 of the method description [NAFCS-PR03], and in the current application to pumps and MOVs [NAFS-PR18, -19], but not yet implemented in the guide text.

the hypothesis-specific impact vectors $\mathbf{v}_i$:

$$\mathbf{v}_{net} = \sum_{i=1}^{N} w_i \cdot \mathbf{v}_i \qquad (3.6)$$

or equivalently for the elements

$$v_{net}(m \mid n) = \sum_{i=1}^{N} w_i \cdot v_i(m \mid n)$$

where the weights of the N hypotheses shall fulfill the following normalization

$$\sum_{i=1}^{N} w_i = 1$$

It is good practice to keep systematic track of all elements of the impact vector, and element sum for verification, even though in the statistical estimation the elements of order 0 and 1 may not be needed in certain estimation models or parametric CCF models.

The hypotheses are usually defined in the straightforward way with a separate hypothesis for each possible failure multiplicity. Only in special cases with specific causal model it may be justified to lay out the hypotheses in a more developed way. The main difficulty lies in assigning the weights for the hypotheses which has to be based on engineering judgement. It is difficult (perhaps impossible) to create exact rules for this. Some general advices were already presented in the begin of this subsection, and some more are given below. The use of physical evidence as support to impact vector construction will be discussed in Section 4.5.

As emphasized in the begin of this section, extrapolation to failure chances of those components, which were not affected according to the evidence, is not recommended. That would be a kind of extrapolation which is not the meaning with the hypothesis method in the context of normal CCF event analysis for statistical estimation purpose. Any extrapolation belongs to CCF modelling and should not be mixed with the basic CCF event analysis. Furthermore, hypotheses with small chances to higher order failure (very weak degradation) should be disregarded. The possible statistical evidence is anyway so small in such cases that it is useless for an ordinary estimation purpose but can on the other hand give a misleading picture of the pertinent dependence level. The screening will be discussed in more detail in Section 3.6.

If the weights are based on plain engineering judgment, values less than 0.1 are not generally recommended for serious use. Lower weights should be based on a model of contributing factors or relative comparison with statistically inferred reference values or probability levels.

It is quite usual that the detected failures of a CCF mechanism are distributed over consecutive TDCs (so called time-spread CCFs). In such a situation it is advisable to construct a joint (sum) impact vector covering the concerned TDCs, i.e. handle the

impact of the CCF mechanism as a whole. This extension will be discussed in Section 4.1.

Specific causal model

In complicated cases with several contributing factors the construction of a specific causal model may be advisable. This approach can be especially desired in the cases where time-dependence of the CCF mechanism is important. A practical example is presented in [T314_TrC], which uses a state model (Markov model) to describe the stochastic process of CCF detection and root cause elimination.

Use of parametric dependence model

In the complicated cases with incomplete knowledge about the contributing factors a parametric CCF model can be used to support the assessment of the conditional dependent failure probabilities for the considered CCF event [CR_ImpVe]. Compare to the cases SF11-12 in the DG Pilot [NAFCS-PR10].

3.4 Failure free cycles

The TDCs without any failures are represented by the basic impact vector:

$$\mathbf{v} = [\,1, 0, 0, \ldots, 0\,] \qquad (3.7)$$

The number of failure free cycles can be derived by subtracting the number of single failure and multiple failure cycles from the total number of demands.

3.5 Sum impact vector

The impact vectors for all TDCs are added together to derive the sum impact vector of the considered failure mode, see illustration in Table 3.2. For simplicity the failure free cycles, single failure cycles and CCF cycles are presented as lumped in this kind of summary table due to the large number of events. (The net impact vectors for each considered CCF of the DG Pilot are presented in a separate summary table, see [NAFCS-PR10, App.1].) For checking purpose it is recommended to add a column for the sum of impact vector elements on each row: the overall sum should equal to the number of TDCs. It should be noticed that Table 3.2 presents results for the pooled data of the DG GGGCs of size 4 at the Nordic NPPs, in total 12 groups, which are assumed to represent a homogeneous population. The total number of TDCs is approximated by the calculated number of test cycles, which is rounded to an integer number.

Table 3.2 Sum impact vector result of the DG pilot study for CCCG size 4 of the Nordic NPPs and lumped mission failure mode covering both failure to start and failure to run. The presented result is the mean of the base and redundant assessment results [NAFCS-PR10].

Entity	Multiplicity					
	0	1	2	3	4	Sum
Failure-free cycles	3635					3635
Single-failure cycles		190				190
CCF cycles	5.94	8.81	2.81	0.27	0.16	18
Sum impact vector	3641	198.8	2.81	0.27	0.16	3843

3.6 Screening of significant CCF cases

Because of work load it usually not worth while to include in the quantitative analysis (impact vector construction) less significant observed cases. The relative uncertainty is large and statistical gain small from the cases with small chance of actual multiple failure. It is difficult to present generally applicable criteria for what is meant by these weak degradation cases or non-significant conditional probability of multiple failure. A meaningful criterion is bound to the specific conditions of each analysis and amount of available event data. Following thumb rules can be used as basis for criteria:

1) Cases with Time Factor equal to 'Null' should be screened out, and placed into a separate category of 'Recurring Failures'. Compare to Section 4.2.
2) Cases where the component impairment values are at most 'Incipient' should be screened out, and placed into a separate category of 'Latent Degradation Cases'. Compare to Section 4.3.
3) Cases where the impairment value of only one component is 'Degraded', while all other components are in 'Incipient' or 'Working' state should also be screened out (and placed into a separate category of 'Latent Degradation Cases') except in a situation of sparse statistics, when these cases can despite of uncertainty be used to obtain some indication of the pertinent dependence.

The above types of cases are discussed in more detail in Sections 4.2-4. If the weak degradation state has been present a longer time (several TDCs or longer), a significant CCF risk can have been accumulated, see Section 4.4.

If there exists good amount of event data, then the screening threshold can be defined on numerical basis, e.g. exclude cases which would add less than one percent to the sum impact vector, considering the elements of order two or higher.

In each analysis it is important to be transparent with the applied screening criteria, and explain the used rationale in the documentation.

4. Advices for specific type cases

This chapter supplements the step-by-step instructions presented in the preceding chapter by discussing specific types of complicated cases in more details.

4.1 Time-spread component events

In many CCF event cases the failure or degradation of components is observed at separate time points. Especially, in staggered testing without rule-based additional test of the remaining components given failure the observed component events often distribute at time-separated test points. The basic advice is to consider the impact of such CCF mechanism jointly for the consecutive test cycles, during which the influence exists. Mostly the consideration of two test cycles is sufficient. It is advisable to bundle the impact vectors for the considered TDCs, because this allows more effective reasoning, e.g. the alternative hypotheses can allocate the failure chances in different ways over the TDCs. The theoretical background is presented in the method description [NAFCS-PR03], while here only a practical example is shown, see Table 4.1. The example is typical in the sense that the influence is divided over two TDCs, and described by the sum impact vector for those two TDCs (numbered in the table for simplicity as TDC1 and TDC2).

Table 3.1 Example of constructing impact vector using hypothesis method for a CCF event with influence distributed in time. This is Case SF08 of DG Pilot [NAFCS-PR10]. The fuel booster pumps failed at consecutive test cycles due to systematic maintenance error. The chance of failures to have occurred more closely in time is regarded substantial.

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.25	1			1			1
			2	1					1
2	Both components fail in TDC2	0.25	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.5	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.25	0.5	0.25	0	0	1
			2	0.25	0.5	0.25	0	0	1
Sum Impact Vector over TDCs				0.5	1	0.5	0	0	2
				Average multiplicity				1	

A good advice to handle more complex time-spread cases is drawing a time chart for the component histories showing test time points, observation time points for the degraded/failed states, maximum latent periods and time points of verified removal of the root causes. For an example, see [T314_TrC].

4.2 Recurring component events

By recurring component events are meant cases where the observed events (of the redundant components) have substantial time distance, i.e. the failed states or significantly degraded states did evidently not coexist, and no random factor is clearly present that could have synchronized the failed states with a big chance. The recurring component events certainly carry qualitatively interesting information about possible CCF mechanism but also indicate the efficiency of some defense feature which

prevents stronger time synchronization. It is generally recommended to keep the recurring component events in a separate basket, not to be contained into the essential CCF events. As a practical rule, if the component events are separated by two or more successful test, the case should be regarded recurring only. For consistency, Time Factor should be set to 'Null' for the cases with recurring component events. (This option is missing from the ICDE coding guideline, because seemingly these kinds of cases are not basically aimed to be covered at all.)

A procedure needs to be developed for handling the recurring component events, for qualitative aims, in the coming NAFCS CCF database.

4.3 Latent degradation states

Another typical type of cases which is common is the situation where some design inadequacy, component wear-out or shortcoming of the instructions is noticed, often having been present some time and relevant for the whole component group. But the problem is still identified at an early stage without any actual CCF. Often, even no severe degradation of any single component has yet occurred. Again, these cases carry qualitatively interesting information about possible CCF mechanism but at the same indicate a slow development of the mechanism in comparison to tests and/or the existence of some defense feature which prevents stronger time synchronization. Also these "weak" CCF mechanisms should be kept separate. An attempt to assess the contained CCF risk is difficult and results uncertain, and the achievable statistical gain would be marginal. As a basic rule, the threshold for statistically significant CCF mechanism would be following (compare to the discussion of screening activity in Section 3.6):

- At least one component is completely failed with coexistent incipient/degraded sates of the redundant components, or
- At least two components are substantially degraded (component impairment assessed as 'D') and degraded states have coexisted.

Similarly as for the recurring component events, a specific procedure needs to be developed also how to handle the latent degradation cases, for qualitative aims, in the coming NAFCS CCF database.

4.4 Special cases with long latent time

In certain special cases the impact of a CCF mechanism may have been present over large number of test cycles related to non-perfect extent of periodic tests, e.g. during the time between consecutive overhaul outages or from an overhaul outage up to a random actual demand. In these kinds of cases already relatively weak influence to conditional failure probability can cumulate as significant. For these cases a joint sum impact vector shall be constructed to cover all affected TDCs.

A particular additional feature for the CCF mechanisms that can stay latent for a longer time can be increasing degradation as the function of time. For the treatment of such a case, see [T314_TrC].

4.5 Connection to physical evidence

It is difficult to create exact rules for assigning values for the hypotheses used in the impact vector construction. In fact it may be detrimental to mechanize the assessment too far. As pointed out one substantial backup to the analyst is constituted by the low and high bounds to be discussed in Section 5. The net impact vector should stay within the range defined by the bounds. The rules for hypothesis weights can first of all be viable to handle similar cases on a consistent scale of assessment.

The scale of assessment should be primarily be connected to observed physical facts, for example in the following way in the case of DGs:

- The hypotheses concerning fire risk due to fuel leaks should have weights that reflect the observed size of leakage, and the variation in the leakage size across different cases
- In the cases of cooling heat exchangers degraded due to crud accumulation the assigned weights of failure states should be connected to the measured remaining heat transfer capacity and time needed for cleaning actions in relation to the available time for such actions in an actual demand.

The further stage in the utilization of the physical facts beyond supporting consistent engineering judgment over similar cases would be the creation of a specific causal model.

5. High and low bounds

The component impairment values represent conditional failure probability of each individual component of CCCG, while the impact vector represents conditional multiple failure probability. As discussed in Section 2.2, there is no one-to-one correspondence between these two entities, especially the impact vector cannot be uniquely calculated from the component impairment values. However, the impact vector and component impairment values are connected by the basic laws of probability. It is of high practical importance to notice that the component impairment values bound the impact vector in the following way:

- The assumption that component impairment values represent mutually independent conditional failure probability of the components leads to a low bound of impact vector
- The assumption of maximum depence between conditional failure probability of the components - as described by the component impairment values - leads to a high bound of impact vector

For the time-spread events the Time Factor (and for "uncertain" CCFs the Shared Cause Factor) can additionally be used in the calculation of the impact vector bounds directly based on the ICDE codes, i.e. component impairment values, Time Factor and Shared Cause Factor. For the details of the derivation procedure, see [NAFCS-PR03].

The high and low bounds of impact vector are very useful for the analyst to know as background to the specific assessment. This was clearly reinforced in the DG Pilot. Staying within the impact vector bounds assures that the assessment fulfills necessary coherence with the laws of probability. Of course, the analyst has to first confirm that he (she) agrees with the ICDE codes (for the component impairment values, Time Factor and Shared Cause Factor), or else to resolve the disagreement, e.g. by contacting the plant specialist for additional clarifications. The currently used crude scale of component impairment values and Time Factor is a drawback: in certain cases it may be advisable to use also other numeric values than 0, 0.1, 0.5 and 1 for these codes. A typical situation where more steps on the numeric scale are needed is the assessment of similar cases, where certain differences exist in the chances of actual failure and it is desired to make corresponding relative differences in the impact vectors.

6. QA and documentation

The DG Pilot used QA practices based on the American procedure [NUREG/CR-6268v1]. The cornerstone is redundant assessment of the impact vectors by two analysts. The followed practices and organization of the documentation is presented in [NAFCS-PR10, Section 1.3 and 2.3].

The missing layer still to develop is the general audit procedure to verify the coherence and sensibility of the assessments, and adequacy of the documentation. Even in other respects the QA and documentation practices need to be better formalized to assure transparency and tractability, in particular to facilitate future updating. The connections to the ICDE frame need to be taken into account.

7. Concluding remarks

The current version of this guideline is much bound to the experiences from the DG Pilot. The next applications of the impact vector assessment were made for the centrifugal pumps and motor-operated valves [NAFCS-PR18, -PR19]. The procedure developed in the course of the DG Pilot could be followed. The new applications brought up certain insights about CCF mechanisms, but these do not have direct implications for the procedure of impact vector assessment. It is expected, however, that the guideline will be upgraded during the course of further practical work to reflect the specific requests imposed by other component types.

Generic open issues requiring further consideration include procedures to handle ”weak” CCF cases such as ’recurring failures’ and ’incipient degradation states’ that are sensible to exclude from the quantitative analysis owing to small statistical gain versus large uncertainty and additional work, but carry useful information for the qualitative analysis, e.g. insights about the efficiency of CCF defences.

Another area requiring further development is the QA and documentation, as well as the linkage of the event analysis to the Nordic CCF database (including so called C Book) that is under planning.

Acknowledgements

Michael Knochenhauer made a review of the early working draft. His comments and the valuable suggestions by Jean-Pierre Bento in the course of redundant assessment greatly helped improving the guide.

References

NAFCS-PR01
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2, 31 August 2003.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 31 October 2002.

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, prepared by Tuomas Mankamo, Issue 1, 29 August 2003.

NAFCS-PR19
Impact Vector Construction to the MOVs. Topical Report NAFCS-PR19 , prepared by Tuomas Mankamo, Issue 1, 30 August 2003.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

CR_ImpVe Expressing the impact of a CCF mechanism. Work notes, Tuomas Mankamo, Avaplan Oy, 17 September 1996.

T314_TrC Mankamo, T., A pressure relief transient with pilot valve function affected by a latent CCF mechanism. Work report NKS/SIK-1(92)35, Avaplan Oy, 31 January 1994.

NUREG/CR-6268v1
Common Cause Failure Database and Analysis System: Overview. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

Abbreviations

Acronym	Description
CCCG	Common Cause Component Group
CCF	Common Cause Failure
DG	Diesel Generator
SGFP	Subgroup Failure Probability
TDC	Test/Demand Cycle
ICDE	International CCF Data Exchange
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
QA	Quality Assurance

Annex: Example cases

This annex contains following example cases taken from the DG Pilot:

Index	Unit	Year	Short description	Remarks
SF-02	OL1	1983	Fuel booster pumps, broken cotter bolt, wrong type used	Example of time-spread event affecting two TDCs
SF-08	OL2	1993	Fuel return pipes, small drop leakage in one DG and spray leak in another DG	Example of a failure mechanism that causes risk in long term operation
SF-25	R2	1997	Poor connection in the generator field circuit	Basic example, impact of the failure mechanism not completely known

Compare to the DG pilot report [NAFCS-PR10]. The presented sheets are from the base assessments.

For the definition and description of the ICDE codes and classifications, see the general coding guideline [ICDECG00], and the specific guide for DGs:

ICDECG03 ICDE Coding Guidelines for Emergency Diesel Generators.
Dale Rasmuson, Wolfgang Werner, Gunnar Johanson, 13 June 1999.

SF02: CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-18729, -18242	
C03	Failure Mode	FS	
G6	Group Size	4	
C04	Exposed Components	4	
C05	Event Description	Olkiluoto 1, plant state: power operation. Fuel booster pump failed in periodic test, because of broken cotter bolt. Wrong type was used in maintenance (train D, OL1.652P044, 83-05-18). Same occurred three weeks later at the redundant DG (train C, OL1.652P034, 83-06-12).	
C07	Event Interpretation	Substantial chance to have occurred more closely in time (at that time, test interval was 2 weeks, pairwise staggered at that time)	
C09	Root Cause	M	Maintenance
C10	Coupling Factor(s)	MP	Maintenance procedure
C11	Shared Cause Factor	H	High
C12	Corrective Action	B	Maintenance/operation practice
C14	Time Factor	M	Medium
C13	Other		
G5	Test Interval	14	days (up to May 1994)
G5-2	Test Staggering	PST	Pair-wise staggered (AC-BD)

SF02: Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	12.06.83	14	C	TI	652P034
D	18.05.83	14	C	TI	652P044

SF02: Impact Vector Construction

The events were separated by three weeks (Sub C was tested successfully once after failure in Sub D). However, owing to the character of the failure mechanism, substantial chance is considered for the possibility for failures to co-exist. Thus effective Weight = 50% is used for double failure in the impact vector construction. Compare to the procedure explained in [NAFCS-PR03, Section 4.1].

SF02: Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.25	1			1			1
			2	1					1
2	Both components fail in TDC2	0.25	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.5	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.25	0.5	0.25	0	0	1
			2	0.25	0.5	0.25	0	0	1
Sum Impact Vector over TDCs				0.5	1	0.5	0	0	2
				Average multiplicity				2	

SF08: CCF Event Description and Classification

Basic description and classifications extracted from [DGs-CCFA].

C01	Event Identifier	OL2-35442, -35456	
C03	Failure Mode	Failure to run	
G6	Group Size	4	
C04	Exposed Components	4	
C05	Event Description	Olkiluoto 2, plant state: power operation. Small drop leak of fuel return line (train D, OL2.651G401, 92-01-09) and large spray leak of fuel return line at the redundant DG one week later (train C, OL2.651G301, 92-01-16). Both detected in test.	
C07	Event Interpretation	Certain risk of leak development at 651G401 and fire in case of actual demand requiring long run (at that time, test interval was 2 weeks, pair-wise staggered, i.e. the failed state of 651G301 and incipient state of 651G401 coexisted)	
C09	Root Cause	I	Internal to component, piece part
C10	Coupling Factor(s)	EI	Environment Internal
C11	Shared Cause Factor	H	High
C12	Corrective Action	G	Fixing of component
C14	Time Factor	M	Medium
C13	Other		
G5	Test Interval	14	days (up to May 1994)
G5-2	Test Staggering	PST	Pair-wise staggered (AC-BD)

SF08: Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	16.01.92		C	TI	651G301
D	09.01.92		I	TI	651G401

SF08: Impact Vector Construction

The leak of fuel oil from the injection pipes, injection nozzles and fuel return pipes has been a generic failure mechanism at the DGs of OL1/OL2. The leaks have mostly been very small drop leakage and also typically spread over time. Compare to CCF event OL2-9965, -11411 in 1983 (DocIndex=SF01).

The failure mechanism shows apparent tendency of growing degradation as the function of start cycles and operation time. The spray leak due to broken fuel return line of aggregate 651G301 was a singular event (no recurring at the near time) in that aggregate but the fuel return line of aggregate 651G401 was affected repeatedly at the following time points within +/- one year:

91-01-09 Drop leak (incipient)

92-01-09 Drop leak (incipient), in conjunction to spray leak at 651G301 one week apart (the considered multiple event)

92-05-07 Spray leak (critical)

92-08-05 Spray leak (critical)

The fire risk in case of spray leak has to be considered significant in an actual demand with mean load running time of about 4 hours. Thus the spray leak events are classified as critical for the failure mode failure to run. The fire risk in case of a drop leak is smaller but still considerable taking also into account the possibility of leak growth during an actual load running time. Based on insights from the growth tendency that risk is assessed to be Weight = 20%, which is then used in the construction of impact vector by hypothesis method.

SF08: Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only 651G301 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
				Average multiplicity			1.2	

SF25: CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R2-RO-013/97-R0-014/97
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	At normal start test of the set, didn't the generator of DG210 generate voltage thereby failing to synchronise to the emergency diesel busbar. The diesel generator was declared not operational at 10.26 and the other three diesels were tested. Other failure was detected at DG220, at 11.28 the generator tripped on high voltage. The reactor power at detection time was 56%. The tech spec requires a cold shut down in then two DG are out of service. Allowable repair time fore one DG is 48 hours. However one hour after the second fault was detected, the first failure was found and repaired. The diesel generator (DG 210) was tested and operational at 12.05. The second DG 220 was declared operational 6 hours later. DG210 An insufficient torqued screw in a connection block in the field circuit of the generator causing poor connection. The cubicle was changed in October 1996 after a fire. Circumstances contributing to a failed control by the technician is the fact that the connection block is located lower left corner of the cubicle and the door makes the check difficult. DG220 The cause was an insufficient torqued screw in a connection block in voltage measuring circuit giving to low voltage to the voltage regulator. DG230 An insufficient torqued screw in a connection block in the protection circuit's was found during the check. No problem was detected at the earlier test run. DG240 An insufficient torqued screw in a connection block in the feed circuit for the generator magnetic field was found during the check. No problem was detected at the earlier test run. The last time the connecting blocks were opened was in 1994. The blocks are mounted horizontal and opens downwards preventing a accidental closure. In this case the plate didn't fall down. Testing showed a single block needed only half turn of the screw to open and the plate fell down. Mounted together 4 turns needed before the plate fell the friction from the nearby blocks holding the plate. The use of improper tools could have misled the operator as a wide driver give friction force against the sides of the blocks especially if not hold at a right angle to the screw. The tools were changed before the incident

		The components were connection blocks manufactured by Phoenix type RTK/S-Ben, voltage 500 V and type URTK/S-Ben, voltage 500 V. Both affected sets were tested 14 respective 7 days before detection at the next test. No other of the sixteen diesel generators at the plant have had similar problems. For other connection blocks in the unit a test programme applied for the next outage. The procedure for the check after maintenance work was not formalised at the time of the event. Written procedures of checks to do and in which cubicle was the long run corrective action.
C07	Event Interpretation	Typical misses in maintenance. Even if not the same person torqued the all blocks there is a connection in maintenance procedures, tools and connection block design. The problem with to wide a tool was identified and corrected. Maybe old tools were still in use or an ordinary screwdriver was used. One insufficient torqued connection block have survived 75 tests and the other 15 tests, when fails within 7 days. Vibration or oxidation of contact surfaces could be a contributing factor.
C09	Root Cause	H Human action
C10	Coupling Factor(s)	O Operation procedure
C11	Shared Cause Factor	H High
C12	Corrective Action	F Test and maintenance policies
C14	Time Factor	H High
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

SF25: Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	01.07.97	14	C	TI	10:08:00 AM
B	01.07.97	7	C	TU	11:28:00 AM
C	01.07.97		I	TU	
D	01.07.97		I	TU	

SF25: Impact Vector Construction

In addition to the evident double failure state there seems to have been substantial chance of the other two DGs also failing in an actual demand as it is said that vibration can be a contributing factor. The chance of higher order failure is estimated to be 20% and is divided in equal shares between triple and total failure state.

SF25: Net Impact Vector

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Degraded Trains C and D would both survive in actual demand	0.8			1			1
2.	One of the degraded trains would also fail in addition to Trains A and B	0.1				1		
3.	Both degraded trains would fail in addition to Trains A and B	0.1					1	1
Net impact vector			0	0	0.8	0.1	0.1	1
			Average multiplicity				2.3	

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
App4.4	**Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)**	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
App5.1	**Data Survey and Review PR02**	**PR02**
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR02**

Title:	**Data Survey and Review**
Author(s):	Tuomas Mankamo
Issued By:	Tuomas Mankamo
Reviewed By:	Michael Knochenhauer, 2002-10-29
Approved By:	Gunnar Johanson 2003-10-17
Abstract:	This report presents the survey and review of the international CCF data sources that are relevant and applicable for the Nordic PSA studies. It is expected that the ICDE data – including the subset of Nordic experience – will gradually satisfy to an increasing degree the CCF data needs. This survey is aimed at giving references to supplementary CCF data for such component types which are not sufficiently represented by the ICDE data. The generic CCF data are also considered, including the description of so called Generic Dependence Classes. The risk-importance of CCFs for main component types is presented using the available information about the importance measures from the Nordic PSA studies.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2001-06-05	TM
Draft 1	2001-09-25	TM
Draft 2	2001-10-31	TM
Draft for Peer Review	2002-01-12	TM
Issue 1	2003-10-10	TM

This survey was closed declaring Draft for Peer Review as final for this phase with small editorial changes only. The needed further work is summarized in the concluding chapter.

Contents

Data Survey and Review

1. Introduction

This topical report documents the survey and description of the internationally published CCF data sources that are relevant and applicable for the Nordic PSA studies.

1.1 Objectives

The primary aim is to give applicable references to find CCF data for such component types which are not sufficiently represented by the Nordic specific data. By "specific" data is meant CCF data that are based on failure statistics of the Nordic NPPs, or foreign CCF event data that is mapped to correspond to our conditions, taking into account differences in component design, testing and maintenance arrangements, physical separation and other CCF defense factors. Mapping can also mean utilization of foreign applicable CCF data as statistical prior data being combined with local statistics by using Bayesian update method. "Generic" data means using available CCF data (often average data over an observed component population) as such after checking its general adequacy for the application case.

The generic CCF data sources are pointed out, including description of the Generic Dependence Classes developed in TVO/PSA. This item can be later developed further to present more specific recommendation about generic CCF parameters, that can be for the less risk-significant component types, for which the laborious data collection is not practically feasible.

The risk-importance of CCFs for main component types is also presented in this connection using the available information about importance measures from the Nordic PSA studies. For the presentation the same unified component type list was aimed at for the description of the coverage in CCF data sources. This objective was not satisfactorily met up to this report issue due to large variability among the sources. The harmonization should be definitely needed, which is a future task.

In fact, there are desired objectives and ambitions for this kind of survey and review that are not met thus far due to resource limitations allocated to this task. Section 5 collects recommendations and suggestions for the further elaboration.

1.2 Scope

First of all the current data contents of ICDE are summarized in Section 2. The ICDE data base is regarded as preferred source of international CCF data. As complementary sources selected references are surveyed in Section 3, including the following:

- NUREG reports
- EPRI reports
- ISPRA/CCF Benchmark
- Nordic specific CCF analyses

It is unknown whether some IAEA guideline would contain some CCF data, presumably not. The generic CCF data from the USA has been quoted in the IAEA working material, see Section 4.1.

It is well acknowledged that the current coverage of references is not complete. It is expected that the review will bring up additional references worth to be considered in the continuation as well.

This task is limited to the description of data coverage with respect to component types. The statistical observation period and component-years or some corresponding exposure measure are described if readily available. In the continuation it is desired to describe the volume of data in a more consistent way when possible. The CCF events or parameter data are not reviewed nor compared (the task can be later extended in that direction if desired, e.g. for selected component types).

1.3 Terminology

It is assumed that the reader and user of this report is familiar with the basic concepts and terminology related to CCF modeling as presented in the Model Survey and Review [NAFCS-PR04]. The ICDE terminology is followed when applicable, see the general coding guideline [ICDECG00]. Annex 1 of [NAFCS-PR04] defines certain special terms, especially Subgroup Failure Probability (SGFP) entities that are being used in many places of this report in connection to data examples and comparisons. The definition of terminology is not replicated here to keep this report concise, and also in order to facilitate future updates by keeping the basic definitions only in one location of NAFCS documentation.

2. Current data coverage in ICDE

The current data contents in ICDE database is presented in Table 2.1. The data collection is going on or in planning for some further component types. The coverage regarding failure modes and different design types and/or functional positions are described in the specific ICDE coding guideline for each component type. The statistical observation times, component years and exposure, and amount of recorded events are presented in the ICDE data summary reports for the covered component types. The referred information is accessible at the ICDE Web Site.

The ICDE database is of fundamental importance. The aim is an efficient use of the ICDE data in the Nordic PSA studies. Pilot cases need to be worked out in order to draw appropriate conclusions how to proceed towards the goal. The first pilot case is in planning to consider diesel generators.

Table 2.1 Current contents of ICDE database, status in December 2001.

Component type	Canada	Finland	France	Germany	Spain	Sweden	Switzerland	United Kingdom	USA
Centrifugal pumps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Diesel generators	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Motor-operated valves	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Safety/Relief valves	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Check valves	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Batteries	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

3. Internationally published CCF data sources

This section reviews selected international CCF data sources, which can provide complementary data for special component types or failure modes. The coverage with respect to component types is shown in Table 3.1, using as starting point the similar CCF data survey prepared for TVO/PSA. Also the coverage of ICDE database is shown for comparison purpose, because gradually the ICDE data is expected to supersede many of the early CCF data compilations.

The component types are classified in Table 3.1 at a very general level with emphasis on components for which CCFs use to be risk-significant. The presented list of component types originate from the early CCF data survey for TVO/PSA. It is generally compatible with the component types covered in the references, but many references make a more refined type division, e.g. for several types of centrifugal pumps, and turbine-driven pumps handled as a separate type from motor-driven pumps. Besides, data are presented in most cases separately for the different failure modes that are specific to component type. The contents of the sources will be discussed in more details in the following subsections.

The insights from the survey of risk-importance by the CCFs presented in Annex show that the coverage is generally incomplete for the measurement and instrumentation components, and also for certain important component types in the electrical power supply systems. It should also be noticed that in the Nordic BWRs the AFW pumps are reciprocating (piston) pumps, which are not covered in the CCF data sources. Collecting local Nordic CCF data and/or mapping of CCF data from other more usual pump types is needed for this specific pump design.

It must be admitted that the coverage of the references in this report version is not as complete as it could be (should be). Besides, the evaluation of the uses could be (should be) more systematic. See recommendations in Section 5 in these regards.

3.1 CCF Database of US NRC

The US NRC has developed a CCF database that (initially) covers operating experiences from 1980 through 1995 at the US BWR and PWR plants. The database collection and analysis procedures are described in detail in multi-volume report [NUREG/CR-6268]. The derived CCF data are presented in [NUREG/CR-5497]. The development started before the establishment of ICDE and has substantially contributed to the build-up of ICDE. The QA program of the USNRC database is comprehensive. The published information gives a good description of the data gathering and treatment procedures. The presented data summaries seem as a viable source of generic CCF data. Naturally, many details such as description, classification and impact vector construction of individual CCF events is accessible only through the database. The database and associated computer program are proprietary information.

Table 3.1 Map of the coverage for CCF data in international sources. For comparison purpose the first source column represents ICDE database, compare to Table 2.1

Component type category	Sources					
Centrifugal pump	I	U	S	E	B	
Reciprocating pump						
Reciprocating compressor						
Screw compressor						
Air operated valve		U	S			
Check valve	I	U			B	
Manual valve						
Motor operated valve	I	U	S	E	B	N
Regulating, motor operated valve						
Safety/relief valve	I	U		E		N
Heat exchanger		U				
Strainer		U				
Battery	I	U				
Switchgear breaker ≥ 0.6 kVAC		U				
Switchgear breaker < 0.6 kVAC		U		E		
Diesel generator	I	U	S	E		N
Rotating DC/AC converter						
Relay			S			
Measurement and instrumentation			S			
Control rods and drives			S			N

Sources

I	ICDE
U	US NRC CCF Database
S	US NRC Special Reliability Studies
E	EPRI/PLG
B	ISPRA/CCF Benchmark
N	Nordic Special CCF Data Analyses

The data input is combined from plant event data in Licensee Event Reports and component event data in Nuclear Plant Reliability Data System. The contents of the (initial) database can be characterized by the following information:

- Number of component types 11
- CCCG Types 42
- CCCG Sets 97
- CCF events 1′533
- complete CCF events 235
- Independent count, about 12′000

"CCCG Type" means groups of components of same type in same plant system and in same reactor type (in some cases data of BWR and PWR are pooled, however, together for same component type and similar system). "CCCG Set" means a subset of CCCG Type for a particular failure mode, i.e. CCCG Set is a population of CCCGs that can be assumed mutually homogeneous with same failure mode so that data can be pooled together (requires mapping up/down to handle different group sizes). It is told that test interval is recorded for the CCCGs but not with what accuracy, and not how the eventual differences in test interval are treated in data pooling. It is similarly unclear how the differences in test staggering are treated in data pooling.

The independent count is for so called "independent" component events (not part of a CCF event). It is gathered in parallel to CCF events from the same sources, i.e. data should be compatible in this sense. Unfortunately, component and group exposure time, and number of component demands and Test and Demand Cycles (TDCs) are not given. (That information can be obtained for those CCCG Sets that are stored in ICDE database.) The total independent count is about 12'000. Consequently, the ratio of CCF events to independent count is above 10%, which is rather high. The overall high dependence level of US CCF data is also discussed in connection to generic CCF data in Section 4.

As said, using CCCG Set as the basic population item for presenting the CCF data summaries in [NUREG/CR-5497] means pooling over different CCCG sizes that requires mapping up/down. Based on the report contents alone it is impossible to control if the homogeneity assumption is reasonable for pooling, e.g. low redundancy CCCGs may be typical for older plant generations with generally weaker physical segregation and other CCF defense measures. Besides, upwards mapping is controversial extrapolation as is discussed in more detail in [NAFCS-PR03]. The parameter value for the conditional failure probability given a non-lethal shock, which is the key parameter used in upwards mapping, is not presented. Altogether, the possible heterogeneity across different CCCG sizes can add substantial uncertainty to average data.

Report [NUREG/CR-5497] contains a subsection for each CCCG Type describing the main attributes, e.g. component boundary, redundancy configuration in the concerned (typical) system and definition of the covered failure modes. The data are then presented in aggregated form for the failure modes separately (CCCG Sets), and

mapped up/down for various CCCG sizes, typically in range from 2 through 6. The following data entities are presented:

- Sum impact vectors; independent count is presented separately and is also adjusted according to CCCG size
- Alpha Factors (maximum likelihood estimators)
- MGL parameters (maximum likelihood estimators)
- Uncertainty distributions of Alpha Factors, including calculated mean values

Basically, the database is intended to be used by the database program developed for the purpose, giving full access to the details such as event specific impact vectors and narrative event descriptions. Using the data summaries alone imposes many limitations as pointed out. It would be very useful to make some comparative evaluations with those components types for which the data are contained in ICDE database to better understand the uses and limitation of the data summaries as a source of generic data.

3.2 Special reliability studies by US NRC

US NRC has published several reliability studies on specific systems, containing also CCF data that provide valuable supplementary information to the CCF database (discussed in Section 3.1). The most noticeable sources are following:

- Auxiliary/Emergency feedwater systems of PWRs [NUREG/CR-5500, vol.1]
- Diesel generators [INEL-95/0035]
- Reactor protection systems, including control rods and drives [NUREG/CR-5500, vol.2 and vol.3]

It is of definitive interest to consider these sources for comparison aims when developing the Nordic CCF database.

3.3 EPRI reports

The more recent CCF data efforts by EPRI are not published in open domain. (The proprietary data has been utilized, for example, in Loviisa/PSA.) The earlier published EPRI report [EPRI-NP 3967] is taken into Table 3.2. It is still of methodological interest, presenting an important milestone in the development of CCF data analysis.

3.4 CCF Benchmark

The CCF Benchmark [CCF-Benchmark] organized by ISPRA in the mid of 80'ies is of course outdated for the contained data. It is still of interest as providing useful background to the techniques, which are since then further developed and established in practical use.

3.5 Nordic CCF data analysis

The Nordic research and development projects include following special CCF data analysis:

- Motor operated valves [NKA/RAS-470]
- Safety/relief valves (BWRs) [SKI TR-91:6]
- Diesel generators [RPC 91-57]
- Reactor shutdown systems, especially control rods and drives (BWRs) [SKI/R96:77]

These studies are characterized by in-depth analysis of operating experience events. Much emphasis has been placed on the qualitative analysis and CCF defense aspects.

The Nordic PSA studies cover known CCF events for some other component types but not based on systematic data collection and analysis. The project SUPER-ASAR presented recommendations on the CCF parameters for use in the Swedish PSA studies. It would be of interest to discuss the relevance of those recommendations as all Swedish PSA studies currently make reference to SUPER-ASAR.

3.6 Other sources

There are published many reports and conference articles that address CCF data, especially in United Kingdom, Germany, France and Spain. As reference sources the most suitable may be published PSA studies, e.g. the German PSAs of the reference BWR [SWR-PSA] and PWR. For the time being those sources are being superseded by ICDE data but can nevertheless be useful in certain cases for comparison aims, possibly also as supplementary source data. For example, the planned NAFCS pilot case for the diesel generators can review the CCF parameters used in the German and French PSA studies for the diesel generators with the same manufacturer as in the Nordic NPPs besides of utilizing the all ICDE event data for the concerned design populations.

4. Generic CCF data

This section will discuss generic CCF data, primarily generic Alpha Factors from the NUREG reports. In addition the Generic Dependence Classes are presented as defined and used in TVO/PSA.

4.1 Generic Alpha Factors

The earlier US reference [NUREG/CR-5801] proposes the generic Alpha Factors of Table 4.1. The same proposal migrated to an earlier version of IAEA guide [IAEA-CCF-DA] and several PSA studies in the mid of 90'ies.

Table 4.1 Generic Alpha Factors proposed in [NUREG/CR-5801].

CCCG size n	$\alpha(1,n)$	$\alpha(2,n)$	$\alpha(3,n)$	$\alpha(3,n)$
4	0.950	0.035	0.010	0.005
3	0.950	0.040	0.010	
2	0.950	0.050		

Generic Alpha Factors, which are based on more recent CCF experience of US NPPs are presented in [NUREG/CR-5485] and also in the current version of [IAEA-CCF-DA], see Table 4.2.

Table 4.2 Generic Alpha Factors (mean of the generic prior distributions) presented in [NUREG/CR-5485].

CCCG size n	$\alpha(1,n)$	$\alpha(2,n)$	$\alpha(3,n)$	$\alpha(3,n)$
4	0.950	0.021	0.010	0.019
3	0.950	0.024	0.026	
2	0.953	0.047		

It is difficult to compare the value of Alpha Factors. Therefore, the parameters of some other CCF models are presented in the numeric part of Figs.4.1-2 corresponding to the Alpha Factors of Tables 4.1-2, respectively. The presented CCF models are following, compare to the model descriptions in [NAFCS-PR04]:

- Primitive dependence parameters $z_k = P_k / P_{k-1}$, where P_k denotes the probability of specific k components, i.e. $P_k = Psg(k|n)$
- Multiple Greek Letter (MGL) model: parameters beta, gamma and delta
- SHACAM parameters y_k: these parameters are defined as the conditional probability of specific k components failing due to CCF given that specific k-1 components have failed due to CCF; this model is similar to MGL model and Alpha Factors but it has the benefit that the parameters y_k are subgroup-invariant in practical approximations [SHACAM]

For the comparison purpose a typical value of 1E-3 is used for the total single failure probability P_1. This is especially needed in order to generate SGFP entities, which are presented on the left hand side in the numeric part of Figs.4.1-2. Transformations are

HiDep/Version 2.3
CCF Parameter Scale Down, 22 Sep 00

This execution sheet is used to calculate for given Alpha Factors and P1 the corresponding SGFP entities and dependence parameters, in each CCCG size 4..2

P1 1.00E-3 is given — Generic Alpha Factors from NUREG/CR-5801

	P1 Q(1|n) peg(1|n) pes(1|n) pts(1|n)	P2 Q(2|n) peg(2|n) pes(2|n) pts(2|n)	P3 Q(3|n) peg(3|n) pes(3|n) pts(3|n)	P4 Q(4|n) peg(4|n) pes(4|n) pts(4|n)	 alpha1 alphat	z2 beta y2 alpha2	z3 gamma y3 alpha3	z4 delta y4 alpha4
CCCG4	1.00E-3	6.02E-5	2.81E-5	1.87E-5		0.060	0.467	0.666
	8.88E-4	2.18E-5	9.35E-6	1.87E-5		0.112	0.417	0.400
	8.85E-4	2.27E-5	9.40E-6	1.87E-5		0.059	0.474	0.667
	3.54E-3	1.36E-4	3.76E-5	1.87E-5	0.950	0.035	0.010	0.005
	3.73E-3	1.92E-4	5.63E-5	1.87E-5	1.070			
CCCG3	1.00E-3	6.70E-5	2.84E-5			0.067	0.424	
	8.96E-4	3.77E-5	2.83E-5			0.104	0.273	
	8.94E-4	3.86E-5	2.84E-5			0.066	0.429	
	2.68E-3	1.16E-4	2.84E-5		0.950	0.040	0.010	
	2.83E-3	1.44E-4	2.84E-5		1.060			
CCCG2	1.00E-3	9.62E-5				0.096		
	9.05E-4	9.52E-5				0.095		
	9.04E-4	9.62E-5				0.095		
	1.81E-3	9.62E-5			0.950	0.050		
	1.90E-3	9.62E-5			1.050			

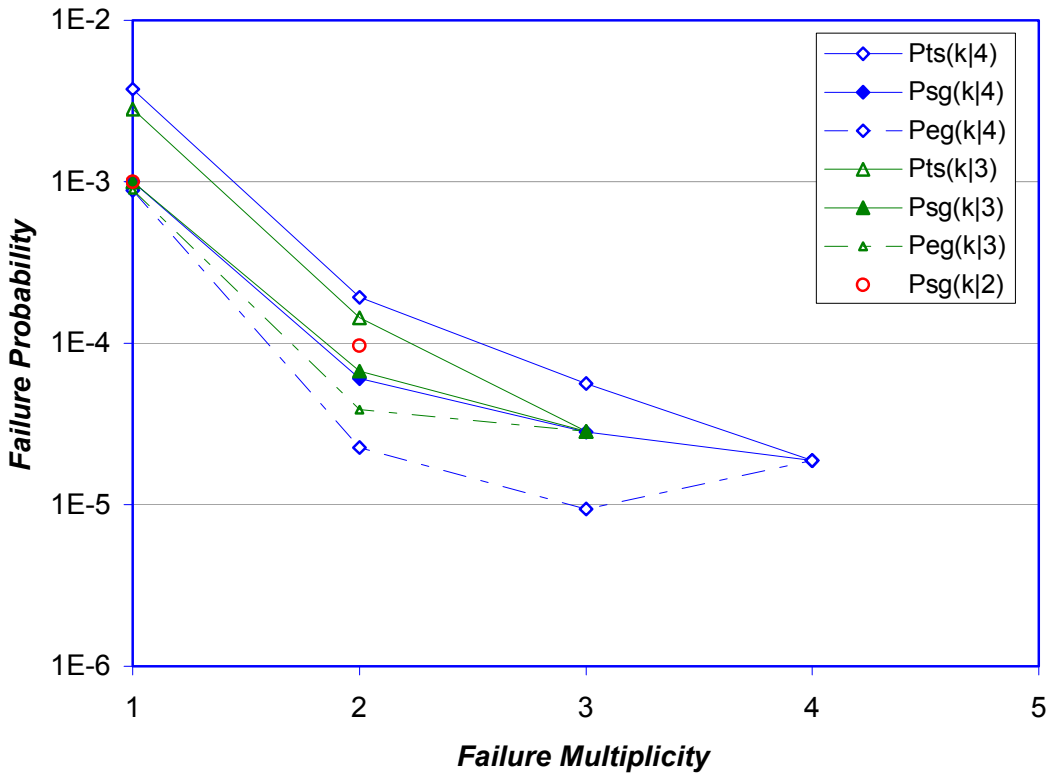


Figure 4.1 Comparison of CCF parameters and SGFP entities in case of the Alpha Factors presented in [NUREG/CR-5801].

HiDep/Version 2.3
CCF Parameter Scale Down, 22 Sep 00

This execution sheet is used to calculate for given Alpha Factors and P1 the corresponding SGFP entities and dependence parameters, in each CCCG size 4..2

P1 1.00E-3 is given — Generic Alpha Factors from NUREG/CR-5485

	P1 Q(1|n) peg(1|n) pes(1|n) pts(1|n)	P2 Q(2|n) peg(2|n) pes(2|n) pts(2|n)	P3 Q(3|n) peg(3|n) pes(3|n) pts(3|n)	P4 Q(4|n) peg(4|n) pes(4|n) pts(4|n)	 alpha1 alphat	z2 beta y2 alpha2	z3 gamma y3 alpha3	z4 delta y4 alpha4
CCCG4	1.00E-3	1.01E-4	7.84E-5	6.93E-5		0.101	0.775	0.883
	8.65E-4	1.28E-5	9.11E-6	6.92E-5		0.135	0.716	0.717
	8.62E-4	1.37E-5	9.14E-6	6.93E-5		0.100	0.782	0.884
	3.45E-3	8.19E-5	3.65E-5	6.93E-5	0.950	0.021	0.010	0.019
	3.64E-3	1.88E-4	1.06E-4	6.93E-5	1.098			
CCCG3	1.00E-3	9.58E-5	7.26E-5			0.096	0.757	
	8.83E-4	2.23E-5	7.25E-5			0.117	0.619	
	8.81E-4	2.32E-5	7.26E-5			0.095	0.765	
	2.64E-3	6.97E-5	7.26E-5		0.950	0.024	0.026	
	2.79E-3	1.42E-4	7.26E-5		1.076			
CCCG2	1.00E-3	9.08E-5				0.091		
	9.10E-4	8.98E-5				0.090		
	9.09E-4	9.08E-5				0.090		
	1.82E-3	9.08E-5			0.953	0.047		
	1.91E-3	9.08E-5			1.047			

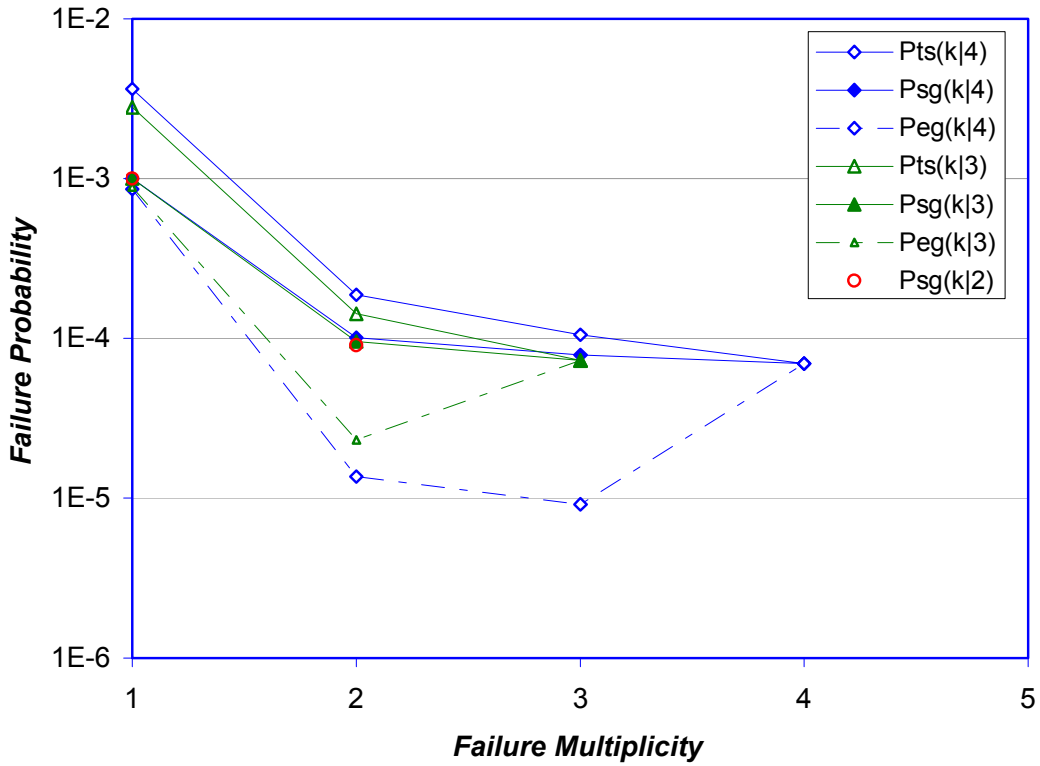


Figure 4.2 Comparison of CCF parameters and SGFP entities in case of the Alpha Factors presented in [NUREG/CR-5485].

done in the following order, see more detailed explanations in Ref.[NAFCS-PR04]:

$$\{ P_1, alfa_k \} \rightarrow \{ Q_k \} \rightarrow \{ P_k \} \rightarrow \{ z_k \}$$
$$\rightarrow \{ Peg(k|n), Pes(k|n), Pts(k|n) \}$$
$$\rightarrow \{ y_k \}$$
$$\rightarrow \{ beta, gamma, delta \} \quad (4.1$$

The CCF parameters here are connected to the probability of CCF basic events Q(k|n) defined in the original way. The recent NUREG reports connect Alpha Factors to Peg(k|n) entities. The difference is, however, more theoretical, because Peg(k|n) and Q(k|n) use to be close to each other.

The following observations can be drawn when comparing the CCF parameters and different SGFP entities:

- The earlier version of the generic Alpha Factors, Fig.4.1, show up non-homogeneous across different CCCG sizes. Especially, the dependence level for double failures (k=2) is about twice as strong for CCCG of size n=2 in comparison to CCCGs of size n=3 and n=4. This can be inferred from the comparison of P_2 (subgroup-invariant per definition) or y_2^n (approximately subgroup-invariant).
- The more recent version of the generic Alpha Factors, Fig.4.2, is reasonably homogeneous across different CCCG sizes, which can be explained by the more consistent combined treatment of CCF experience data from CCCGs of different size – as it is described in [NUREG/CR-5485] – using mapping down and mapping up procedures.
- The more recent version of the generic Alpha Factors, Fig.4.2, represents stronger dependence level at failure multiplicity k=3 and k=4 than earlier generic values. In fact, the dependence is so strong that it is close to a cut-off assumption – or Beta Factor model with Beta ≅ 0.1

The comparisons yield some significant controversies. The earlier generic Alpha Factors for CCCG of size n=2 seem pessimistic as that corresponds to Beta Factor of about 10%. Such a high dependence can be relevant with lack of physical separation and low defence against CCFs in general, and/or with sequential testing. For the larger groups the earlier generic Alpha Factors seem sensible.

The more recent generic Alpha Factors are in overall pessimistic. A tentative explanation is that the averages are biased by outlier components with extra-ordinary high dependence (to be checked). Besides, there is a slight tendency of increasing dependence level for increasing CCCG size (compare values of y_2^n and y_3^n as the function of n). This may be caused by a pessimistic mapping up (extrapolation) of the event data from the small CCCGs. Compare to the discussion of this issue in [NAFCS-PR03].

Due to the controversies a careful position should be taken towards the generic Alpha Factors from US sources. A viable approach can be built on further developing the concept of Generic Dependence Classes, which will be discussed in the following section.

4.2 Generic Dependence Classes

The background to the definition of Generic Dependence Classes (GDCs) was the fact that CCF data of sufficient quality could be found in the open literature only for some main component types for the TVO/PSA in the end of 80'ies. For the remaining component types the generic data were utilized. In order to avoid too strong coupling with the single failure probability, which has often been criticized, generic CCF parameters were assessed specifically in three different classes GDC1 - GDC3 according to the single failure probability's order of magnitude, Fig.4.3. The variable notation is same as discussed in Section 4.1, compare also to Figs.4.1-2.

The CCF parameters of GDCs were chosen in such a way that the failure probability of order four should remain above 10^{-5} in all cases. GDC0 was added later; it is used only for one CCCG, namely switch-over automation equipment of 6.6 kV buses.

For comparison, the earlier generic US data for the Alpha Factors in CCCG of size 4 [NUREG/CR-5801] are also shown in Fig.4.3. For comparison purpose a generic single failure probability $P_1 = 10^{-3}$ is assumed for this case similarly as in Section 4.1, when generating Table/Fig.4.1. It can be concluded, that the US generic data are rather close to GDC2 (this comparison in fact is the behind of using $P_1 = 10^{-3}$ also here). Only the assessment of relative dependence at order 4 is somewhat more pessimistic in the US generic data.

In Fig.4.4 GDC2 is scaled down from n=4 to n=3 and 2 in order to make comparison also to the earlier generic US data for the Alpha Factors in CCCG of size 3 and 2 [NUREG/CR-5801]. The scale-down procedure is equivalent to so called mapping down, which is described in [NAFCS-PR03]. The comparison shows rather good compatibility except the significant difference for $\alpha(2,2)$, see Table/Fig.4.1, which is – as already said – not compatible with the dependence level for the CCCG sizes of n=3 and 4. In fact $\alpha(2,2)=0.050$ corresponds to Beta=10%, see the numeric part of Table/Fig.4.1.

Due to the controversies in the generic Alpha Factors from the US sources it is suggested that the concept of GDCs is further developed. The recommended parameter values should be refined by using the up-to-date information that is applicable to the Nordic NPPs. Furthermore, the coupling between the total single failure probability and dependence level should be investigated in more detail. It is expected that the currently available data can help to understand this coupling better than it was possible in the original definition of GDCs. At that time, i.e. end of 80'ies, a certain coupling could be inferred but on the other hand the probability of higher order failures seemed to generally saturate above or at the level of 10^{-5}. Further attributes that can be connected to GDCs are test interval and staggering, and other CCF defense factors. Based on cumulating insights more practical instructions can be presented in these regards for more specific use of GDCs.

Generic Dependence Classes							
	P1 Q1 alfa1	P2 Q2 alfa2	P3 Q3 alfa3	P4 Q4 alfa4	z2 y2 beta	z3 y3 gamma	z4 y4 delta
GDC0	2.00E-2 1.92E-2 9.80E-1	7.00E-4 2.56E-4 1.96E-2	5.88E-5 9.58E-6 4.89E-4	2.70E-5 2.53E-5 3.23E-4	0.035 0.015 0.041	0.084 0.12 0.07	0.46 0.73 0.47
GDC1	1.00E-2 9.78E-3 9.90E-1	2.00E-4 5.33E-5 8.10E-3	4.00E-5 9.55E-6 9.66E-4	2.80E-5 2.76E-5 6.98E-4	0.020 0.010 0.022	0.20 0.37 0.26	0.70 0.74 0.49
GDC2	1.00E-3 8.97E-4 9.52E-1	5.00E-5 2.52E-5 4.00E-2	2.00E-5 3.93E-6 4.17E-3	1.60E-5 1.60E-5 4.24E-3	0.050 0.049 0.103	0.40 0.41 0.27	0.80 0.80 0.58
GDC3	1.00E-4 6.94E-5 8.59E-1	2.00E-5 4.59E-6 8.52E-2	1.40E-5 1.40E-6 1.73E-2	1.26E-5 1.26E-5 3.90E-2	0.200 0.200 0.306	0.70 0.70 0.55	0.90 0.90 0.75
US Generic	1.00E-3 9.11E-4 9.50E-1	4.45E-5 2.24E-5 3.50E-2	2.02E-5 9.59E-7 1.00E-3	1.92E-5 1.92E-5 5.00E-3	0.044 0.043 0.089	0.45 0.46 0.25	0.95 0.95 0.87

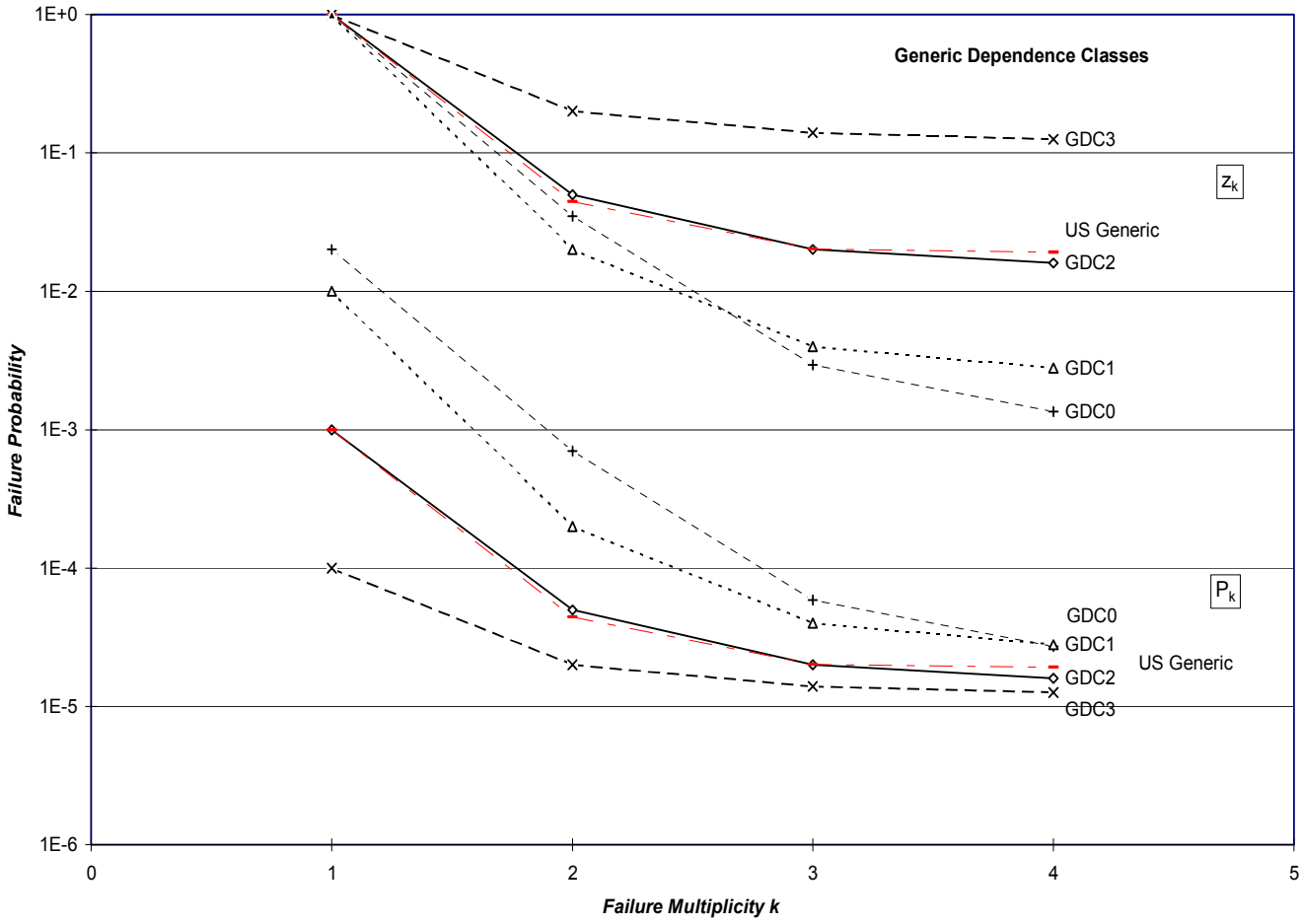


Figure 4.3 Generic Dependence Classes (GDCs) as defined in [Olkiluoto-PSA].

This execution sheet is used to calculate for given Pk-values the corresponding SGFP entities and dependence parameters, scaled from CCCG size of 4 down to 3 and 2.

OL1/OL2 PSA, Generic Dependence Class II

Pk	P1	P2	P3	P4		z2	z3	z4
psg(k|n)	1.00E-3	5.00E-5	2.00E-5	1.60E-5		0.05	0.4	0.8
	Q(1|n)	Q(2|n)	Q(3|n)	Q(4|n)		beta	gamma	delta
	peg(1|n)	peg(2|n)	peg(3|n)	peg(4|n)		y2	y3	y4
	pes(1|n)	pes(2|n)	pes(3|n)	pes(4|n)	alpha1	alpha2	alpha3	alpha4
	pts(1|n)	pts(2|n)	pts(3|n)	pts(4|n)	alphat			
CCCG4	8.97E-4	2.52E-5	3.93E-6	1.60E-5		0.103	0.269	0.576
	8.94E-4	2.60E-5	4.00E-6	1.60E-5		0.049	0.406	0.803
	3.58E-3	1.56E-4	1.60E-5	1.60E-5	0.952	0.040	0.0042	0.0042
	3.76E-3	1.88E-4	3.20E-5	1.60E-5	1.061			
CCCG3	9.22E-4	2.91E-5	1.99E-5			0.078	0.255	
	9.20E-4	3.00E-5	2.00E-5			0.049	0.406	
	2.76E-3	9.00E-5	2.00E-5		0.963	0.030	0.0069	
	2.87E-3	1.10E-4	2.00E-5		1.044			
CCCG2	9.51E-4	4.90E-5				0.049		
	9.50E-4	5.00E-5				0.049		
	1.90E-3	5.00E-5			0.975	0.025		
	1.95E-3	5.00E-5			1.025			

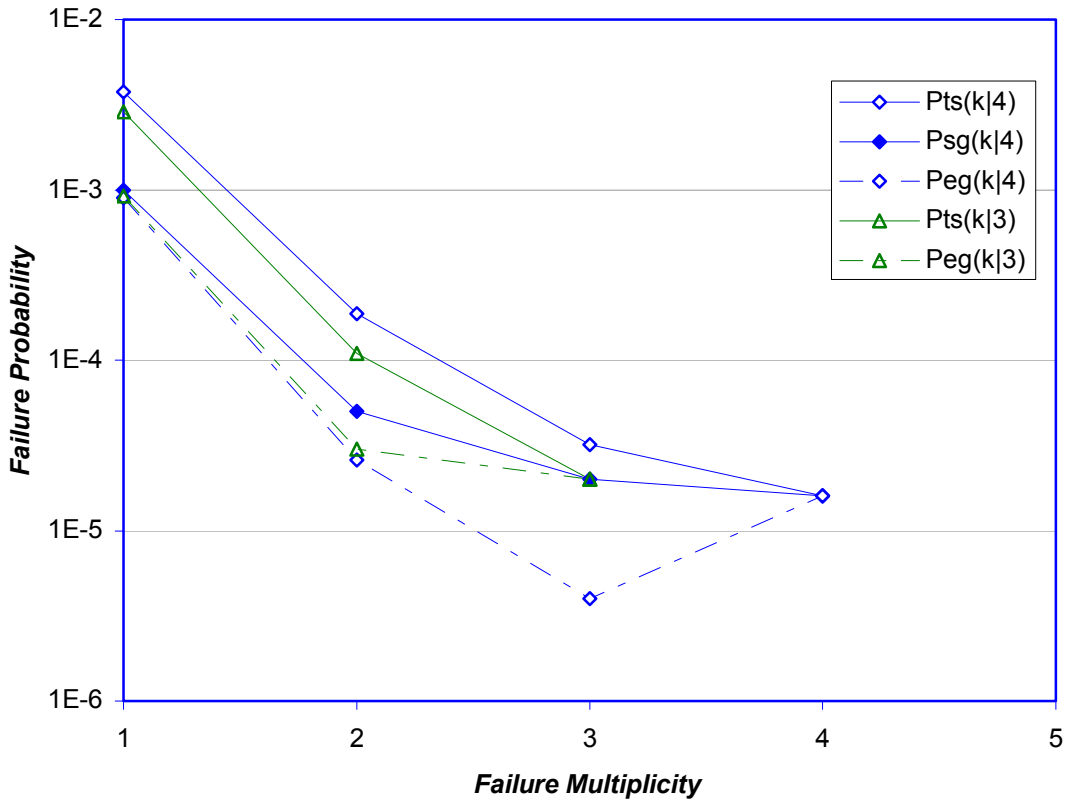


Figure 4.4 CCF parameters and SGFP entities for Generic Dependence Class II [Olkiluoto-PSA]. Typical value 1E-3 of P1 is assumed

5. Perspective of CCF data development

The principal conclusions from this survey are following:

- Many CCF data compilations were made in the 80'ies and form the basis of the CCF parameters currently used in the PSA studies. They are becoming gradually superseded by component-type specific CCF data – such as collected in ICDE database – that better reflect the operating experience and actual conditions including CCF defense measures. The early CCF data compilations can still be useful for comparison and back-up purpose
- The general order of preference among CCF data sources is following:
  1. ICDE data, mapped to the conditions in the Nordic NPPs as far as possible
  2. Component-type specific CCF analysis such as made for the BWR safety/relief valves and control rods/drives
  3. Generic Dependence Classes for the components outside the coverage of the above two sources

It is expected that the ICDE data – including the subset of Nordic experience – will gradually grow in coverage and satisfy to an increasing degree the CCF data needs. Meanwhile, supplementary data are needed for quite many component types. It is recommended that this inventory of CCF data sources is kept up to date in order to help the PSA practitioners. It is also proposed that the generic CCF parameters are further developed by using the concept of Generic Dependence Classes to fill the data needs for special component types and less risk-significant components when the laborious CCF data collection is not reasonable. At the best, the generic CCF data recommendations by NAFCS should reflect the specific conditions at the Nordic NPPs, e.g. physical separation, in-service testing and maintenance arrangements.

This survey presented also a snapshot of risk-importance measures for leading CCF component groups and for selected BWR units. It is recommended to supplement the importance presentations for the other BWR generations of former ASEA Atom design, possibly also for the PWRs in Loviisa and Ringhals.

The recommended and proposed development items for this CCF data survey and review are summarized in Table 5.1.

It has to be emphasized that the detailed system and component specific CCF analyses will have an important role also in the long run. They provide valuable background information about the important contributing factors and conditions, that are reduced in the formalized database information. Such a detailed information will facilitate transferring CCF data from one context to another and is indispensable for dedicated applications such as the analysis and development of in-service testing arrangements. The update of the earlier Nordic CCF analysis of control rods/drives (BWRs) is in fact under planning [NAFCS-PR09].

The ambition level originally defined for this survey and review of CCF data turned out low in comparison to the practical needs and interests as reflected by the comments thus far. More effort is hence recommended to be allocated to supplement this work keeping the focus on the data requirements of the Nordic PSA studies.

Table 5.1 Summary of the recommendations and proposal to further development of this CCF data survey and review (priority is left open for the discussions in the next NAFCS meeting).

#	Item	Priority
1	The current contents of ICDE database should be described and evaluated in more detail with respect to the uses as event data source for the Nordic PSA studies	
2	Comparative in-depth evaluation of the recent CCF data compilation published by USNRC [NUREG/CR-5497]	
3	Review of the further CCF data references, including the SUPER-ASAR which recommended CCF parameters for the Swedish PSA studies	
4	Harmonization of component types to be used in the presentation of CCF data coverage and risk-importance of CCFs, and to facilitate comparisons across different data sources	
5	Development of the Generic Dependence Class concept with shaping factors to reflect test interval and staggering, and other CCF defense measures. Investigation of the correlation between single failure probability and dependence level.	
6	Further compilation of the risk-importance measure information to cover the older and newer Nordic BWR generations, possibly also the Nordic PWRs. Identification and prioritization of the CCF data needs that are common to the Nordic PSA studies.	
7	Survey and review of applicable CCF data sources for the following types of components, that are generally risk-significant according to the Nordic PSA studies : – measurement and instrumentation components – components in electrical power supply systems (except diesel generators for which abundance of CCF data are available) – reciprocating (piston) pumps used in BWR AFW system These component types are characterized by high reliability and/or small population in the Nordic NPPs, thus the local CCF experience is limited if any	

Acknowledgements

The help by Jari Pesonen, TVO, Stefan Pohlred, Forsmark, and Michael Landelius and Fritiof Schwartz, OKG, is acknowledged in providing the information about the risk-importance of CCF groups, being presented in Annex.

The NAFCS members have given valuable contribution in conducting this task through the discussions and comments. Especially the thorough comments by Michael Knochenhauer on the last working draft are acknowledged.

References

NAFCS-Programme-R1
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR03 Impact Vector Method. Prepared by T. Mankamo, Issue 2, 31 August 2003.

NAFCS-PR04 Model Survey and Review. Prepared by T. Mankamo, Issue 1, 10 October 2003.

NAFCS-PR09 Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs – Survey Task Report. Topical Report NAFCS-PR09, prepared by Tuomas Mankamo, Issue 2, 08 January 2002.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

NUREG/CR-5801
Procedures for Analysis of CCFs in PRA. Prepared by .. for USNRC, SAND91-7087, April 1993.

NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

NUREG/CR-5497
CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998

NUREG/CR-5500v1
Reliability Study: Auxiliary/Emergency Feedwater System, 1987-1995. Prepared by J.P.Polowski, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.1., August 1998.

NUREG/CR-5500v2
Reliability Study: Westinghouse Reactor Protection System, 1984-1995. Prepared by S.A.Eide, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.2., April 1999.

NUREG/CR-5500v3
Reliability Study: General Electric Reactor Protection System, 1984-1995. Prepared by S.A.Eide, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.3., February 1999.

NUREG/CR-6268v1
Common Cause Failure Database and Analysis System: Overview. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

NUREG/CR-6268v2
Common Cause Failure Database and Analysis System: Event

Definition and Classification. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.2., June 1998.

NUREG/CR-6268v3
Common Cause Failure Database and Analysis System: Data Collection and Event Coding. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.3., June 1998.

NUREG/CR-6268v4
Common Cause Failure Database and Analysis System: CCF Software Reference Manual. Prepared by K.J. Kvarfrdt, M.J. Cebull, S.T. Wood and A.Mosleh. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

INEL-95/0035
Emergency Diesel Generator Power System Reliability 1987-1993. Prepared By G.M. Grant, et.al., February 1996.

IAEA-CCF-DA
Procedure for CCF Data Analysis in PSA. IAEA-J4-97-CT-1002, Working Draft, March 1998

Olkiluoto-PSA
PSA of Olkiluoto 1 and 2. Teollisuuden Voima Oy.

F1/F2-PSA PSA of Forsmark 1 and 2. Forsmarks Kraftgrupp AB.

O2-PSA PSA of Oskarshamn 2. OKG Aktiebolag.

HR_CCFRe
High redundancy structures, CCF models review. Work report prepared by Mankamo, T., Avaplan Oy, 31 December 1990. A companion document to SKI TR-91:6.

SHACAM Mankamo, T., SHACAM, Shared Cause Model of Dependences - A review of the Multiple Greek Letter Method and a modified extension of the Beta-factor Method. Avaplan Oy, 28 March 1985.

NKA/RAS-470
Hirschberg, S. (Ed.), Dependencies, human interactions and uncertainties in PSA. Final Report of the NKA/RAS-470 project, NORD 1990:57 (1990).

SKI TR-91:6 Mankamo, T., Björe, S. & Olsson, L., CCF analysis of high redundancy systems, SRV data analysis and reference BWR application. Technical report SKI TR-91:6, Swedish Nuclear Power Inspectorate, 1991.

SKI/R96:77 Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Summary report, prepared by T. Mankamo. SKI Report 96:77, December 1996.

SKI/RA-26/96
CCF Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Work reports, prepared by T. Mankamo. SKI/RA-26/96, December 1996.

RPC 91-57 Defences against CCFs and generation of CCF data, pilot study for DGs, quantitative analysis. Staffan Björe, ABB Atom AB, Report RPC 91-57, 15 October 1991

EPRI-NP 3967
Classification and Analysis of Reactor Operating Experience Involving Dependent Events. Prepared by K.N. Fleming and A. Mosleh, PLG 1985.

CCF-Benchmark
Common Cause Failure Benchmark Exercise. Prepared by A. Poucet, A. Amendola and P.C. Cacciabue, ISPRA, November 1986.

SWR-PSA SWR - Sicherheitsanalyse, Abschlussbericht, Teil 1. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-102/1, Juni 1993 (in German).

Abbreviations

Acronym	Description
CCCG	Common Cause Component Group
CCF	Common Cause Failure
GDC	Generic Dependence Class
SGFP	Subgroup Failure Probability
TDC	Test and Demand Cycles
AFM	Alpha Factor Method
CLM	Common Load Model
MGLM	Multiple Greek Letter Method
AOV	Air Operated Valve
BWR	Boiling Water Reactor
DG	Diesel Generator
MOV	Motor Operated Valve
PWR	Pressurized Water Reactor
SRV	Safety/Relief Valve
IAEA	International Atomic Energy Authority
ICDE	International CCF Data Exchange
EPRI	Electric Power Research Institute
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate
USNRC	United States Nuclear Regulatory Commission

Annex: Risk-importance of CCFs for main component types

The need for accurate CCF data naturally correlates with the risk-importance of the CCCG. For less important component groups it is easier to accept the use of generic or crude CCF data. The importance measures for CCCGs (aggregated over CCCG Types, i.e. subset of CCCGs of the same general component type) are presented in the following cases:

- Tables A.1-2 using TVO PSA results [Olkiluoto-PSA]
- Tables A.3-4 using Forsmark 1/2 PSA results [F1/F2-PSA]
- Tables A.5-6 using Oskarshamn 2 PSA results [O2-PSA]

The two primary importance measures are used:

- Fractional Risk Contribution (Fussel-Vesely Importance)
- Risk Increase Factor (Risk Achievement Worth)

In the case of Oskarshamn 2 the importance measures for a CCCG Type are calculated using the basic definitions. In the other cases they are derived from the standard importance measure output for basic events in the following way - for the Fractional Risk Contribution C_X:

$$C_{Type(k)} = \sum_{CCCG_i \in Type(k)} \sum_{CCCBE_{ij} \in CCCG_i} C_{CCBE_{ij}} \qquad (A.1)$$

and for the Risk Increase Factor A_X:

$$A_{Type(k)} = 1 + \sum_{CCCG_i \in Type(k)} \sum_{CCCBE_{ij} \in CCCG_i} \left(A_{CCBE_{ij}} - 1 \right) \qquad (A.2)$$

I.e. summing is done over all Common Cause Basic Events (CCBEs) for the CCCGs that belong to the given Type(k). The above equations are approximations assuming that the concerned CCBEs are present in disjoint MCSs. In practice some CCBEs can be present in joint MCSs which means that the above equation make some overestimation (thus on conservative side). The approximations are acceptable for the general ranking of CCCGs regarding data needs.

The two importance measures give a different perspective to the risk-importance: in Tables A.1, 3 and 5 the CCCG Types are sorted for descending Fractional Risk Contribution, and in Table A.2, 4 and 6 for descending Risk Increase Factor (in the latter case the factors are charted on logarithmic scale for a better resolution). It is seen that the relative order is drastically different for Risk Increase Factor as compared to Fractional Risk Contribution. As in other ranking based on importance measures, it is recommended to consider Fractional Risk Contribution and Risk Increase Factor in parallel. In particular, the uncertainty in CCF data can bias the relative order as represented by Fractional Risk Contribution. Hence, it is essential to consider Risk Increase Factor by side.

It can also be noticed that the CCCG Type importance gets quite different for the different plants. It is not subject of this survey to explore possible explanations (such as the different cover of plant operational states and initiating event categories, e.g. the presented results of TVO PSA cover power operation state with internal initiating events, fires, floods and external hazards, and refueling shutdown with internal initiating events and fires). The evident conclusion is simply that the different PSA studies do have specific priorities about the needs for more accurate CCF data.

It has to be emphasized that this kind of information should be used by an order of magnitude resolution. Looking backward, how the risk-importance of CCCGs has lived, for example, in TVO PSA, shows rather substantial variations connected to PSA extensions, model improvements and data updates as well as system modifications and modernization changes of the plant.

The BWR units covered in the presentation of CCCG importance are all mid-generation BWRs of former ASEA Atom design. It is recommended to supplement this compilation of the risk-importance measure information to cover the older and newer Nordic BWR generations, possibly also the Nordic PWRs. This would facilitate more consistent identification and prioritization of the CCF data needs that are common to the Nordic PSA studies. The component types used for the presentation of importance measures should be harmonized, to be compatible also with the survey of CCF data sources. Besides, some cross-checking for the integrity of the results should be performed, e.g. it is strange that in the current compilation the safety/relief valves and control rods/drives are only present in the results of TVO PSA but missing for Forsmark 1/2 PSA and Oskarshamn 2 PSA?

Table A.1 Risk importance of CCCGs according to the Olkiluoto PSA, sorted with respect to Fractional Risk Contribution.

CCCG Type	Fractional Risk Contribution	Risk Increase Factor
Centrifugal pumps	14.8%	12500
Load sequencing (684)	8.58%	6490
DGs	7.97%	1350
Batteries	6.45%	7450
SRV	3.79%	60000
Lev.meas/imp.pipes	3.56%	112000
Relays	2.11%	253000
Heat Exchangers	1.43%	6860
Check valves	1.11%	11600
354-Scram system	0.97%	297
MOVs	0.71%	277
Main Feedwater (445)	0.71%	1
327- Piston pumps	0.51%	45
Control rods (221/222)	0.18%	1670
649 (313-drives)	0.10%	2
Breakers	0.04%	1129
516-limit value switches	0.020%	17.9
Switchover automation	0.009%	6.47
Screw pumps	0.005%	2.83
POVs	0.002%	1.24
Compressors	0.001%	1.87
CPU-hardware	0.001%	1.20

PSA Rev.330

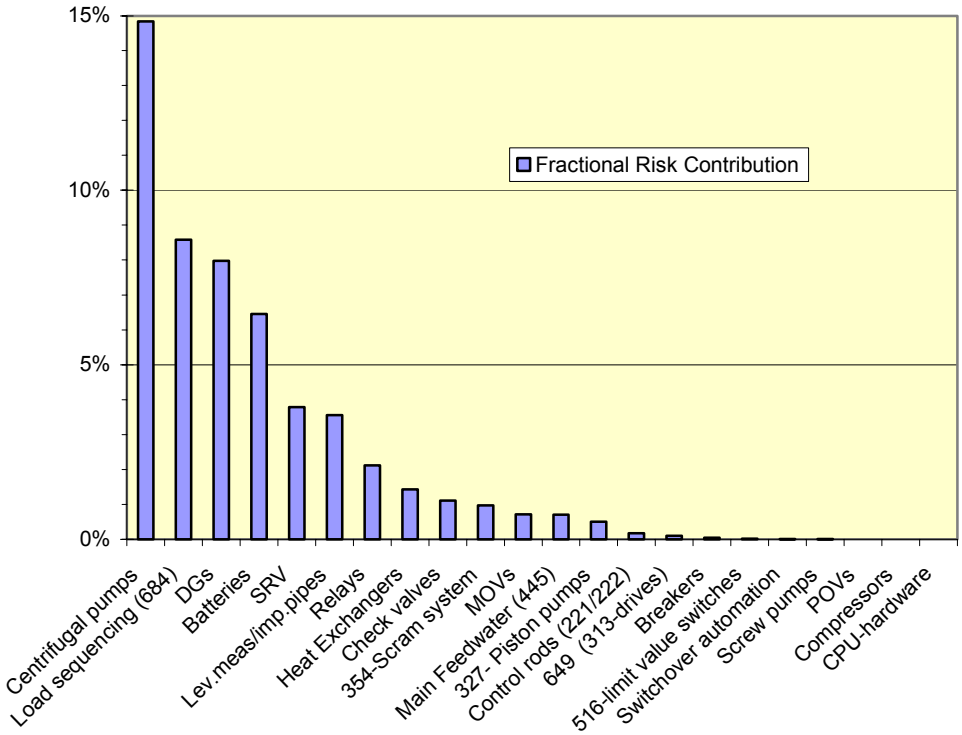


Table A.2 Risk importance of CCCGs according to the Olkiluoto PSA, sorted with respect to Risk Increase Factor.

CCCG Type	Risk Increase Factor	Fractional Risk Contribution
Relays	253000	2.11%
Lev.meas/imp.pipes	112000	3.56%
SRV	60000	3.79%
Centrifugal pumps	12500	14.8%
Check valves	11600	1.11%
Batteries	7450	6.45%
Heat Exchangers	6860	1.43%
Load sequencing (684)	6490	8.58%
Control rods (221/222)	1670	0.18%
DGs	1350	7.97%
Breakers	1129	0.045%
354-Scram system	297	0.97%
MOVs	277	0.71%
327- Piston pumps	45	0.51%
516-limit value switches	17.9	0.020%
Switchover automation	6.47	0.009%
Screw pumps	2.83	0.005%
Compressors	1.87	0.001%
649 (313-drives)	1.79	0.10%
POVs	1.24	0.002%
Main Feedwater (445)	1.23	0.71%
CPU-hardware	1.20	0.001%

PSA Rev.330

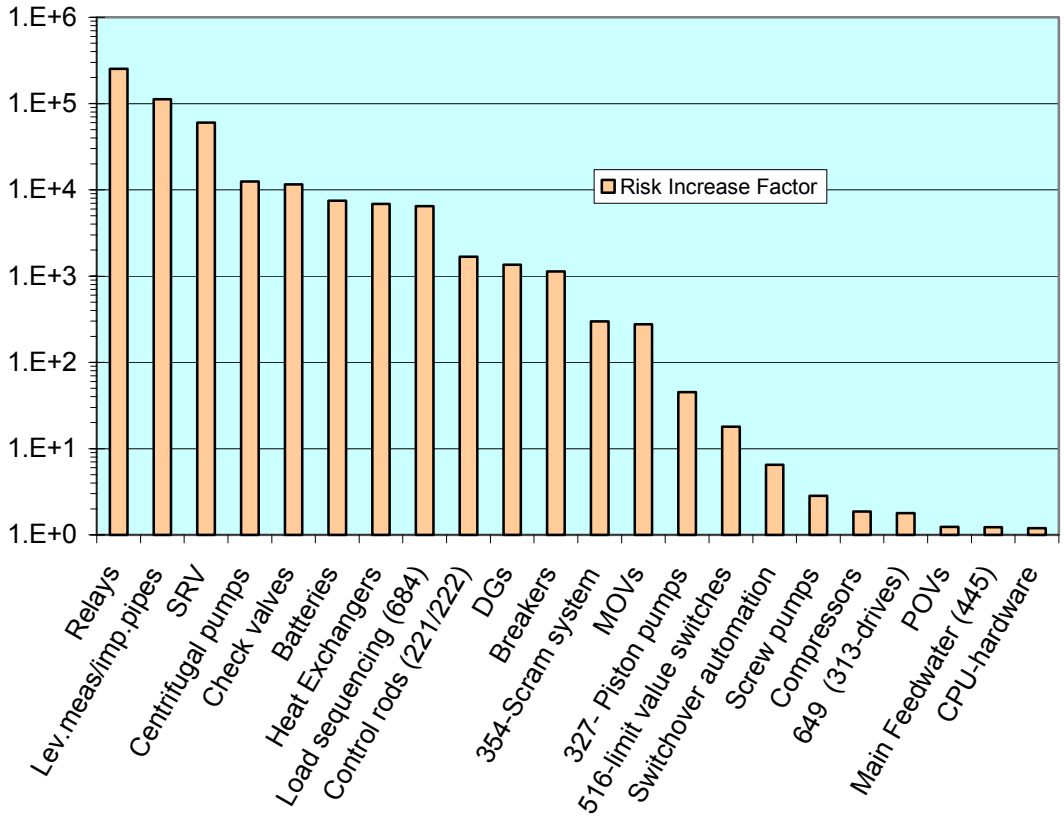


Table A.3 Risk importance of CCCGs according to the Forsmark 1/2 PSA, sorted with respect to Fractional Risk Contribution.

CCCG Type	Fractional Risk Contribution	Risk Increase Factor
Relays	15.5%	7643
516 limit value switches	11.5%	40607
327 - piston pumps	7.1%	2644
Diesel generators	2.6%	1637
Batteries & rectifiers	1.3%	6308
Centrifugal pumps	0.37%	391
Lev. meas/imp. pipes	0.36%	8.5
Reactor pressure vessel	0.33%	451
Check valves	0.25%	67
Main transformer	0.21%	15
Main feedwater	0.079%	1.1
Sprinkling system for containment	0.040%	23
Ventilation system	0.017%	84
Heat exchangers	0.004%	1.02
Switchover automation	0.002%	2.77
Steam system	0.002%	1.03

Stefan Pohlred, Forsmarks Kraftgrupp AB, 10 December 2001

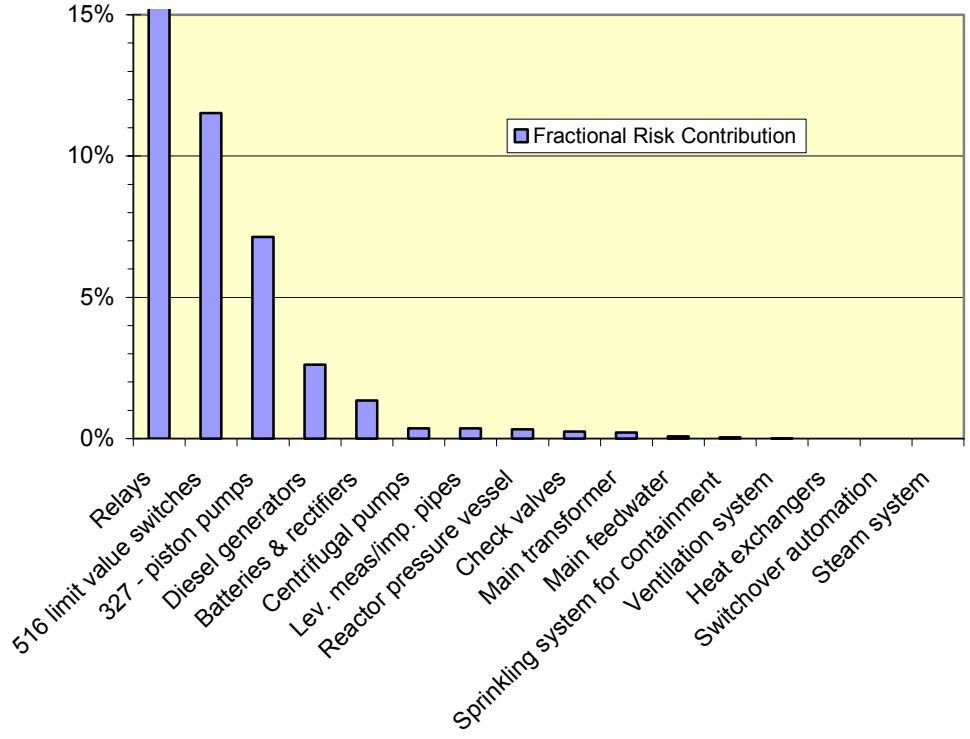


Table A.4 Risk importance of CCCGs according to the Forsmark 1/2 PSA, sorted with respect to Risk Increase Factor.

CCCG Type	Risk Increase Factor	Fractional Risk Contribution
516 limit value switches	40607	11.5%
Relays	7643	15.5%
Batteries & rectifiers	6308	1.3%
327 - piston pumps	2644	7.1%
Diesel generators	1637	2.6%
Reactor pressure vessel	451	0.33%
Centrifugal pumps	391	0.37%
Ventilation system	84	0.017%
Check valves	67	0.25%
Sprinkling system for containment	23	0.040%
Main transformer	15	0.21%
Lev. meas/imp. pipes	8.5	0.36%
Switchover automation	2.8	0.002%
Main feedwater	1.1	0.079%
Steam system	1.03	0.002%
Heat exchangers	1.02	0.004%

Stefan Pohlred, Forsmarks Kraftgrupp AB, 10 December 2001

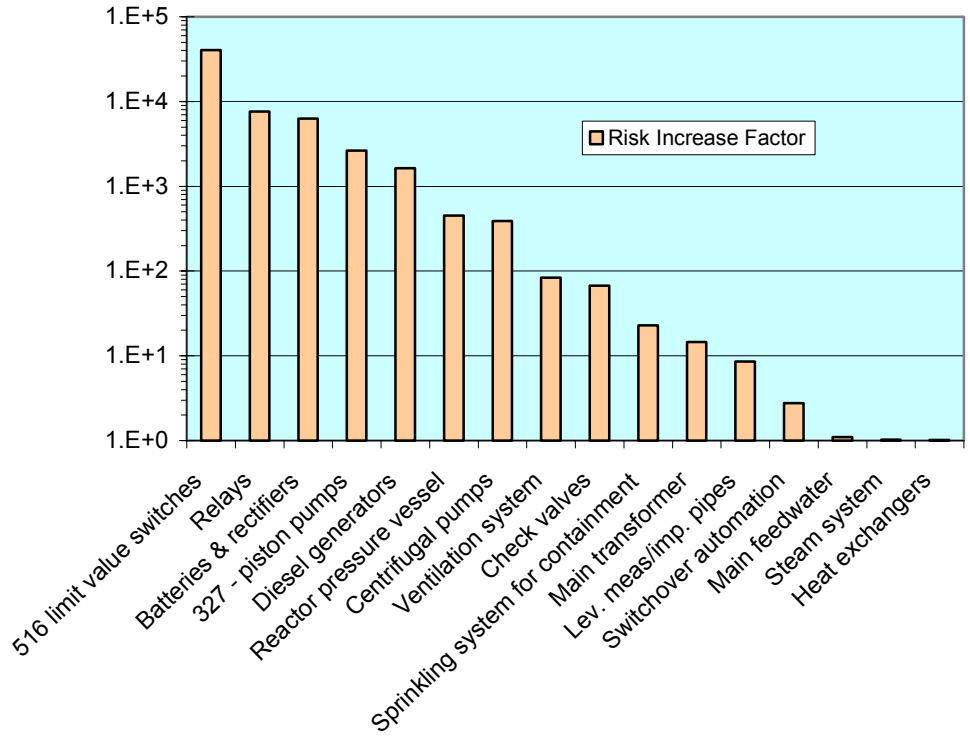


Table A.5 Risk importance of CCCGs according to the Oskarshamn 2 PSA, sorted with respect to Fractional Risk Contribution.

CCCG Type	Fractional Risk Contribution	Risk Increase Factor
Gas Turbines	38.2%	5.4
Check Valves	7.62%	6870
Breakers	3.86%	27400
Batteries	3.64%	3340
Centrigugal pumps	2.89%	484
Air Operated Valves	1.58%	33
Diesel Generators	1.01%	3.3
Transformers	0.91%	4160
Motor Operated Valves	0.76%	431
Level Indication	0.001%	2.0

PSA-O2 modell A0137, 07 December 2001

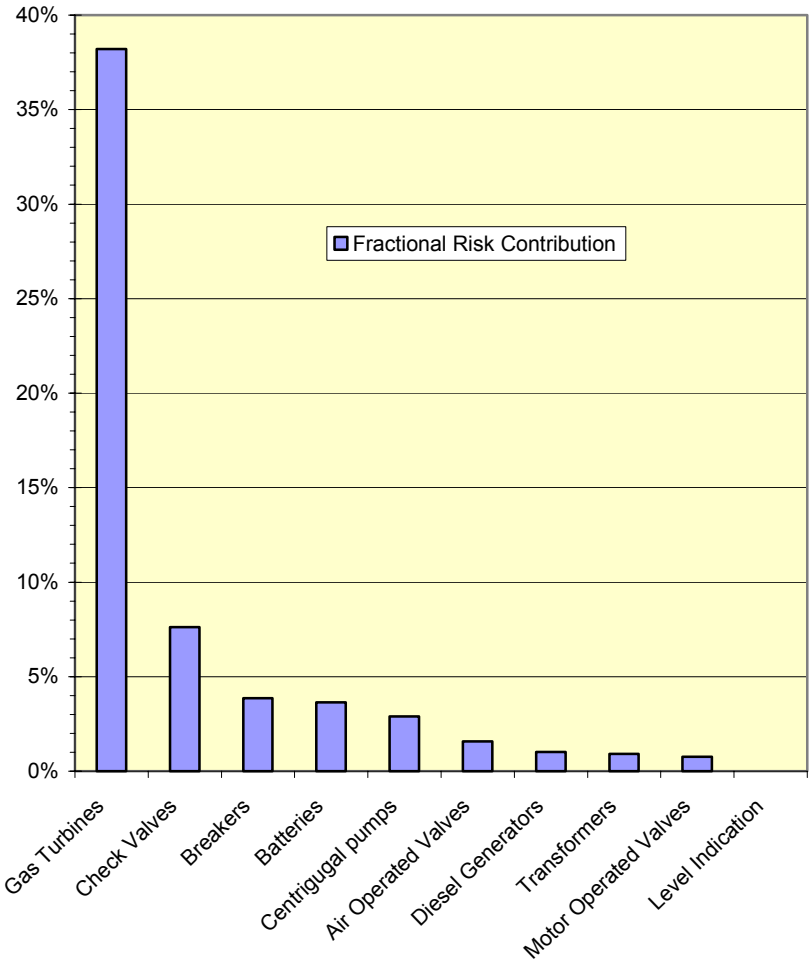
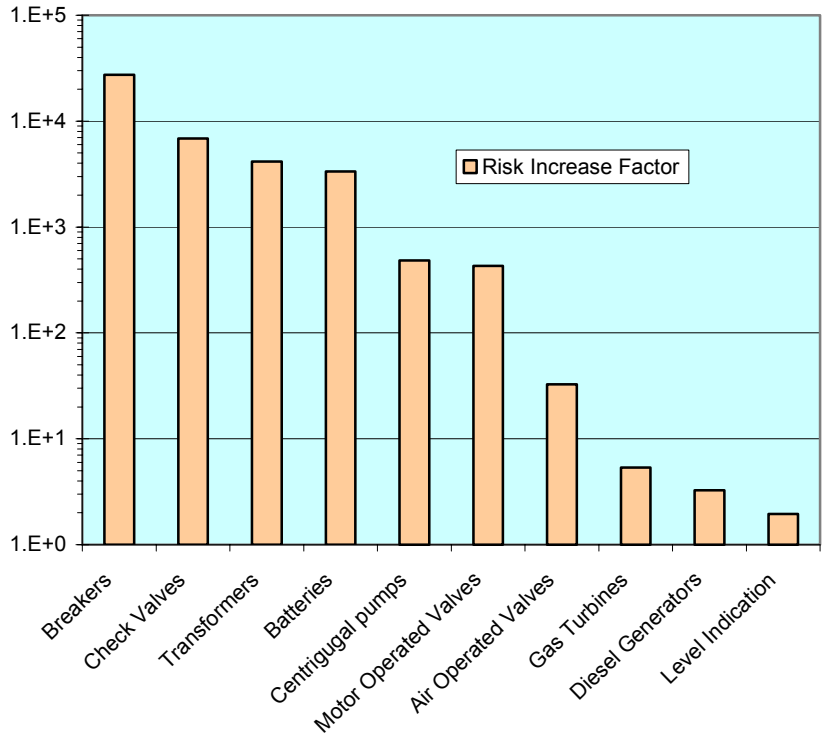


Table A.6 Risk importance of CCCGs according to the Oskarshamn 2 PSA, sorted with respect to Risk Increase Factor.

CCCG Type	Risk Increase Factor	Fractional Risk Contribution
Breakers	27400	3.9%
Check Valves	6870	7.6%
Transformers	4160	0.91%
Batteries	3340	3.6%
Centrigugal pumps	484	2.9%
Motor Operated Valves	431	0.76%
Air Operated Valves	33	1.6%
Gas Turbines	5.4	38.2%
Diesel Generators	3.3	1.0%
Level Indication	2.0	0.001%

PSA-O2 modell A0137, 07 December 2001



Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
App5.2	**Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11**	**PR11**
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title:	Data survey and review of the ICDE-database for Swedish emergency diesel generators
Author(s):	*Jean-Pierre Bento, JPB Consulting AB*
Issued By:	*Jean-Pierre Bento, JPB Consulting AB*
Reviewed By:	Per Hellström
Approved By:	Gunnar Johanson

Abstract: This report presents a quality control of the ICDE-database for the emergency diesel generators in the Swedish nuclear power plants. The survey covers events reported into the ICDE-database for the years 1994 – 1997, and is based on a comparison of the data points in the ICDE- and MTO-databases (Man – Technology – Organisation). The survey has been complemented by a review of the Swedish operating experiences for the years 1998 – 2001.

The review has identified a significant number of additional events for diesel generators fulfilling the ICDE criteria for CCF and interesting events. The results thus suggest that the ICDE-database should be updated consequently.

The report summarizes insights gained during the course of the study concerning interpretation of events and utilised coding factors. The report also presents recommendations based on these insights.

Finally, this report refers to NAFCS-PR08 “Qualitative analysis of the ICDE-database for Swedish emergency diesel generators”.

Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
A1	2002-04-30	JPB

List of Content

List of Tables

List of Figures

1. Introduction

The purpose of this report is to provide insights from a quality control of the ICDE-database based on a review of CCF events in the Swedish emergency diesel generators. The review has included a comparison of the ICDE- and the MTO-databases, and the study objectives are found in section 2.

Section 3 presents shortly the structure and specificities of the MTO-database utilised in this review.

Section 4 presents results of the quantitative comparison of the data points in the ICDE- and MTO-databases completed with data points describing hardware CCF events. The section also presents the coding of the component impairment vector for all the identified events.

Section 5 provides recommendations and comments based on insights gained during the course of the study.

2. Study objectives

The main objectives of the data survey and review of the ICDE-database for the emergency diesel generators in the Swedish nuclear power plants are:

- Quality control of the content of the ICDE-database based on a comparison of the data points in the ICDE- and MTO-databases, including an assessment of the utilised classification categories.
- Presentation and classification of data points eventually not already included in the ICDE-database.
- Formulation of recommendations based on insights gained from the review of the data points.

3. MTO-database

For informative purposes the MTO-database[1] is shortly presented below.

All Licensee Event Reports (LERs) and scrams reported to the Swedish Nuclear Power Inspectorate (SKI) are since many years reviewed from an MTO-perspective (Man – Technology – Organisation). One specific feature of the review is that the events are also assessed from a CCF point of view.

The event reports are screened independently, presently with a quarterly frequency. For some plants, all MTO-related events have been classified after discussions with plant specialists. For other plants these discussions have taken place on a case by case basis. For some events, the classification is based on exhaustive event investigations performed by the staff of the involved unit/plant or by external specialists.

[1] The so called MTO-database is maintained by JPB Consulting AB.

After review the events caused by weaknesses in the interaction MTO are classified and entered into the MTO-database. The event reports entered into this database pertain only to events within the plant and its organisation, including contractors. This means that events relating to conditions at, for example, a valve manufacturing company are normally not further analysed, except for those cases where the plant QA-programme reasonably should have identified the deficiencies.

The structure of the MTO-database is built on a classification at two levels of the event contributing factors. The first level is defined as the overall causal category level, exemplified by "Plant management & organisation", "Work organisation", "Work practice", etc. The second level is defined as the root cause level, exemplified for "Work organisation" by "Deficient planning", "Staffing with deficient training/ competence", "Deficient operability readiness control (Driftklarhetsverifiering, DKV)", etc.

The structure of the MTO-database encompasses also the event consequences for the involved components/systems, etc. This allows for the classification of CCF related to MTO-deficiencies.

The MTO-database structure has presently 11 MTO causal categories and about 70 MTO root cause categories. More than 1200 events are classified in the database, and slightly more than 440 of these exhibit a CCF character.

4. Data survey and review

4.1 Quantitative comparison of the data points in the ICDE- and MTO-databases

The ICDE-database presently covers the years 1986 – 1997 and contains 15 data points related to CCF in emergency diesel generators in the Swedish nuclear power plants. Four of the data points cover two LERs each. The ICDE-database contains five data points for the years 1994 – 1997 (the data point for year 1997 relates to two events occurred the same day).

The present survey of operating experiences identifies, for years 1994 – 1997, 12 CCF events according to ICDE definition based on test interval, out of 14 CCF events for years 1994 – 2001.

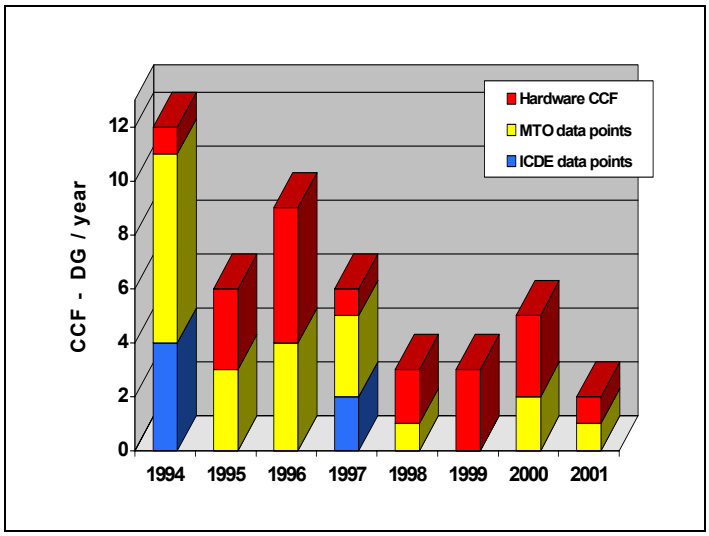
The equivalent figures for the MTO-database are 23 data points for the years 1994 – 1997, out of 27 data points for the years 1994 – 2001. For the years 1994 – 1997, the data points in the MTO-database include the five data points in the ICDE-database.

In addition to the MTO-related CCF events, the review has identified 10 data points related to hardware deficiencies in emergency diesel generators for the years 1994 - 1997, out of 19 data points for the years 1994 – 2001.

Several of the additional data points related to MTO and hardware deficiencies have been identified based on the corrective actions taken at the plants subsequent to the

occurred events, in accordance with the coding guidelines for emergency diesel generators, ICDECG03. These general results are presented in figure 1.

Figure 1: Comparison of CCF data points (LERs) for diesel generators (DG) in the Swedish nuclear power plants according to the ICDE- and MTO-databases.*

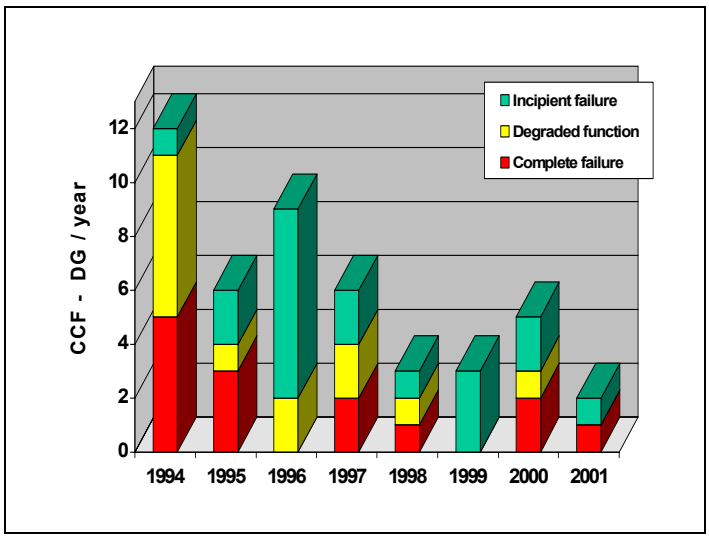


* For years 1994 and 1997, the data points in the MTO-database include the data points in the ICDE-database.

Figure 1 indicates a noteworthy discrepancy, for years 1994 – 1997, between the content of the ICDE-database and the plant experiences encompassing both MTO-and hardware related CCF events. This discrepancy is discussed in section 5.

The data points in Figure 1 have been further analysed with regard to the impairment of the component function. The result is presented in Figure 2.

Figure 2: CCF events and impairment of the component function.*



* Complete failure means that at least one component belonging to the component group failed to fulfil its function. Mention has hereby to be made that none of the data points in Figures 1 and 2 corresponds to a complete failure having occurred during a real start or running demand of an emergency diesel generator.

4.2 Repartition of the CCF events among the Swedish units

The identified CCF events in the Swedish emergency diesel generators have been listed for each unit in Table 1. The spread of the repartition obtained is worth to notice, namely three units have not experienced any CCF event, meanwhile Ringhals 2 has experienced 15 CCF events during the eight years considered in this study.

Table 1: Repartition of CCF events among the Swedish nuclear power plants.

Unit	**Diesel Manufacturer**	**Number of DG units**	**Number of CCF events for years**				**Total number of CCF events**
			1994 - 1997		**1998 - 2001**		
			MTO	H*	MTO	H*	
Barsebäck 1 (closed 2000)	MTU	2					0
Barsebäck 2	MTU	2					0
Forsmark 1	SACM	4			1		1
Forsmark 2	SACM	4		2		1	3
Forsmark 3	NOHAB	4		1			1
Oskarshamn 1	MTU	2	3				3
Oskarshamn 2	MTU	2					0
Oskarshamn 3	NOHAB	4	4	1		2	7
Ringhals 1	SACM	4	1	1	2	2	6
Ringhals 2	SACM	4	9	4		2	15
Ringhals 3	NOHAB	4	3		1	1	5
Ringhals 4	NOHAB	4	3	1		1	5
TOTAL			**23**	**10**	**4**	**9**	**46**

* H, abbreviation for hardware failure

The figures in Table 1 are further discussed in section 5.

4.3 Qualitative comparison of the data points in the ICDE- and MTO-databases

The data points included in Figures 1 and 2 are specifically presented in Table 2 below. The identification of CCF events has been made according to the general ICDE coding guidelines (ICDECG00, Revision 4, 2000-10-19) and to the coding guidelines for emergency diesel generators (ICDECG03, Draft 2, 1999-01-13). Considering the latter, special attention has been devoted to # 4 and #5 of the section "Coding rules and exceptions".

In addition to the data points presently included in the ICDE-database (the shadowed lines in Table 2), the CCF events for years 1994 - 1997 identified within the present review have been discussed with representatives from the Swedish utilities. A consensus thus exists about the content of Table 2 for years 1994 – 1997.

The table contains both MTO-related and hardware CCF events. For clarity, a column is also provided for the classification of CCF events identified based on corrective actions taken after the events by the plants on several or all other group components. The component impairment vector is, because of its importance for PSA applications, also included in Table 2.

Table 2: CCF events related to emergency diesel generators in the Swedish nuclear power plants (1994 – 2001) according to the ICDE-database and to the present study.

LER	Title	ICDE CCF[1)]	ICDE CCF[2)]	MTO CCF	T [3)] CCF	Component Impairment Vector [4)]
R3-RO-01/06	DG340 not ready for operation due to leakage in the internal cooling system				X	W W C W
R3-RO-01/16	Fuel transport pumps removed from operation for repair of external leakage		X	X		I I I I
F1-RO-00/10	Low level in DG reserve fuel tank due to wrong level indication		X	X		I I I I
F2-RO-00/09	DG220 power limitation		X		X	I C I I
O3-RO-00/03	DGB not ready for operation during periodical testing (see O3-RO-99/17) (“Interesting Event”)				X	I D I I
R1-RO-00/17	Fuel supply for DG110-DG140 not operational	X		X		I I I I
R2-RO-00/02	DG230 start blocked due to deficient lubrication oil gauge		X		X	I C I I
O3-RO-99/17	DGB not ready for operation (see O3-RO-00/03) (“Interesting Event”)		X		X	I C I I
R1-RO-99/15	DG130 external fuel leak from injection pipe to cylinder 9				X	C I I I
R4-RO-99/12	DG440 not ready for operation due to faulty connection breaker		X		X	I I I C
R1-RO-98/51	Fire alarm system for DG130 not operational due to blocked fire detectors	X		X		W W I W
R1-RO-98/55	DG110 external leak on cooling pipe to turbo-engine		X		X	D I I I
R2-RO-98/06	DG240 broken crankshaft bearing		X		X	I I I C
F2-RO-97/03	Redundant pump for filling the day tanks of DG 210-240 shut down for repair				X	I I I I
R1-RO-97/08	Incorrect setting of level alarms on the reserve fuel tank for the DGs	X		X		I I I I
R2-RO-97/13	DG210 does not increase voltage (970701)	O		X		C C I I
R2-RO-97/14	DG220 stops on high voltage (970701)	O		X		C C I I
R4-RO-97/18	DG440 not operational due to low setting of load limit		X	X		I I I D
R4-RO-97/56	Weakened DG440 due to faulty mechanical parts		X	X		I I I D
F3-RO-96/24	DG310: loose starting air valve on cylinder 3		X		X	I I C I
O3-RO-96/02	653 DGA not operational due to activated over speed protection (see O3-RO-96/06, 96/11) (“Interesting Event”)		X	X		C W W I
O3-RO-96/06	653 DGA not operational due to activated over speed protection (see O3-RO-96/02, 96/11) (“Interesting Event”)		X		X	C W W I
O3-RO-96/11	653 DGD stopped during test on over speed protection (see O3-RO-96/02, 96/06) (“Interesting Event”)		X	X		W W W C
R1-RO-96/22	DG120 stopped on over speed protection due to faulty over speed gauge		X		X	I C I I
R2-RO-96/02	DG230 activated over speed protection due to burned contacts in the generator start magnetic circuit		X		X	I C I I
R2-RO-96/14	DG220 external leak in fuel pipe (960531)		X	X		I D I I

LER	Title	ICDE CCF[1)]	ICDE CCF[2)]	MTO CCF	T [3)] CCF	Component Impairment Vector [4)]
R2-RO-96/20	DG240 external leak in fuel pipe (960820)		X	X		I I I D
R2-RO-96/24	DG210 Short circuit (fire) in manoeuvre panel		X		X	I C I I
F2-RO-95/30	DG210 does not start during test due to leaking starting air valves				X	I C I I
O1-RO-95/17	DG111 does not start during test	X		X		C C
R2-RO-95/09	6 kV busbar not operational during test of DG210 frequency system		X	X		D I W W
R2-RO-95/28	DG210 mechanical damages in cylinders 4, 12		X		X	C I I I
R2-RO-95/29	Low level in the DG reserve fuel tank	X		X		I I I I
R4-RO-95/09	Deficient flow transmitter stopped both fuel pumps to the DG reserve fuel tank	X			X	I I I I
O1-RO-94/10	DG111 and DG112 start blocked due to wrong signal for activated CO2	O		X		C I
O1-RO-94/16	DG111 and DG112 not operational due to damaged cable	O		X		C C
O3-RO-94/04	DGB not operational due to high exhaust temperature	O		X		W D C I
O3-RO-94/28	DGD not operational due to high exhaust temperature (“Interesting Event”)			X		W W W D
R2-RO-94/02	Closed valve to the fuel transport line to the DG day tanks	X		X		I I I I
R2-RO-94/06	DG210 stopped on overload and was then start blocked due to defective relay in phasing circuit of the speed regulator				X	I C I I
R2-RO-94/08	DG230 stopped pre-lubrication oil pump			X		I I D I
R2-RO-94/23	Low level in the DGs reserve fuel tank	X		X		I D I I
R3-RO-94/10	DG310 starting air compressor stopped on over current due to broken socket			X		W W D W
R3-RO-94/24	DG340 defective starting air magnetic valve (see R4-RO-94/03)		X	X		I I D I
R3-RO-94/43	DG340 alarm for high crankcase pressure due to seized piston in cylinder 15	O		X		W W C W
R4-RO-94/03	DG440 leaking starting air magnetic valve (see R3-RO-94/24)		X	X		I I I D
TOTAL		**14**	**23**	**27**	**19**	

Notes to Table 2:

1) CCF according to the ICDE definition relating to test interval
O: The event is a data point in the ICDE-database.

2) X: The event has been assessed as a data point, based on the corrective actions taken by the plants after the event, and directed toward several group components.

3) Hardware related failure.

4) Abbreviations according to ICDECG00 (C = Complete failure, D = Degraded function, I = Incipient failure, W = Working) .

Compared with the present content of the ICDE-database, the noticeable additional number of CCF events, as presented in Table 2, underlines the benefit of performing an independent quality control of the database, at least as exemplified for the emergency diesel generators in Swedish nuclear power plants. A discussion based on the content of Table 2 is presented in section 5.

4.4 Assessment of the utilised classification categories in the ICDE-database

An assessment has been made of the classification categories utilised for the data points (1994 – 1997) for Swedish emergency diesel generators presently included in the ICDE-database.

This assessment can be summarized according to the following:

- With only very few exceptions, it is judged that the classification categories of the ICDECG00 have been utilised pertinently by the ICDE data analysts. Identified differences in classification of "Component Impairment Vector" are presented in section 4.5, Table 3.
- The ICDE coding factor C9 (Root Cause) does not in fact represents what is widely meant by "Root Cause". The content of C9 accordingly describes overall factors contributing to events. Notwithstanding this remark, the studied events in the ICDE-database are classified correctly outgoing from the available classification scheme.
- The ICDE coding factor C12 (Corrective actions) is coarse. This means that the specialists entering data points in the ICDE-database have only a limited set of general alternatives. Furthermore, and due to the fact that several root causes normally contribute to each identified CCF event, several corrective actions have been, or should be, taken at the plants. This fact is not reflected in the ICDE-database for CCF events relating to human and organisational deficiencies. Notwithstanding this remark, the studied events are classified correctly outgoing from the available classification scheme.

4.5 Assessment of the utilised classification for the category "Component Impairment Vector"

A comparison has been made of the classification utilised in the ICDE-database and in the present study for the category "Component Impairment Vector" according to the definitions in ICDECG00. The comparison is presented in Table 3 for the six LERs (five data points) included in the ICDE-database for years 1994 – 1997.

Table 3: Comparison of "Component Impairment Vector" as classified in the ICDE-database and in the present study.

LER number	LER title	Classification according to ICDE	Classification according to present study
O1-RO-94/10	DG111 and DG112 start blocked due to wrong signal for activated CO_2	C W	C I
O1-RO-94/16	DG111 and DG112 not operational due to damaged cable	C C	C C
O3-RO-94/04	DGB not operational due to high exhaust temperature	D I W W	W D C I *
R3-RO-94/43	DG340 alarm for high crankcase pressure due to seized piston in cylinder 15	C W W W	W W C W
R2-RO-97/13	DG210 does not increase voltage	I I C C	C C I I
R2-RO-97/14	DG220 stops on high voltage		C C I I

** DGC was already start blocked due to planned maintenance when DGB became not operational. Some two months later (O3-RO-94/28) DGD was found not operational due to the same cause as for DGB in O3-RO-94/04.*

One interesting difference in Table 2 relates to LER O3-RO-94/04, and more specifically to the fact that DGD failed some two months after the failure of DGB and due to the same cause. The classification of DGD as "W" or "I" is within a grey zone. DGD was successfully tested when DGB was found in a degraded state. It can however be argued that DGD was at that time already exposed to an incipient failure.

This LER exemplifies one uncertainty existing when classifying some events as either interesting recurrent events due to a shared cause or CCF events. This issue is further discussed in section 5.

5 Discussion and recommendations

The data survey and review of the ICDE-database has provided several insights deemed of broad applicability. These insights are discussed below. The discussion is completed with recommendations.

5.1 Quality and credibility

This data survey and review indicates the need, for the years 1994 – 1997, to complement with a noticeable number of data points the ones actually entered in the ICDE-database for emergency diesel generators in the Swedish nuclear power plants.

In light of the impact of the CCF-estimates utilised in the quantification of PSAs for different component groups, the importance for the ICDE-database to exhibit high quality and proven credibility is obvious. This is even more valid when considering organisational and human aspects of CCF events.

The review demonstrates the benefit of a quality control of the ICDE-database. Such an effort has to be weighted against the resources allocated to the development of CCF models which, no matter their strengths and weaknesses, are all basically dependent of high quality inputs.

Recommendation: An emergency diesel generator is a complex "component" compared to other components in the ICDE-database (valves, batteries, etc.). Well aware of this basic difference, it is recommended to assess the applicability of the obtained results to another group of components belonging to the Swedish plants and included in the ICDE-database. The overall goal of such an exercise is to assess if the results obtained for emergency diesel generators are singular or generic ones for the Swedish data points.

In addition, based on the insights gained during the review, and in order to further enhance the credibility of the ICDE-database, it is recommended that another country member of the ICDE group performs a similar review of its data for emergency diesel generators. This recommendation is probably most pertinent for a country with a

significant number of plants having a proportionally limited number of events in the ICDE-database.

5.2 Repartition of CCF events

As indicated in Table 1, a significant spread exists among the Swedish units concerning the amount of CCF events in diesel generators each unit has experienced. Accordingly, for the eight operational years studied the spread varies from zero event (three units) to 15 CCF events (one unit).

Recommendation: The significant spread among the Swedish units of CCF events for diesel generators is another example confirming the benefit to gather unit specific data for PSA applications. The result also underlines the knowledge required and the precautionary measures that the licensees have to take when utilizing external/foreign component failure data, and especially CCF data, in the quantification of their PSA.

5.3 Coding Guidelines

As mentioned in section 4.3, this review has been made according to the general ICDE coding guidelines (ICDECG00, Revision 4, 2000-10-19) and to the coding guidelines for emergency diesel generators (ICDECG03, Draft 2, 1999-01-13).

During discussions with plant representatives about the data points identified in the present study, it was noted that the classification of the data points earlier entered for the diesel generators had been made in accordance to the first draft of ICDECG03.

Even if the two draft contents are relatively similar, differences exist (for example concerning #5 in Draft 2) which have to be recognized as one possible source of discrepancy between existing and proposed (in this study) data points in the ICDE-database.

In all, such differences had however a limited impact on the identification and classification of a few CCF events in this study.

Recommendation: Updating the coding guidelines and other documentation is a given part of the improvement process for any database. The implications of such updates have however to be assessed, and decision has to be taken as to whether or not update the database in order to guarantee over time an acceptable consistency of the data points.

5.4 Residual CCF and Interesting Events

Some ambiguity arose during the study in assessing recurrent non random failures due to a shared cause, when the failures occurred within a time interval longer (for example two months) than the test interval of two weeks for diesel generators.

This issue is important, especially when one of the causes behind the first occurred failure remained hidden or latent – in spite of corrective maintenance and subsequent successful test of the component - until the same then identified cause contributed to a recurrent failure of another group component.

Discussions with plant representatives indicate that the latter have to a significant extent – if not solely – considered the test interval as a prime parameter in their assessment of the CCF events.

Recommendation: From a plant safety and PSA point of view, it is recommended that the ICDE data analysts follow a conservative decision making when identifying interesting events that, in spite of a time interval between failures longer that the stipulated component test interval, are examples of recurrent non random failures due to a shared cause.

5.5 CCF events and Corrective Actions Taken

In the course of this study, efforts have been directed toward the identification of corrective actions taken by the licensees, and especially those resulting in the replacement of failed parts on other diesel generators at the unit and even at other units of the plant. In relation with some events, it has been difficult to assess the time interval until the replacement went completed.

One reason for the discrepancy between the number of data points in the ICDE-database and in this study is possibly that the ICDE data analysts have principally paid attention to the subsequent controls mentioned in the LER(s) and not followed the outcome of these controls – not always mentioned in the LERs - as ground for the replacement of component parts.

In this context, the reporting in the LERs from earlier years was for some events not exhaustive enough to allow a direct assessment of the above. One frequent example is that the licensee, in the LER, mentions that check of and eventually part replacement will be made on other group components at the unit/plant. The problem for the ICDE data analyst is that the LER is not always updated, and information is thus not provided about the result of the control and replacement eventually performed on other group components. Contacts have thus to be taken with the unit specialists as ground for a correct assessment of the events.

Recommendation: The importance of the CCF issue for plant safety and PSA results should be fully considered in the plant operating experience programme. It is consequently recommended that the LERs should be revised whenever a replacement of similar parts on other group components is made following controls after failure of one component of the same group. As indicated by the study, replacements can even relate to other units at the same site.

5.6 Component Boundaries

This study has identified several additional CCF events satisfying the coding guidelines with respect to component boundaries, and especially such related to failures in the fuel oil system. According to ICDECG03 Revision 2 this system encompasses all storage tanks permanently connected to the engine supply.

During discussions about such additional CCF events, ICDE data analysts mentioned that these events had been disregarded based on the fact that the fuel system for the diesel generators was separately modelled in, at least, some of the existing PSAs.

A similar situation might apply for other component boundaries, as busbars of vital electrical loads, etc.

Recommendation: In order to guarantee a good consistency of the data points in the ICDE-database, it is recommended that the ICDE data analysts closely adhere to the existing coding guidelines concerning component boundaries.

This approach makes it unambiguous and easy for the end users of CCF data to later on disregard some of the data points, depending on the specific system models in their PSAs.

5.7 ICDE Event Record - Root Causes

As shortly mentioned in section 4.4, the ICDE coding factor C9 (Root Cause) is judged relatively coarse and is not in good agreement with what is broadly meant by "Root Cause".

It is however recognized that the structure of this coding factor might fully deserve the objectives of the ICDE-database. One emergent problem with a coarse classification of contributing event causes is the difficulty to put light on certain areas, especially MTO-related issues, and to formulate efficient corrective actions.

The first point concerning MTO-related issues is discussed in NAFCS-PR08 entitled "Qualitative analysis of the ICDE-database for Swedish emergency diesel generators".

Comment: Although the present coding factor for "Root Cause" is coarse, it fulfils the original objectives of the ICDE-database as far as CCF data points and estimates for PSA use is concerned.

Should special needs arise in relation with future CCF/HRA analyses, it might be more resource effective to connect the ICDE-database to other databases. An obvious reason is that a thorough update of the ICDE-database will implicate significant costs and burden on the specialists involved.

This question should however be discussed in front of the input into the ICDE-database of new data points.

5.8 ICDE Event Record – Corrective Actions

As mentioned in section 4.4, the ICDE coding factor C12 (Corrective actions) is coarse. This fact is directly related to the chosen structure and detail of the coding factor C9 (Root Cause). This coding factor is however judged suitable for the PSA applications originally planned with the ICDE-database.

As indicated in Figure 1 and Table 2, the CCF events identified in this study are, in the majority, MTO-related events. As such, most of them are caused by two or more root causes. In order words several corrective actions are needed/taken in order to prevent the CCF events from reoccurring.

The structure and coverage of the ICDE coding factor for corrective actions is thus judged somewhat ineffective for the identification and proposal of the most focussed corrective actions.

Comment: The same comment as the one previously mentioned for "Root Cause" applies here.

5.9 MTO-related CCF Events

One result of the present review indicates that 60% of the identified CCF events for Swedish emergency diesel generators are MTO-related events. This represents an important fact with many implications.

One of them relates to the adequacy of the ICDE-database to put light on MTO aspects, and subsequently to contribute to the identification of efficient corrective actions.

This issue has been shortly touched upon in this report, and is discussed in more details in NAFCS-PR08.

5.10 Learning Curve

The yearly number of identified CCF events for Swedish diesel generators exhibits a clearly decreasing trend between the years 1994 – 2001, as shown in Figures 1 and 2. These figures indicate furthermore that the share of "complete failure" events – during testing - and the share of MTO-related CCF events have decreased noticeably over the years.

Mention has hereby to be made that none of the identified data points corresponds to a failure having occurred during a real start or running demand of an emergency diesel generator

The main explanation behind the decreasing trend is assessed to be the tangible result of the focussed efforts, toward remedial and prevention of CCF events, spent by the operation and maintenance staff at the plants.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
App5.3	**Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08**	**PR08**
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title:	Qualitative analysis of the ICDE database for Swedish emergency diesel generators
Author(s):	*Jean-Pierre Bento, JPB Consulting AB*
Issued By:	*Jean-Pierre Bento, JPB Consulting AB*
Reviewed By:	Michael Knochenhauer
Approved By:	Gunnar Johanson

Abstract:

This report presents a qualitative analysis of the ICDE-database for the emergency diesel generators in the Swedish nuclear power plants. The analysis covers events reported into the database for years 1994-1997, and of CCF events additionally identified for years 1998-2001.

The study results confirm the broad applicability to other units of the data points.

The study shows that the present structure of the ICDE-database does not allow to put light on MTO-related (Man – Technology – Organisation) aspects of the CCF events. Recommendations are made about potential improvements of the ICDE coding factors "Root cause" and "Corrective actions" in the light of identified weaknesses in these two coding factors.

An analysis of CCF events based on a study of the MTO-database identifies the dominating causes (root causes) to CCF events as:

- Work practices (Self-checking)
- Work organisation (Work preparation, Operability readiness control)
- Procedure (Procedure content)
- Ergonomics (Ergonomics/MMI, Design, Accessibility).

Based on the identification of these underlying factors, the study finally proposes potential corrective actions against CCF in the Swedish emergency diesel generators.

This report refers to NAFCS-PR11 "Data survey and review of the ICDE-database for Swedish emergency diesel generators".

Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
A1	2002-04-30	JPB
A2	2002-06-24, corr. table 1	GJ
Final	2002-06-24	GJ

List of Content

List of Tables

List of Figures

1. Introduction

The purpose of this report is to provide insights from a qualitative assessment of the ICDE-database for emergency diesel generators in the Swedish nuclear power plants. This report complements NAFCS-PR11 entitled "Data survey and review of the ICDE-database for Swedish emergency diesel generators".

Section 3 presents the assessment of the applicability to other units of data points in the ICDE-database, and of additionally identified data points according to NAFCS-PR11.

Section 4 discusses the potentiality of the ICDE-database to put light on MTO-aspects (Man – Technology – Organisation), and provides recommendations directed toward the improvement of two ICDE coding factors.

Section 5 presents important MTO-related aspects of CCF events, based on an analysis of the MTO-database for the events identified in NAFCS-PR11.

Potential corrective actions against CCF events in the Swedish emergency diesel generators are discussed in section 6.

2. Study objectives

The objectives of this study are:

- Assessment of the applicability of identified data points to other units/plants.
- Assessment of the potentiality of the ICDE-database to put light on MTO-aspects.
- Presentation of salient aspects of identified CCF from an MTO perspective.
- Proposal for potential corrective actions against CCF events.

3. Applicability of the CCF data points to other units/plants

The emergency diesel generators in the eleven operating (twelve until year 2000) Swedish nuclear power units amount to 38 (40). As presented in NAFCS-PR11, 33 CCF events were identified for these diesel generators for the years 1994 – 1997, including the five data points (six events) contained in the ICDE-database. In addition 13 CCF events were identified for the years 1998 – 2001. The ICDE-database contains furthermore 10 data points for the years 1986 – 1993.

A study has been performed about the applicability to other units of the ICDE data points and of the additionally CCF events identified in NAFCS-PR11. In the present study, a CCF event in plant A has been judged of "applicability" for plant B if:

- some of the contributing factors behind the CCF event in plant A could exist in plant B,
- some of the corrective actions implemented at plant A has/have been implemented at plant B,

- some of the lessons learned at plant A subsequent to the CCF event is/are relevant for the preventive safety work and diesel generator maintenance at plant B.

According to the above conditions, the results of the study of the ICDE data points and of the additionally identified CCF events indicate that all CCF events are of applicability for other units/plants. The applicability is thus not dependent of whether the event causes were MTO-related or hardware failures.

This result represents a remarkable aspect of CCF events, notwithstanding the fact that this aspect was rather expected based on the three conditions mentioned above.

4. Potentiality of the ICDE-database to put light on MTO-aspects

According to the results presented in NAFCS-PR11 for the years 1994 - 2001, 27 out of 46 CCF events in the Swedish emergency diesel generators are MTO-related events. This means that about 60% of these CCF events are related to human and organisational deficiencies.

The overall assessment is made in this study that the structure of the ICDE-database exhibits a limited potentiality to put light on the MTO-aspects of CCF events. This assessment is principally based on identified weaknesses in the coding factors for "Root cause" and for "Corrective actions". The referred coding factors are the ones described in the coding guidelines ICDECG00, revision 4.

From a strict MTO-point of view, it is judged that the identification of the underlying causes and of potential corrective actions have only been given a secondary focus in the ICDE-database.

4.1 ICDE coding factor "Root cause"

The coding factor "Root cause" includes "D – design, manufacture or construction inadequacy" and "M – maintenance". From an MTO-perspective these codes refer in fact to different work types. Each work type can be divided into a number of work activities (preparation, decision, action, control and reporting). Each work activity can finally be performed inadequately through error of commission or of omission, or not performed timely or in other way be quantitatively deficiently (too much or too little of the required action). The above provides the possibility to explain "HOW" the MTO-event occurred, not "WHY".

Against this short background, neither "D" nor "M" represents a root cause in the commonly used sense of the word. Responses to the "WHYs" will provide the analyst with the root causes of the events. For example:

Why was the maintenance deficient:

- was it a weakness in the maintenance programme, in the task organisation, in the competence of the staff, in the communication between workers and supervisor, or/and
- was is caused by a stress situation, a cramped work place, etc?

In addition to a consistent set of recognized root causes, the above indicates the analytical depth needed to be reached in the evaluation of the events in order to correctly assess the root causes. The structure of the ICDE-database does not presently allow such an exercise.

Another code utilised in ICDECG00, namely "H – human actions", is to be viewed as one general causal category. The latter can in fact be subdivided in a number of underlying causes (root causes). One such is "non-respect of procedure", another is "deficient self-checking", etc. Further, a deficient human action can be caused for example by tiredness (during night shift) or stress (during refuelling outage), in addition to other contributing factors. The two examples are related to the causal category "work schedule".

This short discussion hopefully exemplifies the structure required for the ICDE-database to have the potentiality to put light on MTO-aspects, both organisational and individual ones, of CCF events. The ICDE-database does not presently fulfil such a requirement.

Recommendation: Considering the dominating share of human and organisational related CCF to the identified CCF events, and the significantly weak potentiality of the ICDE coding factor "Root cause" to put light on MTO-aspects, it is recommended to improve without excessive delay the shortcomings inherent to this ICDE coding factor.

Such an improvement represents a necessary condition for the adequate classification and retrieval of the factors contributing to a majority of CCF events, as ground for the formulation of pertinent proposals for corrective actions. Three general alternatives exist for such an improvement:

- *To redesign/modify the existing ICDE coding factor "Root cause".*
- *To add the required information as free text – with possibility for searching - in the existing ICDE-classification scheme.*
- *To connect the ICDE-database to or to utilise another database containing specific information on the MTO-aspects of CCF events.*

The first alternative above is judged to be the most suitable from a root cause analysis perspective, but unfortunately probably the most resource consuming.

Recommendation: Several LERs about events in the Swedish emergency diesel generators suffers from an information content that is not exhaustive enough for allowing a robust and independent assessment. The licensees should fully realise that a correct assessment and classification of underlying causes to CCF events presupposes a high qualitative event reporting. It is thus important that the licensees

update the event reports (LERs), whenever needed, in order to unequivocally reflect results from analyses performed subsequently to the events and taken/decided corrective actions on components belonging to the same component group.

Based on the importance of CCF events for the plant safety and for PSA applications, and also considering the difficulties for the ICDE analysts to gather correct information a long time after the event occurrence, the recommendation is for the licensees to devote increased focus on the quality of the reporting of plant events.

It is hereby recognised that a noticeable improvement of the LER reporting quality has been achieved during the latest years by several units/plants, meanwhile some efforts still have to be spent at the other units/plants in order to reach the same level of qualitative information.

4.2 ICDE coding factor "Corrective actions"

The comments expressed for the coding factor "Root cause" are applicable for the coding factor "Corrective actions". This coding factor is thus judged coarse in the meaning that several of the listed codes relate to general corrective measures. This fact depends on the structure of the ICDE-database, e.g. of the coarse identification of the causes/root causes having contributed to the CCF events.

In addition, and valid for most coding factors, a general remark can be made concerning the coding factor "U – unknown". The structure of a high qualitative database should, as much as possible, force the analysts to classify events according to explicit codes only. This is especially valid for CCF events due to their decisive importance for the plant safety and in PSA applications. In this respect, a quite obvious requirement is that both root causes and corrective actions have to be clearly identified and classified. Considering the efforts spent on the reporting into the ICDE-database, this exercise should be relatively manageable in consideration of the relatively limited data points that CCF events represent.

<u>Recommendation</u>*: Considering the fact that the ICDE coding factor "Corrective actions" suffers of weaknesses similar to the ones pertaining to the coding factor "Root cause", it is recommended to improve the possibility within the ICDE-database to classify and retrieve specific proposals for corrective actions.*

This recommendation and the first one in section 4.1 are tightly connected. They should be viewed as one entity when discussing the accomplishment of the recommended improvements. The three alternatives for improvement mentioned above for "Root cause" apply even for "Corrective actions".

The discussion in sections 4.1 and 4.2 is illustrated in Table 1 for the data points common to the ICDE- and the MTO-databases.

Table 1: Review of the CCF data points in the ICDE-database with respect to root causes and proposed corrective measures

Report Number	ICDE ID nr	Event	ICDE causes	Event causes & root causes according to the MTO-database	Proposed corrective actions according to ICDE	Potentially preventive measures according to the MTO-database - Improvement of:
B1-RO-93/22	51	Spurious stop of DG sub A during test caused by low lubrication oil pressure due to difficulty to read the level gauge properly	Human action	- Work organisation (def. planning) - Ergonomics (instrumentation reading) - Procedure (deficient content) - Training/ Competence	General administrative & procedure controls	- Work organisation (task planning) - Procedure - Ergonomics/design of instrumentation - Self-checking
O1-RO-94/10	49	Both diesel generators were unable to start during test caused by a faulty signal from the fire extinguishing system due to malfunctioning reset knob	Design, manufacture or construction inadequacy	- Deficient maintenance/testing programme - Deficient self-checking (wrong action during on-going work in the fire extinguishing system)	Fixing of component	- PM-programme - Self-checking
O1-RO-94/16	46	Cable indicating the operability of both design mistakenly cut off during modernisation work	Human action	- Work organisation (deficient preparation) - Work practice (poor self-checking)	Fixing of component	- Work organisation (preparation) - Individual work practice (self-checking during development of work documentation)
O3-RO-94/04	44	DG B: High exhaust temperature during test due to change in the fuel pump adjustment due to vibrations	Maintenance	- Work organisation (deficient planning & DKV) - Procedure (deficient content) - Work practice (deficient self-checking)	Specific operation & maintenance practices	- Work organisation (planning) - DKV (operational readiness verification) - Individual work practice (self-checking) - Experience feedback
R3-RO-94/43	53	During test, the DG was stopped due to alarm for high crankcase pressure caused by too effective lower oil ring in cylinder 15	Design, manufacture or construction inadequacy	- Competence	Design modifications	- Experience feedback - Test programme
R2-RO-97/13 R2-RO-97/14	50	DG210: during test the DG did not increase voltage and failed to synchronise to its busbar due to insufficiently torqued screw in the generator field circuit. DG220 tripped on high voltage due to loose screw in a connection block to voltage measurement	Human action	- Ergonomics (limited access for testing, maintenance, etc) - Work practice (deficient self-checking) - Procedure (for checking the screw torques does not exist)	Test & maintenance policies	- Ergonomics - Self-checking - Maintenance procedure - Operational readiness control

5. MTO-aspects of CCF events

Each one of the 27 MTO-related CCF events in the emergency diesel generators in the Swedish plants for the years 1994 – 2001 has, on an average, been caused by two general causes, representing ca 2,4 root causes per event.

5.1 Causes of CCF events

The contribution of the different general causes is presented in figure 1 for the most frequent work types performed on the diesel generators. These work types are:

- Maintenance / Repair
- Testing / Calibration
- Operation
- Installation / Modification (Change management).

Figure 1: MTO-related causes to CCF events in Swedish emergency diesel generators

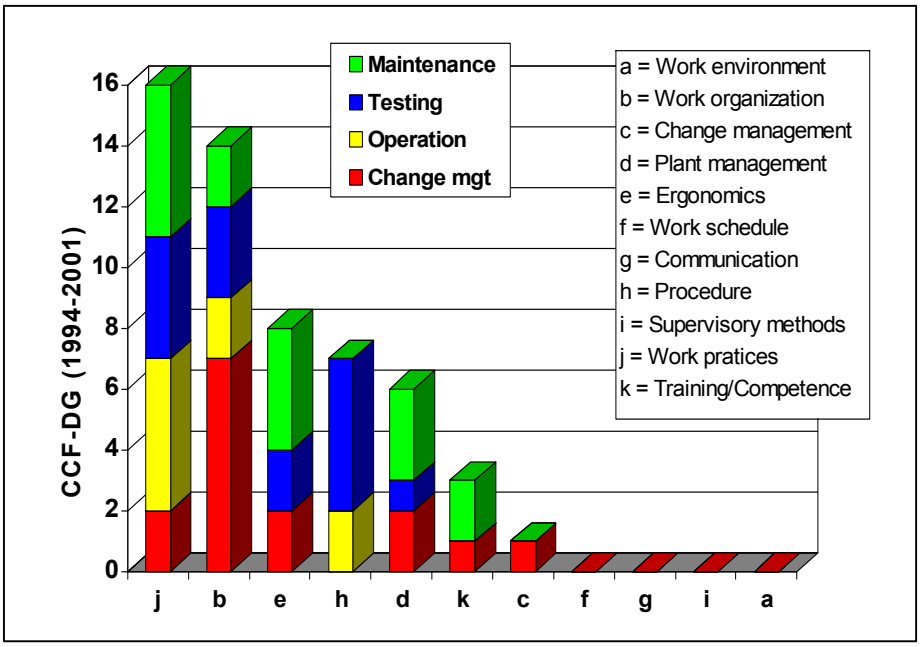


Figure 1 indicates that deficient "Work practices" has contributed to ca 60% of the MTO-related CCF events in the Swedish diesel generators. Figure 1 shows furthermore a noticeable contribution from such deficiencies related to operational, maintenance and test activities.

Similarly, deficient "Work organisation" has contributed to ca 52% of the CCF events. The contribution from deficiencies related to installation and change tasks is significant.

Deficient "Ergonomics" has contributed to ca 30% of the CCF events. Maintenance tasks appear to be most sensitive to this type of deficiencies.

Finally, the contribution from deficient "Procedure" related to testing / calibration tasks is also worth to notice. In the present study, "Procedure" is defined as all written documentation used for the planning, performance and control of the tasks necessary for the operation and maintenance of the plants. Of interest is also the result that the five deficiencies in testing / calibration procedures occurred at the same plant, and the two deficiencies in operational procedures occurred at one unit at another plant.

5.2 Root causes of CCF events

The topography of root causes contributing to MTO-related CCF events in the Swedish diesel generators is dominated by deficiencies in:

- Self-checking
- Work preparation
- Operability readiness control (DKV)
- Procedure content
- Ergonomics / design / accessibility.

Deficiencies in "Self-checking" (equivalent to the Swedish acronym "STARK") have contributed to 50% of the MTO-related CCF events, equivalent to one third of all CCF events identified in the present study. Deficient self-checking related to installation and modification tasks has contributed to as many CCF events as similar deficiencies related to the three other work types (operation, maintenance and testing) together. The deficiencies have occurred during task preparation, performance, control or reporting.

Deficiencies in "Work preparation" and "Operability readiness control" have equally contributed to deficient "Work organisation". Each of these root causes has thus contributed to 25% of the MTO-related CCF events.

Deficient "Procedure content" has also contributed, as a root cause, to ca 25% of the MTO-related CCF events.

Finally, poor "Ergonomics" and poor "Accessibility" has contributed to ca 15% and ca 18% respectively of the MTO-related CCF events.

The identification of the above dominating causes and root causes is of prime importance in the identification process of potential corrective actions against CCF.

It should hereby be mentioned that the topography of the root causes contributing to the CCF events in diesel generators exhibits several similarities with the topography of the root causes generally contributing to the Swedish MTO-related LERs. The similarities are especially valid for the dominating root causes discussed above. This insight is important to consider when discussing potential corrective actions against

CCF. This insight also reinforces the ground for the proposal of corrective actions, and also the validity and credibility of this proposal.

6. Potential corrective actions against CCF

To propose potentially efficient corrective actions against CCF events in emergency diesel generators in the Swedish plants is a delicate task, at least for an outside reviewer. The following paragraphs have thus to be considered as one input in a broader discussion within the industry about potential physical and organisational barriers against CCF.

As previously mentioned, 60% of the identified CCF events in the Swedish diesel generators were MTO-related and about 40% were caused by hardware failures. Efforts have consequently to be directed toward the proposal of corrective actions against both MTO-related CCF events and hardware CCF.

Based on the identification of the dominating root causes having contributed to the CCF events, the potentially most efficient corrective actions against such events are assessed to be the improvement of the:

- Experience feedback programme.
- Preventive maintenance programme.
- Corrective maintenance programme.
- Work practices / self-checking.
- Work organisation / work preparation and operability readiness control.
- Content of procedures and of other administrative documentation.

These proposals have to be viewed of general applicability for an “average” diesel generator in an “average” Swedish unit/plant. As presented in NAFCS-PR11, significant variations exist between units as to the number of CCF events and the root cause topography of these.

6.1 Follow-up and mitigation of ageing

Results from the study indicate that slightly more than 70% of the hardware CCF - or one third of all the identified CCF events - are related to ageing phenomena. These phenomena encompass both ageing of electronic equipment (electronic cards, EG10 relays, etc) and of mechanical equipment. For the latter, vibration induced fatigue represents an important factor.

Based on these results, it is judged that potential corrective actions should be directed toward:

- Efficient experience feedback (within and between plants, with component manufacturers) for the timely identification, assessment and resolution of ageing phenomena.
- Focussed preventive maintenance programme based on insights from the experience feedback programme.

- Expeditious corrective maintenance programme for the replacement of parts and components sensitive for CCF risks already identified by the plants/industry.

6.2 Improved self-checking (STARK)

As mentioned earlier, deficient self-checking is the dominating root cause having contributed to MTO-related CCF events in the Swedish emergency diesel generators. This result is in agreement with the ones obtained from the root cause analysis of the Swedish LERs.

This conclusion indicates that the probably most cost effective corrective action against the occurrence of CCF events in diesel generators in particular – and the occurrence of LERs in general - is to reinforce, throughout the whole organisation(s), the sustained efforts directed toward increased consciousness about self-checking. According to the present study, particular efforts should be directed toward installation and modification tasks within the diesel engines boundaries.

It is here important to underline that this proposal represents neither an economical burden nor dramatic organisational changes. Reducing successfully the frequency of CCF events is basically dependent of a long-term motivation of, and information to the whole staff about the benefit of careful self-checking practices.

Outgoing from the fact that work practices are strongly connected to other causes and root causes, a betterment of work practices, and especially of self-checking, will positively influence these other causes – for example work organisation / preparation - having contributed to CCF events.

6.3 Improved work preparation

As mentioned in the previous section, deficient “Work preparation” is one of the two equally contributing root causes representing weaknesses in “Work organisation”. In this study, work preparation includes both the organisational planning of the task(s), the preparation of the needed documentation, the control that the task(s) can be performed safely or according to the Technical Specifications, and guidance about task verification and reporting.

“Work preparation” represents often tasks in which several individuals and departments are involved. The value of high standard work practices in relation with careful work preparation is thus obvious, as well as good practices in supervisory methods, communication, etc. Checking the adequacy and the content of needed administrative documents (work order, maintenance / test procedure, etc) is also a necessary part of a good work preparation.

The proposal of corrective actions toward improved work preparation is thus strongly linked to the high professional standards and carefulness the involved individuals should follow and exhibit before physically performing the work tasks. The value and benefit of good self-checking practice during the different steps of the work preparation are clearly apparent.

6.4 Improved operability readiness control

The issue of "Operability readiness control" (DKV) came into focus in Sweden for several years ago, both in the industry – plants and regulatory body – and in the media. The issue was then related to safety system operability readiness control.

In the frame of the present study, the notion of operability readiness control is as well applied to the correct alignment of valves after testing / maintenance, correct setting of instrumentation after testing / calibration, etc.

The study indicates that deficient "Operability readiness control" is the dominating root cause – in parity with deficient work preparation – behind CCF events related to weaknesses in "Work organisation".

The proposal of corrective actions aimed at a betterment of the operability readiness control should be considered in the light of the significant efforts devoted on the issue by the licensees and the regulatory body. Within the limited frame of the present study, MTO-related insights about CCF events underline the need of careful preparation, performance, control and reporting of the different steps constituting operability readiness control.

In other words, following high professional standards and exhibiting good self-checking practices are two prerequisites for a successful DKV. The wording of this proposal is thus the same as the one formulated above for "Work preparation".

6.5 Improved content of procedures

Deficiencies in "Procedure" constitute the fourth contributor to CCF events in the Swedish emergency diesel generators. One has however to remember that low numbers are involved in this study. Deficient operational procedures (for the definition of "Procedure", please refer to section 5.1, contributed to two CCF events in one unit and deficient test/calibration procedures contributed to five CCF events at another plant.

All these deficiencies were related to incorrect, or otherwise deficient, content of the procedures.

The proposal of corrective actions has, also here, to be considered in the light of the significant human and monetary resources allocated by the licensees since many years to the sustained improvement of "Procedures". Special focus was earlier directed toward operational procedures, but during the latest years increasing efforts have been made to improve both test and maintenance procedures.

As indicated above, corrective actions toward an additional betterment of the content of procedures touch principally one unit and one plant.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
App 5.4	**Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09**	**PR09**
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Survey Task Report

Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs

This survey is undertaken to create basis for planning the update of the earlier CCF study of the control rods and drives completed in 1996.

The revised issue adds in Section 5 a comparison table/diagram of the reference PSA results for the control rods and drives. Also details of the Nordic PSA applications are refined.

Contents in brief

Version control

Version	Date	Description
Outline	2001-11-15	Initial draft
Draft 1	2001-11-26	To be discussed in Working Meeting, November 29, 2001
Issue 1	2001-12-31	Completed report, indexed as NAFCS document
Issue 2	2002-01-08	Supplemented version

Contents list

1 BACKGROUND AND OBJECTIVES

The earlier research program of the Swedish Nuclear Power Inspectorate (SKI) included the project completed in 1996:

> "A Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants"

The project was co-supported by the Finnish Centre for Radiation and Nuclear Safety (STUK) and Teollisuuden Voima Oy (TVO power company operating OL1/OL2 plant). The documentation encompasses the summary report [SKI R-96:77] and work reports collected in the compendium [SKI/RA-26/96]. A compact summary exists in the form of the conference paper [RS-PSA99]. These documents will be made available at the Web site of the Nordic CCF Analysis Group (NAFCS). Similarly, this survey task report is indexed as NAFCS report.

The objective of this survey is to provide basis to planning of the database update for the Control Rod and Drive Assemblies (CRDAs), and related PSA applications.

A utility survey was carried out based on a questionnaire about specific development needs for the CCF analysis of the CRDAs [NPSAG-CRDAs-USO]. This was performed as part of a more comprehensive NAFCS survey, see details in [NAFCS-PR06].

The draft survey report was discussed in the Working Meeting on November 29, 2001, see [CRDA-Agenda-011129], and the report is supplemented accordingly. The proposal for the update project with work and resource plan will be presented separately for the next NPSAG meeting on January 16, 2002

The contribution by Per Hellström, RELCON AB, is acknowledged regarding the utility survey part.

2 SCOPE

The scope is limited to BWRs of former Asea Atom design. An extension to the Nordic PWRs (Ringhals 2-4 and Loviisa 1-2) can be considered in the continuation.

3 EVENT DATA, NORDIC

The earlier event analysis of CRDA events is summarized in [SKI R-96:77]. The details are documented in the following work reports that are part of the compendium [SKI/RA-26/96]:

- TVO data for 1981-1993 in [TV_RSCCE]; this was a pioneering event analysis during which a new scheme evolved to handle the functional failure modes of CRDAs
- Swedish BWR data for 1983-1995, based on ROs in [RS_SweDB]; App.1 of this work report describes a high order CCF that affected Ringhals 1 in 1993; App.2 pools the TVO data and Swedish BWR data together

This section will discuss the addition to the event volume from the more recent years. As background, the definition and classification scheme of CRDA failure modes is reproduced in Table 3.1, for details see [SKI R-96:77].

3.1 ERFNOVA

The event count for the CRDAs including the associated control and instrumentation equipment is presented in Table 3.2 for the earlier analysis period and the recent years (it is crudely assumed that the ERFNOVA database, which was provided in September 2001, covers events up to the first half of year 2001 when counting the reactor years).

The brief look-through indicates that the more recent events contain similar failure mechanisms as observed and classified in the earlier analysis. There shows up some interesting new events connected to jamming by loose objects.

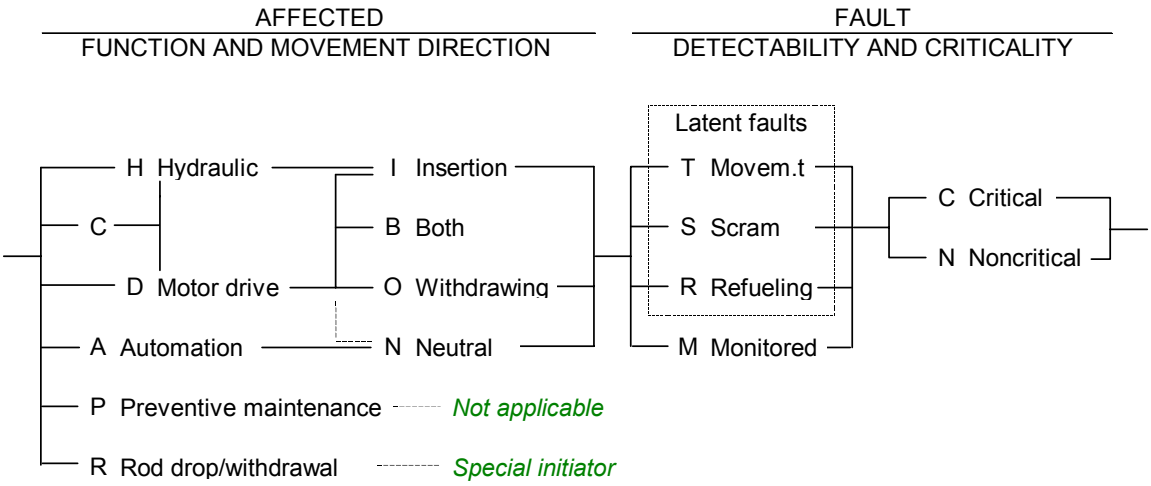
It is of emphasis to notice that the bulk volume of the events shows a substantial positive trend. It would be interesting to see whether this is valid also for the functionally critical failures and not merely caused by a decrease in the majority of non-critical events.

It should also be checked in which extent the comments presented on the classifications and other details of the RO reports have been taken into account [CR_RO22x].

Table 3.2 Event volume of the CRDAs in Swedish BWRs.

		Observation period		
System	Description	1983-95	1996-2001/6	In total
221	Control rod drive including the electric motor and mechanical accessories	196	54	250
222	Control rod	5	2	7
532	Control equipment of the motor drives	28	28	56
533	Instrumentation and mechanical equipment for position indication	100	13	113
	In total	329	97	426
	Reactor years	109	49.5	158.5
	Event frequency [/ry]	3.0	2.0	2.7

Table 3.1 Failure mode classification for Control Rod and Drive Assembly (CRDA).



AFFECTED FUNCTION
- H Hydraulic function
- D Motor drive function
- C Common to hydraulic and motor drive function
- A Automation and instrumentation, including position measurement

AFFECTED MOVEMENT DIRECTION
- I Insertion only
- B Both directions
- O Withdrawing only
- N Neutral or negligible

SPECIAL CLASSES
- P Preventive, scheduled maintenance, undertaken in plant shutdown state
- R Rod drop or inadvertent withdraval, special type of initiator

FAULT DETECTBILITY
- L Latent faults
  - T Detectable in periodic movement tests
  - S Detectable only in scram test or demand
  - R Refueling outage: overhaul inspections and maintenance
- M Monitored faults (detected shortly by instrumentation or process symptoms)

FAULT CRITICALITY
- C Critical
- N Noncritical

GENERIC CLASSES OF FAILURE MECHANISMS

FrObj	Foreign object, jamming
FuIns	Fully inserted position, jammed into pos. = 0%
NutSp	Drive nut separation at pos. > 0%
MetPd	Metal powder problem at TVO I in 1989-90
MTrip	Moment trip
CrRod	Cracking of control rod
PosMs	Position measurement failure
DChkV	Drive check valve blocked
SLeak	Seal leaks, external leaks
ErrRM	Faults introduced in repair or maintenance

Special classes

PrevM	Preventive maintenance
RDrop	Rod drop or inadvertent withdrawal

3.2 TUD

3.2.1 General comparison

The earlier analysis of the Swedish CRDA experience [RS_SweDB] was solely based on RO data. Due to resource limits no comprehensive cross-checking with TUD classifications were done. But a general comparison already showed drastic differences [T-BokenR]. The classification used in TUD was not consistent at that time (T Book Version 4). The primary recommendation was to consider the following three functional failure modes of CRDA:

Fun = D: Screw drive insertion fails

Fun = H: Hydraulic insertion fails

Fun = C: Both hydraulic and screw drive insertion fails

And not to make distinction whether the fault was in rod, drive or auxiliaries – as well as not to consider failures that disable withdrawing as critical (exclude from T Book). Compare to the failure mode classification scheme reproduced in Table 3.1 and further explanations in [SKI R-96:77, RS_SweDB].

The reclassification has then been adapted in T Book Version 5. Generally, the compatibility is now better with the classifications of [RS_SweDB] but there are still rather substantial differences which should be clarified in the coming database update of CRDAs.

3.2.2 Critical failures of both hydraulic and screw insertion function

The most crucial classification concerns criticality with respect to both insertion functions (Fun = C) as this functional failure mode is the most risk-significant. Table 3.3 shows the events that are classified in this regard critical in TUD classification or in [RS_SweDB]. The comparison shows significant discrepancies that are discussed in the following paragraphs.

Barsebäck 1 event in 1982 was considered in the earlier CRDA/CCF analysis separately even though outside the nominal observation period 1983-95. It was noticed because

Table 3.3 CRDA events that are classified as critical for both hydraulic and screw insertion function in TUD (T Book 5) versus the earlier CRDA/CCF analysis [RS_SweDB].

Unit/CRDA Event date Report	Classification in TUD (T Book 5)	Classification in the earlier CRDA/CCF study [RS_SweDB]
B1.221.D23 1982-04-14 B1-RO-6/82	Critical for screw insertion function (included in Table 5.1.2), mismatch in event date	Critical for Fun = C; FMode = CI.SC (outside observation period, but noticed from T Book 4)
O2.221.C53 1982-07-16 O2-RO-23/82	Critical for both functions (included in Table 5.1.3)	Not covered as being outside the observation period 1983-95, and no separate notice of this event
F3.221.AH40 1985-06-21 F3-RO-26/85	Not included at all	Critical for Fun = C; FMode = CI.SC
T1.225.I45 1989-10-18 38219	Critical for both functions (included in Table 5.1.3), mismatch in event description	Noncritical, only withdrawing disabled; FMode = CO.SN

of being present in the earlier T Book versions, e.g. Version 4, Table 27.1. Besides, it was noticed and taken into account already in the early TVO/PSA in 1989. The criticality of this event for both functions was verified by the plant experts in 1994. There are strange mismatches in the TUD information for this event and also in the current ERFNOVA report in comparison to the earlier RO report.

Oskarshamn 2 event in 1982 was not considered in the earlier CRDA/CCF analysis because of being outside the nominal observation period 1983-95, and lack of notice for being separately taken into account. It is peculiar why it was not present along the Barsebäck 1 event in 1982 in the earlier T Book versions?

Forsmark 3 event in 1985 was specifically verified by the plant experts being critical for both functions during the course of the earlier CRDA/CCF analysis. Besides, the RO report clearly – although briefly – states that the control rod failed to insert in reactor scram.

The TUD classification of Olkiluoto 1 event in 1989, related to metal powder problem, is really strange. In TVO's failure event database altogether 37 events were recorded at Unit 1 as being caused by the metal powder problem in 1989-90 [TV_RSCCE]. The functional influence was slow screw movement at the end of insertion and in many cases jamming in the fully inserted position, i.e. impossible to withdraw. It would be interesting to know, why one of the metal powder events has been exceptionally classified in TUD as critical for both hydraulic and screw insertion?

In conclusion, the explanations to the mismatches and classification discrepancies should be carefully explored, not least in order to maintain credibility of the databases.

3.2.3 Strange failure rate estimates of T Book 5

The failure rate estimates presented in T Book 5 for the failure of both hydraulic and screw insertion (Table 5.1.3) are anomalous – does not make common sense in the following respects:

- The mean estimates for Oskarshamn 2 and Olkiluoto 1, both with one failure event, are 3.1E-6 /h and 3.6E-6 /h, respectively. But the simple point estimates are 5.0E-8 /h and 5.9E-8 /h. I.e. about two orders of magnitudes different?
- The presented estimate for Olkiluoto 2 with no recorded failure is three orders of magnitude lower than for Olkiluoto 1, with one failure. Such a ratio seems not meaningful?
- The generic average over all units is 4.1E-7 /h, while the simple point estimate calculated from 2 events is 9.7E-9 /h. Again a huge difference?

The generic average failure rate from T Book 5, Table 5.1.3 corresponds to the mean unavailability (failure of both hydraulic and screw insertion) of as high as 1E-3 per single CRDA, assuming two actual scrams during power cycle (as way of detection). Compare to [RS_SweDB, App.2, Section 3.3]. The use of the presented generic estimate would drastically increase the risk-significance of reactor scram failure. It should also be noticed that the corresponding expected number events would be 83 for the past experience of 234 reactor years up to 1996, Swedish plants and Olkiluoto together.

This anomaly was in fact noticed already in connection to a TVO application in August 2001, but the given explanation related to the skewness of the distributions used in the estimation model is difficult to understand. Is there perhaps something changed in the estimation method in comparison to the earlier T Book versions?

3.3 TVO

The event volume for the CRDAs in OL1/OL2 according to TVO's failure event database is presented in Table 3.4 (it is crudely assumed that the query provided in October 2001 covers events up to the first half of year 2001 when counting the reactor years).

There seems to be only a few failures that are critical to screw insertion function based on the brief look-through. Thus the classification of the additional events would be relatively easy job. The overall trend is somewhat positive, not so strong as for the Swedish BWRs. Conclusions regarding the possible trend of functionally critical failures is pending for the classification.

Table 3.4 Event volume of the CRDAs in OL1/OL2.

		Observation period		
System	Description	1981-93	1994-2001/6	In total
221	Control rod drive with auxiliaries	132	66	198
222	Control rod	11	1	12
	In total	143	67	210
	Reactor years	26	15	41
	Event frequency [/ry]	5.5	4.5	5.1

3.4 Conclusions about the Nordic event data

The brief consideration of the new CRDA events since the earlier CCF analysis indicates that the added events would be relatively easy to analyze and classify. The main emphasis is in

- verification of the earlier (potentially) significant events regarding the affected function, criticality and detectability (a qualified verification succeeded during the earlier analysis only for Olkiluoto and Forsmark plants)
- assessment of the multiple events and degradations to serve the estimation and quantification of CCFs as well drawing conclusions for defense strategies against CCFs.

Also the discrepancies with respect to TUD classifications should be clarified. The explanations behind the huge failure rate estimates presented in T Book 5, Table 5.1.3 should be explored.

The extension of the database to the recent years is of interest to for a trend analysis and for obtaining more up-to-date statistical estimates.

The needed extent of transferring data into ICDE format should be agreed, or to prepare this option for a later transfer. For this purpose it is desired to outline the classification guideline for the CRDAs in cooperation with those ICDE members who already have collected CCF data for the CRDAs.

4 EVENT DATA, INTERNATIONAL

This section will discuss the available CRDA data from outside the Nordic countries with main emphasis on the USA. The CCF data for the CRDAs are not yet gathered in the ICDE.

4.1 USA

As part of the more recent extensive collection of CCF data in the USA also CRDAs are covered. The results are reported for BRWs in [NUREG/CR-5500v3], including also a quantification of the failure of reactor scram for a reference plant as will be discussed in Section 5.1 in more detail.

The data analysis in [NUREG/CR-5500v3] encompasses the whole Reactor Protection System (RPS) for the BWRs of General Electric design and covers years 1984-95. The design is different in comparison to the BWRs of ABB Atom design as in the US BWR each control rod has its own hydraulic control unit with redundant scram valves, and the screw insertion is not a credited safety function. Consequently, the US BWR data for the control rods and drives is comparable to the Nordic BWR data when pooling together the failures affecting hydraulic insertion and the failures affecting both hydraulic and screw insertion. The failures related to scram discharge volume (typically two tanks in US BWRs) constitute a separate specific risk.

The gathered event data contains for the control rods and drives 4 actual CCFs and 18 multiple degradation events that are taken into account by using impact vector method. The most remarkable actual CCF concerned 10 control rods that were pinched by fuel support plugs. The other three actual CCFs were of multiplicity 2. A significant positive trend could be observed in the CCF frequency.

The gathered US BWR data is definitely of high interest at least for comparison purpose, e.g. to infer the corresponding CLM parameters, and possibly also for the use as prior data. However, the influence of the design differences should be carefully tracked. For this purpose the event reports are needed for the CCF events but they are expected to be obtained from the USA via ICDE contacts.

4.2 Germany

The German PSA study of a BWR [SWR-PSA] used US and Swedish event data as prior, combining that with the zero German statistics by Bayesian method. The details are not fully explained.

4.3 AIRS

The earlier CRDA/CCF analysis included a review of the events reported to the Advanced Incident Reporting System (AIRS) managed jointly by the IAEA and NEA. It proved very useful in qualitative respects [RS_WWExp]. The incomplete coverage does not make possible to use that data for real statistical estimation purpose. Anyway, it is recommended to update also this review.

4.4 Conclusions about the international event data

The primary interest is in the deeper review of the US BWR data, especially because it could possibly be used as prior data in combination with the Nordic data (by using Bayesian estimation method).

5 METHODOLOGY AND APPLICATIONS

The recent quantitative analysis of CRDAs are discussed here starting from abroad. The results from considered references are compared in Fig.5.1 – the details and insights will be discussed in the following subsections. It must be noticed in the comparisons that the uncertainty factor of the estimated CCF probabilities for the CRDAs is about one order of magnitude (at the best). The results for the Barsebäck 1 and 2, for the failure mode of screw drive and hydraulic insertion both failing are as obtained in the reference application completed in 1994 [RS_BRAwr]. The results for the other failure modes are produced by using compatible assumptions with the original reference application, the joint data base compiled in 1996 [RS_SweDB] and following a similar quantification procedure as in the recent PSA update for the Olkiluoto plant.

5.1 USA

As said the RPS data analysis reported in [NUREG/CR-5500v3] is accompanied with an application to a reference design (BWR/4, Peach Bottom 2). The Alpha Factor Method (AFM) was used for the control rods and drives. This was made possible by using so called mapping up procedure for the CCF event impact vectors and sophisticated Bayesian estimation method. The main results for the control rods and drives are as follows:

- Total single failure probability is Q_T = 5.1E-5
- CCF event probability is Q_{CCF} = 2.5E-7 based on the criterion that 61 out of 185 (33%) failing rods is critical (in random pattern)

The results seem generally comparable to the Nordic studies that use a more limited data base and CLM - taking into account uncertainties and also differences in system design that can have certain influence. Besides, the reactivity shutdown criteria used in the reference application of [NUREG/CR-5500v3] is relatively optimistic, without consideration of the risk from adjacent rods failing, which contributes to the low calculated CCF risk. A controversial area is also mapping up of the impact vectors in the highly redundant configuration, which can have contributed to the low probability of high order failure, see [NAFCS-PR03]. (It has to be pointed out again – as stated in Section 4.1 – that the US case is comparable to the Nordic case when pooling together the failures affecting hydraulic insertion and the failures affecting both screw and hydraulic insertion.)

There would be high interest to investigate the analysis methodology in more depth for insights and uses. From the report [NUREG/CR-5500v3] alone that is not possible because the details of impact vector construction, mapping up of the impact vectors and crediting for positive trend are not described in sufficient detail. A full recalculation would require laborious tool programming. Thus the recommended option for comparison would be joint Benchmarking, which has been preliminary discussed in the ICDE context.

Report [NUREG/CR-5500v3] presents also a brief review of the US PSA studies and compares the quantitative assessments.

PSA Application	Number of rods n	Single failure probability Q_T	Probability assessment		Failure criterion	
			One rod [1]	Scram function	Adjacent placement	Random placement
Barsebäck 1/2 - screw insertion	109	9.3E-4	7.9E-2	2.6E-5	>=4	>=25%
Barsebäck 1/2 - hydraulic	109	1.4E-4	1.3E-2	3.6E-6	>=4	>=25%
Barsebäck 1/2 - screw & hydraulic	109	3.2E-5	2.9E-3	4.5E-7	>=4	>=25%
US BWR [NUREG/CR-5500v3]	185	5.1E-5	9.5E-3	2.5E-7	-	>=33%
SWR (GRS)	193	4.0E-5	1.8E-3	2.9E-5	>=4	-
				1.8E-4	2..3	-

Notes: 1) One or more rods fail, i.e. Pts(1|n); for US BWR estimated as $n*Q_T$

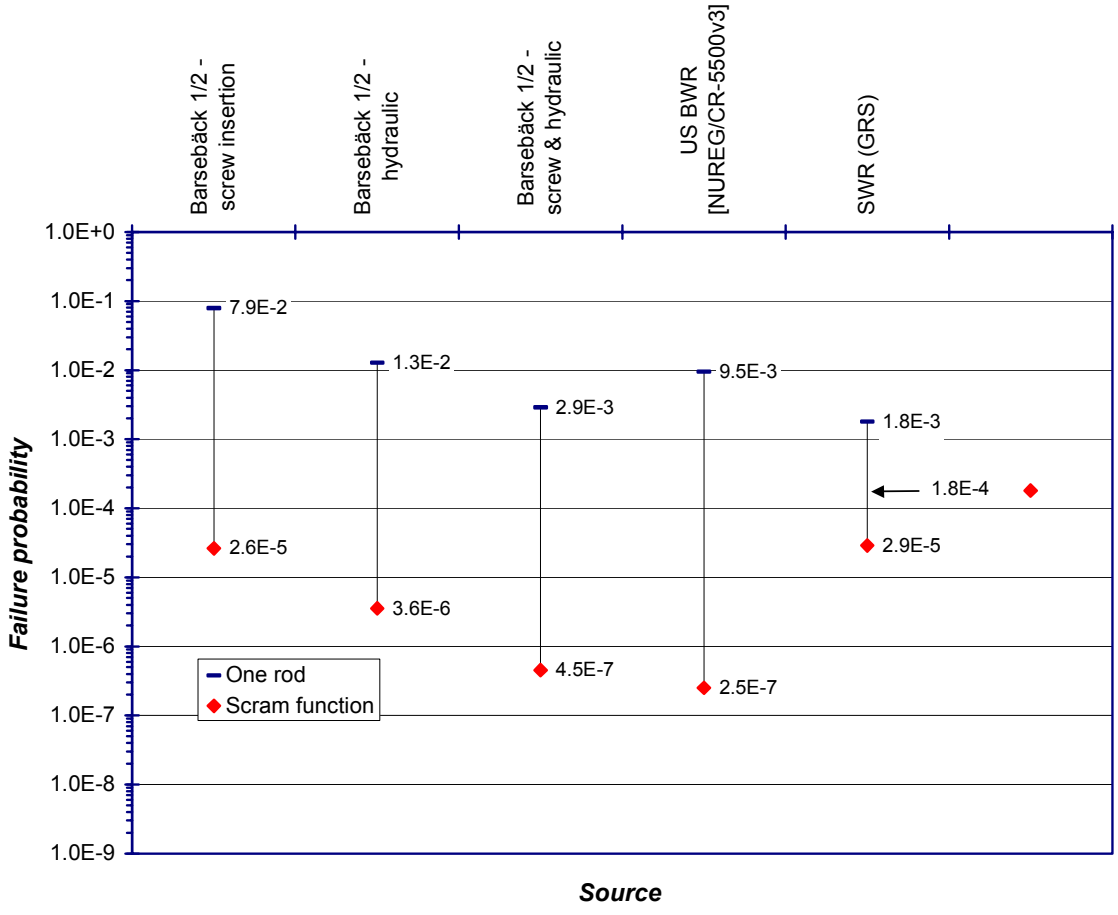


Figure 5.1 Comparison of the failure probability estimates for CRDAs in the PSA applications.

5.2 Germany

The German PSA study of a BWR [SWR-PSA] used an extension of Binomial Failure Rate Model (BFRM) to quantify CRDAs. The reactivity shutdown criterion is defined so that the failure of 2-3, or 4 or more adjacent rods are critical (depending on the initiating event). The obtained results for the two cases are 1.8E-4 and 2.9E-5, respectively. The results are more pessimistic than in the Nordic PSA studies and the difference is really big with respect to US reference study (especially when taking into account that the US case covers also CRDA failures for the hydraulic insertion function while the German case only the failures with respect to both screw drive and hydraulic insertion). It would be worth to explore in more detail whether the differences are attributed to the input data, or to specific assumptions or features in the estimation/ quantification methodology, compare to Section 4.2 regarding the input data.

A methodologically interesting detail is the use of Monte Carlo simulation to derive the conditional probability that a random combination for a certain number of failing rods contains the minimum critical pattern of adjacent rods. An analytic direct evaluation of this fraction is difficult (generally impossible precisely).

The used methodology is not described in sufficient depth to make detailed comparison (recalculation) practically feasible. Hence a closer comparison would require also in this direction an ICDE Benchmark.

5.3 France

A pilot study has been conducted for the CRDAs of the French PWR 1300 design using CLM [ICDE-S-EdF]. Due to the large PWR population in France they have a reasonable statistical basis. It is, however, questionable to transfer CRDA data from PWRs to BWRs.

5.4 Nordic applications

The main Nordic CCF studies of CRDAs and applications in PSA are listed in Table 5.1 using the information gathered in the utility survey [NAFCS-PR06]. The CLM has been used in all these studies. For quite many PSA studies updating the CCF analysis of CRDAs is currently in progress.

Table 5.1 Nordic CRDA studies and PSA applications (sorted in historical order).

Unit	Year	Description, references	Update in progress
OL1/OL2	1989 1997	Early method development and PSA application PSA update	
B1/B2	1994	SKI project, Barsebäck reference application [SKI R-96:77, SKI/RA-26/96]	X
O1/O2/O3	1994-99	PSA application	X
R1	1996	PSA application	
F1/F2/F3	2000	PSA application	

It is of interest to notice that in the current results of TVO/PSA the Fractional Risk Contribution of CRDAs is 0.18% and the Risk Increase Factor is 1670 [NAFCS-PR02]. The level of Fractional Risk Contribution means in the general scale a small risk-significance but

the high Risk Increase Factor implies criticality for a possible failure situation and also significance of uncertainties in the probability estimates.

ABB Atom has done recently a reliability analysis of the CRDAs based on a contract from Forsmark [SPC 99-048]. The report contains an in-depth qualitative analysis of the experienced failure mechanisms which can be especially useful for the development of CCF defense strategies, see Section 6. The presented CCF probability estimate 1E-7 is a plain engineering judgment. The background probability calculations for independent failures show up shortcomings [CR-SPC-99-048, CR-Combinatorics]. However, those calculations are not directly linked with the probability judgment. The CCF probability estimate 1E-7 is within the uncertainty band in comparison to the reference studies, Fig.5.1, regarding the failures affecting both screw and hydraulic insertion. But it is told to have been used for the other two failure modes also, which shows up optimistic in light of the operating experience, due to the CCFs that have affected the screw or hydraulic insertion separately.

The CLM has been reviewed by Sven Erick Alm [Alm-HCCF]. He proposes a new model named as “Beta CCF Method”. This turns out to be a variant of Distributed Failure Probability Method [CR-Alm-Review]. Because the Beta CCF Method has only two parameters it is already from that point of view not applicable to CRDAs which constitute an ultra-highly redundant system. A more detailed commenting of the proposed method would require comparison calculations.

5.5 Reactivity shutdown criteria

The currently used criteria for the reactivity shutdown may be simplified conservative. For example, TVO/PSA assumes the following relatively simple criteria

- Failure of 5 adjacent rods in a specific tight pattern is directly critical
- Failure of randomly placed 31 out of 121 rods or more (25%) is generally critical

The utility survey covered this issue. The insights are briefly summarized here. For the details see [NAFCS-PR06]. The variations in the used criteria from unit to unit are substantial, e.g. the critical number of adjacent failing rods varies from 2 to 6, partly related to different assumed demand condition, and of course, also related to differences in the core design. The critical number of randomly placed failing rods shows much smaller variation, which seems not logical in comparison to the large variation in the criteria for adjacent failing rods. Furthermore, the failure criteria for the hydraulic scram system (354 trains) seem not consistent in all respects with the failure criteria of CRDAs.

The dependence on the initiating event and core condition may be necessary to consider in more detail, as well as the assurance of the sub-criticality both in hot condition directly after scram and in long term in cold core state. The refinement of the criteria can help to remove undue conservatism.

The study of the reactivity shutdown criteria has already been suggested to be included in the NPSAG program. That proposal is supported, i.e. to have a separate specialized study, including needed deterministic analyses. It is only desired that the (deterministically oriented) study of reactivity shutdown criteria and (probabilistically oriented) CCF analysis of CRDAs are linked together in order to assure that failure criteria will be defined in a practicable manner to make the quantification of CCFs possible, including the needed combinatorial analyses.

5.6 Conclusions about the methodology

It is believed that the CCF model itself – assuming adequacy for highly redundant systems – has a small impact on the results in comparison to the determining role of the used event data, and event interpretation and processing for the estimation of CCF model parameters. In fact, it is generally possible to transform parameters of one model to another and yield reasonable compatibility in that way. Compare also to the insights from the earlier systematic comparison of the CCF models [HR_CCFRe].

The model comparisons would nevertheless be very useful, preferably covering the whole quantification process starting from event data. A practically feasible way for the comparisons would be an international Benchmark, e.g. in the ICDE context. The primary CCF models of interest (for CRDAs) are AFM, BFRM and CLM, as well as Beta CCF Method.

Special emphasis should be devoted to handling the combinations of adjacent failing rods which have thus far been considered with simplifications. Method development is needed for a more precise treatment of both combinatorial aspects and extra dependence between adjacent rod positions. The latter issue is also a question for the event analysis to verify the degree of position correlation in the dependence mechanisms.

5.7 Conclusions about the applications

The application for highly redundant systems, and for CRDAs in particular, require expertise and can be rather laborious in isolation. It is hence recommended to encourage exchanging the application expertise within the NPSAG domain.

6 CCF DEFENSE STRATEGIES

The utility survey included questions about CCF defenses: what specific approaches have been implemented for the CRDAs, and ideas about further improvements to be considered [NPSAG-CRDAs-USO, NAFCS-PR06].

Generally, the defense strategies against CCFs of CRDAs are similar to what is applicable for other component types, and divide up into following two categories:

- Strategies to prevent common root causes and coupling factors, e.g. by avoiding maintenance of adjacent CRDAs in the same overhaul, avoiding placement of the CRDAs with same age in adjacent core positions (also avoiding the placement of the fuel elements of same age in adjacent positions).
- Strategies to enhance early detection and removal of gradually developing CCF mechanisms, e.g. by periodic tests, follow-up and trending of performance characteristics, and follow-up and exchange of operating experience

Intensified performance trend analysis, e.g. follow-up of insertion times, could be a development option. But here are practical problems, because of the following facts:

- Reactor scrams (actual demands) and scram tests are infrequent in comparison to maintenance cycle. The maintenance events mean discontinuities that are difficult to control in verifying possible trends.
- Fuel elements are relocated and/or replaced in the refueling, which breaks certain failure mechanisms of control rod jamming and the possible associated trend
- Control rods and drives can also be replaced by spare components in maintenance. Therefore a CRDA individual may stay only limited time in the certain functional position (core position). And typically, the dismantled component undergoes maintenance before being possibly used in turn as a spare part.

On the other hand these facts – which make the performance trend analysis difficult – are effective CCF defenses as they break up the internal symmetry of the CRDA component group.

The effect of the defense strategies were discussed to some extent already in the earlier CRDA data analysis [SKI R-96:77, Sections 2.5 and 2.6]. More emphasis can be placed on this topic in the coming data analysis update. The wider database can facilitate a deeper investigation of various aspects such as statistical trends, recurrence patterns and time to effective removal of the root cause. It can be especially useful to infer the possible benefit of implemented design and maintenance changes to explain the positive statistical trend through preventing recurrence of certain generic failure types that caused problems in the earlier years.

The review of international experience and extensive literature about defense strategies can also be useful. Compare also to the work done in connection to diesel generator pilot study [RPC 91-57].

7 SUMMARY OF THE PROPOSALS

The survey conclusions are summarized in Table 7.1 in the form of proposed tasks for the CCF analysis update. The needed resources are not presented here; they depend much on the extent of desired contribution from the plants.

A further developed work and resource plan will be elaborated up to the next NPSAG meeting on January 16, 2002.

Table 7.1 Proposed tasks for the CRDA/CCF analysis update.

#	Task	
	NORDIC DATABASE	
1	Analysis and classification of the new events: - 1996-2001 for the Swedish BWRs - 1994-2001 for the Olkiluoto plant	
2	Verification of the event analysis for the earlier period (1983-95) for the Swedish BWRs; clarification of the discrepancies with respect to TUD classifications and failure rate estimations	
3	Drawing insights for the development of CCF defense strategies, e.g. periodic tests, preventive maintenance and performance follow-up	
4	Transfer of CCF event data into ICDE format including the outline for the CRDA classification guide	
	INTERNATIONAL DATA	
5	Review and evaluation of the CCF data used in the US and German studies for possible use as prior data for the Nordic PSA applications	
6	Complementary review of the world-wide BWR incident data in AIRS	
	CCF MODELS	
7	ICDE Benchmark for the CCF models applicable to CRDAs, e.g. CLM, AFM and Extended BFRM, as well as Beta CCF Method	
8	Placement of the validated CCF model tools into NPSAG/NAFCS domain	
	PSA APPLICATIONS	
8	Refinement of the reactivity shutdown criteria: separate study	
10	PSA updates for the reactor shutdown function, exchange of application expertise within NPSAG/NAFCS domain	

References

SKI R-96:77 Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Summary report, prepared by T. Mankamo. SKI Report 96:77, December 1996.

SKI/RA-26/96 CCF Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Work reports, prepared by T. Mankamo. SKI/RA-26/96, December 1996.

RS_BRAwr Barsebäck reference application. SKI/CCF Analysis of BWR reactor shutdown systems, Work report prepared by T. Mankamo, Avaplan Oy, 12 April 1994. Part of SKI/RA-26/96.

RS_SweDB BWR/Reactor shutdown systems, CCF data base, Swedish experience 1983-1995. Work report, T. Mankamo, Avaplan Oy, 30 December 1996. Part of SKI/RA-26/96.

TV_RSCCE CCF analysis of BWR reactor shutdown systems, based on the operating experience at the TVO I/II in 1981-1993. Prepared by T. Mankamo, Avaplan Oy, for the Finnish Centre for Radiation and Nuclear Safety, Report STUK-YTO-TR 100, April 1996. Also part of SKI/RA-26/96.

CR_RO22x Sammanställning av kommentarer vid RO-analys för drivdon/styrstavar (BWR). Anmärkningar, 1996-12-30. Part of SKI/RA-26/96.

T-BokenR T-Bokens data om drivdon/styrstavar (BWR). Anmärkningar, 1996-12-30. Part of SKI/RA-26/96.

RS_WWExp World-wide BWR experience on CCFs affecting reactor scram function. Work report, Avaplan Oy, 30 November 1996. Part of SKI/RA-26/96.

RS-PSA99 T. Mankamo, Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Int. Topical Meeting of Probabilistic Safety Assessment PSA'99, August 22-26, 1999, Washington, D.C.

NPSAG-CRDAs-USO
Outline for the Utility Survey. Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs. T. Mankamo, 11 September 2001.

CRDA-Agenda-011129
Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs - Survey Task. Working Meeting on 29 November 2001, Stockholm.

SWR-PSA SWR - Sicherheitsanalyse, Abschlussbericht, Teil 1. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-102/1, Juni 1993 (in German).

NUREG/CR-5500v3
Reliability Study: General Electric Reactor Protection System, 1984-1995. Prepared by S.A.Eide, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.3., February 1999.

RPC 91-57 Defences against CCFs and generation of CCF data, pilot study for DGs, quantitative analysis. Staffan Björe, ABB Atom AB, Report RPC 91-57, 15 October 1991

HR_CCFRe High redundancy structures, CCF models review. Work report prepared by Mankamo, T., Avaplan Oy, 31 December 1990.

ICDE-S-EdF
Vasseur D., Voicu A., Mankamo T., Bonnet C and Dewailly J., CCF Analysis in Progress at EdF. Overview of EdF Involvement in CCF

Analysis, e.g. Control Rod Application. ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, 12-13 Stockholm, 2001.

NAFCS-PR02
Data Survey and Review. Topical Report NAFCS-PR02, prepared by Tuomas Mankamo, Draft 2, 30 October 2001.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Draft 3, 18 October 2001.

NAFCS-PR04
Model Survey and Review. Topical Report NAFCS-PR04, prepared by Tuomas Mankamo, Draft 3, 23 October 2001.

NAFCS-PR06
Compilation and Results of Plant Survey. Topical Report NAFCS-PR06, under preparation by Per Hellström.

SPC 99-048 Forsmark 1 och 2, utvärdering av händelser för styrstavar. Mikael Heldesjö, ABB Atom AB, Rapport SPC 99-048, Rev.1, 1999-06-07.

CR-SPC-99-048
Kommentarer till SPC 99-048. T. Mankamo, Avaplan Oy, 10 August 2001.

CR-Combinatorics
Forsmark 1 and 2, evaluation of control rod failures [SPC 99 –048] – comments and remarks on the probability calculation and rod combinations. Tuomas Mankamo, Avaplan Oy, 17 August 2001.

Alm-HCCF Modellering av för högredundant CCF. Sven Erick Alm, Uppsala Universitet, 27 April 2001.

CR-Alm-Review
Response on Alm's Review of Extended Common Load Model. Tuomas Mankamo, 28 November 2001.

Acronyms

Acronym	Description
AFM	Alpha Factor Method
AIRS	Advanced Incident Reporting System (event database managed jointly by the IAEA and NEA)
BFRM	Binomial Failure Rate Model
BWR	Boiling Water Reactor
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CLM	Common Load Model
CRDA	Control Rod and Drive Assembly
ICDE	International CCF Data Exchange
NAFCS	Nordic CCF Analysis Group (task group of NPSAG)
NPSAG	Nordic PSA Group
NPP	Nuclear Power Plant
PWR	Pressurized Water Reactor
RO	Licensee Event Report (Rapportervärda Omständigheter)
RPS	Reactor Protection System
SKI	Swedish Nuclear Power Inspectorate
TUD	Information System for Reliability, Maintenance and Operation (Tillförlitlighet, Underhåll och Drift)

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
App 5.5	**Impact Vector Application to Diesels PR10**	**PR10**
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR10**

Title:	**Impact Vector Application to Diesel Generators**
Author(s):	*Tuomas Mankamo*
Issued By:	
Reviewed By:	*Michael Knochenhauer, 2002-10-30*
Approved By:	Gunnar Johanson
Abstract:	The Impact Vectors are constructed for Common Cause Failure events using diesel generators as a pilot object. The Nordic data are primarily processed. The foreign data are explored for comparison aims.

Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2002-01-15	TM
Draft 1	2002-05-31	TM
Draft 2	2002-08-26	TM
Draft 3	2002-10-04	TM
Issue 1	2002-10-31	TM
Final	2003-10-17	GJ

Contents

1. Introduction

1.1 Objective

This report documents the pilot task for the construction of Impact Vectors to interpret and pre-process Common Cause Failure (CCF) event information for the use in quantitative analysis, for the estimation of CCF parameters or direct estimation of multiple failure probabilities. Background work has been done in preparing a method description for the Impact Vectors based on the earlier uses of the method including international experiences. During the completion of this pilot application the method report was split into a practically oriented guideline [NAFCS-PR17] and theoretically oriented method description [NAFCS-PR03]. The interface with the quantitative analysis has been discussed also in connection to the CCF model survey [NAFCS-PR04].

The choice of diesel generators (DGs) for the pilot task is justified because of relatively good amount of event statistics as compared to other component types, see the CCF data survey [ICDE-PR02]. Besides, a detailed CCF analysis has been conducted for the DGs of Olkiluoto NPP (OL1/OL2), including construction of Impact Vectors and quantitative estimation [DGs-CCFA]. Furthermore, the earlier DG pilot study of the Nordic NPPs can be also benefited [RPC 91-57].

The objective of the pilot task is to develop framework, working procedures, database structures and QA procedures for the construction of Impact Vectors. The insights will be used for the further development of the Impact Vector guideline, adding type examples to facilitate practical work in the continuation.

1.2 Scope

The pilot task covers DG events as reported to ICDE (status in December 2001) for the Nordic NPPs, including Loviisa NPP (LO1/LO2). The observation period reported to ICDE for the Swedish NPPs is reduced, meaning a need to extend the coverage in the continuation. The Nordic DG CCF events will be handled in Section 2 (summary tables of the processed events are presented in Appendix 1). A redundant assessment of the Impact Vectors has been conducted and proved very useful for the enhanced quality and accuracy of the results, see Section 2.3. The assessments presented in this issue are the completed ones after discussion of arguments for the differences in the base and redundant assessments. Specific insights from the Impact Vector construction are gathered in Section 2.7.

Selected foreign CCF data, particularly of a same DG manufacturer as in the Nordic NPPs was also aimed for the comparison aims, and to experiment with mapping to Nordic target configurations and using the foreign information as a prior data. This part of the pilot task was completed with reduced ambition level due to difficulties encountered, and was reduced to pooling of ICDE data for all DGs of group size 4, generating only high and low bounds of the Impact Vectors for comparison, see Section 3. The data pooling and mapping practices could not thus be really experimented.

General insights and recommendations about the continued work will be summarized in Section 4.

1.3 QA and documentation

The principal QA action was constituted by the redundant assessment of the Impact Vectors by Jean-Pierre Bento, JPB Consulting AB. The followed procedure will be described in Section 2.3, and details in the logging notes [NAFCS-WN-TM02].

The working material has been discussed in several NAFCS meetings during the course of the pilot. At the end, Michael Knochenhauer, Impera-K AB, made a comprehensive review of the final draft for this topical report.

The overall QA procedure proposes that the members of the NAFCS group perform a general audit of the Impact Vector construction to verify the coherence and sensibility of the assessments and adequacy of the documentation, see [NAFCS-PR17]. This activity is not yet (systematically) undertaken. It has to be planned into the coming NAFCS activities.

In addition to this topical report, working material is collected into several documents, see Table 1.1. The working material will be archived as part of the NAFCS CCF database system, and will be accessible to the data users. Besides, central additional information, if existing in a document form such as plant incident report, will also be stored in order to facilitate future exploration aims. (These references are named in the Impact Vector construction sheets but not collected into Table 1.1.)

Table 1.1 Documents of the DG pilot, compare to the reference list.

Document index	Title	Last update
NAFCS-PR10	Impact Vector Application to Diesel Generators	31-Oct-02
NAFCS-DG-SF-ImpVe-TM-V2	Base Assessment of the Impact Vectors in DG Pilot	07-Sep-02
R0209-ES-Impact Vector	Redundant Assessment of the Impact Vectors in DG Pilot	06-Sep-02
NAFCS-WN-TM02	Logging Notes of the Impact Vector Assessment in the DG Pilot	18-Sep-02
NAFCS-WN-TM03	Comments on the ICDE database for the information stored about the Finnish and Swedish DGs, feedback from the Impact Vector assessment	23-Sep-02

The procedure and practical steps of the Impact Vector construction are described in the guideline [NAFCS-PR17], which is backed up by the separate method description [NAFCS-PR03]. The methodological report discusses in more detail special cases that can be encountered when considering complicated CCF mechanisms. It also covers the interface to the quantitative analysis and estimation of CCF model parameters. The insights gained during the DG pilot have been benefited when upgrading the guideline and method description.

2. Nordic CCF events of DGs

2.1 Observed population and coverage of the ICDE data

The observed DG population of the Nordic NPPs and general exposure data are summarized in Table 2.1. The reactor units are grouped and sorted in the order of plant generation and DG manufacturer. The observation times for the Swedish units are limited to 1989-97, except 1987-97 for B1/B2 (partially assumed, the statistical records are not complete in the ICDE database). For OL1/OL2 the observation period is 1983-97, same as in the recent plant specific CCF analysis [DGs-CCFA]. For LO1/LO2 the observation period is from the start of the operation up to 1997.

Table 2.1 The observed DG population of the Nordic NPPs (ICDE database in Dec.2001).

Units	CCCG size	DGs	Manufacturer diesel/generator	CCCG years	DG years	CCF events
B1/B2	2	2 x 2	MTU	22	44	3
O1/O2		2 x 2	MTU	18	36	4
F1/F2	4	2 x 4	SACM	18	72	1
R1/R2		2 x 4	SACM	18	72	1
OL1/OL2		2 x 4	SACM/ASEA	30	120	12
F3	4	1 x 4	NOHAB Wärtsilä	9	36	1
O3		1 x 4	NOHAB Polar	9	36	1
R3/R4		2 x 4	NOHAB Wärtsilä	18	72	4
LO1/LO2	4	2 x 4	AGO/Strömberg	40	160	2
Sum		56		182	648	29

Table 2.1 summarizes the number of reported CCF events, summing up different failure modes. In the average one CCF event has occurred per DG group in every six years (CCCG year which is same as reactor year in the considered population). Or actually, so many events have been reported to ICDE. The Swedish units are close to this average taking into account the statistical uncertainty, while there are

- more events for OL1/OL2, about one CCF event every three CCCG year, and
- less for LO1/LO2, F1/F2 and R1/R2, only one CCF event in about twenty CCCG years

These deviations seem to be statistically significant and it would be highly interesting to infer, whether the differences are real, or perhaps related to different screening threshold of ICDE reporting.

The rate of CCF events per CCCG year is about by a factor of 2 higher for CCCG size of 2 than for CCCG size of 4. This is somewhat strange, because the ratio should be in the opposite direction, typically in the range of 2 to 4, depending on the level of dependence. (This is basically related to the fact in a CCCG size of 4 there are altogether 11 combinations of the components for multiple failure of degree two through four, while in a CCCG size of 4 only one combination.) Tentative explanations are following:

- The most apparent explanation may be that the reactor units with two DGs represent older plant generations. Several of the observed CCFs in these groups are related to aging effects
- The physical, process and functional separation of the redundancies is not as effective at the older units as at the newer units.

Due to the relatively small number of CCFs at the older units it is not possible to confirm the actual reasons with statistical significance. Anyway, the observed difference has relevance for any pooling of the statistics such as by mapping up event data from DG groups of size 2 to size 4. This controversial issue is discussed more comprehensively in [NAFCS-PR03].

2.2 Procedure for Impact Vector construction

The analysis of the CCF events and Impact Vector construction is generally organized so that CCCG size 2 and 4 are handled separately. The work was started from OL1/OL2 events as they are familiar to the author from the earlier plant specific analysis [DGs-CCFA]. (There did not appear any need to reconsideration of OL1/OL2 events, only the earlier processed information was transferred into the new format.) Otherwise, the analysis order followed plant generations as presented in Table 2.1.

The general scheme of the Impact Vector construction is presented in Fig.2.1. For the details of Impact Vector construction sheet, see Appendix 2 (which shows two examples, the full material is documented in [NAFCS-DG-SF-ImpVe-TM-V2, R0209-ES-Impact Vector] for the base and redundant assessment, respectively). Briefly described, the CCF event description and selected classifications which are used in the Impact Vector construction are extracted into the first table on the sheet. The second table reproduces component event vectors describing event timing, detection and impairment (degradation) assessment for each component in the group, for the considered CCF event. The supplementary sources are needed (desired) to more thoroughly understand the complicated cases, including past events related to the considered failure mechanism. This may require the exploration of several related plant event reports. Insights about the additional gain from the use of supplementary sources will be discussed in Section 2.7.

The derived Impact Vectors are summarized with primary event information in spreadsheet tables for CCCG size 2 and 4, respectively, see Appendix 1. The principal observations are gathered and discussed in Sections 2.5-7.

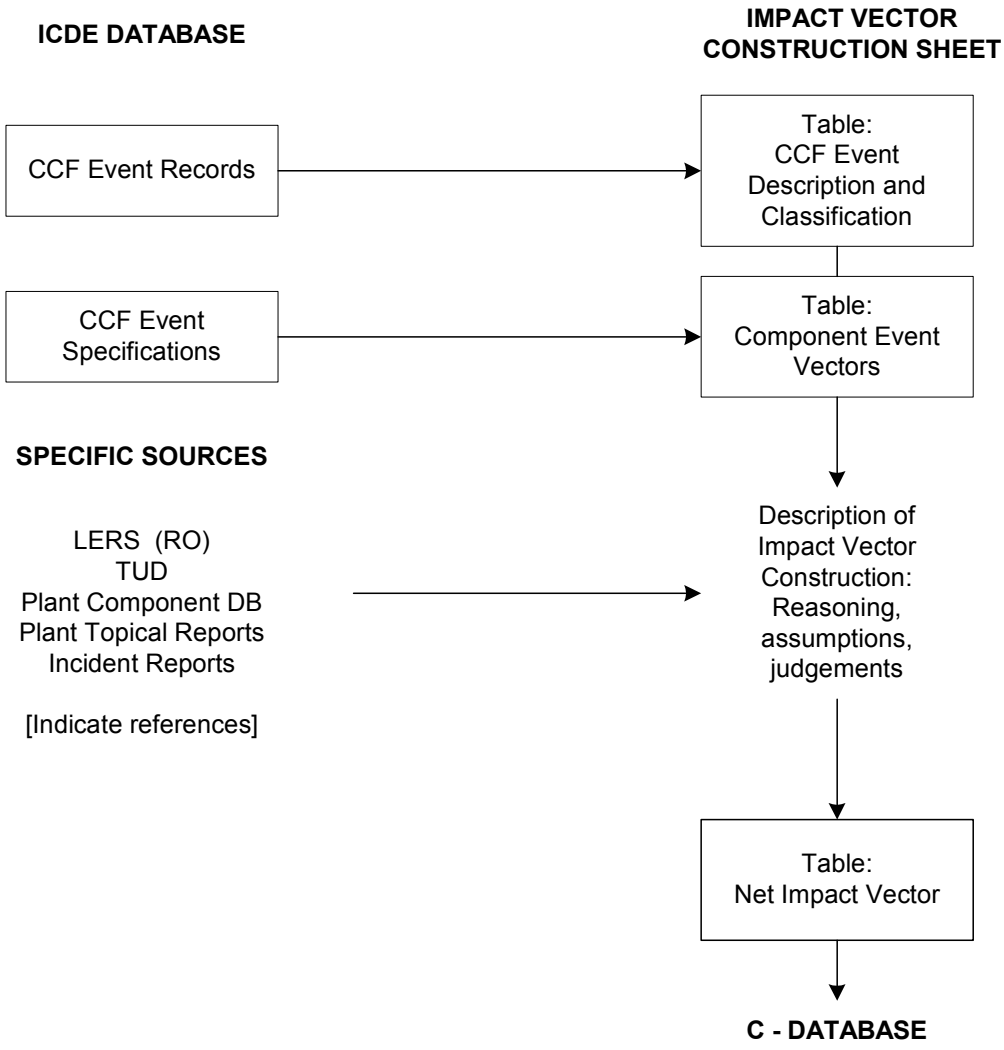


Figure 2.1 Impact Vector construction scheme.

2.3 Redundant construction of Impact Vectors

The American QA procedures for CCF analysis and classification (compare to [NUREG/CR-6268v3]) are followed in the aspect, that a redundant assessment of the Impact Vectors is conducted by Jean-Pierre Bento, JPB Consulting AB. For this purpose the versions of the Impact Vector sheets reduced to event description part were submitted to the redundant analyst. The drafted method description and guideline for Impact Vector construction and other source references as well as the Swedish ROs were available to him. The 1st versions of the redundant assessment and 2nd round of the base assessments were exchanged on August 08, 2002. The differences were identified and grouped according to the type. The arguments behind the differences were discussed between the analysts on August 28, 2002. The procedure for completion and documentation was agreed, including retrieval of additional information about some more complicated events. As expected, in part of the differing assessments the mutual clarification of the arguments resulted in consensus. In the remaining differing cases the following resolutions are suggested in the quantification stage:

- Same logic but quantitative judgments differ (different weights of the hypotheses): the best estimate of the net Impact Vector is derived by average of the weights. The differing initial weights are still documented to serve the uncertainty assessment in the CCF parameter estimation
- Different logic (different hypothesis structure): the best estimate of the net Impact Vector is derived by average of the net Impact Vectors of the two analysts. The initial hypothesis structures are still documented to serve the uncertainty assessment in the CCF parameter estimation

Effectively, in both types of the cases equal weights are given to the assessments of the two analysts. The final documentation includes:

- Completed assessments of the two analysts [NAFCS-DG-SF-ImpVe-TM-V2, R0209-ES-Impact Vector]
- Logging notes of the differences and their resolution [NAFCS-WN-TM02]
- Feedback comments on the information stored to ICDE database, e.g. proposals to supplement event descriptions and align the code classifications for consistency from plant-to-plant [NAFCS-WN-TM03]

The logging notes describe also in more detail difficulties encountered in the analysis of more complicated events and the way of problem solving. The general insights and lessons learnt will be discussed in Section 2.7.

It is indispensable that this suggested documentation approach will be confirmed by the side of the quantitative assessment as providing adequate and sufficient input to the CCF parameter estimation and uncertainty assessment.

In order to complete the QA it is proposed that the other members of the NAFCS group perform a general audit of the Impact Vector construction to verify the coherence and sensibility of the assessments and adequacy of the documentation. It is important that the QA verification is formally documented including any observations, comments and reservations.

2.4 Connection to CCF database

There is still no outline for the planned (quantitative) CCF database. This section will discuss preliminary how the Impact Vector construction and results are linked to the coming database:

- The primary link is constituted by the assessed net Impact Vectors (to be mainly displayed by hypothesis structure and assessed weights of the alternative hypotheses)
- The redundant assessment is to be documented as presented in the previous section
- The essential supplementary sources (e.g. ROs) used in the Impact Vector construction in addition to ICDE information should both be explicitly referenced and an electronic copy to be stored into a special folder in the coming CCF database (in the cases where the supplementary source influences the assessment)

In addition, the guideline and method description [NAFCS-PR03, -PR17] should be kept up-to-date in order to facilitate homogeneity and coherence of the assessments. Example cases should be gradually developed further. In type cases the specific

assessments should refer to the guideline and examples to make documentation more compact and to reduce unnecessary repetition of the similar types of argumentation.

2.5 Summary of the results

The Impact Vector assessment results are summarized in Tables 2.2-3 and Figs.2.2-3. In the summaries presented here the latent failure modes and monitored failure modes are lumped together, respectively, to simplify the comparisons, see Table 2.4. The generation of high and low bounds will be discussed in Section 2.6. The average multiplicity is defined for the basic Impact Vector v(m|n) in the following way:

$$\text{AvMult} = \sum_{m=1}^{n} m.v(m|n) \qquad (2.1)$$

For the sum Impact Vector of the observed population it is derived as an average over the CCF events. It characterizes the mean failure multiplicity in the observed statistics.

An important aspect is the need to make distinction between latent and monitored failures (and CCFs) which may not been clearly understood thus far in ICDE context. This is particularly essential in the quantitative analysis (CCF parameter estimation, modelling and quantification). The assessment of Impact Vector is usually much simpler for the monitored failures. The distribution of analysed events are summarized in this regard in Table 2.4.

Table 2.4 Distribution of the CCF events with respect to functional failure modes.

Failure Mode	CCG Size		Sum
	2	4	
Latent failures: FS Failure to start FR Failure to run	5	15	20
Monitored failures: MC Monitored critical MR Monitored repair-critical	2	7	9
Any	7	22	29

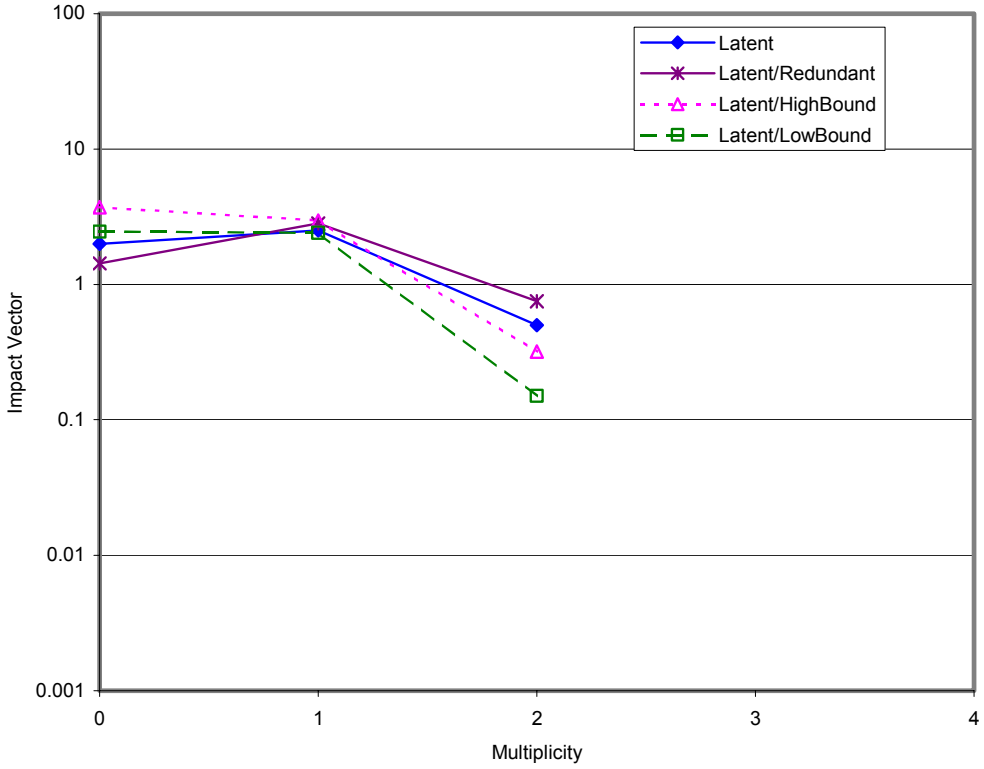
The differences in the base and redundant assessment are reasonable taking into account the difficulties in the assessment and all uncertainties. The differences are larger for some events but are levelled off in the combined statistics. It is important to notice that the judgments deviated into both directions, i.e. no bias between the two analysts in the DG Pilot. The comparison can be further facilitated by transferring the sum Impact Vectors into form of SGFPs, and looking Psg entity, see Fig.2.4. The great benefit of using Psg entities for comparison is the fact that it describes the dependence profile of the increasing failure multiplicity without “disturbance” of combinatorics and order exclusion which affect the other SGFP entities and Impact Vector as well.

Table 2.2 Summary of the assessed Impact Vectors for CCCG Size = 2.
See graphical comparison in Fig.2.2.

	Impact Vector						Average
	0	1	2	3	4	Sum	multiplicity
Latent	2	2.5	0.5			5	0.70
Monitored		0.5	1.5			2	1.75
	2	3	2			7	
L_Redundant	1.43	2.82	0.75			5	0.86
M_Redundant		0.5	1.5			2	1.75
	1.43	3.32	2.25			7	
L_HighBound	3.72	2.96	0.32			7	0.51
M_HighBound		1	1			2	1.50
	3.72	3.96	1.32			9	
L_LowBound	2.45	2.4	0.15			5	0.54
M_LowBound		1	1			2	1.50
	2.45	3.4	1.15			7	

Table 2.3 Summary of the assessed Impact Vectors for CCCG Size = 4. .
See graphical comparison in Fig.2.3.

	Impact Vector						Average
	0	1	2	3	4	Sum	multiplicity
Latent	6.735	7	2.743	0.324	0.198	17	0.84
Monitored	3.14	1.66	1.19	0.01	1	7	1.15
	9.875	8.66	3.933	0.334	1.198	24	
L_Redundant	5.15	10.63	2.882	0.21	0.13	19	0.92
M_Redundant	3.36	1.41	1.22	0.01	1	7	1.13
	8.51	12.04	4.102	0.22	1.13	26	
L_HighBound	8.73	5.94	3.83	0.1	0.4	19	0.82
M_HighBound	3.2	0.5	2.2	0.1	1	7	1.31
	11.93	6.44	6.03	0.2	1.4	26	
L_LowBound	11.01	8.044	2.601	0.331	0.015	22	0.65
M_LowBound	5.58	1.642	1.779	5E-04	1	10	0.92
	16.59	9.686	4.38	0.332	1.015	32	



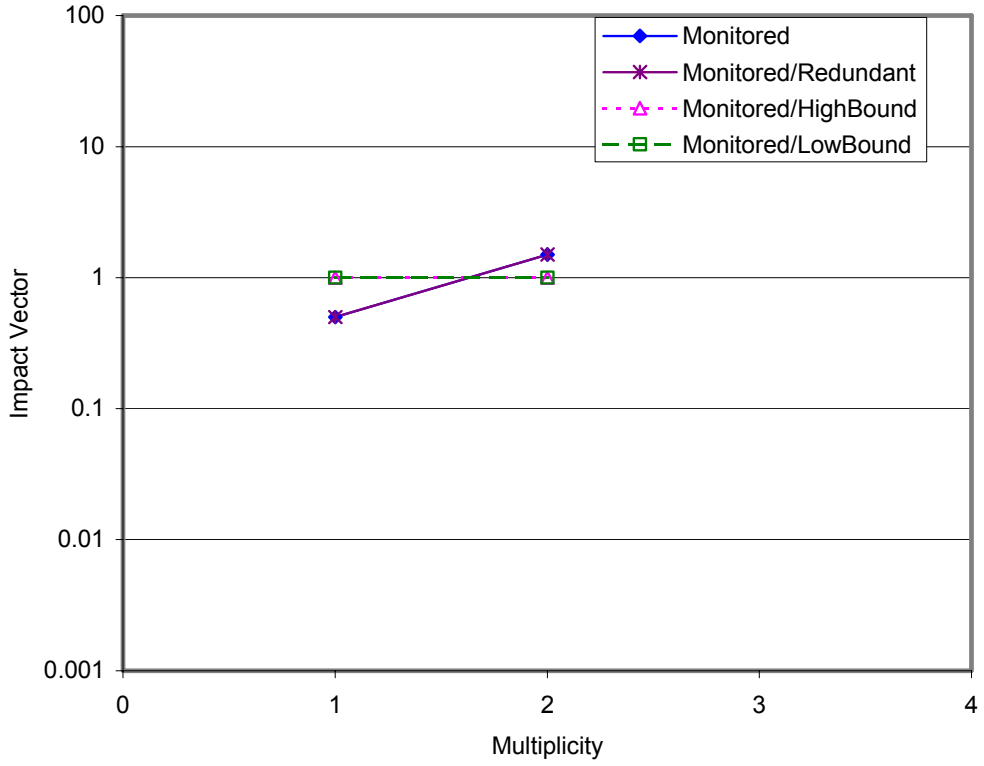
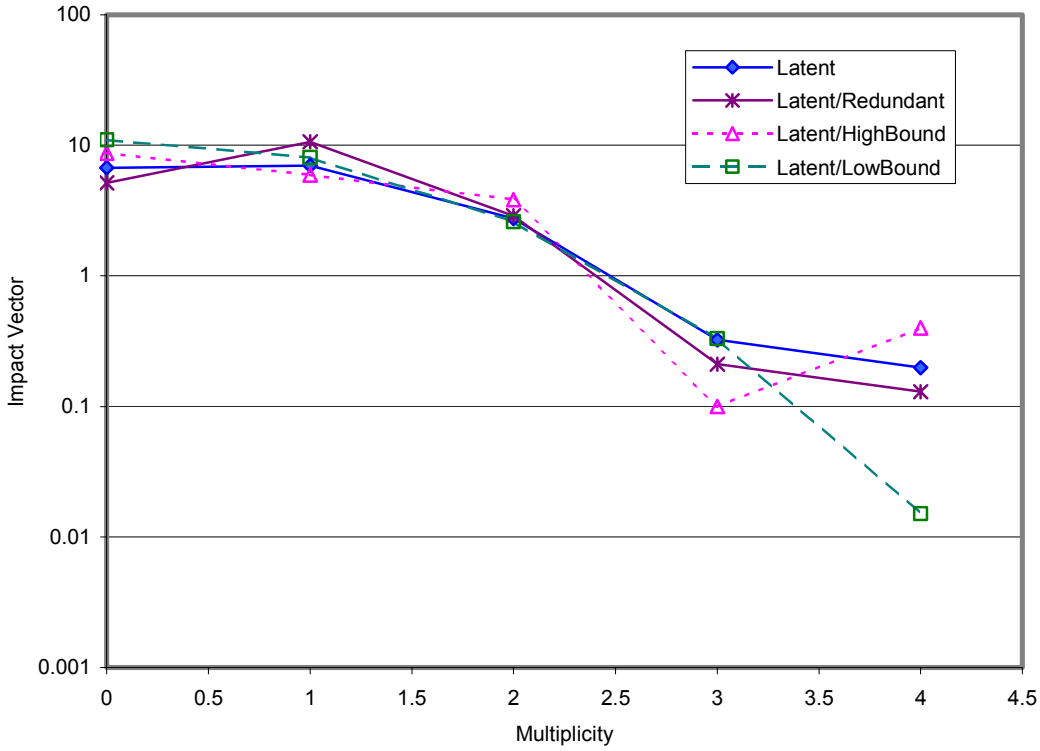


Figure 2.2 Comparison of the assessed Impact Vectors for CCCG Size = 2.
See numeric data in Table 2.2.



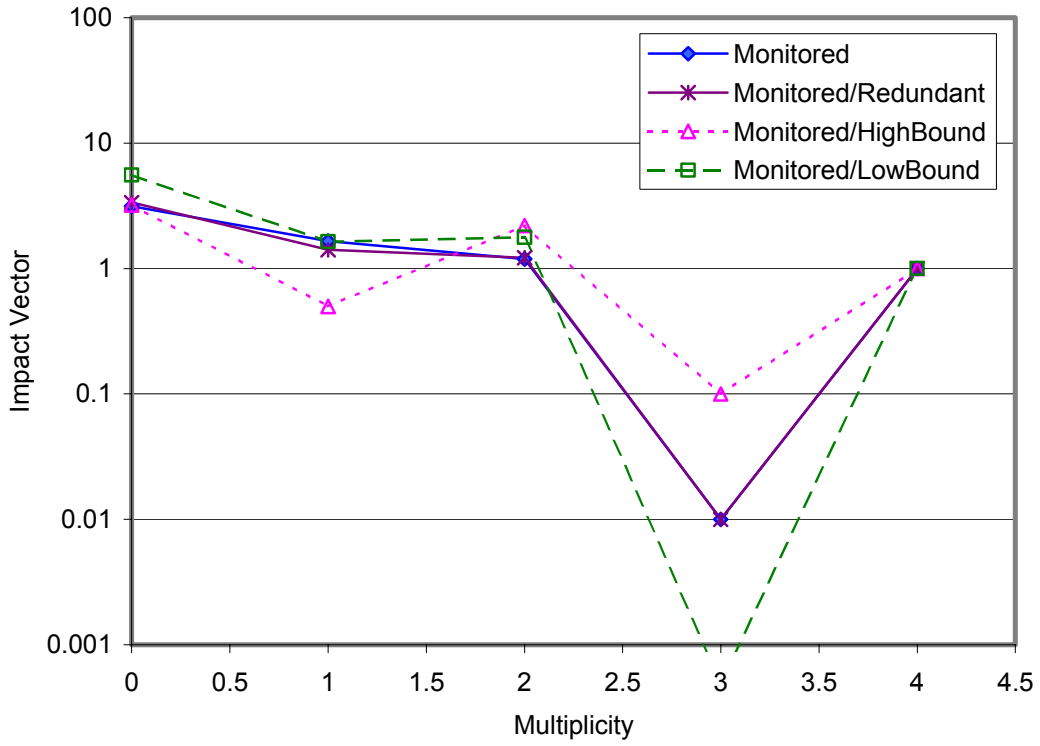


Figure 2.3 Comparison of the assessed Impact Vectors for CCCG Size = 4.
See numeric data in Table 2.3.

Entity		Multiplicity				
	0	1	2	3	4	Sum
Failure-free cycles	3635.5					3635.5
Single-failure cycles		190				190
CCFs, base	6.74	7.00	2.74	0.32	0.20	17.00
CCFs, redundant	5.15	10.63	2.88	0.21	0.13	19
	0	1	2	3	4	Sum
Sum Impact Vector, base	3642.2	197.00	2.74	0.32	0.20	3842.5
Sum Impact Vector, redundant	3638.7	200.63	2.88	0.21	0.13	3842.5
		1	2	3	4	
Alpha Factors, base		0.9837	1.37E-2	1.62E-3	9.90E-4	
Alpha Factors, redundant		0.9842	1.41E-2	1.03E-3	6.38E-4	
	0	1	2	3	4	
Pes(m|n), base	0.9479	5.13E-2	7.14E-4	8.43E-5	5.16E-5	1
Peg(m|n), base	0.9479	1.28E-2	1.19E-4	2.11E-5	5.16E-5	
Psg(m|n), base	1	1.33E-2	2.13E-4	7.26E-5	5.16E-5	
Pts(m|n), base	1	5.21E-2	8.50E-4	1.36E-4	5.16E-5	
	0	1	2	3	4	
Pes(m|n), redundant	0.9469	5.22E-2	7.50E-4	5.47E-5	3.38E-5	1
Peg(m|n), redundant	0.9469	1.31E-2	1.25E-4	1.37E-5	3.38E-5	
Psg(m|n), redundant	1	1.35E-2	1.86E-4	4.75E-5	3.38E-5	
Pts(m|n), redundant	1	5.31E-2	8.39E-4	8.85E-5	3.38E-5	
Psg(m|n), average	1	1.34E-2	1.99E-4	6.01E-5	4.27E-5	

Statistical input:			
Number of TDCs	ND	3842.5	
Independent count	Ni	190	
Number of TDCs with CCF	Nccf	17	
Total single failure probability	p_tot	1.33E-2	Base
		1.35E-2	Redundant

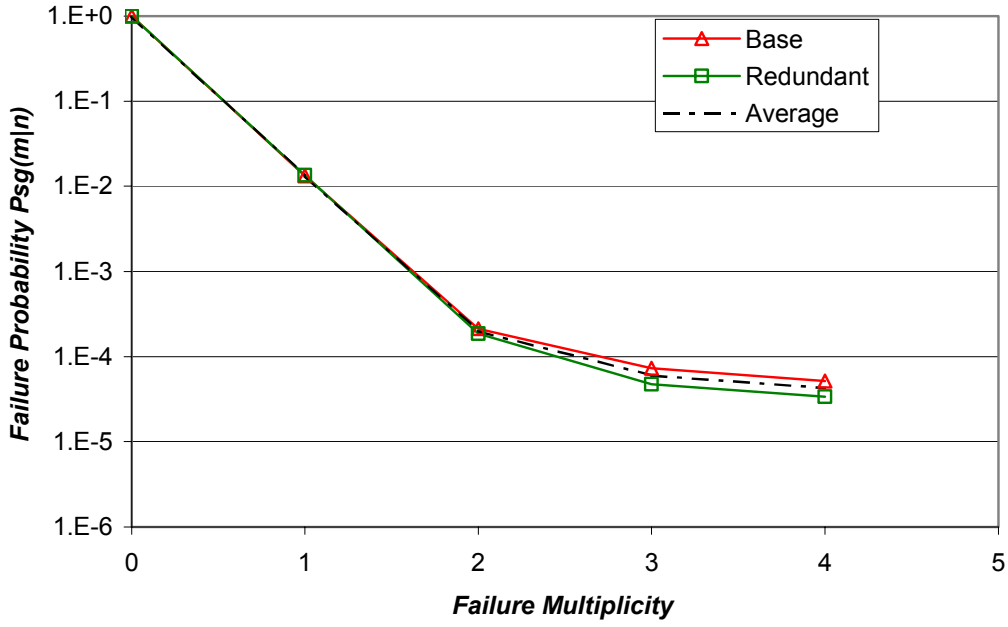


Figure 2.4 Comparison of the assessment results for CCCG Size = 4, when generated into form of Alpha Factors and SGFPs. The diagram compares derived Psg entities.

2.6 Comparison with Impact Vectors generated from ICDE codes directly

It was also experimented with the "formula-driven" US procedure [NUREG/CR-5485] to handle time-spread events and mixed degradation cases. This procedure assumes independence of the component degradation values (interpreted as conditional failure probability in the degraded condition), which may be optimistic in many cases. Thus the results obtained in this way can be regarded as a low bound of Impact Vector. For the details, see [NAFCS-PR03].

Correspondingly, a high bound of Impact Vector can be generated assuming complete dependence of the component degradation values. The details of the procedure for the calculation of the high bound are described in [NAFCS-PR03].

The results are summarized and compared to the mean of the specific assessments Fig.2.5.

The bounding calculations give very useful insights. They can be valuable also in the uncertainty analysis. However, it has to be noticed that the bounds are generated using component degradation values, Shared Cause Factor and Time Factor as presented in the ICDE database, and they include uncertainty. One principal use of the bounds derived for the event to be analysed is to support the specific assessment, which should stay within the bounds, assuming that the analyst agrees with the component degradation values, Shared Cause Factor and Time Factor.

2.7 Summary of the insights

The principal conclusion of the pilot underlines the worth and necessity to perform redundant assessments by two analysts in order to reach high quality CCF data. The count of type classes from the comparison between base and redundant assessment is presented in Table 2.5.

The possibility of large difference in the Impact Vector assessment is evidently connected to such situations where one of the analysts has less complete description of the event, or both analysts have different incomplete descriptions of the event. The lesson learnt is the vital importance of checking the plant event reports especially for any more complicated cases. It is also highly desired that the analysts have access to the plant experts to ask clarifications regarding uncertain event interpretations. In the DG Pilot, the additional information can be regarded essential for about 40% of the cases. In future work it is highly recommended that the Impact Vector assessment is made in parallel with the collection of the ICDE data, because this would save significant efforts for the plant experts and the analysts, and facilitate improved overall QA.

Entity		Multiplicity				
	0	1	2	3	4	Sum
Failure-free cycles	3633.5					3633.5
Single-failure cycles		190				190
CCFs, high bound	8.73	5.94	3.83	0.10	0.40	19
CCFs, low bound	11.01	8.04	2.60	0.33	0.015	22
	0	1	2	3	4	Sum
Sum Impact Vector, high bound	3642.23	195.94	3.83	0.10	0.40	3842.5
Sum Impact Vector, low bound	3641.51	198.04	2.60	0.33	0.0151	3842.5
		1	2	3	4	
Alpha Factors, high bound		0.9784	1.91E-2	4.99E-4	2.00E-3	
Alpha Factors, low bound		0.9853	1.29E-2	1.65E-3	7.51E-5	
	0	1	2	3	4	
Pes(m|n), high bound	0.9479	5.10E-2	9.97E-4	2.60E-5	1.04E-4	1
Peg(m|n), high bound	0.9479	1.27E-2	1.66E-4	6.51E-6	1.04E-4	
Psg(m|n), high bound	1	1.34E-2	2.83E-4	1.11E-4	1.04E-4	
Pts(m|n), high bound	1	5.21E-2	1.13E-3	1.30E-4	1.04E-4	
	0	1	2	3	4	
Pes(m|n), low bound	0.9477	5.15E-2	6.77E-4	8.62E-5	3.93E-6	1
Peg(m|n), low bound	0.9477	1.29E-2	1.13E-4	2.15E-5	3.93E-6	
Psg(m|n), low bound	1	1.33E-2	1.60E-4	2.55E-5	3.93E-6	
Pts(m|n), low bound	1	5.23E-2	7.67E-4	9.01E-5	3.93E-6	

Statistical input:

Number of TDCs	ND	3842.5	
Independent count	Ni	190	
Number of TDCs with CCF	Nccf	19	
Total single failure probability	p_tot	1.34E-2	High
		1.33E-2	Low

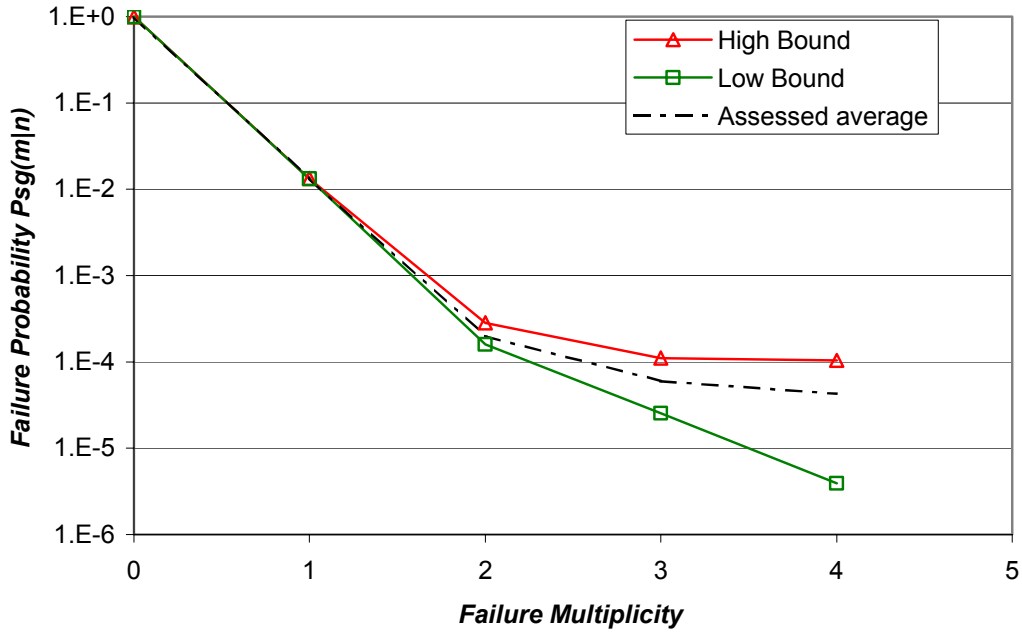


Figure 2.5 Comparison of the bounding Impact Vectors for the Nordic CCCG Size = 4, when generated into form of Alpha Factors and SGFPs. The diagram compares derived Psg entities.

Table 2.5 Comparison type classes.

Type class	Description	Count
1	Identical assessment, evident impact	3
2	Identical assessment, follows guide example	3
3	Identical assessment, consensus reached after discussion of the arguments, typically additional clarification had to be obtained from the plant	4
4	Same hypothesis structure, differing weights	7
5	Differences in hypothesis structure, typically weak degradation cases where one of the analysts considered the chances of higher order failure	10
6	Basic differences in the assessment logic, e.g. one of the analysts used a specific causal model or parametric dependence model to support the assessment	2
		29

In most part of the cases (the simpler end of the spectrum) the information stored in the ICDE database was felt quite sufficient for Impact Vector construction. In fact, in some cases the event descriptions prepared for the ICDE are better (more informative and more logically made) than the original plant event report. In more complicated cases the read-through of the plant event reports, and plant incident reports when available, are essential to adequately (sufficiently) understand what happened. This is especially valid for time spread events (gradually developing, recurring failure mechanisms).

The 1st round of base assessments for the Swedish events were made merely using ICDE information. In the 2nd round the read-through of the Swedish plant event reports (RO/LERs) resulted in the change of the assessment in two cases (SF23 and SF25). In three cases (SF16, SF21 and SF22) RO gave essential detailed information which, however, supported the initial assessment. In the other cases (about two thirds of all Swedish cases) the event description in ICDE was about as well as in the RO for the purpose of Impact Vector construction.

The event analysis during the DG Pilot revealed several remarkable inconsistencies or essential shortcomings in the ICDE event descriptions. The comments in these regards will be gathered separately and submitted to the ICDE contact persons at the plant for further measures [NAFCS-WN-TM03].

3. Foreign CCF events of DGs

3.1 Overview of the ICDE database contents for DGs

The overall number of observed CCCGs and reported CCFs are presented in Table 3.1. It is peculiar to notice that the reporting threshold seems to be significantly lower for the Nordic NPPs. It shall also be noticed that the covered DG population is not homogeneous. There are some gas turbines and several types of dedicated diesels by side of the ordinary DGs for emergency power supply. The pilot application was confined to the ordinary DGs for emergency power supply.

Table 3.1 DG data in the ICDE database as of December 2001.

Member country	CCCG count	CCF count
Finland	6	14
Sweden	12	15
France	13	15
Germany	40	9
Spain	8	3
Switzerland	6	3
United Kingdom	28	11
USA	110	48
In total	223	118

The CCCG records for Loviisa 1 and 2 are duplicated. Presumably intention is to include the dedicated DGs of the Additional Emergency Feedwater System besides of the ordinary DGs for emergency power supply? (A question mark has been presented about this observation in [NAFCS-WN-TM03].)

The ICDE summary report for the DGs contains useful insights, e.g.

- Summary CCF statistics [ICDE-PR02, Table 5-1]
- Distribution of CCCG size [ICDE-PR02, Table 5-2]
- Discussion of root causes/coupling factors/affected subsystem/degree of impact (partial – complete CCF)

These collected insights will be useful in the future mapping of the foreign statistics to the Nordic target applications.

3.2 Exploration of selected foreign populations

Preferred foreign sources are as homogeneous sub-populations as possible. One recommended option is to consider the data from the DGs with same manufacturer. For example, for the needs of Olkiluoto PSA it would be of interest to look after the SACM diesels. There are in 22 CCCGs of SACM diesels in the current ICDE database; Finland: 2, Sweden: 4, France: 7, Germany: 4, Spain: 3 and Switzerland: 2. Compare to Table 2.1, which shows the SACM diesels of the Nordic NPPs. The data volume of the SACM diesels is presented in Table 3.2. Seemingly, only part of the SACM DGs at the French NPPs are covered in the ICDE databse. All in all there

are unfortunately only two CCCGs of size 4 or 5 in the other European countries. The utilization of the data from smaller groups would necessitate the use of controversial and uncertain mapping up to the Nordic target size of 4 (compare to the deeper discussion of this problem in [NAFCS-PR03]). Thus this route must be regarded as not meaningful at the time being for practical purposes.

Table 3.2 Existing data for SACM DGs in the ICDE database as of December 2001.

CCCG size	Region	Group count	CCF count
2	Europe	11	9
3	Europe	3	2
4	Europe	1	0
	Nordic	6	13
5	Europe	1	0
Any		22	24

Another initial idea was to utilize US data. For this aim the data volume for the DGs from the US plants are presented in Table 3.3. Unfortunately, for this option also, no meaningful statistics exist for the CCCGs of size 4 to 5. The component impairment values for the three reported CCF events in the bigger DG groups of the US plants are: `CCWW, IIII, DDIII`. They carry relatively little information. For CCCG size of 2 there are abundant statistics from the USA, but as reference data for the Nordic target size of 2 it is preferred to take processed CCF data (including Alpha Factors as well) directly from [NUREG/CR-5497]. Mapping up would not be meaningful as already noted.

Table 3.3 Existing data for DGs at US plants in the ICDE database as of December 2001.

CCCG size	Region	Group count	CCF count
2	USA	76	24
3	USA	17	20
4	USA	13	2
5	USA	2	1
Any		108	47

3.3 Foreign pooled data of CCCG size of 4

After the two non-successful attempts described in the previous section it was decided to conduct following exercise:

- Simply pool the data of all foreign CCCGs of size 4
- Only calculate mechanically high and low bounds of the Impact Vectors similarly as in Section 2.6 for the Nordic data
- Skip the specific Impact Vector assessment and mapping to the Nordic conditions as too laborious task in comparison to the expected gain; compare to further discussion of this aspect in the next section.

The volume of the pooled data are shown in Table 3.4. The gas turbines (three groups) from Great Britain are excluded. But the special type of DGs for dedicated use to supply EW pumps (7 out of the 21 German groups) are retained for simplicity. This means no direct effect to the comparisons that will be presented. It is peculiar to notice that the total number of reported CCFs is relatively small in comparison to the Nordic plants, i.e. their use as a priori data is poor. Furthermore, it should be noticed that the number of reported CCFs is as low as one per 18 group years, which is by a factor of three lower as the average of the Nordic plants, but in line with the data from LO1/LO2, F1/F2 and R1/R2.

Table 3.4 Pooled data for DG CCCGs of size 4 in the ICDE database as of December 2001. (Mostly latent failures, see text.)

Region	Group count	Group years	CCF count
Czech	1	10	0
Germany	21	105	7
Great Britain	7	63	3
Spain	2	12	3
USA	13	78	2
In total	44	268	15

In the comparison that follows all reported 15 foreign events are conservatively handled as latent failures (failure modes FS and FR, compare to Table 2.4 for the statistics of the Nordic DG groups of size 4). The background is that failure detection (ICDE code C06) is not consistently used in the foreign countries. According to the event descriptions it seems that three cases may be monitored failures. However, the component impairment values in each of these three cases are `IIII`, so their inclusion has negligible effect to the bounding Sum Impact Vectors.

The bounding Sum Impact Vectors are presented in Table 3.5. For the complete statistics the following additional steps are needed, compare to the similar procedure used in Section 2.6 for the Nordic data:

- The number of TDCs is approximated by dividing the group years by the nominal test interval
- The number of single-failure cycles (independent count) is available in the ICDE data only for Czech, Spain and USA. For the whole population it is derived by assuming constant single failure rate
- Finally, the number of failure-free cycles is obtained by subtracting single-failure cycles and CCF cycles (sum of the Impact Vector elements) from the total number of TDCs

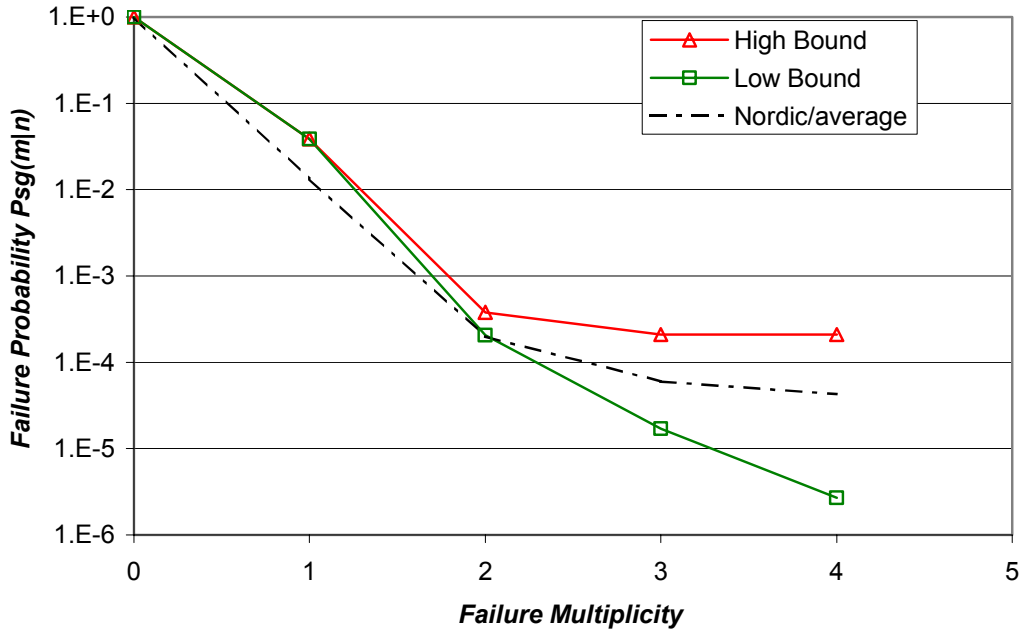
In order to facilitate comparisons, the Impact Vector results are then used to derive Alpha Factors and SGFP entities. For the details of the derivation procedure, see [NAFCS-PR04].

For comparison purpose the Psg diagram below Table 3.5 shows also the mean Impact Vector of the Nordic data. The main insight from the comparison with respect to the

Table 3.5 Generated high and low bound Impact Vectors for the pooled data for foreign DG CCCGs of size 4 in the ICDE database as of December 2001. The lower part of the table presents corresponding Alpha Factors and SGFP entities.

Entity	Multiplicity					
	0	1	2	3	4	Sum
Failure-free cycles	2618.4					2618.4
Single-failure cycles		463.6				463.6
CCFs, high bound	11.30	8.90	3.15	0	0.65	24
CCFs, low bound	9.82	10.76	3.24	0.18	0.0083	24
	0	1	2	3	4	Sum
Sum Impact Vector, high bound	2629.70	472.50	3.15	0	0.65	3106
Sum Impact Vector, low bound	2628.22	474.36	3.24	0.18	0.0083	3106
		1	2	3	4	
Alpha Factors, high bound		0.9920	6.61E-3	0	1.36E-3	
Alpha Factors, low bound		0.9928	6.78E-3	3.71E-4	1.74E-5	
	0	1	2	3	4	
Pes(m|n), high bound	0.8467	1.52E-1	1.01E-3	0	2.09E-4	1
Peg(m|n), high bound	0.8467	3.80E-2	1.69E-4	0	2.09E-4	
Psg(m|n), high bound	1	3.87E-2	3.78E-4	2.09E-4	2.09E-4	
Pts(m|n), high bound	1	1.53E-1	1.22E-3	2.09E-4	2.09E-4	
	0	1	2	3	4	
Pes(m|n), low bound	0.8462	1.53E-1	1.04E-3	5.71E-5	2.68E-6	1
Peg(m|n), low bound	0.8462	3.82E-2	1.74E-4	1.43E-5	2.68E-6	
Psg(m|n), low bound	1	3.87E-2	2.05E-4	1.69E-5	2.68E-6	
Pts(m|n), low bound	1	1.54E-1	1.10E-3	5.97E-5	2.68E-6	

Statistical input:			
Number of TDCs	ND	3106	
Independent count	Ni	463.6	
Number of TDCs with CCF	Nccf	24	
Total single failure probability	p_tot	3.87E-2	High
		3.87E-2	Low



Nordic data is qualitatively reasonable compatibility. The level of failure probability is by a factor of about two higher in the foreign data in comparison to the Nordic data. This holds also for the total single failure probability, compare p_tot estimates in Table 3.5 and Fig.2.5.

3.4 Application considerations

The uses of the foreign data prove to be reduced at the time being to general comparisons and qualitative uses. The principal shortcoming is the lack of specific Impact Vector assessments for the foreign data made by the source analysts. Besides, one can expect substantial variability in how, for example, the ICDE codes are interpreted and applied in the event classification from country to country. The insights from the Impact Vector assessments for the Nordic events show that doing the work for the foreign events with acceptable quality and controlled uncertainty is not possible from abroad. It is thus highly desired that the ICDE data would be processed further for quantitative aims in each ICDE country with proper support from the plant specialists. Guidance should be developed to enhance consistency of the severity scaling and assessment by different analysts.

Generating high and low bound Impact Vectors is, however, relatively simple and useful for comparison aims, facilitating also qualitative uses of the foreign data, and reasonably robust with respect to the uncertainties.

Observation: only two CCCGs (size 2) are tested sequentially, in all other groups of DGs in the current ICDE database testing is staggered. This is “unfortunate” regarding the possibility to see the eventual influence of test staggering on CCFs. Test interval varies from 14 days through 56 days, which may allow to draw insights from the test interval impact.

4. Concluding remarks

The insights from the pilot are encouraging. Especially the redundant assessment of the Impact Vectors proved highly useful to reach good quality results. The specific insights from the pilot were discussed in Section 2.7 in detail, and will not be repeated here. One of the lessons learnt is the importance for the analysts to have access to additional information beyond ICDE data about more complicated events, e.g. plant event reports and possibility to contact plant specialists. Related to this aspect, the utilization of foreign data proved difficult except qualitative and comparison aims.

It is expected that the labour requirements will be reduced in the continuation for new assessment efforts (valves and pumps are planned as next steps) due to learning effect and possibilities to unburden the documentation work by moving from the use of standard office software to relational database platform (under design). At the best, the assessment of the Impact Vectors should be done in parallel to the initial ICDE data collection. This would save significant efforts for both the plant experts and analysts, and facilitate improved overall QA.

Improving the possibilities to utilize foreign data for comparison and pooling purpose requires that similar event processing for quantitative aims would be undertaken in each ICDE member country.

Recommendations for the next steps:

- Develop the general audit procedure to verify the coherence and sensibility of the assessments, and adequacy of the documentation. The QA verification should be formally documented including any observations, comments and reservations
- Check the working interface with the quantification (parameter estimation, uncertainty evaluation)
- Develop database system including documentation and archive framework (this should integrate both Impact Vector assessment and quantification)
- Improve the Impact Vector guideline and method description, supplement example cases

Acknowledgements

The key contribution of Jean-Pierre Bento, JPB Consulting AB, is acknowledged in the form of redundant assessment of the Impact Vectors, bringing in the pilot an independent professional grip and in-depth knowledge about the Swedish experience. This greatly enhanced the quality of the results.

Michael Knochenhauer, Impera-K AB, reviewed the final draft. His comments and suggestions have contributed in many respects to the completed report.

The NAFCS members have in general given valuable contribution in conducting this task at various stages through the discussions and comments.

References

NAFCS-Programme-R1
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR03 Impact Vector Method. Prepared by Tuomas Mankamo, Issue 2/Outline, 12 October 2002.

NAFCS-PR04 Model Survey and Review. Prepared by T. Mankamo, Draft for Peer Review, 12 January 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-DG-SF-ImpVe-TM-V2
Base Assessment of the Impact Vectors in DG Pilot. Third round by Tuomas Mankamo, 07 September 2002.

R0209-ES-Impact Vector
Redundant Assessment of the Impact Vectors in DG Pilot. Second round by Jean-Pierre Bento, 06 September 2002.

NAFCS-WN-TM02
Logging Notes of the Impact Vector Assessment in the DG Pilot. Work notes by T. Mankamo and J-P. Bento, 18 September 2002.

NAFCS-WN-TM03
Comments on the ICDE database for the information stored about the Finnish and Swedish DGs, feedback from the Impact Vector assessment. Work notes by J-P. Bento and T. Mankamo, 31 October 2002.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

ICDE-PR02 Collection and Analysis of CCFs of EDGs. ICDE Project Report 02, prepared by T.E. Wierman, D.M. Rasmuson and F.M. Marshall, INEEL, 17 May 2000.

DGs-CCFA CCF Analysis of Diesel Generators, Olkiluoto 1 and 2 Experience 1983-1997. Work report prepared by T. Mankamo, Rev. 07 April 1999.

NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

NUREG/CR-5497
CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998

NUREG/CR-6268v1
Common Cause Failure Database and Analysis System: Overview. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

NUREG/CR-6268v2
Common Cause Failure Database and Analysis System: Event Definition and Classification. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.2., June 1998.

NUREG/CR-6268v3
Common Cause Failure Database and Analysis System: Data Collection and Event Coding. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.3., June 1998.

NUREG/CR-6268v4
Common Cause Failure Database and Analysis System: CCF Software Reference Manual. Prepared by K.J. Kvarfrdt, M.J. Cebull, S.T. Wood and A.Mosleh. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

INEL-95/0035
Emergency Diesel Generator Power System Reliability 1987-1993. Prepared By G.M. Grant, et.al., February 1996.

RPC 91-57 Defences against CCFs and generation of CCF data, pilot study for DGs, quantitative analysis. Staffan Björe, ABB Atom AB, Report RPC 91-57, 15 October 1991

Abbreviations

Acronym	Description
CCCG	Common Cause Component Group
CCF	Common Cause Failure
TDC	Test and Demand Cycles
BWR	Boiling Water Reactor
DG	Diesel Generator
PWR	Pressurized Water Reactor
IAEA	International Atomic Energy Authority
ICDE	International CCF Data Exchange
EPRI	Electric Power Research Institute
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate
USNRC	United States Nuclear Regulatory Commission

Appendix 1: Summary Tables of the Impact Vectors

In the current version this appendix is shipped as an embedded MS-Excel file "NACFS-PR10-App1-V3.xls". Double-click the icon to open the Excel workbook.

NAFCS-PR10-App 1-V3.xls

Appendix 2: Impact Vector Construction Sheet Examples

In the current version this appendix is shipped as an embedded MS-Word file "NACFS-PR10-App2-V3.doc". Double-click the icon to open the document.

NAFCS-PR10-App 2-V3.doc

NACFS - Impact Vector Construction
DG Pilot

CCCG Size = 2

Index	Unit	Year	Description	*C03* Failure mode	Generic Class	*C08* Comp. Impair-ment	*C11* Shared Cause Factor	*C14* Time Factor	Impact Vector 0	1	2		Sum	Average multiplicity
SF15	B1	1986	Control of reactive power degraded due to potentiometer failure	FR		DI	H	empty	1				1	0
SF16	B2	1991	Break of the elastic coupling between motor and generator due to aging	FR		CI	H	empty		1			1	1
SF17	B1	1993	Inadequate instructions to check low level of lubrication oil	FR		CI	H	empty	0	0.9	0.1		1	1.1
SF20	O1	1990	Sacrificial anode lost in the cooling circuit due to loosened screw	FR		II	H	H	1				1	0
SF21	O1	1991	Loosened rubber muff in the cooling cicuit caused leak and blockage	FR		ID	H	H	0	0.6	0.4		1	1.4
SF22	O1	1994	Cut signal cables in connection to modernization works	MC		CC	H	H	0	0	1		1	2
SF23	O1	1994	Incorrect signal from fire system disabled start	MC		CW	H	H	0	0.5	0.5		1	1.5
									2	3	2		7	1.00
									0	1	2		Sum	Average multiplicity

CCCG Size = 2

			Redundant Impact Vector					Average		High Bound Comparison Impact Vector					Average
Index	Unit	Year	0	1	2		Sum	multiplicity	Comment	0	1	2		Sum	multiplicity
SF15	B1	1986	0.45	0.45	0.1		1	0.65		1.41	0.58	0.01		2	0.3
SF16	B2	1991	0	0.95	0.05		1	1.05		0.91	1.08	0.01		2	0.55
SF17	B1	1993	0	0.8	0.2		1	1.2		0	0.9	0.1		1	1.1
SF20	O1	1990	0.98	0.02	0		1	0.02		0.9	0	0.1		1	0.2
SF21	O1	1991	0	0.6	0.4		1	1.4		0.5	0.4	0.1		1	0.6
SF22	O1	1994	0	0	1		1	2		0	0	1		1	2
SF23	O1	1994	0	0.5	0.5		1	1.5		0	1	0		1	1
			1.43	3.32	2.25		7	1.12		3.72	3.96	1.32		9	0.73
			0	1	2		Sum	Average		0	1	2		Sum	Average
								multiplicity							multiplicity

CCCG Size = 2

			Low Bound Comparison Impact Vector					Average
Index	Unit	Year	0	1	2		Sum	multiplicity
SF15	B1	1986	1.4	0.6	0		2	0.3
SF16	B2	1991	0.9	1.1	0		2	0.55
SF17	B1	1993	0	0.9	0.1		1	1.1
SF20	O1	1990	0.81	0.18	0.01		1	0.2
SF21	O1	1991	0.45	0.5	0.05		1	0.6
SF22	O1	1994	0	0	1		1	2
SF23	O1	1994	0	1	0		1	1
			3.56	4.28	1.16		9	0.73
			0	1	2		Sum	Average
								multiplicity

Impact Vector Application to Diesel Generators

Appendix 2: Impact Vector Construction Sheet Examples

This appendix presents two examples of the impact vector construction sheet, using the same cases as the guideline [NAFCS-PR03]. The examples are reproduced from the base assessment documentation.

In order to facilitate tracking the event documentation, the table below presents the indexing scheme utilized in the DG pilot.

Index	C01 CCF event identifier	Unit	Year
SF01	OL2-9965, -11411	T2	1983
SF02	OL1-18729, -18242	T1	1983
SF03	OL1-28866, -28867	T1	1987
SF04	OL2-24071, -26396	T2	1988
SF05	OL2-26618, -W16501	T2	1988
SF06	OL1-46770, -46781	T1	1991
SF07	OL1-46975, -46985, -48203	T1	1991
SF08	OL2-35442, -35456	T2	1992
SF09	OL2-38804, -38801	T2	1992
SF10	OL1-5006737, -5007550	T1	1995
SF11	OL1-TR-R7-2/95	T1	1995
SF12	OL2-TR-R7-2/95	T2	1995
SF13	Lo1/H12/77	L1	1977
SF14	LOTI-244922A	L1	1997
SF15	RO-B1-86/033	B1	1986
SF16	RO-B2-91/005	B2	1991
SF17	RO-B1-93/022	B1	1993
SF18	F2-RO-008/92-RO-01092	F2	1992
SF19	F3-RO-014/89	F3	1989
SF20	RO-O1-90/027	O1	1990
SF21	RO-O1-91/19	O1	1991
SF22	RO-O1-94/016	O1	1994
SF23	RO-O1-94/010	O1	1994
SF24	RO-O3-94/004	O3	1994
SF25	R2-RO-013/97-R0-014/97	R2	1997
SF26	R3-RO-003/89-R0-009/89	R3	1989
SF27	R3-RO-032/89	R3	1989
SF28	R4-RO-034/89-R0-040/89	R4	1989
SF29	R3-RO-043/94	R3	1994

SF02: CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-18729, -18242
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. Fuel booster pump failed in periodic test, because of broken cotter bolt. Wrong type was used in maintenance (train D, OL1.652P044, 83-05-18). Same occurred three weeks later at the redundant DG (train C, OL1.652P034, 83-06-12).
C07	Event Interpretation	Substantial chance to have occurred more closely in time (at that time, test interval was 2 weeks, pairwise staggered at that time)
C09	Root Cause	M
C10	Coupling Factor(s)	MP
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	M
C13	Other	
G5	Test Interval	14 days (up to May 1994)
G5-2	Test Staggering	PST Pair-wise staggered (AC-BD)

SF02: Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	12.06.83	14	C	TI	652P034
D	18.05.83	14	C	TI	652P044

SF02: Impact Vector Construction

The events were separated by three weeks (Sub C was tested successfully once after failure in Sub D). However, owing to the character of the failure mechanism, substantial chance is considered for the possibility for failures to co-exist. Thus effective Weight = 50% is used for double failure in the impact vector construction. Compare to the procedure explained in [NAFCS-PR03, Section 4.1].

SF02: Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.25	1			1			1
			2	1					1
2	Both components fail in TDC2	0.25	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.5	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.25	0.5	0.25	0	0	1
			2	0.25	0.5	0.25	0	0	1
Sum Impact Vector over TDCs				0.5	1	0.5	0	0	2
				Average multiplicity				2	

SF08: CCF Event Description and Classification

Basic description and classifications extracted from [DGs-CCFA].

C01	Event Identifier	OL2-35442, -35456	
C03	Failure Mode	Failure to run	
G6	Group Size	4	
C04	Exposed Components	4	
C05	Event Description	Olkiluoto 2, plant state: power operation. Small drop leak of fuel return line (train D, OL2.651G401, 92-01-09) and large spray leak of fuel return line at the redundant DG one week later (train C, OL2.651G301, 92-01-16). Both detected in test.	
C07	Event Interpretation	Certain risk of leak development at 651G401 and fire in case of actual demand requiring long run (at that time, test interval was 2 weeks, pair-wise staggered, i.e. the failed state of 651G301 and incipient state of 651G401 coexisted)	
C09	Root Cause	I	Internal to component, piece part
C10	Coupling Factor(s)	EI	Environment Internal
C11	Shared Cause Factor	H	High
C12	Corrective Action	G	Fixing of component
C14	Time Factor	M	Medium
C13	Other		
G5	Test Interval	14	days (up to May 1994)
G5-2	Test Staggering	PST	Pair-wise staggered (AC-BD)

SF08: Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	16.01.92		C	TI	651G301
D	09.01.92		I	TI	651G401

SF08: Impact Vector Construction

The leak of fuel oil from the injection pipes, injection nozzles and fuel return pipes has been a generic failure mechanism at the DGs of OL1/OL2. The leaks have mostly been very small drop leakage and also typically spread over time. Compare to CCF event OL2-9965, -11411 in 1983 (DocIndex=SF01).

The failure mechanism shows apparent tendency of growing degradation as the function of start cycles and operation time. The spray leak due to broken fuel return line of aggregate 651G301 was a singular event (no recurring at the near time) in that aggregate but the fuel return line of aggregate 651G401 was affected repeatedly at the following time points within +/- one year:

91-01-09 Drop leak (incipient)

92-01-09 Drop leak (incipient), in conjunction to spray leak at 651G301 one week apart (the considered multiple event)

92-05-07 Spray leak (critical)

92-08-05 Spray leak (critical)

The fire risk in case of spray leak has to be considered significant in an actual demand with mean load running time of about 4 hours. Thus the spray leak events are classified as critical for the failure mode failure to run. The fire risk in case of a drop leak is smaller but still considerable taking also into account the possibility of leak growth during an actual load running time. Based on insights from the growth tendency that risk is assessed to be Weight = 20%, which is then used in the construction of impact vector by hypothesis method.

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Only 651G301 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

SF08: Net Impact Vector

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF01	NAFCS Index	
C01	OL2-9965, -11411	ICDE Event Identifier	
	Fuel injection nozzles, small drop leakage and spray leak	Description	
	LeakFI	Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A			W			
B			W			
C	651G301	27/04/1983	I	0.1		TI
D	651G401	13/04/1983	C	1		TI

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only 651G401 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0.8	0.2	0	0	1
Average multiplicity				1.2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485

	Impact vector 0	1	2	3	4	Element sum
High	0	0.9	0.1	0	0	1
Low	0.95	1	0.05	0	0	2
					1.1	
					0.55	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF02	NAFCS Index	
C01	OL1-18729, -18242	ICDE Event Identifier	
	Fuel booster pumps, broken cotter bolt, wrong type used	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A			W	0		
B			W	0		
C	652P034	12/06/1983	C	1	14	TI
D	652P044	18/05/1983	C	1	14	TI

Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.25	1			1			1
			2	1					1
2	Both components fail in TDC2	0.25	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.5	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.25	0.5	0.25	0	0	1
			2	0.25	0.5	0.25	0	0	1
Sum Impact Vector over TDCs				0.5	1	0.5	0	0	2
				Average multiplicity				1	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.5	1	0.5	0	0	2
Average multiplicity				1	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0	1	0	0	1
Low	0.5	1	0.5	0	0	2
	Average multiplicity				2	
					1	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF03	NAFCS Index
C01	OL1-28866, -28867	ICDE Event Identifier
	Erroneous operation of sea water gate caused large amount of sludge moving	Description
	HxBloc	Generic Class
C11	H	Shared Cause Factor
C14	H	Time Factor
G5	14	Test Interval
G5-2	Pair-wise staggered	Test Staggering

1	
1	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652E101	24/05/1987	C	1		MC
B			W	0		
C	652E301	24/05/1987	C	1		MC
D			W	0		

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
	This case is an actual CCF of order 2	1			1			1
Net impact vector			0	0	1	0	0	1
			Average multiplicity				2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0	1	0	0	1
Average multiplicity				2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0	1	0	0	1
Low	0	0	1	0	0	1
Average multiplicity					2	
					2	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF04	NAFCS Index
C01	OL2-24071, -26396	ICDE Event Identifier
	Sea water heat exchangers, reduced heat transfer capacity	Description
	HxBloc	Generic Class
C11	H	Shared Cause Factor
C14	H	Time Factor
G5	14	Test Interval
G5-2	Pair-wise staggered	Test Staggering

1	
1	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652E101	04/05/1988	I	0.1		MA
B			W	0		
C	652E301, 652E302	05/05/1988	I	0.1		MA
D			W	0		

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both affected trains A and C would survive in actual demand	0.9	1					1
2	Train A or C would survive but not both the in actual demand	0.08		1				1
3	Both affected trains A and C would not survive in actual demand	0.02			1			1
Net impact vector			0.9	0.08	0.02	0	0	1
			Average multiplicity				0.12	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.93	0.06	0.01	0	0	1
Average multiplicity				0.08	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.9	0	0.1	0	0	1
Low	0.81	0.18	0.01	0	0	1
	Average multiplicity				0.2	
					0.2	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF05	NAFCS Index	
C01	OL2-26618, -W16501	ICDE Event Identifier	
	Sludge movement invoked by post-repair test of sea water piping	Description	
	HxBloc	Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652E101	10/05/1988	D	0.5		MC
B			W	0		
C	652E301	10/05/1988	D	0.5		MC
D			W	0		

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both affected trains A and C would survive in actual demand	0.49	1					1
2	Train A or C would survive but not both the in actual demand	0.5		1				1
3	Both affected trains A and C would not survive in actual demand	0.01			1			1
Net impact vector			0.49	0.5	0.01	0	0	1
			Average multiplicity				0.52	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.65	0.3	0.05	0	0	1
Average multiplicity				0.4	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.5	0	0.5	0	0	1
Low	0.25	0.5	0.25	0	0	1
	Average multiplicity				1	
					1	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF06	NAFCS Index	
C01	OL1-46770, -46781	ICDE Event Identifier	
	Sea water heat exchangers, reduced heat transfer capacity	Description	
	HxBloc	Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A			W	0		
B	652E201	02/05/1991	I	0.1		MA
C			W	0		
D	652E401	06/05/1991	I	0.1		MA

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both affected trains B and D would survive in actual demand	0.9	1					1
2	Train B or D would survive but not both the in actual demand	0.08		1				1
3	Both affected trains B and D would not survive in actual demand	0.02			1			1
Net impact vector			0.9	0.08	0.02	0	0	1
			Average multiplicity				0.12	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.93	0.06	0.01	0	0	1
Average multiplicity				0.08	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.9	0	0.1	0	0	1
Low	1.805	0.19	0.005	0	0	2
	Average multiplicity				0.2	
					0.1	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF07	NAFCS Index	
C01	OL1-46975, -46985, -48203	ICDE Event Identifier	
	Sea water heat exchangers, reduced heat transfer capacity	Description	
	HxBloc	Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652E101	17/07/1991	I	0.1		MA
B	652E201	24/07/1991	I	0.1		MA
C			W	0		
D	652E401	10/07/1991	I	0.1		MA

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All affected trains A, B and D would survive in actual demand	0.85	1					1
2.	Two of the affected three trains would survive but not all in actual demand	0.1		1				1
3.	One of the affected three trains would survive but not the two other	0.04			1			1
4.	All affected trains A, B and D would not survive in actual demand	0.01				1		1
Net impact vector			0.85	0.1	0.04	0.01	0	1
			Average multiplicity				0.21	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.85	0.09	0.05	0.01	0	1
Average multiplicity				0.22	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.9	0	0	0.1	0	1
Low	2.715	0.272	0.014	5E-04	0	3
	Average multiplicity				0.3	
					0.1	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF08	NAFCS Index	
C01	OL2-35442, -35456	ICDE Event Identifier	
	Fuel return pipes, small drop leakage and spray leak	Description	
	LeakFR	Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Pair-wise staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A			W			
B			W			
C	651G301	16/01/1992	C	1		TI
D	651G401	09/01/1992	I	0.1		TI

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only 651G301 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0.8	0.2	0	0	1
Average multiplicity				1.2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0.9	0.1	0	0	1
Low	0.95	1	0.05	0	0	2
	Average multiplicity				1.1	
					0.55	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF09	NAFCS Index	
C01	OL2-38804, -38801	ICDE Event Identifier	
	Sludge movement invoked by inadv. operation of sea water gate in test	Description	
	HxBloc	Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	28	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A			W	0		
B	652E201	20/06/1992	C	1		MC
C			W	0		
D	652E401	20/06/1992	D	0.5		MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Train D would survive in actual demand, i.e. only Train B would fail	0.9		1				1
2.	Both Trains B and D would not survive in actual demand	0.1			1			1
Net impact vector			0	0.9	0.1	0	0	1
			Average multiplicity				1.1	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0.9	0.1	0	0	1
Average multiplicity				1.1	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0.5	0.5	0	0	1
Low	0	0.5	0.5	0	0	1
	Average multiplicity				1.5	
					1.5	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF10	NAFCS Index	
C01	OL1-5006737, -5007550	ICDE Event Identifier	
	Rpm guards, loose tachometer connections	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	L	Time Factor	0.1
G5	28	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652K961	16/08/1995	C	1	28	TI
B			W			
C	652K963	05/07/1995	C	1	28	TI
D			W			

Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.05	1			1			1
			2	1					1
2	Both components fail in TDC2	0.05	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.9	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.05	0.9	0.05	0	0	1
			2	0.05	0.9	0.05	0	0	1
Sum Impact Vector over TDCs				0.1	1.8	0.1	0	0	2
				Average multiplicity				1	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.3	1.4	0.3	0	0	2
Average multiplicity				1	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.5	1	0.5	0	0	2
Low	0.1	1.8	0.1	0	0	2
	Average multiplicity				1	
					1	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF11	NAFCS Index	
C01	OL1-TR-R7-2/95	ICDE Event Identifier	
	Snow blocked air intake filter, CCI and unit-unit dependence	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	28	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652C107	01/02/1995	D	0.5	28	MC
B	652C207	01/02/1995	I	0.1	28	MC
C	652C307	01/02/1995	D	0.5		MC
D	652C407	01/02/1995	I	0.1		MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Reasoning supported by CLM	1	0.356	0.289	0.198	0.111	0.045	1.0000
Net impact vector			0.356	0.289	0.198	0.111	0.045	1.0000
			Average multiplicity				1.2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.59	0.2	0.15	0.04	0.02	1
Average multiplicity				0.7	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.5	0	0.4	0	0.1	1
Low	0.203	0.45	0.295	0.05	0.003	1
	Average multiplicity				1.2	
					1.2	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF12	NAFCS Index	
C01	OL2-TR-R7-2/95	ICDE Event Identifier	
	Snow blocked air intake filter, CCI and unit-unit dependence	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	28	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	652C107	01/02/1995	I	0.1		MC
B	652C207	01/02/1995	I	0.1		MC
C	652C307	01/02/1995	I	0.1		MC
D	652C407	01/02/1995	I	0.1		MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Reasoning supported by CLM	1	0.779	0.16	0.045	0.013	0.003	1.0000
Net impact vector			0.779	0.16	0.045	0.013	0.003	1.0000
			Average multiplicity				0.3	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.72	0.15	0.1	0.02	0.01	1
Average multiplicity				0.45	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0.9	0	0	0	0.1	1
Low	0.656	0.292	0.049	0.004	1E-04	1
	Average multiplicity				0.4	
					0.4	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF13	NAFCS Index	
C01	Lo1/H12/77	ICDE Event Identifier	
	Spurious start/stop signal caused short inoperability of all DGs	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	14	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	EY01	17/10/1977	C	1		MC
B	EY02	17/10/1977	C	1		MC
C	EY03	17/10/1977	C	1		MC
D	EY04	17/10/1977	C	1		MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
	This case is an actual CCF of order 4	1					1	1
Net impact vector			0	0	0	0	1	1
			Average multiplicity				4	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0	0	0	1	1
Average multiplicity				4	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0	0	0	1	1
Low	0	0	0	0	1	1
Average multiplicity					4	
					4	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF14	NAFCS Index	
C01	LOTI-244922A	ICDE Event Identifier	
	Degraded pumps and valves in the cooling circuit due to wear-out	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	M	Time Factor	0.5
G5	14	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	EY01 (assumed)	18/03/1997	I	0.1	14	MA
B	EY02 (assumed)	25/03/1997	I	0.1	14	MA
C	EY03	25/02/1997	D	0.5	14	TI
D	EY04	05/04/1997	C	1	14	TI

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Degraded trains would survive in actual demand, only Train D would fail	0.7		1				1
2.	Two least degraded trains would survive and Trains C and D fail	0.2			1			1
3.	Also one of the two least degraded trains would fail, only one survive	0.05				1		1
4.	All trains would fail in an actual demand condition	0.05					1	1
Net impact vector			0	0.7	0.2	0.05	0.05	1
			Average multiplicity				1.45	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0.8	0.2	0	0	1
Average multiplicity				1.2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0.5	0.4	0	0.1	1
Low	2.65	1.053	0.248	0.048	0.003	4
Average multiplicity					1.7	
					0.425	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF18	NAFCS Index
C01	F2-RO-008/92-RO-01092	ICDE Event Identifier
	Leak of cooling circuit due to couple action and erosion	Description
		Generic Class
C11	H	Shared Cause Factor
C14	H	Time Factor
G5	14	Test Interval
G5-2	Staggered	Test Staggering

1	
1	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
C	DG230	22/05/1992	C	1	7	MW
D	DG240	26/05/1992	D	0.5	15	MW
A	DG210	26/05/1992	I	0.1		MA
B	DG220	26/05/1992	W	0		MA

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only Train C would fail, degraded A and D would survive in actual demand	0.45		1				1
2.	One of the degraded trains would also fail in addition to Train C	0.5			1			
3.	Both degraded trains would fail in addition to Train C	0.05				1		1
Net impact vector			0	0.45	0.5	0.05	0	1
			Average multiplicity				1.6	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0.75	0.2	0.05	0	1
Average multiplicity				1.3	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0.5	0.4	0.1	0	1
Low	0	0.45	0.5	0.05	0	1
	Average multiplicity				1.6	
					1.6	

Impact Vector Construction Sheet

CCF Event Description and Classification

	SF25	NAFCS Index
C01	R2-RO-013/97-R0-014/97	ICDE Event Identifier
	Poor connection in the generator field circuit	Description
		Generic Class
C11	H	Shared Cause Factor 1
C14	H	Time Factor 1
G5	14	Test Interval
G5-2	Staggered	Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	DG210	01/07/1997	C	1	14	TI
B	DG220	01/07/1997	C	1	7	TU
C	DG230	01/07/1997	I	0.1	7	TU
D	DG220	01/07/1997	I	0.1		TU

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Degraded Trains C and D would both survive in actual demand	0.8			1			1
2.	One of the degraded trains would also fail in addition to Trains A and B	0.1				1		
3.	Both degraded trains would fail in addition to Trains A and B	0.1					1	1
Net impact vector			0	0	0.8	0.1	0.1	1
			Average multiplicity				2.3	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0	0	0.8	0.1	0.1	1
Average multiplicity				2.3	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2	3	4	Element sum
High	0	0	0.9	0	0.1	1
Low	0	0	0.81	0.18	0.01	1
Average multiplicity					2.2	
					2.2	

Mixed Assessment

Hypothesis		Mixture	Impact vector 0	1	2	3	4	Element sum
1.	Shared cause (potential to systematic error) present	0.5	0	0	0.8	0.1	0.1	1
3.	The assumption of independent degradation is applicable	0.5	0	0	0.81	0.18	0.01	1
Net impact vector			0	0	0.805	0.14	0.055	1
			Average multiplicity				2.25	

Impact Vector Construction Sheet (CCCG Size 4)

CCF Event Description and Classification

	SF##	NAFCS Index	
C01		ICDE Event Identifier	
		Description	
		Generic Class	
C11		Shared Cause Factor	1
C14		Time Factor	0
G5		Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
				1		
				0		
				0		
				0		

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.		0.8		1				1
2.		0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2	3	4	Element sum
0.95	1	0.05	0	0	2
Average multiplicity				0.55	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485

	Impact vector 0	1	2	3	4	Element sum
High	0	1	0	0	0	1
Low	0	1	0	0	0	1
	Average multiplicity				1	
					1	

Impact Vector Construction Sheet (CCCG Size 2)

CCF Event Description and Classification

	SF##	NAFCS Index	
C01		ICDE Event Identifier	
		Description	
		Generic Class	
C11		Shared Cause Factor	1
C14		Time Factor	1
G5		Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
				0.1		
				0.1		

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.		0.8		1			1
2.		0.2			1		1
Net impact vector			0	0.8	0.2		1
			Average multiplicity			1.2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2		Element sum
0.95	1	0.05		2
Average multiplicity			0.55	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2		Element sum
High	0.9	0	0.1		1
Low	0.81	0.18	0.01		1
	Average multiplicity			0.2	
				0.2	

Impact Vector Construction Sheet (CCCG Size 2)

CCF Event Description and Classification

	SF17	NAFCS Index
C01	RO-B1-93/022	ICDE Event Identifier
	Inadequate instructions to check low level of lubrication oil	Description
		Generic Class
C11	H	Shared Cause Factor
C14	empty	Time Factor
G5	14	Test Interval
G5-2	Staggered	Test Staggering

1	
1	Set equal to 1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A		15/07/1993	C	1	14	MC
B		15/07/1993	I	0.1	14	empty

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	The DG in Sub A with incipent state would survive in the actual demand	0.9		1			1
2.	Both would fail in the actual demand	0.1			1		1
Net impact vector			0	0.9	0.1		1
			Average multiplicity			1.1	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2		Element sum
0	0.8	0.2		1
Average multiplicity			1.2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2		Element sum
High	0	0.9	0.1		1
Low	0	0.9	0.1		1
				1.1	
				1.1	

Impact Vector Construction Sheet (CCCG Size 2)

CCF Event Description and Classification

	SF21	NAFCS Index
C01	RO-O1-91/19	ICDE Event Identifier
	Loosened rubber muff in the cooling cicuit caused leak and blockage	Description
		Generic Class
C11	H	Shared Cause Factor
C14	H	Time Factor
G5	14	Test Interval
G5-2	Staggered	Test Staggering

1	
1	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A		03/05/1991	I	0.1	14	DE
B	Date corrected	09/05/1991	D	0.5	14	DE

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	DGA would fail but DGB survive in the actual demand	0.6		1			1
2.	Also DGB would fail due to moisture/flooding effects	0.4			1		1
Net impact vector			0	0.6	0.4		1
			Average multiplicity			1.4	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2		Element sum
0	0.6	0.4		1
Average multiplicity			1.4	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2		Element sum
High	0.5	0.4	0.1		1
Low	0.45	0.5	0.05		1
	Average multiplicity			0.6	
				0.6	

Impact Vector Construction Sheet (CCCG Size 2)

CCF Event Description and Classification

	SF22	NAFCS Index
C01	RO-O1-94/016	ICDE Event Identifier
	Cut signal cables in connection to modernization works	Description
		Generic Class
C11	H	Shared Cause Factor 1
C14	H	Time Factor 1
G5	14	Test Interval
G5-2	Staggered	Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A		12/09/1994	C	1		MC
B		12/09/1994	C	1		MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	This case is an actual CCF of order 2	1			1		1
Net impact vector			0	0	1		1
			Average multiplicity			2	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2		Element sum
0	0	1		1
Average multiplicity			2	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2		Element sum
High	0	0	1		1
Low	0	0	1		1
Average multiplicity				2	
				2	

Impact Vector Construction Sheet (CCCG Size 2)

CCF Event Description and Classification

	SF23	NAFCS Index	
C01	RO-O1-94/010	ICDE Event Identifier	
	Incorrect signal from fire system disabled start	Description	
		Generic Class	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	14	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	DG111	09/05/1994	C	1	14	MC
B	DG112	09/05/1994	W	0	14	MC

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	Only DG111 would fail, DG112 successfully started	0.5		1			1
2.	DG112 would fail also due to blocked start signal	0.5			1		
Net impact vector			0	0.5	0.5		1
			Average multiplicity			1.5	

Redundant Assessment

See details in
R0209-ES-Impact Vector, 08 August 2002
(and comments by TM 16 August 2002)

Impact vector 0	1	2		Element sum
0	0.5	0.5		1
Average multiplicity			1.5	

Comparison Impact Vector

Constructed from the Impairment Values,
Shared Cause Factor and Time Factor
according to NUREG/CR-5485
- for High Bound see Work Notes by TM

	Impact vector 0	1	2		Element sum
High	0	1	0		1
Low	0	1	0		1
Average multiplicity				1	
				1	

CCF Event Description and Classification

CCF Event Description and Classification

Basic description and classifications extracted from [DGs-CCFA].

C01	Event Identifier	OL2-9965, -11411	
C03	Failure Mode	FR	
G6	Group Size	4	
C04	Exposed Components	4	
C05	Event Description	Olkiluoto 1, plant state: power operation. Large Spray leak of one fuel injection nozzle (train D, OL2.651G401, 83-04-13) and small drop leak at the redundant DG two weeks later (train C, OL2.651G301, 83-04-27). Both detected in test.	
C07	Event Interpretation	Certain risk of leak development at 651G301 and fire in case of actual demand requiring long run (at that time, test interval was 2 weeks, pairwise staggered at that time, , i.e. the failed state of 651G301 and incipient state of 651G401 coexisted).	
C09	Root Cause	I	Internal to component, piece part
C10	Coupling Factor(s)	EI	Environment Internal
C11	Shared Cause Factor	H	High
C12	Corrective Action	G	Fixing of component
C14	Time Factor	M	Medium
C13	Other		
G5	Test Interval	14	days (up to May 1994)
G5-2	Test Staggering	PST	Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			WI		
B			WI		
C	27.04.83	14	I	TI	651G301
D	13.04.83	14	C	TI	651G401

Impact Vector Construction

The leak of fuel oil from the injection pipes, injection nozzles and fuel return pipes has been a generic failure mechanism at the DGs of OL1/OL2. The leaks have mostly been very small drop leakage and also typically spread over time. Compare to CCF event OL2-35442, -35456 in 1992 (DocIndex = SF08).

The failure mechanism shows apparent tendency of growing degradation as the function of start cycles and operation time. The history of adjacent events is following:

- Drop leakage of the two fuel nozzles at 651G401 on 23.03.1983, i.e. three weeks earlier than the considered critical spray leak
- Recurring drop leakage of nozzle seals at 651G401 in March 1984 and again one year later in April 1985

– The considered drop leakage of injection pipe at 651G301 in April 1983 was a singular event for that aggregate within +/- one year, but during the period from April 184 through March 1985 altogether five drop leakages were detected in the injection pipes and nozzles at 651G301

The fire risk in case of spray leak has to be considered significant in an actual demand with mean load running time of about 4 hours. Thus the spray leak events are classified as critical for the failure mode failure to run. The fire risk in case of a drop leak is smaller but still considerable taking also into account the possibility of leak growth during an actual load running time. Based on insights from the growth tendency that risk is assessed to be Weight = 20%, which is then used in the construction of impact vector by hypothesis method.

Net Impact Vector

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Only 651G401 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-18729, -18242
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. Fuel booster pump failed in periodic test, because of broken cotter bolt. Wrong type was used in maintenance (train D, OL1.652P044, 83-05-18). Same occurred three weeks later at the redundant DG (train C, OL1.652P034, 83-06-12).
C07	Event Interpretation	Substantial chance to have occurred more closely in time (at that time, test interval was 2 weeks, pairwise staggered at that time)
C09	Root Cause	M
C10	Coupling Factor(s)	MP
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	M
C13	Other	
G5	Test Interval	14 days (up to May 1994)
G5-2	Test Staggering	PST Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	12.06.83	14	C	TI	652P034
D	18.05.83	14	C	TI	652P044

Impact Vector Construction

The events were separated by three weeks (Sub C was tested successfully once after failure in Sub D). However, owing to the character of the failure mechanism, substantial chance is considered for the possibility for failures to co-exist. Thus effective Weight = 50% is used for double failure in the impact vector construction. Compare to the procedure explained in [NAFCS-PR03, Section 4.1].

Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.25	1			1			1
			2	1					1
2	Both components fail in TDC2	0.25	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.5	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.25	0.5	0.25	0	0	1
			2	0.25	0.5	0.25	0	0	1
Sum Impact Vector over TDCs				0.5	1	0.5	0	0	2
				Average multiplicity				2	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-28866, -28867
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: refuelling. All 712-trains were at operation (due to RHR via 321-721-712). System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A, C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652. Erroneous closing of sea water gates (711-system) invoked large amounts of sludge (mussels etc) movement in main sea water channel, which is connected to AC- and BD-channels. Sea water heat exchangers blocked in trains A and C (OL1.652E101 and OL1.652E301 on 87-05-24). B, D exchangers were unaffected. Directly detected (monitored failure). Clean-up maintenance: (652E101: 24.5 8.55-23.10, 653E301: 24.5 14.50 - 25.5 1.20).
C07	Event Interpretation	Diesels were stanby-state during these events. A and C diesels werw inoperable due to blockage of heat exhangers.
C09	Root Cause	H
C10	Coupling Factor(s)	MP
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	1-KK-R7-2/87. Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	14 days (up to May 1994)
G5-2	Test Staggering	PST Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	24.05.87		C	MC	
B			W		
C	24.05.87		C	MC	
D			W		

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF05 and SF09. Blocking events to gradually reduce heat transfer capacity are following: DocIndex = SF04, SF06 and SF07.

The considered case is an actual CCF of order 2. It was related to an operation, which is characteristic to the annual overhaul outage. Besides, the failure mode is of monitored type. Hence, a specific treatment is needed, when considering this event in CCF parameter estimation. No special judgment is needed for the impact vector construction in this case.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
	This case is an actual CCF of order 2	1			1			1
								0
Net impact vector			0	0	1	0	0	1
			Average multiplicity				2	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL2-24071, -26396
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 2, plant state: refuelling. Reduced heat transfer capacity of sea water heat exchangers in A and C trains due to sludge movement, monitored/ detected (OL2.652E101, 88-05-04, OL2.652E301, 88-05-05) and heat exchangers were taken into clean-up maintenance at separate time. System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A, C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652.
C07	Event Interpretation	Diesels were stanby-state during these events. In case of an actual demand would exist, the cooling water temperature in A, C trains could gradually rise to the trip limit and thus prevent diesel operation. Some risk to double failure if long run demand exists during the clean-up of first HX.
C09	Root Cause	A
C10	Coupling Factor(s)	EE
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	H
C13	Other	Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	14 days (up to May 1994)
G5-2	Test Staggering	PST Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	04.05.88		I	MA	
B			W		
C	05.05.88		I	MA	
D			W		

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF06, SF07. Blocking events connected to abrupt flow changes are following: DocIndex = SF03, SF05 and SF09.

The considered potential CCF event is of type gradual reduction of heat transfer, i.e. monitored type of failure and cause unavailability during the repair cleanup time. A specific treatment is again needed, when considering these events in CCF parameter estimation. The conditional probability for multiple failure in assessed from the chances that the inoperability of heat exchangers could overlap in redundant subs. Due to the slow development rate only chances of 10% are given for failure state in general assuming an actual demand during the degraded condition, and this is divided in proportion 4:1 between single and double failure state reflecting judgment of weak dependence .

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both affected trains A and C would survive in actual demand	0.9	1					1
2	Train A or C would survive but not both the in actual demand	0.08		1				1
3	Both affected trains A and C would not survive in actual demand	0.02			1			1
Net impact vector			0.9	0.08	0.02	0	0	1
			Average multiplicity				0.12	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL2-26618, -W16501
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 2, plant state: refuelling. Temporary discharge pipelines was removed in diesel-backed normal operation service water system (713) during annual overhaul. System 713 draws water from the same sea water channel as shutdown service water system (712 A- and C-trains). System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A, C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652. When 713-pumps were stopped/started, flow conditions changed in the sea water channel, which caused sludge (mussels etc.) unfastening, see also event OL2-24071, -26396 few days before. Partial blocking occured in A and C heat exchangers in systems 652/721. As consequence the heat removal capacity was decreased due to reduced flow through heat exchangers (OL2.652E101 and OL2.652E301 on 88-05-10). Directly detected (monitored failure) and diesel heat exchangers were taken into clean-up maintenance.
C07	Event Interpretation	Diesels were stanby-state during these events. In case of an actual demand would exist, the cooling water temperature in A, C trains could gradually rise to the trip limit and thus prevent diesel operation. Some risk to double failure if long run demand exists during the clean-up of first HX.
C09	Root Cause	H
C10	Coupling Factor(s)	HS
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	H
C13	Other	Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	14 days (up to May 1994)
G5-2	Test Staggering	PST Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	10.05.88		D	MC	
B			W		
C	10.05.88		D	MC	
D			W		

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF03 and SF09. Blocking events to gradually reduce heat transfer capacity are following: DocIndex = SF04, SF06 and SF07.

In the considered case the sludge movement was invoked by test maneuvers. It can be assumed that those types of tests will not be carried out during the mission time of DGs (undertaken in the presence of an actual demand situation). The failure mode is thus of monitored type with respect to the unavailability in standby state. Hence, a specific treatment is needed, when considering this event in CCF parameter estimation. In the considered case it is estimated that cleaning work would be successful to prevent total blockage of one out of two trains with 50% chances with respect to the risk of actual demand. Only 1% chance is estimated for the possibility that cleaning work would not yet be far enough but both trains could get blocked if an actual demand had occurred.

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both affected trains A and C would survive in actual demand	0.49	1					1
2	Train A or C would survive but not both the in actual demand	0.5		1				
3	Both affected trains A and C would not survive in actual demand	0.01			1			1
Net impact vector			0.49	0.5	0.01	0	0	1
			Average multiplicity				0.52	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-46770, -46781
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. Reduced heat capacity of sea water heat exchangers in B and D trains due to sludge movement, monitored/ detected (OL1.652E201 on 91-05-02 and OL1.652E401 on 91-05-06) taken into clean-up maintenance at separate time for the redundant DGs. System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A, C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652.
C07	Event Interpretation	Diesels were stanby-state during these events. In case of actual demand would exist, the cooling water temperature in trains B and D could gradually rise to the trip limit and thus prevent diesel operation. Some risk to double failure if long run demand exists during the clean-up of first HX.
C09	Root Cause	A
C10	Coupling Factor(s)	EE
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	M
C13	Other	Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	14 days
G5-2	Test Staggering	PST Pair-wise staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B	02.05.91		I	MA	
C			W		
D	06.05.91		I	MA	

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF04, SF07. Blocking events connected to abrupt flow changes are following: DocIndex = SF03, SF05 and SF09.

The considered potential CCF event is of type gradual reduction of heat transfer, i.e. monitored type of failure and cause unavailability during the repair cleanup time. A specific treatment is again needed, when considering these events in CCF parameter estimation. The conditional probability for multiple failure in assessed from the chances that the inoperability of heat exchangers could overlap in redundant subs. Due to the slow development rate only chances of 10% are given for failure state in general assuming an actual demand during the degraded condition, and this is divided in proportion 4:1 between single and double failure state reflecting judgment of weak dependence .

Net Impact Vector

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Both affected trains B and D would survive in actual demand	0.9	1					1
2	Train B or D would survive but not both the in actual demand	0.08		1				
3	Both affected trains B and D would not survive in actual demand	0.02			1			1
Net impact vector			0.9	0.08	0.02	0	0	1
			Average multiplicity				0.12	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-46975, -46985, -48203
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. Reduced heat capacity of sea water heat exchangers in A, B and D trains due to sludge movement, monitored/ detected (OL1.652E401 on 91-07-10, OL1.652E101 on 91-07-17 and OL1.652E201 on 91-07-24), taken into clean-up maintenance (at separate time). System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A,C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652.
C07	Event Interpretation	Diesels were stanby-state during these events. In case of actual demand would exist, the cooling water temperature in trains A, B, D could gradually rise to the trip limit and thus prevent diesel operation. Some risk to multiple failure if long run demand exists during the clean-up of first HX.
C09	Root Cause	A
C10	Coupling Factor(s)	EE
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	M
C13	Other	Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	14 days
G5-2	Test Staggering	PST Pair-wise staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	17.07.91		I	MA	
B	24.07.91		I	MA	
C			W		
D	10.07.91		I	MA	

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF04, SF06. Blocking events connected to abrupt flow changes are following: DocIndex = SF03, SF05 and SF09.

The considered potential CCF event is of type gradual reduction of heat transfer, i.e. monitored type of failure and cause unavailability during the repair cleanup time. A specific treatment is again needed, when considering these events in CCF parameter estimation. The conditional probability for multiple failure in assessed from the chances that the inoperability of heat exchangers could overlap in redundant subs. Due to the slow development rate only chances of 15% are given for failure state in general assuming an actual demand during the degraded condition, and this is divided in proportion 10:4:1 between single, double and triple failure state reflecting judgment of weak dependence .

Net Impact Vector

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	All affected trains A, B and D would survive in actual demand	0.85	1					1
2	Two of the affected three trains would survive but not all in actual demand	0.1		1				
3	One of the affected three trains would survive but not the two other	0.04			1			
3	All affected trains A, B and D would not survive in actual demand	0.01				1		1
Net impact vector			0.85	0.1	0.04	0.01	0	1
			Average multiplicity				0.21	

CCF Event Description and Classification

Basic description and classifications extracted from [DGs-CCFA].

C01	Event Identifier	OL2-35442, -35456	
C03	Failure Mode	Failure to run	
G6	Group Size	4	
C04	Exposed Components	4	
C05	Event Description	Olkiluoto 2, plant state: power operation. Small drop leak of fuel return line (train D, OL2.651G401, 92-01-09) and large spray leak of fuel return line at the redundant DG one week later (train C, OL2.651G301, 92-01-16). Both detected in test.	
C07	Event Interpretation	Certain risk of leak development at 651G401 and fire in case of actual demand requiring long run (at that time, test interval was 2 weeks, pair-wise staggered, i.e. the failed state of 651G301 and incipient state of 651G401 coexisted)	
C09	Root Cause	I	Internal to component, piece part
C10	Coupling Factor(s)	EI	Environment Internal
C11	Shared Cause Factor	H	High
C12	Corrective Action	G	Fixing of component
C14	Time Factor	M	Medium
C13	Other		
G5	Test Interval	14	days (up to May 1994)
G5-2	Test Staggering	PST	Pair-wise staggered (AC-BD)

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B			W		
C	16.01.92		C	TI	651G301
D	09.01.92		I	TI	651G401

Impact Vector Construction

The leak of fuel oil from the injection pipes, injection nozzles and fuel return pipes has been a generic failure mechanism at the DGs of OL1/OL2. The leaks have mostly been very small drop leakage and also typically spread over time. Compare to CCF event OL2-9965, -11411 in 1983 (DocIndex=SF01).

The failure mechanism shows apparent tendency of growing degradation as the function of start cycles and operation time. The spray leak due to broken fuel return line of aggregate 651G301 was a singular event (no recurring at the near time) in that aggregate but the fuel return line of aggregate 651G401 was affected repeatedly at the following time points within +/- one year:

91-01-09 Drop leak (incipient)

92-01-09 Drop leak (incipient), in conjunction to spray leak at 651G301 one week apart (the considered multiple event)

92-05-07 Spray leak (critical)

92-08-05 Spray leak (critical)

The fire risk in case of spray leak has to be considered significant in an actual demand with mean load running time of about 4 hours. Thus the spray leak events are classified as critical for the failure mode failure to run. The fire risk in case of a drop leak is smaller but still considerable taking also into account the possibility of leak growth during an actual load running time. Based on insights from the growth tendency that risk is assessed to be Weight = 20%, which is then used in the construction of impact vector by hypothesis method.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only 651G301 would fail in load running demand	0.8		1				1
2.	Both 651G301 and G401 would fail due to fuel fire in demand condition	0.2			1			1
Net impact vector			0	0.8	0.2	0	0	1
			Average multiplicity				1.2	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL2-38804, -38801
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 2 - Rundown to cold shutdown. All 712-trains were at operation due to RHR via 321-721-712. System 712 is an open-circuit sea water cooling system consisting four (A-D) identical trains. Trains A, C and trains B, D are located in separete buildings and draw water via separate sea water channels from the main sea water channel. Each 712 train is connected to a heat exchanger in shutdown secondary cooling system (721) and to heat exhangers associated with one diesel (system 652). When system 712 operates the sea water cooling flow goes through exchangers in systems 721 and 652. Testing of specific limits in system 711 caused inadvertent opening of sea water recirculation gates in both sea water channels (AC/BD-trains). Therefore the flow conditions changed in sea water channels and unfastening of sludge (mussels etc.) occurred. The sea water heat exchanger in B-train was blocked totally (OL2.652E201 on 92-06-20) and thus diesel in B-train was inoperable. According to the flow measurement no sea water flow through the diesel heat exchanger exists in B-train. Redundant D-train heat exchanger was blocked partially (OL2.652E401). The sea water flow through the diesel heat exchangers in A and C train were normal. Event was directly detected (monitored failure).
C07	Event Interpretation	Diesels were stanby-state during this event. In case of actual demand should exist, the cooling water temperature in D-train may gradually rise to trip limit and thus prevent the diesel operation. Some risk to double failure if long run demand exists during the clean-up of first HX.
C09	Root Cause	H
C10	Coupling Factor(s)	MF
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	T2-09/92 (AOT 30 days). Mussel strainers were installed in system 712 in 1992. This decreases the risk of blockage of the heat exchangers.
G5	Test Interval	28 days
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A			W		
B	20.06.92		C	MC	
C			W		
D	20.06.92		D	MC	

Impact Vector Construction

In the earlier years the sea water heat exchangers (652E101-401 and 652E102-402) have been affected by blocking mechanism due to mussels etc., which constitutes a remarkable CCF mechanism (GenCl=HxBloc). Heat exchangers 652E101-401 are first in the circuit and thus more vulnerable to blocking. These problems were concentrated to summer months. It is of emphasis to notice that this CCF mechanism contains a coupling between reactor blocks. It is also of interest to notice that the sub pairs AC or BD, which have shared sea water channel, tend to be affected at the same time. In most cases the reduction in the heat transfer capacity developed gradually and could be thus controlled. In some cases abrupt flow changes invoked exceptional amount of sludge moving. The mussel strainers were installed in 1992. Thereafter, the problem disappeared.

The other similar CCF events at OL1/OL2 are following: DocIndex = SF03 and SF05. Blocking events to gradually reduce heat transfer capacity are following: DocIndex = SF04, SF06 and SF07.

In the considered case the sludge movement was invoked by inadvertent opening of the sea water gate. It can be assumed that those types of maneuvers will not be carried out during the mission time of DGs (undertaken in the presence of an actual demand situation). The failure mode is thus of monitored type with respect to the unavailability in standby state. Hence, a specific treatment is needed, when considering this event in CCF parameter estimation. In the considered case it is estimated that cleaning work would be successful to prevent total blockage of Train D (partially blocked initially) with 90% chances with respect to the risk of actual demand occurring. In the earlier CCF analysis in 1997 higher chances of 99% were used, but this estimate was changed to better reflect the coding of the component impairment as ‘D’.

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Train D would survive in actual demand, i.e. only Train B would fail	0.9		1				1
2.	Both Trains B and D would not survive in actual demand	0.1			1			1
Net impact vector			0	0.9	0.1	0	0	1
			Average multiplicity				1.1	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-5006737, -5007550
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. DG failed to start in test due to rpm guard, because of loose tachometer connection in train C (OL1.652K963, 95-07-05). In this event the connector was broken. Loose connection occurred six weeks later a the redundant DG in train A (OL1.652K961, 95-08-16).
C07	Event Interpretation	Some risk to have occurred more closely in time
C09	Root Cause	I
C10	Coupling Factor(s)	EI
C11	Shared Cause Factor	H
C12	Corrective Action	G
C14	Time Factor	L
C13	Other	T1-14/95 (AOT 30 days)
G5	Test Interval	28 days (from May 1994)
G5-2	Test Staggering	EST Evenly staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	16.08.95	28	C	TI	652K961
B			W		
C	05.07.95	28	C	TI	652K963
D			W		

Impact Vector Construction

The events were separated by six weeks (Sub A was tested successfully once after failure in Sub C). However, owing to the character of the failure mechanism as slowly developing in time, some chance is considered for the possibility for failures to co-exist. Thus effective Weight = 10% is used for double failure in the impact vector construction. Compare to the procedure explained in [NAFCS-PR03, Section 4.1].

Net Impact Vector

Hypothesis		Weight	TDC	Impact vector 0	1	2	3	4	Element sum
1.	Both components fail in TDC1	0.05	1			1			1
			2	1					1
2	Both components fail in TDC2	0.05	1	1					1
			2			1			1
3	As detected, component fail at separate TDC	0.9	1		1				1
			2		1				1
Net Impact Vector per TDC			1	0.05	0.9	0.05	0	0	1
			2	0.05	0.9	0.05	0	0	1
Sum Impact Vector over TDCs				0.1	1.8	0.1	0	0	2
				Average multiplicity				2	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL1-TR-R7-2/95
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 1, plant state: power operation. Snow blocked partially the burning air filter of DG in train A during periodic load running test. The pressure difference over the air filter alarmed after one hour running time and test was decided to interrupt after two hours running time. Filter was replaced by a spare component before continuing the test run. (OL1.652C107, 95-02-01). The partial blocking of the income air filter did not cause any noticeable disturbance to the running DG. Simultaneous problem at the OL2, compare to OL2-TR-R7-2/95. The weather conditions were unusual: wind speed 7.5 m/s, direction SSE along the walls with air intake of DGs, temperature -3 centigrade and very dense snowing; the turbulent wind also whirled up the snow from ground.
C07	Event Interpretation	The assessment of the impact reflects variations in extreme snowing conditions with respect to placement of air intake to different DGs. Notice unit-unit dependence and CCI coupling. Details in [CR_ImpVe].
C09	Root Cause	A
C10	Coupling Factor(s)	EE
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	Design modifications implemented. As a first stage measure, the operators were more specifically instructed about the procedure to remove the income air filter in case of snow blockage.
G5	Test Interval	28 days
G5-2	Test Staggering	EST Evenly staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	01.02.95		D	MC	652C107(primary event)
B	01.02.95		I	MC	652C207
C	01.02.95		D	MC	652C307
D	01.02.95		I	MC	652C407

Impact Vector Construction

The impact vector construction was based on using Common Load Model (CLM). The judgment of possible conditionality and dependence in actual average demand conditions were reflected in the CLM parameters (extreme load part and correlation coefficients). The details are explained in [CR_ImpVe]. Notice that the impact vector assessment also incorporates the fact that the concerned vulnerability was present from the start of the plant operation. Design changes have been implemented to decrease the possibility and consequences of blocking of air intakes in heavy snowing conditions. Notice also that the other Olkiluoto unit was similarly affected, compare to event OL2-TR-R7-2/95 (DocIndex = SF12). These events are relevant also for CCI dependence.

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Reasoning supported by CLM	1	0.356	0.289	0.198	0.111	0.045	1.0000
Net impact vector			0.356	0.289	0.198	0.111	0.045	1.0000
			Average multiplicity				1.2	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	OL2-TR-R7-2/95
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Olkiluoto 2, plant state: power operation. Snow blocked partially the combustion air filter of DG in train A during periodic load running test. The pressure difference over air filter alarmed at close by end of the test. The filter was replaced by a spare component after completing the test run. (OL2.652C107, 95-02-01). The partial blocking of the income air filter did not cause any noticeable disturbance to the running DG. Simultaneous problem at the OL1, compare to OL1-TR-R7-2/95. The weather conditions were unusual: wind speed 7.5 m/s, direction SSE along the walls with air intake of DGs, temperature -3 centigrade and very dense snowing; the turbulent wind also whirled up the snow from ground.
C07	Event Interpretation	The assessment of the impact reflects variations in extreme snowing conditions with respect to placement of air intake to different DGs. Notice unit-unit dependence and CCI coupling. Details in [CR_ImpVe].
C09	Root Cause	A
C10	Coupling Factor(s)	EE
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	Design modifications implemented. As a first stage measure, the operators were more specifically instructed about the procedure to remove the income air filter in case of snow blockage.
G5	Test Interval	28 days
G5-2	Test Staggering	EST Evenly staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	01.02.95		I	MC	652C107(primary event)
B	01.02.95		I	MC	652C207
C	01.02.95		I	MC	652C307
D	01.02.95		I	MC	652C407

Impact Vector Construction

The impact vector construction was based on using Common Load Model (CLM). The judgment of possible conditionality and dependence in actual average demand conditions were reflected in the CLM parameters (extreme load part and correlation coefficients). The details are explained in [CR_ImpVe]. Notice that the impact vector assessment also incorporates the fact that the concerned vulnerability was present from the start of the plant operation. Design changes have been implemented to decrease the possibility and consequences of blocking of air intakes in heavy snowing conditions. Notice also that the other Olkiluoto unit was similarly affected, compare to event OL1-TR-R7-2/95 (DocIndex = SF11). These events are relevant also for CCI dependence.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Reasoning supported by CLM	1	0.779	0.16	0.045	0.013	0.003	1.0000
Net impact vector			0.779	0.16	0.045	0.013	0.003	1.0000
			Average multiplicity				0.3	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	Lo1/H12/77
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	Dieselgenerators started and stopped due to a spurious signal 17.10.1977. This signal was caused by a repair work done at a reactor protection system cubicle. The dieselgenerators stopped simultaneously when the "large leakage" signal disappeared, because there was no delay circuit of the start-up signal. Delay circuits were installed later on.
C07	Event Interpretation	All the dieselgenerators were simultaneously unavailable about two minutes after stopping. The spurious signal was caused by a human error and the unavailability was caused by design inadequacy.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	17.10.77		C	MC	
B	17.10.77		C	MC	
C	17.10.77		C	MC	
D	17.10.77		C	MC	

Impact Vector Construction

This case represents an actual CCF of order 4, i.e. complete CCF of the group. The failure mode is of monitored type, inoperability time only two minutes, which means the need of special treatment in the CCF quantification.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
	This case is an actual CCF of order 4	1					1	1
Net impact vector			0	0	0	0	1	1
			Average multiplicity				4	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	LOTI-244922A
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	The flow of the cooling water (sea water) pump of diesel generator EY03 was decreased at a test 25.2.1997 and the vibration values were high. The cooling water flow was decreased because the pressure side check valve was stuck. The valve was replaced and the pump was checked 13.3.1997. The body of the lowest bearing was corroded. The lowest bearings were replaced. Checking of other pumps and valves were started, one pump per week. 5.4.1997 the pressure side check valve of EY04 was stuck closed in the normal test and prevented the cooling water flow, and therefore also diesel operation. The check valve was replaced. The bearings and worn shaft couplings of all the cooling water pumps have been replaced. The other check valves were replaced in the refuelling outage in August.
C07	Event Interpretation	The components, check valves and pump shafts and bearings, were worn due to corrosion and normal wear. The pumps would have operated in spite of the vibration but the sticking of one valve prevented the cooling water flow and the sticking of another valve led to a decreased flow. This flow would have been probably enough for a long operation of the diesel.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	H
C12	Corrective Action	G
C14	Time Factor	M
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
C	25.02.97	14	D	TI	
	18.03.97	14	I	MA	
	25.03.97	14	I	MA	
D	05.04.97	14	C	TI	

Impact Vector Construction

The evident component-to-component variation decreases in this case the estimated chances for multiple failure with respect to an actual demand. But a part of the measures to remove root causes took place about half a year from the initial detection of the problem, which increases the chances of multiple failure condition being latent. This aspect is difficult to express by Time Factor. The Impact Vector is assessed effectively for one TDC for simplicity.

Hypothesis		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Degraded trains would survive in actual demand, only Train D would fail	0.7		1				1
2.	Two least degraded trains would survive and Trains C and D fail	0.2			1			1
3.	Also one of the two least degraded trains would fail, only one survive	0.05				1		1
4.	All trains would fail in an actual demand condition	0.05					1	1
Net impact vector			0	0.7	0.2	0.05	0.05	1
			Average multiplicity				1.45	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-B1-86/033
C03	Failure Mode	FR
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	During periodic testing of diesel generator 1, a failure in the potentiometer was discovered. Reactive power loading could not be done in a controllable way. The construction of the potentiometer is considered to be unreliable and the potentiometers have therefore been replaced.
C07	Event Interpretation	Only diesel generator 1 was affected by this event. Since the failed component will be replaced on all EDGs as a precautionary measure this is coded as incipient component impairment for diesel generator 2 in accordance with the coding guidelines for EDGs.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	empty
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	10.10.86	14	D	MA	
B	10.10.86	14	I	empty	

Impact Vector Construction

Event description gives no evidence about redundant DGs to be affected simultaneously. It is not meaningful to make any judgment for the chances of criticality for DG in Sub A in the context of CCF analysis.

Net Impact Vector

This case can be regarded as a failure free-failure TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-B2-91/005
C03	Failure Mode	FR
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	During periodic testing of diesel generator 2 the elastic coupling between motor and generator broke. The coupling was 17 years old but according to the supplier the life-time is supposed to be 20 years. The coupling was immediately replaced and the corresponding coupling on diesel generator 1 was replaced during refuelling outage. In the future the couplings will be replaced every 10 years
C07	Event Interpretation	Only diesel generator 2 was affected by this event. Since the coupling was replaced at diesel generator 1 and the couplings will be changed more frequently in the future, this is coded as incipient component impairment for diesel generator 1 in accordance with the coding guidelines for EDGs.
C09	Root Cause	I
C10	Coupling Factor(s)	HQ
C11	Shared Cause Factor	H
C12	Corrective Action	F
C14	Time Factor	empty
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
B	29.04.91	14	C	MA	
A	29.04.91	14	I	empty	

Impact Vector Construction

Event description gives no evidence about redundant DGs to be affected simultaneously. The original event report RO-B2-91/005 tells that the coupling in DG Sub A was changed in the next annual overhaul in 1992, i.e. one year later, which indicates that the failure mechanism is slowly developing.

Net Impact Vector

This case can be regarded as a single failure failure TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-B1-93/022
C03	Failure Mode	FR
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	During reactor shutdown diesel generator 1 was running in order to feed 6 kV power bus 662A1. Low lubrication oil pressure caused diesel generator to stop automatically. The oil level is checked during operation with a dipstick. Due to difficulties in reading the dipstick when the diesel is running it was not discovered that the oil level was low and hence the diesel generator stopped. The diesel generators consume a large amount of oil during operation and must be refilled during long time operation. This is highly dependent on the load. During full load the consumtion is well-knowned but with a varying load the consumtion is harder to judge and it then becomes difficult to determine when to refill oil. Because of the large oil consumtion actions have been taken in order to reduce the consumtion. Furher on the instructions that control the supervision of the oil level are revised.
C07	Event Interpretation	Only diesel generator 1 was affected by this event. Since actions have been taken to lower the oil consumtion and the instructions have been changed this is coded as incipient component impairment for diesel generator 2 in accordance with the coding guidelines for EDGs.
C09	Root Cause	H
C10	Coupling Factor(s)	OF
C11	Shared Cause Factor	H
C12	Corrective Action	A
C14	Time Factor	empty
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	15.07.93	14	C	MC	
B	15.07.93	14	I	empty	

Impact Vector Construction

Some chance to systematic error in checking of the low oil level in the condition of actual demand having occurred. Weight = 10% is given to the possibility of double failure.

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	The DG in Sub A with incipent state would survive in the actual demand	0.9		1			1
2.	Both would fail in the actual demand	0.1			1		1
Net impact vector			0	0.9	0.1		1
			Average multiplicity			1.1	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	F2-RO-008/92-RO-01092
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	DG 230 was run as back-up during maintenance on a rotary converter, then a minor leakage was detected in the cooling water system: By touching the leak, the flow increased causing an immediate shut down of the diesel necessary. DG 240 normal start test of the diesel showed a similar leak this time the leak was minor and the diesel was able to run. A day later the pipe was replaced and the other sets checked. On DG 220 no fault detected but on DG 210 indications 2 –3 mm deep showed after radio-graphy The cause of the leaks was couple action and erosion. The potential of remaining material pipe/flange and cooler was altered after a change to titanium tubes in the cooler seven years earlier. A change to pipe and flange in titanium is planned to 1992.
C07	Event Interpretation	The secod leak was minor but occured within 5 days of the mayor one. The incidet caused replacement of all sets.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
C	22.05.92 9:26:00 AM	7	C	MW	
D	26.05.92 9:56:00 AM	15	D	MW	
A	26.05.92		I	MA	
B	26.05.92		W	MA	

Impact Vector Construction

There seems to be a substantial chance of double failure (Train D in addition to Train C) but only small chances of even the third degraded train failing with respect to actual demand condition.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only Train C would fail, degraded A and D would survive in actual demand	0.45		1				1
2.	One of the degraded trains would also fail in addition to Train C	0.5			1			
3.	Both degraded trains would fail in addition to Train C	0.05				1		1
Net impact vector			0	0.45	0.5	0.05	0	1
			Average multiplicity				1.6	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	F3-RO-014/89
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	A number of cracks were discovered in two of twelve con-rods inspected after cracks were discovered in Ringhals on engines from the same supplier. Laboratory examination showed fatigue cracks caused by insufficient fitting in of the tooth joint of the connecting rods big end bearing cap. In agreement with the manufacturer it was decided to chance the rods in all diesel generators to a stronger design. As the cracks were to small to have no immediate effect on rod failure and the manufacturer didn't have any failures of rod caused by this type of initial damage before. So it was decided that the diesels could be in service until a planned rod change.
C07	Event Interpretation	This reports as a CCF regarding to Coding Guidelines for Emergency Diesel Generators page 2 point 6. Replacement of the failed component as a precautionary measure.
C09	Root Cause	D
C10	Coupling Factor(s)	H
C11	Shared Cause Factor	L
C12	Corrective Action	C
C14	Time Factor	empty
C13	Other	
G5	Test Interval	7
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
	25.10.89		I	TA	
			W		
			W		
			W		

Impact Vector Construction

According to the event description the CCF risk seems negligible in this case.

Net Impact Vector

This case can be regarded as a failure-free TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-O1-90/027
C03	Failure Mode	FR
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	The station was at 100 % power when dissonance in the cooler was discovered during a periodic test of the diesel generator, sub B. The cause was that the sacrificial anode was loose. The sacrifical anode, made by zinc, was corroded and the screw holding the anode in place had loosened. A similar event was discovered the next day for diesel generator, sub A. The corrective actions were to change the sacrifical anode and the screw.
C07	Event Interpretation	These two events fullfill the definition of a common cause event. The two component fault states existed within a short time interval and were a direct result of a shared cause. However, a diesel generator can probably run for a long time (one week or longer) with a loose anode.
C09	Root Cause	D
C10	Coupling Factor(s)	HQ
C11	Shared Cause Factor	H
C12	Corrective Action	G
C14	Time Factor	H
C13	Other	RO-O1-90/27 and RO-O1-90/28 (Oskarshamn 1)
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
B	31.10.90	14	I	TI	
A	31.10.90	14	I	TI	

Impact Vector Construction

The lost anode was discovered at an early stage. Margin to even single failure seems large, and CCF risk negligible.

Net Impact Vector

This case can be regarded as a failure free-failure TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-O1-91/19
C03	Failure Mode	FR
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	The dieselgenerator in sub A started automatically together with the cooling pumps (712P1-P3). A pressure peak occurred which caused a rubber muff on the outlet pipe of the cooling system to slip off, causing leakage. A similar event occured six days later for dieselgenerator, sub B. The corrective actions were to change the design of the coupling.
C07	Event Interpretation	The two events differ in one significant way. The first event, 1991-05-03, affected the outlet pipe and the diesel generator did not loose the cooling. The leaking cooling water could, however, in the long run cause a flooding. The second event, 1991-05-09, affected the inlet pipe and the diesel generator lost the cooling.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	H
C13	Other	RO-O1-91/19 and RO-O1-91/20 date of event: 1991-05-09 (Oskarshamn 1)
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	03.05.91	14	I	DE	
B	09.05.91	14	D	DE	Date corrected

Impact Vector Construction

It was difficult to deduce the potential criticality of the failure mechanism both from the ICDE event description and original event reports RO-O1-91/19 and /20. The impact vector assessment was changed after obtaining additional information from the plant (compare to the redundant assessment). The event occurrences are being interpreted in the following way: The leak in Sub A can impose some moisture/flooding risk to electrical and electronic components with assessed criticality w = 40%. The cooling circuit blockage in Sub B has to be regarded as complete failure with respect to actual demand conditions. The component events happened during overhaul outage with 6 days interval (test interval 14 days, staggered test scheme). It is unclear if DG Sub B was additionally tested once the leak was detected in Sub A, and that DG was taken into repair. Anyway, there was a substantial chance of simultaneous failure if an actual demand had occurred close before detecting the degraded conditions. For simplicity the events are handled with respect to the CCF chance during one TDC.

The leak in Sub A was invoked in the functional tests during overhaul outage causing pressure excursions in service water system. The slip-off of the rubber muff in Sub B was invoked by startup of 712 pumps in overhaul operations causing also pressure peaks in the cooling circuit. It is assumed that these kinds of pressure excursions can occur in the connection of an actual demand for DG operation also during power operation (generally in any plant state), where 712 pumps first loose power and are then powered again with DG and started up.

Net Impact Vector

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	DGA would fail but DGB survive in the actual demand	0.6		1			1
2.	Also DGB would fail due to moisture/flooding effects	0.4			1		1
Net impact vector			0	0.6	0.4		1
			Average multiplicity			1.4	

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-O1-94/016
C03	Failure Mode	FS
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	Cut signal cable to diesel generators: During the modernizing of the plant, old cables were removed from relay rooms. By accident a cable designed for manoeuvring and indicating the operability of the diesel genarators was cut off by a worker affecting both diesel units. The station was in cold shut down mode during outage. When the cable was cut, several alarms occured affecting the diesel generators. According to Technical Specification one of the two diesels must be operable during current conditions.
C07	Event Interpretation	According to Technical Specification one of the two diesels must be operable during current conditions. During the event the busbars were powered by the ordinary grid. In case of an emergency is it possible to manually connect gas turbines to the diesel busbars.
C09	Root Cause	H
C10	Coupling Factor(s)	O
C11	Shared Cause Factor	H
C12	Corrective Action	G
C14	Time Factor	H
C13	Other	RO-O1-94/016 (Oskarshamn 1)
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	12.09.94		C	MC	
B	12.09.94		C	MC	

Impact Vector Construction

This case represents an actual CCF of order 2, i.e. complete CCF of the group. The failure mode is of monitored type, which means the need of special treatment in the CCF quantification. The event description lacks the information about the inoperability times for each DG, which is essential to know for quantification. The original event report RO-O1-94/016 tells that the inoperability times were 5h45min and 8h48min for DG Sub A and DG Sub B, respectively.

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	This case is an actual CCF of order 2	1			1		1
Net impact vector			0	0	1		1
			Average multiplicity			2	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-O1-94/010
C03	Failure Mode	FS
G6	Group Size	2
C04	Exposed Components	2
C05	Event Description	Both generators were unable to start due to an incorrect signal from the fire-extinguisher-system in the diesel room.The signal in the control room indicated that the fire-extinguisher-system was initiated. Before the event happened work was done with the fire-extinguisher-system which was locked in an inoperable state. The knob to restore it to an operable state did not function due to corrosion on the contact surfaces. DG 112 was made operable 4 minutes later and DG 111 one hour after the signal. The knob was replaced for DG112 and checked for DG111.The station was in cold shut down mode during outage. According to Technical Specification one of the two diesels must be operable during current conditions.
C07	Event Interpretation	Both diesel generators appeared to be blocked during 4 minutes but a later analysis showed that DG112 was operable the whole time. According to Technical Specification one of the two diesels must be operable during current conditions
C09	Root Cause	D
C10	Coupling Factor(s)	HQ
C11	Shared Cause Factor	H
C12	Corrective Action	G
C14	Time Factor	H
C13	Other	RO-O1-94/010 (Oskarshamn 1)
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	09.05.94	14	C	MC	
B	09.05.94	14	W	MC	DG Sub B was operable throughout the event

Impact Vector Construction

The event description is somewhat confusing about the inoperability times but the original event report RO-O1-94/010 confirms that only DG111 (Sub A) was inoperable about one hour while DG112 (Sub B) was operable throughout the event. It was only misbelieved by the operators that DG112 had been initially inoperable (start signal blocked out). However, the actual condition was more complicated as revealed by the additional information provided by the plant expert. Blocking of start signal was related to the degree of corrosion in the reset button for fire signal. The fact that the DG112 was not affected by the event is a consequence that the contact surfaces of the reset button were heavily corroded. Had this corrosion been less significant, the actual blocking signal from the fire extinguishing system would also have prevented the start of DG112. Thus the chances for both mutually exclusive consequences existed: estimated as 50% - 50%. It has to be emphasized that the ICDE codes for the component impairment (CW) are misleading in this case.

Hypothesis		Weight	Impact vector 0	1	2		Element sum
1.	Only DG111 would fail, DG112 successfully started	0.5		1			1
2.	DG112 would fail also due to blocked start signal	0.5			1		
Net impact vector			0	0.5	0.5		1
			Average multiplicity			1.5	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	RO-O3-94/004
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	The station was at 100 % power when high exhaust temperatures were measured for cylinder 9 and 10 after a periodic test of the diesel generator, sub B . The cause was that the fuel pump was affected by vibrations which made fuel ignition occur at the time when the exhust valves were open.The vibrations losened a screw nut which changed the adjustments of the fuel pump. A similar event happened 9 months later for diesel generator, sub D, for cylinder 10. The corrective actions were to fasten the screw nut and adjust the pump.Two DG were operable and one DG was out of service for maintenance during the event.Technical Specifcations were fullfilled.
C07	Event Interpretation	It´s not clear if these events can be classified as potential CCF-event according to the definitions in the ICDE-project due to the long time interval between two similar events, see RO-O3-94/028. Perhaps this event should be classified as a reccurent failure? Damaged exhaust valves in cylinders can lead to power losses for the diesel generator. The importance of well tightened screw-nuts can be pointed out for diesel-components affected by vibrations.
C09	Root Cause	M
C10	Coupling Factor(s)	MP
C11	Shared Cause Factor	H
C12	Corrective Action	B
C14	Time Factor	L
C13	Other	RO-O3-94/004 (Oskarshamn 3) It is not clear if FR is the right code because the DG will compensate the powerloss for one cylinder automatically.
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
	16.02.94	1	D	TI	
	01.11.94	14	I	TI	
			W		
			W		

Impact Vector Construction

According to the event description the CCF risk seems negligible in this case. Notice especially the substantial time spread between the component events in Train B and D (nine months). There is little meaning to make judgment for the chance of single failure state. Thus this case can be considered as a failure-free TDC in CCF quantification.

Net Impact Vector

This case can be regarded as a failure-free TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R2-RO-013/97-R0-014/97
C03	Failure Mode	FS
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	At normal start test of the set, didn't the generator of DG210 generate voltage thereby failing to synchronise to the emergency diesel busbar. The diesel generator was declared not operational at 10.26 and the other three diesels were tested. Other failure was detected at DG220, at 11.28 the generator tripped on high voltage. The reactor power at detection time was 56%. The tech spec requires a cold shut down in then two DG are out of service. Allowable repair time fore one DG is 48 hours. However one hour after the second fault was detected, the first failure was found and repaired. The diesel generator (DG 210) was tested and operational at 12.05. The second DG 220 was declared operational 6 hours later. DG210 An insufficient torqued screw in a connection block in the field circuit of the generator causing poor connection. The cubicle was changed in October 1996 after a fire. Circumstances contributing to a failed control by the technician is the fact that the connection block is located lower left corner of the cubicle and the door makes the check difficult. DG220 The cause was an insufficient torqued screw in a connection block in voltage measuring circuit giving to low voltage to the voltage regulator. DG230 An insufficient torqued screw in a connection block in the protection circuit's was found during the check. No problem was detected at the earlier test run. DG240 An insufficient torqued screw in a connection block in the feed circuit for the generator magnetic field was found during the check. No problem was detected at the earlier test run. The last time the connecting blocks were opened was in 1994. The blocks are mounted horizontal and opens downwards preventing a accidental closure. In this case the plate didn't fall down. Testing showed a single block needed only half turn of the screw to open and the plate fell down. Mounted together 4 turns needed before the plate fell the friction from the nearby blocks holding the plate. The use of improper tools could have misled the operator as a wide driver give friction force against the sides of the blocks especially if not hold at a right angle to the screw. The tools were changed before the incident The components were connection blocks manufactured by Phoenix type RTK/S-Ben, voltage 500 V and type URTK/S-Ben, voltage 500 V. Both affected sets were tested 14 respective 7 days before detection at the next test.

		No other of the sixteen diesel generators at the plant have had similar problems. For other connection blocks in the unit a test programme applied for the next outage. The procedure for the check after maintenance work was not formalised at the time of the event. Written procedures of checks to do and in which cubicle was the long run corrective action.
C07	Event Interpretation	Typical misses in maintenance. Even if not the same person torqued the all blocks there is a connection in maintenance procedures, tools and connection block design. The problem with to wide a tool was identified and corrected. Maybe old tools were still in use or an ordinary screwdriver was used. One insufficient torqued connection block have survived 75 tests and the other 15 tests, when fails within 7 days. Vibration or oxidation of contact surfaces could be a contributing factor.
C09	Root Cause	H
C10	Coupling Factor(s)	O
C11	Shared Cause Factor	H
C12	Corrective Action	F
C14	Time Factor	H
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	01.07.97	14	C	TI	10:08:00 AM
B	01.07.97	7	C	TU	11:28:00 AM
C	01.07.97		I	TU	
D	01.07.97		I	TU	

Impact Vector Construction

In addition to the evident double failure state there seems to have been substantial chance of the other two DGs also failing in an actual demand as it is said that vibration can be a contributing factor. The chance of higher order failure is estimated to be 20% and is divided in equal shares between triple and total failure state.

Hypothesis		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Degraded Trains C and D would both survive in actual demand	0.8			1			1
2.	One of the degraded trains would also fail in addition to Trains A and B	0.1				1		
3.	Both degraded trains would fail in addition to Trains A and B	0.1					1	1
Net impact vector			0	0	0.8	0.1	0.1	1
			Average multiplicity				2.3	

Net Impact Vector

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R3-RO-003/89-R0-009/89
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	A small leak was detected in the high-pressure pipe between injection pump and the injector on diesel DG 310. The other three Diesels were tested according to the Technical Specifications with no leaks found. The pipe was replaced in 2 h and 15 min. Examination revealed a small crack. Fuel pipes with better vibration resistance have been designed. All spare parts was replaced with new design later all diesels where fitted with the new design pipe. The second leak was on diesel DG340 and exactly identical. (New design not yet fitted.)
C07	Event Interpretation	This CCF is not within the 28 days window (2 times testing interval). But falls within the recommendations to report cases when decisions are taken to make design changes of the population. The degradation of the diesels are low as the power output could be met with 15 cylinders working and one shut of.
C09	Root Cause	D
C10	Coupling Factor(s)	H
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	L
C13	Other	A third case occurred 89 09 28 at the identical diesels of unit 4. At that time the new designed pipes was not yet delivered to site so the old design was still in operation.
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
	17.01.89 2:15:00 AM		I	MW	
	24.03.89		I	MW	
			W		
			W		

Impact Vector Construction

According to the event description the CCF risk seems negligible in this case, especially due to the time spread between the component events (two months which corresponds to 4 test intervals).

Net Impact Vector

This case can be regarded as a failure-free TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R3-RO-032/89
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	A number of cracks were discovered in one con-rod in a routine inspection during overhaul of diesel DG330. The extended inspection showed cracks in 11 of 16 con-rods of the engine. Laboratory examination showed fatigue cracks caused by insufficient fitting in of the tooth joint of the connecting rods big end bearing cap. In agreement with the manufacturer it was decided to chance the rods in all diesel generators to a stronger design. The decision includes the four diesels of Ringhals 4 (SE-10). As the cracks were to small to have no immediate effect on rod failure and the manufacturer didn't have any failures of rod caused by this type of initial damage before. So it was decided that the diesels could be in service until a planned rod change.
C07	Event Interpretation	This reports as a CCF regarding to "Coding Guidelines for Emergency Diesel Generators" page 2 point 6. Replacement of the failed component as a precautionary measure.
C09	Root Cause	D
C10	Coupling Factor(s)	H
C11	Shared Cause Factor	L
C12	Corrective Action	C
C14	Time Factor	empty
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
C	11.10.89		I	MA	
			W		
			W		
			W		

Impact Vector Construction

The CCF risk seems negligible in this case.

Net Impact Vector

This case can be regarded as a failure-free TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R4-RO-034/89-R0-040/89
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	A small leak was detected in the high-pressure pipe between injection pump and the injector on diesel DG 410. The pipe was replaced in 25 min. Examination revealed a small crack at the same spot as previously detected on diesels of unit 3. Fuel pipes with better vibration resistance have been designed. All spare parts was replaced with new design later all diesels where fitted with the new design pipe. The second leak was on diesel DG430 and exactly identical. New design not yet fitted. Repair time 14 min.
C07	Event Interpretation	This CCF is not within the 28 days window (2 times testing interval). But falls within the recommendations to report cases when decisions are taken to make design changes of the population. The degradation of the diesels are low as the power output could be met with 15 cylinders working and one shut of.
C09	Root Cause	D
C10	Coupling Factor(s)	H
C11	Shared Cause Factor	H
C12	Corrective Action	C
C14	Time Factor	L
C13	Other	This is an identical report to the report from unit 3
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
A	28.09.89		I	TI	9:00:00 AM
C	26.11.89		I	MW	8:40:00 AM
			W		
			W		

Impact Vector Construction

According to the event description the CCF risk seems negligible in this case, especially due to the time spread between the component events (two months which corresponds to 4 test intervals).

Net Impact Vector

This case can be regarded as a failure-free TDC.

CCF Event Description and Classification

Basic description and classifications extracted from ICDE database as of 27 August 2001.

C01	Event Identifier	R3-RO-043/94
C03	Failure Mode	FR
G6	Group Size	4
C04	Exposed Components	4
C05	Event Description	During load test, alarm for high crankcase pressure caused the engine to shut down. The cooling water temperature of cylinder 15 was 6 centigrade above the other cylinders. The piston and liner of No15 cylinder was changed due to tightening. The cause was a too effective lower oil ring. The remedy is to remove the lower oil ring of all diesel engines. Some smaller earlier problems with tightening engines was also explained by the investigation made by the manufacturer, who recommended removal of the lower oil-ring. The work was performed during normal overhaul of the engines after some initial test on one engine.
C07	Event Interpretation	This reports as a CCF regarding to “Coding Guidelines for Emergency Diesel Generators” page 2 point 6. Replacement of the failed component as a precautionary measure.
C09	Root Cause	D
C10	Coupling Factor(s)	HC
C11	Shared Cause Factor	L
C12	Corrective Action	C
C14	Time Factor	L
C13	Other	
G5	Test Interval	14
G5-2	Test Staggering	Staggered

Component Events

Sub	Date:Time	Latent	Impairment	Detection	Notes
	02.12.94		C	TI	12:56:00 AM
			W		
			W		
			W		

Impact Vector Construction

Event description gives no evidence about redundant DGs to be affected simultaneously.

Net Impact Vector

This case can be regarded as a single-failure TDC.

Work Notes

Logging Notes of the Impact Vector Assessment in the DG Pilot

Date/Version:	07 September 2002	Version 0	
	18 September 2002	Version 1	
Prepared by:	Tuomas Mankamo	Avaplan Oy	TM
	Jean-Pierre Bento	JPB Consulting AB	JPB

1 Assessment Process

The principal milestones are described in Table 1. The 1st Version of the redundant assessments was made independently, i.e. without seeing the base assessments. The completed assessments are based on the discussion of the arguments for different hypotheses and judgments, and retrieval and exchange of additional specific information about several more complicated events.

Table 1 Milestones of the Impact Vector assessment in the DG Pilot.

Date	Description
01 June 2002	The base assessments by TM, 1st Version, were circulated among NAFCS and discussed in the WG meeting on 04 June 2002, in Stockholm
13 June 2002	The extracted ICDE data, guideline NAFCS-PR03 and methodological references were submitted for the redundant assessment to JPB
27 June 2002	The procedure of the redundant assessment was agreed in the WG meeting in Stockholm
08 August 2002	The redundant assessment results (1st Version) and base assessment results (2nd Version, including some modifications based on the read-through of the Swedish ROs by TM) were exchanged
28 August 2002	The insights from the assessment differences were discussed in the WG meeting in Stockholm. The procedure for completion and documentation was agreed, including retrieval of additional information about some more complicated events
06 September 2002	The completed assessments were exchanged (2nd Version by JPB and 3rd Version by TM). The logging notes were finalized.

2 Specific Details

The observations and remarks about assessment details and outcome, which are of general interest regarding the use of the results or methodology, are gathered in Table 3. The comparison type classes of the base and redundant assessment are defined in Table 4. It shows also the count of events for type classes: the more general insights will be discussed in Section 3. In order to facilitate the discussion of the assessment per CCF event type and mechanism, the second column in Table 3 indicates so called Generic Failure Class, see the definitions in Table 2, and compare to the introduction of this concept in [DGs-CCFA].

Heat exchanger blockages at Olkiluoto

Blockage of the seawater heat exchangers (HXs) is one of the Generic Failure Classes, denoted as 'HxBloc'. In all cases of this type at Olkiluoto (SF03-07 and SF09) the degree of blockage, need for cleaning actions (during mission time of a possible actual demand) and required time to complete the cleaning could not be sufficiently inferred from the ICDE event descriptions. The degree of HX blockage was considered in more detail during the CCF analysis for Olkiluoto DGs in 1997. The impact was classified into categories W, I, D and C (i.e. ICDE code categories of component impairment) based on the measurement logs of heat transfer capacity and system expert's judgment. After submitting the analysis report [DGs-CCFA] – made by the base analyst - to the redundant analyst, the assessments converged substantially. One observation is, that without more detailed background information, the analyst has to rely much on the ICDE codes for component impairment values, but these prove out generally not to be on consistent scale or relation from case to case. Besides, the four categories W, I, D and C represent quite a crude scale, especially thinking of the desire to consistently assess similar cases. So here is an example of the set of cases where it is very beneficial to do the Impact Vector construction parallel with the initial collection of ICDE data and in co-operation with the plant expert.

Several of the HxBloc events (SF03, SF05 and SF09) were related to abrupt operation of sea water gate in the shutdown cooling water system 712 which circulates water to DG HXs. As explained in the ICDE event description, each sub pair AC and BD has its own intake channel for seawater (for system 712), where the concerned gate is located (one gate in each channel). The abrupt opening of the gate and invoked sludge movement impacts thus only HXs in one sub pair. It is unlikely that the gates in different channels had been operated – in the considered cases – simultaneously or close in time. This vital configuration aspect, even though told in the ICDE description, is difficult to infer at the first reading. This can easily lead to pessimistic Impact Vector assessment. A graphical presentation of the cooling circuit would directly help. In these kinds of cases it is important that the correct understanding of the system configuration can be verified with the plant expert.

Table 2 Generic Failure Classes applicable to the events in the DG Pilot.

Generic Failure Class	Description
HxBloc	Sea water heat exchangers, blocking and reduced heat transfer capability
LeakFI	Leak of fuel injection piping
LeakFR	Leak of fuel return piping

Snow storm causing blockage of air intake filters at Olkiluoto

The two cases SF11-12 related to snow storm at Olkiluoto in 1995 represent the extreme end of complexity. It must be admitted that preparing sufficient brief description to ICDE format is challenging, perhaps impossible. It is especially difficult to describe the interdependence of the influences for the redundant components. In fact, that is not encouraged by the ICDE coding guideline, which directs emphasis on the description of the influences at each individual component separately (impairment values). Fortunately, there exists a well-written plant incident report for these cases (classified as INES = 1) both in Finnish and Swedish [1-TR-R7-2/95; 2-1-TR-R7-2/95]. Besides, the base assessment could utilize the earlier work for ICDE Benchmark [CR_ImpVe]. Submitting the plant incident report and Benchmark work notes to the redundant analyst helped in converging in the assessments within a reasonable uncertainty range.

The base assessment used CLM as supporting tool showing an example where a parametric dependence model can be helpful in the logical reasoning for Impact Vector construction. Anyway, it has to be emphasized that these cases represent an assessment situation, which even at the best contains large uncertainty.

Rubber muffs slipping off causing DG cooling circuit leaks at O1

In this case (SF21) DG B lost adequate cooling because the leak affected the inlet pipe of the cooling circuit. Similar slipping off of the rubber muff had occurred six days earlier at DG A but the main difference was that the leak was on the outlet pipe. Based on the recent discussion with plant specialists led to the assessment that the leak on the outlet pipe did not directly affect DG cooling. However, spraying water and moisture could have caused problems to electrical and electronic components during a longer load running mission. It is uncertain whether an additional test of DG B was undertaken at the first event affecting DG A as requested by the Technical Specifications. This crucial aspect makes substantial difference for the condition-specific likelihood of CCF being present but was not mentioned in the ICDE event description. Also the criticality of the leak of DG A was difficult to infer without judgment of the plant specialists.

The initial assessments for the Impact Vector were in this case {0.25, 0.50, 0.25} and {0, 0.05, 0.95} but converged to {0, 0.6, 0.4} after retrieval of additional clarification from the plant experts. It has to be emphasized that the ICDE codes for the component impairment (ID) are misleading in this case.

Incorrect fire signal prevented DG start at O1

This event SF 23 represents a very dedicated failure mechanism: blocking of start signal to the two DGs was related to the degree of corrosion in the reset button for the fire signal. The fact that the second DG was not affected by the event is a consequence that the contact surfaces of the reset button were heavily corroded. Had this corrosion been less significant, the actual blocking signal from the fire extinguishing system would also have prevented the start of the second DG. Thus the chances for both mutually exclusive consequences existed. The above details were not contained in the ICDE description, but were obtained from plant experts when asking for additional clarifications. It has to be emphasized that the ICDE codes for the component impairment (CW) are misleading in this case.

The initial base assessment of Impact Vector was in this case {0, 1, 0}. It converged with the redundant assessment {0, 0.5, 0.5} after getting more complete description of the failure mechanism.

Table 2 Observations from the Impact Vector assessment. The highlighted indexes in the first column indicate cases, where additional information was essential to complete the ICDE event description.

Case	Generic Failure Class	Observations	Comparison Type Class
SF01	LeakFI	Identical assessment, example case in NAFCS-PR03	2
SF02		Identical assessment, example case in NAFCS-PR03	2
SF03	HxBloc	Identical assessment, evident impact (impairment vector = CCWW)	1
SF04	HxBloc	Same hypothesis structure, base assessment more conservative in the quantitative judgment	4
SF05	HxBloc	Same hypothesis structure, redundant assessment more conservative in the quantitative judgment	4
SF06	HxBloc	Same hypothesis structure, base assessment more conservative in the quantitative judgment	4
SF07	HxBloc	Same hypothesis structure, minor difference in the quantitative judgment	4
SF08	LeakFR	Identical assessment, example case in NAFCS-PR03	2
SF09	HxBloc	Identical assessment, consensus reached after discussion of the arguments	3
SF10		Same hypothesis structure, redundant assessment more conservative in the quantitative judgment	4
SF11		Snow storm causing blockage of air intake filters, base assessment used CLM as supporting tool, redundant assessment standard hypothesis method	6
SF12		Same observations as for SF11	6
SF13		Identical assessment, evident impact (impairment vector = CCCC)	1
SF14		Different hypothesis structure, base assessment considered also the possibility of higher order failure at degree 3-4 (impairment vector = CDII)	5
SF15		Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of CCF (impairment vector = DI, time factor = 0)	5
SF16		Different hypothesis structure, base assessment regarded this as single-failure cycle, redundant assessment considered the possibility of CCF (impairment vector = CI, time factor = 0)	5
SF17		Same hypothesis structure, redundant assessment more conservative in the quantitative judgment	4
SF18		Same hypothesis structure, base assessment more conservative in the quantitative judgment	4

Case	Generic Failure Class	Observations	Comparison Type Class
SF19		Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of single failure (impairment vector = IWWW)	5
SF20		Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of single failure (impairment vector = II)	5
SF21		Identical assessment, consensus reached after discussion of the arguments and retrieval of additional information from the plant	3
SF22		Identical assessment, evident impact (impairment vector = CC)	1
SF23		Identical assessment, consensus reached after discussion of the arguments and retrieval of additional information from the plant	3
SF24		Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of CCF (impairment vector = DIWW, Time Factor = 0)	5
SF25		Identical assessment, consensus reached after discussion of the arguments	3
SF26	LeakFI	Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of CCF (impairment vector = IIWW, Time Factor = 0)	5
SF27		Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of single failure (impairment vector = IWWW)	5
SF28	LeakFI	Different hypothesis structure, base assessment regarded this as failure-free cycle, redundant assessment considered the possibility of CCF (impairment vector = IIWW, Time Factor = 0)	5
SF29		Different hypothesis structure, base assessment regarded this as single-failure cycle, redundant assessment considered the possibility of CCF (impairment vector = CWWW)	5

3 Summary of the Insights

The general conclusion of this pilot work underlines the worth and necessity to perform comparative assessments by two analysts in order to reach high quality CCF data.

The count of type classes from the comparison between base and redundant assessment is presented below. The main insights will be discussed below.

Table 4 Comparison type classes.

Type class	Description	Count
1	Identical assessment, evident impact	3
2	Identical assessment, follows guide example	3
3	Identical assessment, consensus reached after discussion of the arguments, typically additional clarification had to be obtained from the plant	4
4	Same hypothesis structure, differing weights	7
5	Differences in hypothesis structure, typically weak degradation cases where one of the analysts considered the chances of higher order failure	10
6	Basic differences in the assessment logic, e.g. one of the analysts used a specific causal model or parametric dependence model to support the assessment	2
		29

The possibility of large difference in the impact vector assessment is evidently connected to such situations where:

- One of the analysts has less complete description of the event, or
- The analysts have different incomplete descriptions of the event.

The lesson learnt is the vital importance of checking the plant event reports especially for any more complicated cases. It is also highly desired that the analysts have access to the plant experts to ask clarifications regarding uncertain event interpretations. In the DG Pilot, the additional information can be regarded essential for 11 out of 29 cases, i.e. about 40% of the cases. Compare to the highlighted indexes in Table 3. In future work it is highly recommended that the impact vector assessment is made in parallel with the collection of the ICDE data, because this would save significant efforts for the plant experts and the analysts, and facilitate improved overall QA.

The event analysis during the DG Pilot revealed several remarkable inconsistencies or essential shortcomings in the ICDE event descriptions. The comments in these regards will be gathered separately and submitted to the ICDE contact persons at the plant for further measures.

Further insights are connected to following observations:

- Type class 4 concerns cases, where uncertainty remains, i.e. completion of event description is not possible or would not anyway facilitate interpretation for impact vector

assessment. It is important to notice that in this kind of cases the judgments deviated into both directions, i.e. no bias between the two analysts in the DG Pilot

- Type class 5 contains mostly events where the risk for CCF is small, i.e. boundary cases, typically recurring events with substantial time spread between the component events (see later bullet discussing further the recurring time-spread events). In the continuation it would be desirable to define rules, and set screening threshold for the cases to be covered in the impact vector assessment. For the achievable statistics these boundary cases have a small influence. Qualitative analysis aims and completeness requirement may justify setting the screening threshold low.
- In type class 5 the redundant assessment used in many cases – especially during the first round – the assumption of independent component degradation, which may lead to optimistic results. The guideline should be improved in these regards to better express the circumstances where that assumption can be regarded as reasonable.
- Among type class 5 are several cases where the component (degradation) events have substantial time interval, i.e. no evidence of coexistent significantly degraded component states. It is characteristic for the varying reporting quality that in many of these cases the ICDE code for Time Factor is set 'Low', while it should be set 'Null'. If the recurring failures (degradations) are wanted to be processed for the aims of qualitative analysis, they might be best to handle in a specific way separate from coexistent failed/degraded component states carrying measurable CCF risk.

The conducted work is restricted to the events as currently stored in the ICDE database, i.e. no completeness verification is performed. Compare to the discussion of this issue in [NAFCS-PR08 and –PR11]. Furthermore, so called coincident multiple failures are not covered (not presented in the ICDE data). Compare to the discussion of this issue in [NAFCS-PR03]. It can be noted that the Olkiluoto experience of DGs contains several cases of this kind and they should be part of adequate overall quantification of multiple failures [DGs-CCFA].

References

CR_ImpVe Expressing the Impact of a CCF Mechanism. Work notes by T. Mankamo, Avaplan Oy, 17 September 1996.

DGs-CCFA CCF Analysis of Diesel Generators, Olkiluoto 1 and 2 Experience 1983-1997. Work report prepared by T. Mankamo, Rev. 07 April 1999.

NAFCS-DG-SF-ImpVe-TM-V2
Base Assessment of the Impact Vectors in DG Pilot. Third round by Tuomas Mankamo, 07 September 2002.

R0209-ES-Impact Vector
Redundant Assessment of the Impact Vectors in DG Pilot. Second round by Jean-Pierre Bento, 06 September 2002.

NAFCS-PR03 Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Draft for Peer Review, 12 January 2002.

NAFCS-PR08 Qualitative analysis of the ICDE database for Swedish emergency diesel generators. Topical Report NAFCS-PR08, prepared by Jean-Pierre Bento, JPB Consulting AB, Version A1, 30 April 2002.

NAFCS-PR11 Data survey and review of the ICDE-database for Swedish emergency diesel generators. Topical Report NAFCS-PR11, prepared by Jean-Pierre Bento, JPB Consulting AB, Version A1, 30 April 2002.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
App 5.6	**Impact Vector Application to Pumps PR18**	**PR18**
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS

Nordisk Arbetsgrupp för CCF studier **NAFCS-PR18**

Title:	**Impact Vector Construction to Pumps**
Author(s):	*Tuomas Mankamo*
Issued By:	
Reviewed By:	*Jean-Pierre Bento*
Approved By:	Gunnar Johanson
Abstract:	The Impact Vectors are constructed for the centrifugal pumps of the Nordic NPPs based on the current ICDE data. Foreign pump events are explored for comparison purpose.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2002-10-14	TM
Draft 1	2003-02-07	TM
Draft 1+	2003-05-06	TM
Issue 1	2003-08-29	TM
Final	2003-08-29	GJ

Contents

Impact Vector Construction to Pumps

1. Introduction

1.1 Objective and scope

The Impact Vector assessments are made here for the CCF events of centrifugal pumps of the Nordic NPPs following the procedure developed in the course of the earlier application to diesel generators, so called DG Pilot [NAFCS-PR10]. The ICDE database was also explored for the foreign pump CCFs for comparison purpose, see [ICDECG01, NEA/CSNI/R(99)2].

The method description and practical guideline for Impact Vector construction [NAFCS-PR03, -PR17] were further enhanced based on the new insights.

The Licensee Event Reports (ROs) were used as additional information for the Swedish events. The earlier detailed CCF analysis for the pumps of OL1/OL2 could be benefited in this application [Pumps-CC].

1.2 QA and documentation

The principal QA action was constituted by the redundant assessment of the Impact Vectors. The produced documents as listed in Table 1.1. See further details of the working procedure, QA and documentation in Section 2.3.

Issue 1 of the application report takes into account the internal review comments. These did not imply changes in the Impact Vector assessments nor in the presented results. The documentation package is thus same as in spring 2003, except some text improvements in the application report.

Table 1.1 Documents of the application, compare to the reference list.

Document index	Title	Last update
NAFCS-PR18	Impact Vector Construction to Pumps	29-Aug-03
CCF-P-Nordic-Descriptions-V1.xls	CCF Event Descriptions for the Pumps in the Nordic NPPs	06-Mar-03
CCF-P-ImpVe-Construction-AV2.xls	Impact Vector Assessment for the Nordic Pump CCFs, Analyst A	03-Apr-03
CCF-P-ImpVe-Construction-BV2.xls	Impact Vector Assessment for the Nordic Pump CCFs, Analyst B	03-Apr-03
NAFCS-WN-TM08	Comments on the ICDE database for the information stored about the Finnish and Swedish pumps, feedback from the impact vector assessment	25 April 2003
NAFCS-WN-TM09	Logging Notes of the Impact Vector Assessment for the Pump Events	25 April 2003

2. Nordic CCF events of pumps

2.1 Observed pump population, coverage of ICDE data

The observed (centrifugal) pump population of the Nordic NPPs and general exposure data are summarized in Table 2.1. The reactor units are grouped and sorted in the order of country and then in alphabetic order. The observation times for the Swedish units are limited to selected years (partially assumed, the statistical records are not complete in the ICDE database). For LO1/LO2 the observation period is from the start of the operation up to 1997. For OL1/OL2 the observation period is 1983-97, same as in the recent plant specific CCF analysis [Pumps-CC].

Table 2.1 Summary of the ICDE data for the centrifugal pumps in the Nordic NPPs (as of December 1998).

Units	Pump groups	Remarks	Reactor years	CCCG years	CCF events
B1/B2	2x11		16	176	0
F1/F2	2x4	Note 1	18	72	0
F3	3	Note 1	9	27	0
O1	9		11	99	1
O2	9		11	99	2
O3	7		11	77	0
R1	7	Note 2	6	42	1
R2	6		6	36	1
R3/R4	2x7	Note 3	14	98	7
LO1/LO2	2x4	Note 4	34	136	2
OL1/OL2	2x7		26	182	1
Sum	107		162	1044	15

Note 1: Observation period assumed as 9 years (missing from the statistical record)

Note 2: Observation period assumed as 6 years (missing from the statistical record)

Note 3: CCF events includes six events of type to be explicitly modelled

Note 4: CCF events includes two events of type to be explicitly modelled

Table 2.1 summarizes also the number of reported CCF events, pooled over different failure modes. Three reported cases actually concern replicate events of two separate CCCGs at twin reactor units. These cases are split into separate CCF events with proper cross-referencing in the Impact Vector assessment. This makes in total 15 events. One CCF event has occurred per pump group in every seventy years in the average. The CCF rate is thus relatively low, about one order of magnitude lower than for the DGs, compare to [NAFCS-PR10, Section 2.1]

Six CCF events of R3/R4 affected the water lubrication system for the sea water pumps in system715, representing functional and operator action dependencies which

ought to be explicitly modelled, i.e. not well adapted to be covered by (parametric) CCF data. The two LO1/LO2 events are of that type also. If these events that are recommended to be explicitly modelled are drawn separate, only seven events are left as data for parametrically modelled CCFs. They are dispersed over the reactor units without possibility to infer any statistically significant difference in the CCF rate among the plants.

Besides of different failure modes the data covers also many different pump types with respect to design and operation. These characteristics will be discussed in the next section. An implication is that the observed data are very split. It can provide at the best only generic quantitative insights – but does not allow pump type-specific data acquisition.

2.2 Normal state and failure mode

A characteristic feature, which differs from the DG Pilot, is the fact that the standby state is the normal state for only a part of the pump groups. The pumps can be grouped into the following categories with respect to the normal state (as applied also in the ICDE data collection):

- SB Standby state (except test and demand missions)
- Int Intermittently operated (typically rolling change-over scheme followed among redundant pumps)
- OP Operating state (over whole operating/overhaul cycle)

The CCF mechanisms and their detection differ significantly depending on the normal state. This influences Impact Vector assessment besides of fundamental implications to the CCF quantification. The failure modes of the pumps are following:

- MC/MR Monitored critical or repair-critical failure in standby state, detectable in standby state
- FS Failure to start
- FR Failure to run

MC/MR has to be treated strictly separately (applies to the pumps with normal state = SB or Int), because the functional impact and hence the quantitative treatment is much different. The distribution of the CCF events is shown in Table 2.2

Table 2.2 Distribution of the observed CCF events of the Nordic pumps with respect to failure mode and normal state.

Failure mode	SB	Int	OP	Any
MC/MR	1	1	N/A	2
FS	2	2	0	4
FR	2 (1	7 (1	0	9
In total	5	10	0	15

1) Two events of FR/SB (LO1/LO2) and six events of FR/Int (R3/R4) represent functional and operator action dependencies which ought to be explicitly modelled

with respect to failure mode and normal state. As already noted, the data are very split – and also sparse, when taking into account that eight events are of the type recommended to be explicitly modeled.

2.3 Procedure for Impact Vector construction

The scheme of the Impact Vector construction as developed in the DG Pilot is generally followed with some minor changes. Again the cornerstone of the QA was the redundant assessment of the Impact Vectors, conducted by Jean-Pierre Bento, JPB Consulting AB.

The order of assessment flow was changed in comparison to DG Pilot. The event descriptions were discussed between the analysts before the first assessment round in order to identify and handle the most significant information deficiencies. This change proved successful. The discrepancies at the first assessment round were thus reduced. The final documentation includes:

- The event description material arranged in the workbook: [CCF-P-Nordic-Descriptions-V1.xls]
- Completed assessments of the two analysts for Analyst A and B, respectively: [CCF-P-ImpVe-Construction-AV2.xls] and [CCF-P-ImpVe-Construction-BV2.xls]
- Logging notes of the differences and their resolution [NAFCS-WN-TM09]
- Feedback comments on the information stored to ICDE database, e.g. proposals to supplement event descriptions and align the code classifications for consistency from plant-to-plant [NAFCS-WN-TM08].

The logging notes describe in more detail the difficulties encountered in the analysis of complicated events and the way of solving the discrepancies. The general insights and lessons learnt will be presented in Section 2.5.

2.4 Summary of the Impact Vector results

The assessment results are shown in Table 2.3 for the cases that are recommended to be explicitly modeled (these cases concerned only CCCG size 4 and failure mode FR), and in Table 2.4 for the cases that provide input to the parametric CCF modeling. The best estimate is the mean of the assessments by the two analysts. The assessments were relatively close to each other. The differences are discussed in more detail in the logging notes [NAFCS-WN-TM09]. No quantitative comparison is prepared here because the data are dispersed over failure modes and group sizes, which makes difficult to present meaningful point estimates of the multiple failure probabilities in the same way as in the DG Pilot. Besides, the statistical records are available only for a part of the pump groups.

Table 2.3 Summary of the Impact Vector assessment for the CCF events that are recommended to be explicitly modeled (group size 4 only, failure mode FR only).

		Sum Impact Vector						Average
Failure Mode		0	1	2	3	4	Sum	multiplicity
Latent	High	1.6	0	4	0	2.4	8	2.20
FS+FR	Best	1.15	0.45	4.145	0.14	2.115	8	2.20
	Low	0.819	0.819	4.307	0.0512	2.003	8	2.20

Table 2.4 Summary of the Impact Vector assessment for the CCF events that provide data input to parametric estimation/quantification (group sizes 4, 3, 2).

		Sum Impact Vector						Average
Failure Mode		0	1	2	3	4	Sum	multiplicity
Monitored	High							
MC/MR	Best							
	Low							
Latent	High	0.95	1	0.05			2	0.55
FS+FR	Best	0.971	0.481	0.043	4.4E-3	9.0E-4	1.5	0.39
	Low	0.910	1.080	0.010			2	0.55

		Sum Impact Vector					Average
Failure Mode		0	1	2	3	Sum	multiplicity
Monitored	High	1.85	0.1	0.05		2	0.10
MC/MR	Best	2	0	0	0	2	0.00
	Low	1.801	0.198	0.001		2	0.10
Latent	High	0.5	0.5		1	2	1.75
FS+FR	Best	0.995	0.005	0	1	2	1.50
	Low	0.500	0.500		1	2	1.75

		Sum Impact Vector				Average
Failure Mode		0	1	2	Sum	multiplicity
Monitored	High			1	1	2.00
MC/MR	Best			1	1	2.00
	Low			1	1	2.00
Latent	High		1	1	2	1.50
FS+FR	Best	0.000	0.925	1.075	2	1.54
	Low		1	1	2	1.50

2.5 Summary of the engineering insights

The new observation from the pump application was the relatively large portion of the events that ought to be explicitly modelled. These cases were related to the following two CCF mechanisms:

- Operational disturbances in Ringhals 3 and 4 where sea water pumps in system 715 were tripped due to loss of lubrication water. The lubrication water is primarily supplied from the service water system, and alternatively from the demineralized water system. The breaks in lubrication water were caused by erroneous flow arrangements or test maneuvers, and could be recovered by the operator typically in about ten minutes. The CCF mechanism and consequences are very specific to the plant design, being thus not meaningful to be covered implicitly by parametric CCFs. Mapping to another plant requires especially explicit modeling, if applicable at all.
- Possibility of trip-start cycling of HPSI pumps in Loviisa 1 and 2 due to local protection for bearing temperature. The problem was relevant only in a specific type of Small LOCA and the operator control actions play an important role in mitigating the consequences. Besides, the CCF mechanism (with constant impact) had been latent from the start of the plant operation, which needs to be taken into account in a particular way in the quantification. Therefore, this CCF mechanism can be treated in a meaningful way only by explicit modeling.

The Impact Vector assessments were nevertheless done for completeness in those cases. For the events in Ringhals 3 and 4 the Impact Vector assessments were relatively straightforward. For both CCF mechanisms the principal difficulty will be connected to modeling of recovery actions in actual demand condition.

In other respects the small number of CCF events for the Nordic pumps obscures drawing further insights. For more global insights, see the ICDE summary report for the pumps [NEA/CSNI/R(99)2].

3. Foreign CCF events of pumps

The summary statistics for the centrifugal pumps in the ICDE database are quoted in Table 3.1, see [NEA/CSNI/R(99)2]. Due to similar difficulties as for the DG events, it had to be concluded too difficult to make Impact Vector assessments for the foreign pump events. The pump types, component and system design details and operational aspects are very much dispersed. The recommended way would be, as already stated, that the assessments should be done by each member country for their own data and in cooperation with the plant experts. The Impact Vector results could then be exchanged for mutual benefits.

Generating high and low bound Impact Vectors would be relatively simple and useful for comparison aims, as done in the DG Pilot. The bounding Impact Vectors are not generated at this stage for the pumps (foreign events), because the meaningful point estimates for the Nordic pump data could not be produced, i.e. lack of comparison objective.

Table 3.1 Summary of the CCF events for the centrifugal pumps in the ICDE database [NEA/CSNI/R(99)2]

	Size of CCCG				
	2	3	4	Other	Total
ICDE events	40	29	41	15	125
Failure to run	24	15	25	7	71
Failure to start	16	14	16	8	54
Standby pumps	39	17	15		71
Operating and intermittent	1	12	26	15	54
Complete CCFs	14	3	2		19
Failure to run	4		1		5
Failure to start	10	3	1		14
Standby pumps	14	1	1		16
Operating and intermittent		2	1		3
Number of CCCGs	396	163	171	63	793

4. Concluding remarks

The insights from the pump application are generally similar to those from the DG Pilot. Again the redundant assessment of the Impact Vectors proved highly useful to reach good quality results. The more difficult assessment cases were also for the pumps related to the complicated events, where the ICDE event descriptions were not sufficient but additional information was needed, e.g. from the plant event reports and by contacts with the plant specialists. Related to this aspect, the utilization of foreign data proved difficult also for the pumps.

The pump application reinforced the earlier conclusion that the assessment of the Impact Vectors should be preferably done in parallel to the initial ICDE data collection. This would save significant efforts for both the plant experts and analysts, and contribute to improved overall QA.

New insights from this application are following:

- Quite many cases represented CCF mechanisms that ought to be explicitly modeled, i.e. are not well adapted to be covered by (parametric) CCF data and models. The construction of Impact Vectors is still useful in these cases but specific advices should be given for the explicit modeling, and determining the relevance to other plants (so called mapping to target application)
- One of the observed CCF mechanisms (representing two CCF events) had been latent from the beginning of plant operation with permanent impact. For these kinds of cases also specific advice are needed for the quantitative treatment and mapping to target application

Consequently, the ICDE guidelines should be supplemented with proper orientation to handle both types of CCF mechanisms, i.e. handling the input both to explicit and implicit CCF modelling.

Appendix 1: Summary Tables of the Impact Vectors

This appendix is shipped as an embedded MS-Excel file "NACFS-PR18-App1-V1.xls". Double-click the icon to open the Excel workbook.

NAFCS-PR18-App 1-V1.xls

References

NAFCS-Programme-R1
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2/Draft 1, 31 October 2002.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 31 October 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-WN-TM08
Comments on the ICDE database for the information stored about the Finnish and Swedish pumps, feedback from the impact vector assessment. Work notes by J-P. Bento and T. Mankamo, Version 1, 25 April 2003.

NAFCS-WN-TM09
Logging Notes of the Impact Vector Assessment for the Pump Events. Work notes by T. Mankamo and J-P. Bento, Version 1, 25 April 2003.

CCF-P-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic NPPs. Version 1, 06 March 2003.

CCF-P-ImpVe-Construction-AV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Tuomas Mankamo, Version 2, 03 April 2003.

CCF-P-ImpVe-Construction-BV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Jean-Pierre Bento, Version 2, 03 April 2003.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

ICDECG01 Coding Guideline for Centrifugal Pumps. Draft 2.1, 12 February 2001.

NEA/CSNI/R(99)2
Collection and Analysis of CCFs of Centrifugal Pumps. ICDE Project Report, prepared by ??. 29 February 2000.

Pumps-CC CCF Analysis of Pumps, Olkiluoto 1 and 2 Experience 1983-1995. Work report prepared by T. Mankamo, 14 May 1997.

NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

NUREG/CR-5497
CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998

NUREG/CR-6268v1
Common Cause Failure Database and Analysis System: Overview. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.1., June 1998.

Abbreviations

Acronym	Description
CCCG	Common Cause Component Group
CCF	Common Cause Failure
TDC	Test and Demand Cycles
BWR	Boiling Water Reactor
DG	Diesel Generator
PWR	Pressurized Water Reactor
IAEA	International Atomic Energy Authority
ICDE	International CCF Data Exchange
EPRI	Electric Power Research Institute
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate
USNRC	United States Nuclear Regulatory Commission

NACFS - Impact Vector Construction
Nordic Pumps

CCF Event List

Index	C01 CCF event identifier	Unit	Year	System	CCCG Size
SF01	RO-O1-88/018	O1	88	323 Core Spray System	2
SF02	RO-O2-96/015	O2	96	327 Auxiliary Feed Water	2
SF03	RO-O2-96/043	O2	96	323 Core Spray System	2
SF04	R1-RO48-93/R1-RO54-93	R1	93	322 Containment Spray System	3
SF05	R2-RO013-90	R2	90	311 Component Cooling System	3
SF06a	R3-RO014-93/R4-RO012-93	R3	93	715 Salt Water Pumps	4
SF06b	- " -	R4	93	715 Salt Water Pumps	4
SF07a	R4-RO026-91	R4	91	715 Salt Water Pumps	4
SF07b	- " -	R3	91	715 Salt Water Pumps	4
SF08	R4-RO22-93/R3-RO08-94	R4	93	334 Charging Pumps of ECCS	3
SF09	R4-RO015-94	R4	94	715 Salt Water Pumps	4
SF10	R4-RO024-95	R4	95	715 Salt Water Pumps	4
SF11a	LOTI-180181A-1	L1	93	HPSI	4
SF11b	- " -	L2	93	HPSI	4
SF12	OL2-5009449	T2	96	712 Shutdown Service Water System	4

Version control

Version 0	Working draft	06 April 2003
Version 1	Some text enhancments, to be embedded into PR18 Issue 1	29 August 2003

NACFS - Impact Vector Construction
Nordic Pumps

CCCG Size = 4

				C03		*C08*	*C11*	*C14*							
				Failure	Modeling	Comp. Impair-	Shared Cause	Time	Impact Vector - Analyst A						Average
Index	Unit	Year	Description	mode	Class	ment	Factor	Factor	0	1	2	3	4	Sum	multiplicity
SF06a	R3	93	Pump trip due to loss of lubrication water, cause unkown	FR	Explicit	CCWW	H(1)	H(1)	0	0	1	0	0	1	2.00
SF06b	R4	93	Pump trip due to loss of lubrication water, cause unkown	FR	Explicit	CCWW	H(1)	H(1)	0	0	1	0	0	1	2.00
SF07a	R4	91	Pump trip due to loss of lubrication water, erroneous valve maneuver	FR	Explicit	CCCC	H(1)	H(1)	0	0	0	0	1	1	4.00
SF07b	R3	91	Pump trip due to loss of lubrication water, erroneous valve maneuver	FR	Explicit	CCCC	H(1)	H(1)	0	0	0	0	1	1	4.00
SF09	R4	94	Pump trip due to loss of lubrication water, erroneous test maneuver	FR	Explicit	CCWW	H(1)	H(1)	0	0	1	0	0	1	2.00
SF10	R4	95	Pump trip due to loss of lubrication water, erroneous valve maneuver	FR	Explicit	CCWW	H(1)	H(1)	0	0	1	0	0	1	2.00
SF11a	L1	93	Vulnerability to high temperature trip and start-stop cycling due to inade-quate bearing design, replicate SF11b	FR	Explicit	DDDD	H(1)	H(1)	0.65	0.15	0.1	0.05	0.05	1	0.70
SF11b	L2	93	Replicate to SF11a	FR	Explicit	DDDD	H(1)	H(1)	0.65	0.15	0.1	0.05	0.05	1	0.70
SF12	T2	96	Blockage of pump suction by plywood boards in the seawater channel	FR	Implicit	CIWW	L(0.1)	L(0.1)	1.164	0.761	0.067	0.008	8E-04	2	0.92
									2.464	1.061	4.267	0.108	2.101	10	1.83
									0	1	2	3	4	Sum	Average multiplicity

CCCG Size = 4

			Impact Vector - Analyst B						Average	
Index	Unit	Year	0	1	2	3	4	Sum	multiplicity	Comment
SF06a	R3	93	0	0	0.9	0.05	0.05	1	2.15	
SF06b	R4	93	0	0	0.9	0.05	0.05	1	2.15	
SF07a	R4	91	0	0	0	0	1	1	4.00	
SF07b	R3	91	0	0	0	0	1	1	4.00	
SF09	R4	94	0	0	0.99	0	0.01	1	2.02	
SF10	R4	95	0	0	1	0	0	1	2.00	
SF11a	L1	93	0.5	0.3	0.15	0.04	0.01	1	0.76	
SF11b	L2	93	0.5	0.3	0.15	0.04	0.01	1	0.76	
SF12	T2	96	0.778	0.2	0.02	0.001	0.001	1	0.25	
			1.778	0.8	4.11	0.181	2.131	9	2.01	
			0	1	2	3	4	Sum	Average multiplicity	

CCCG Size = 4

			High Bound Comparison Impact Vector						Average	Low Bound Comparison Impact Vector						Average
Index	Unit	Year	0	1	2	3	4	Sum	multiplicity	0	1	2	3	4	Sum	multiplicity
SF06a	R3	93	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
SF06b	R4	93	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
SF07a	R4	91	0	0	0	0	1	1	4.00	0	0	0	0	1	1	4.00
SF07b	R3	91	0	0	0	0	1	1	4.00	0	0	0	0	1	1	4.00
SF09	R4	94	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
SF10	R4	95	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
SF11a	L1	93	0.8	0	0	0	0.2	1	0.80	0.41	0.41	0.154	0.026	0.002	1	0.80
SF11b	L2	93	0.8	0	0	0	0.2	1	0.80	0.41	0.41	0.154	0.026	0.002	1	0.80
SF12	T2	96	0.95	1	0.05	0	0	2	1.10	0.91	1.08	0.01	0	0	2	1.10
			2.55	1	4.05	0	2.4	10	1.87	1.729	1.899	4.317	0.051	2.003	10	1.87
			0	1	2	3	4	Sum	Average multiplicity	0	1	2	3	4	Sum	Average multiplicity

NACFS - Impact Vector Construction
Nordic Pumps

CCCG Size = 3

				C03		*C08*	*C11*	*C14*														
				Failure	Modeling	Comp. Impair-	Shared Cause	Time	Impact Vector - Analyst A					Average	Impact Vector - Analyst B					Average
Index	Unit	Year	Description	mode	Class	ment	Factor	Factor	0	1	2	3	Sum	multiplicity	0	1	2	3	Sum	multiplicity
SF04	R1	93	Leakages in the mechanical seal of the axle	MR	Implicit	IIW	M(0.5)	L(0.1)	2	0	0	0	2	0	2	0	0	0	2	0
SF05	R2	90	Faulty logic installed due to incorrect circuit diagrams	FS	Implicit	CCC	H(1)	H(1)	0	0	0	1	1	3	0	0	0	1	1	3
SF08	R4	96	Ageing problems in the contactor of the lubrication oil pumps	FR	Implicit	DWW	H(1)	L(1)	1	0	0	0	1	0	0.99	0.01	0	0	1	0.01
									3	0	0	1	4	0.75	2.99	0.01	0	1	4	0.75
									0	1	2	3	Sum	Average multiplicity	0	1	2	3	Sum	Average multiplicity

CCCG Size = 3

				High Bound Comparison Impact Vector						Low Bound Comparison Impact Vector					
Index	Unit	Year	Comment	0	1	2	3	Sum	Average multiplicity	0	1	2	3	Sum	Average multiplicity
SF04	R1	93		1.85	0.1	0.05	0	2	0.2	1.801	0.198	0.001	0	2	0.2
SF05	R2	90		0	0	0	1	1	3	0	0	0	1	1	3
SF08	R4	96		0.5	0.5	0	0	1	0.5	0.5	0.5	0	0	1	0.5
				2.35	0.6	0.05	1	3	1.23	2.301	0.698	0.001	1	3	1.23
				0	1	2	3	Sum	Average multiplicity	0	1	2	3	Sum	Average multiplicity

NACFS - Impact Vector Construction
Nordic Pumps

CCCG Size = 2

				C03		*C08*	*C11*	*C14*													
				Failure	Modeling	Comp. Impair-	Shared Cause	Time	Impact Vector - Analyst A					Average	Impact Vector - Analyst B					Average	
Index	Unit	Year	Description	mode	Class	ment	Factor	Factor	0	1	2		Sum	multiplicity	0	1	2		Sum	multiplicity	Comment
SF01	O1	88	Systematic error to restore power supply after maintenance	MC	Implicit	CC	H(1)	H(1)	0	0	1		1	2	0	0	1		1	2	
SF02	O2	96	Contactor failure due to inadequate dimensioning	FS	Implicit	CW	Empty(1)	H(1)	0	0.95	0.05		1	1.05	0	0.9	0.1		1	1.1	
SF03	O2	96	Systematic error to restore power supply after containment leak test	FS	Implicit	CC	H(1)	H(1)	0	0	1		1	2	0	0	1		1	2	
									0	0.95	2.05		3	1.68	0	0.9	2.1		3	1.70	
									0	1	2		Sum	Average	0	1	2		Sum	Average	
														multiplicity						multiplicity	

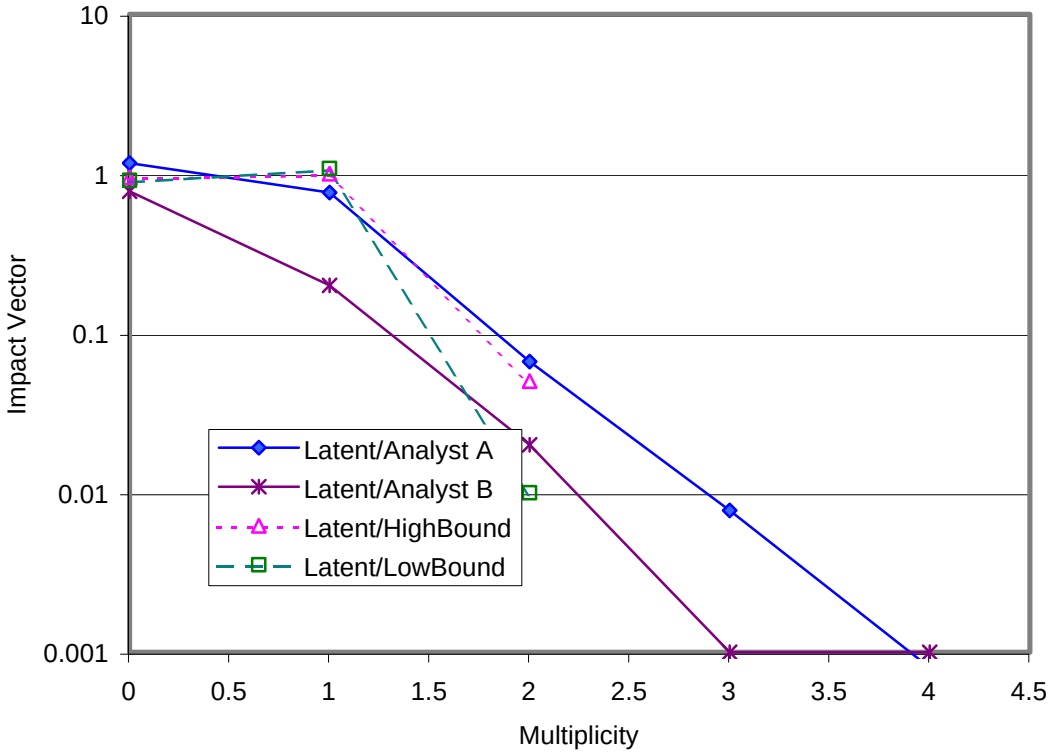
CCCG Size = 2

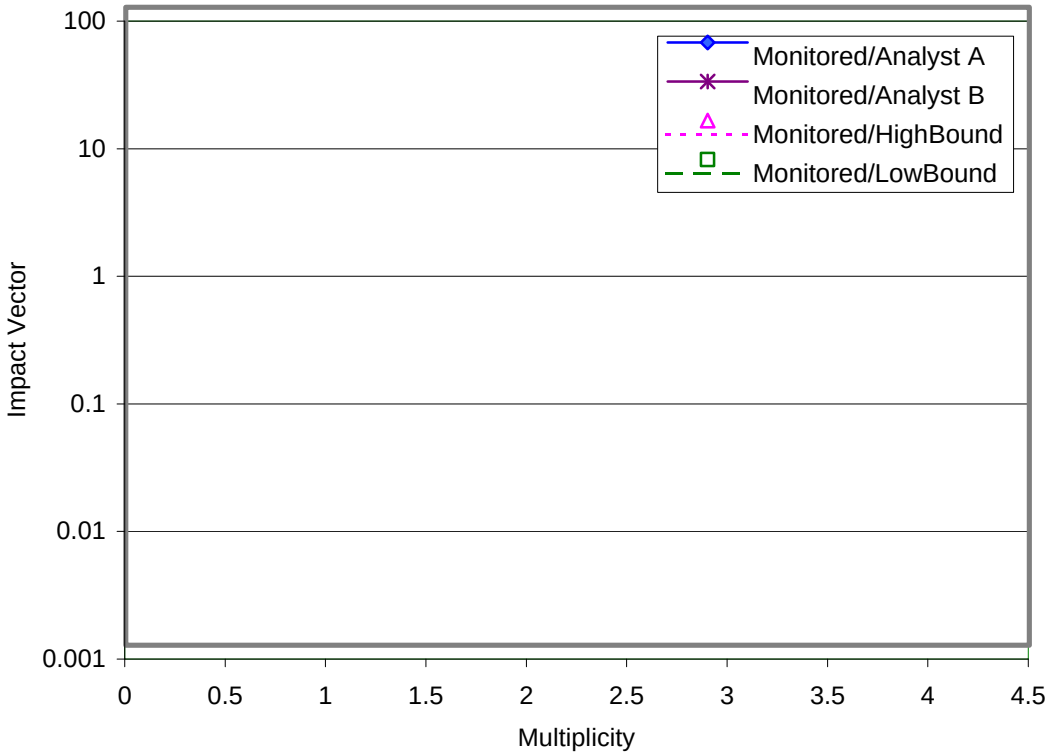
			High Bound Comparison Impact Vector					Average	Low Bound Comparison Impact Vector					Average
Index	Unit	Year	0	1	2		Sum	multiplicity	0	1	2		Sum	multiplicity
SF01	O1	88	0	0	1		1	2	0	0	1		1	2
SF02	O2	96	0	1	0		1	1	0	1	0		1	1
SF03	O2	96	0	0	1		1	2	0	0	1		1	2
			0	1	2		3	1.67	0	1	2		3	1.67
			0	1	2		Sum	Average	0	1	2		Sum	Average
								multiplicity						multiplicity

Summary of the Impact Vector Assessment (CCCG Size 4)

Modeling Class Implicit

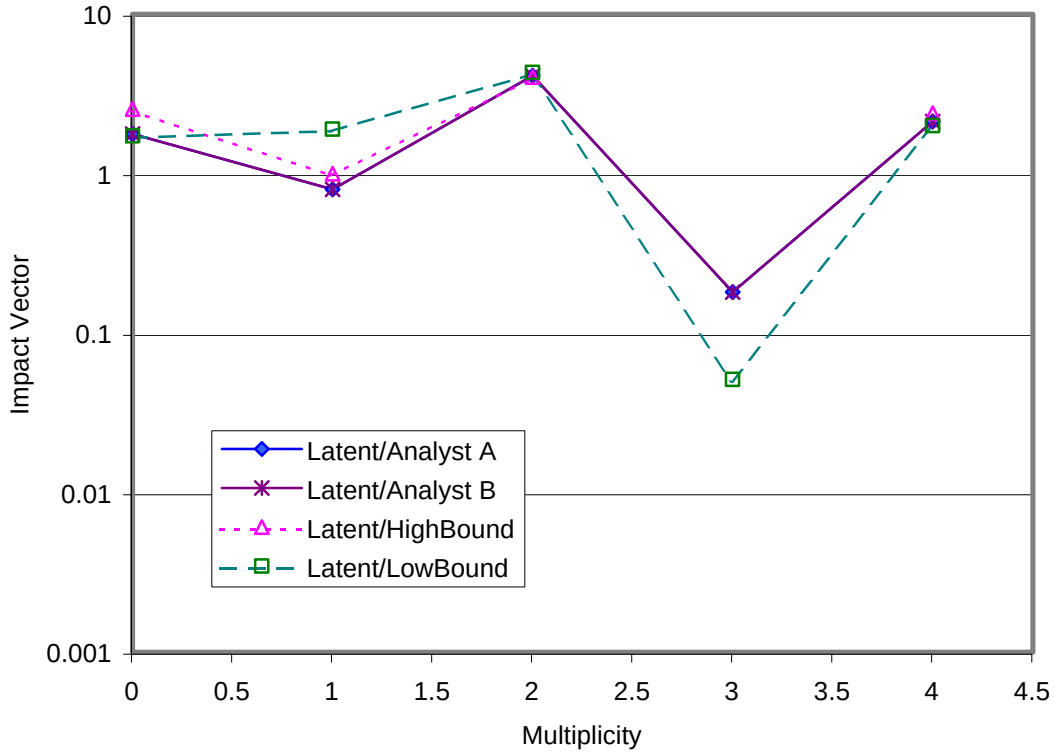
	Impact Vector						Average
	0	1	2	3	4	Sum	multiplicity
Latent_A Monitored_A	1.164	0.761	0.067	0.008	8E-04	2	0.46
	1.164	0.761	0.067	0.008	8E-04	2	
Latent_B Monitored_B	0.778	0.2	0.02	0.001	0.001	1	0.25
	0.778	0.2	0.02	0.001	0.001	1	
L_BestEstimate M_BestEstimate	0.971 0	0.481 0	0.043 0	0.004 0	9E-04 0	2	0.29
	0.971	0.481	0.043	0.004	9E-04	1.5	
L_HighBound M_HighBound	0.95	1	0.05			2	0.55
	0.95	1	0.05	0	0	2	
L_LowBound M_LowBound	0.91	1.08	0.01			2	0.55
	0.91	1.08	0.01	0	0	2	

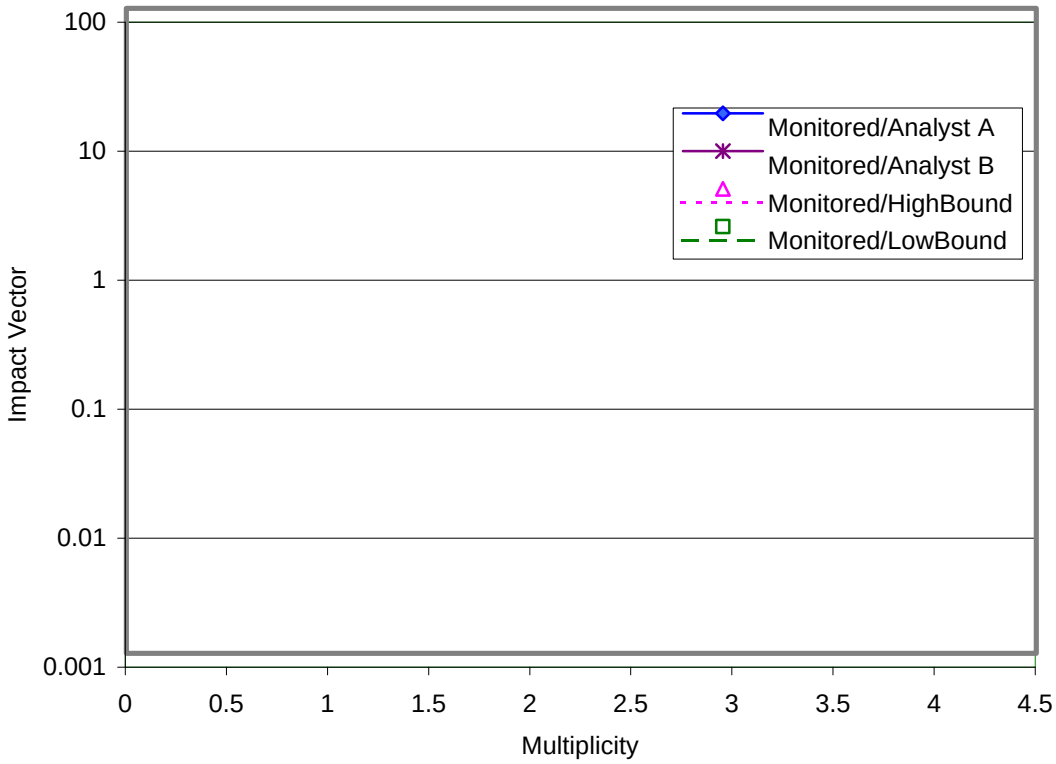

10
1
0.1
0.01
0.001
Impact Vector
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Multiplicity
Latent/Analyst A
Latent/Analyst B
Latent/HighBound
Latent/LowBound


100
10
1
0.1
0.01
0.001
Impact Vector
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Multiplicity
Monitored/Analyst A
Monitored/Analyst B
Monitored/HighBound
Monitored/LowBound

Summary of the Impact Vector Assessment (CCCG Size 3)
Modeling Class Any

	Impact Vector						Average
	0	1	2	3	4	Sum	multiplicity
Latent_A	1			1		2	1.50
Monitored_A	2					2	0.00
	3	0	0	1		4	
Latent_B	0.99	0.01		1		2	1.51
Monitored_B	2					2	0.00
	2.99	0.01	0	1		4	
L_BestEstimate	0.995	0.005	0	1		2	1.50
M_BestEstimate	2	0	0	0		2	0.00
	2.995	0.005	0	1		4	
L_HighBound	0.5	0.5		1		2	1.75
M_HighBound	1.85	0.1	0.05			2	0.10
	2.35	0.6	0.05	1		4	
L_LowBound	0.5	0.5		1		2	1.75
M_LowBound	1.801	0.198	0.001			2	0.10
	2.301	0.698	0.001	1		4	

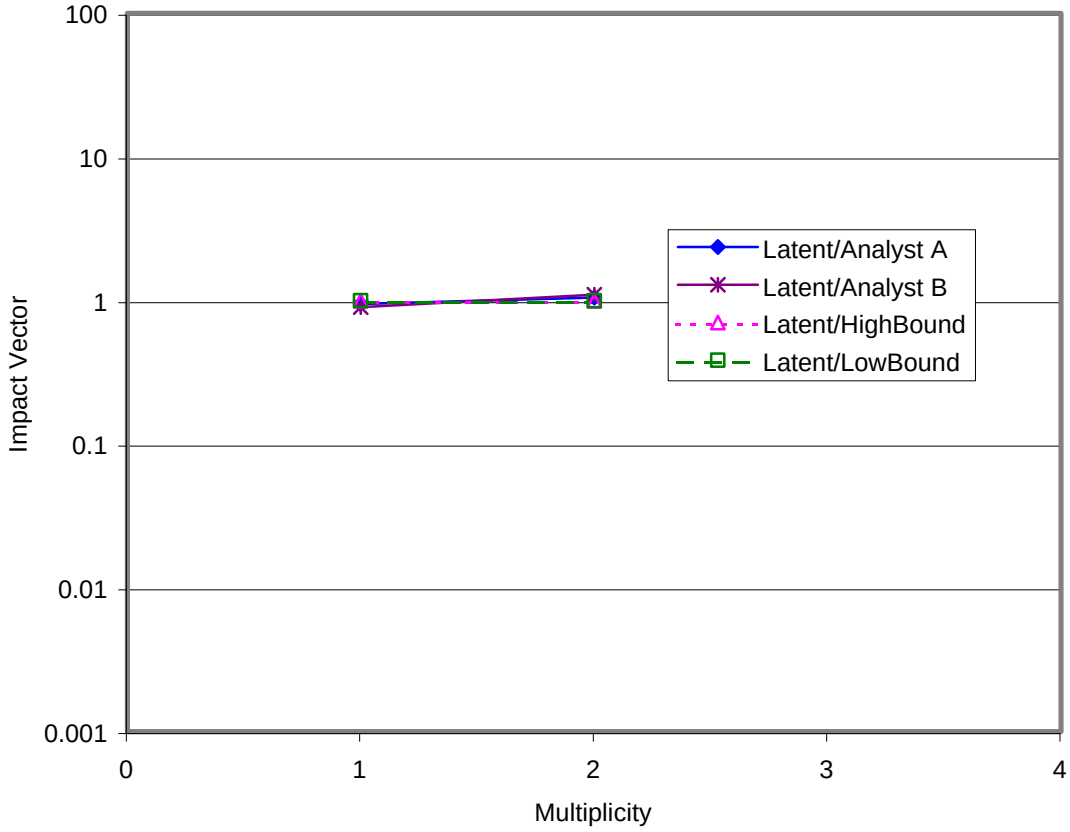

10
1
0.1
0.01
0.001
Impact Vector
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Multiplicity
Latent/Analyst A
Latent/Analyst B
Latent/HighBound
Latent/LowBound

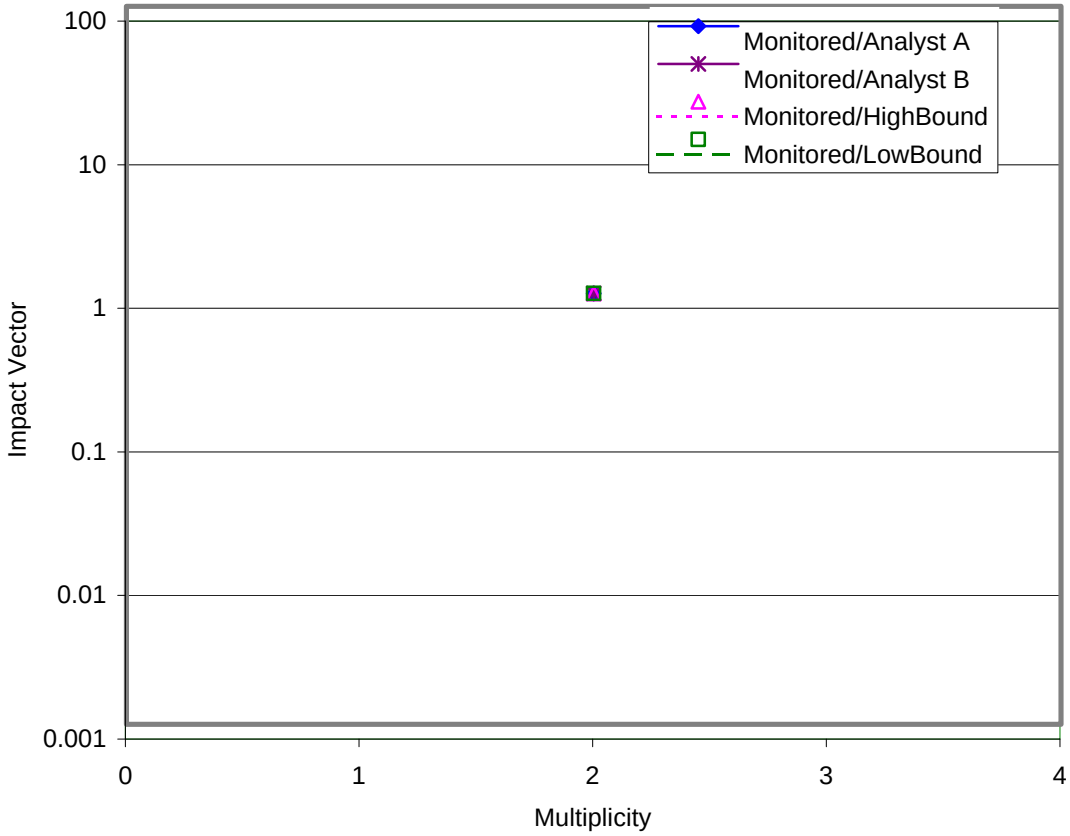

100
10
1
0.1
0.01
0.001
Impact Vector
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Multiplicity
Monitored/Analyst A
Monitored/Analyst B
Monitored/HighBound
Monitored/LowBound

Summary of the Impact Vector Assessment (CCCG Size 2)

Modeling Class Implicit

	Impact Vector						Average
	0	1	2	3	4	Sum	multiplicity
Latent_A		0.95	1.05			2	1.53
Monitored_A			1			1	2.00
	0	0.95	2.05			3	
Latent_B		0.9	1.1			2	1.55
Monitored_B			1			1	2.00
	0	0.9	2.1			3	
L_BestEstimate	0	0.925	1.075			2	1.54
M_BestEstimate	0	0	1			1	2.00
	0	0.925	2.075			3	
L_HighBound		1	1			2	1.50
M_HighBound			1			1	2.00
	0	1	2			3	
L_LowBound		1	1			2	1.50
M_LowBound			1			1	2.00
	0	1	2			3	


100
10
1
0.1
0.01
0.001
Impact Vector
0
1
2
3
4
Multiplicity
Latent/Analyst A
Latent/Analyst B
Latent/HighBound
Latent/LowBound


100
10
1
0.1
0.01
0.001
Impact Vector
0
1
2
3
4
Multiplicity
Monitored/Analyst A
Monitored/Analyst B
Monitored/HighBound
Monitored/LowBound

Summary of the Impact Vector Assessments
Explicitly Modeled CCF Mechanisms

		Sum Impact Vector						Average
Failure Mode		0	1	2	3	4	Sum	multiplicity
Latent	High	1.6	0	4	0	2.4	8	2.20
FS+FR	Best	1.15	0.45	4.145	0.14	2.115	8	2.20
	Low	0.819	0.819	4.307	0.0512	2.003	8	2.20

Summary of the Impact Vector Assessments
Implicitly Modeled CCF Mechanisms

		Sum Impact Vector						Average
Failure Mode		0	1	2	3	4	Sum	multiplicity
Monitored	High							
MC/MR	Best							
	Low							
Latent	High	0.95	1	0.05			2	0.55
FS+FR	Best	0.971	0.481	0.043	4.4E-3	9.0E-4	1.5	0.39
	Low	0.910	1.080	0.010			2	0.55

		Sum Impact Vector					Average
Failure Mode		0	1	2	3	Sum	multiplicity
Monitored	High	1.85	0.1	0.05		2	0.10
MC/MR	Best	2	0	0	0	2	0.00
	Low	1.801	0.198	0.001		2	0.10
Latent	High	0.5	0.5		1	2	1.75
FS+FR	Best	0.995	0.005	0	1	2	1.50
	Low	0.500	0.500		1	2	1.75

		Sum Impact Vector				Average
Failure Mode		0	1	2	Sum	multiplicity
Monitored	High			1	1	2.00
MC/MR	Best			1	1	2.00
	Low			1	1	2.00
Latent	High		1	1	2	1.50
FS+FR	Best	0.000	0.925	1.075	2	1.54
	Low		1	1	2	1.50

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF01	
C01	ICDE Event Identifier	RO-O1-88/018	
	Short Description	Systematic error to restore power supply after maintenance	
C03	Failure Mode	MC	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	323P1	14/09/88	C	1	34	MC	
B	323P2	14/09/88	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1			1
		Average multiplicity					2	

Impact Vector Assessment

Actual CCF of order 2 (complete CCF for this group).

Failure Mode is MC, thus special treatment needed in quantification (normal state = SB).

Time Factor should be 'High', is empty in the ICDE data.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF02	
C01	ICDE Event Identifier	RO-O2-96/015	
	Short Description	Contactor failure due to inadequate dimensioning	
C03	Failure Mode	FS	
C11	Shared Cause Factor	Empty	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	327P3	22/03/96	C	1	35	TI	
B	327P4	22/03/96	W	0	14		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Only 327P3 would fail in an actual demand	0.95		1				1
2.	Both pumps would fail in an actual demand	0.05			1			1
Net Impact Vector			0	0.95	0.05			1
	Average multiplicity						1.05	

Impact Vector Assessment

Due to the recurring failure of 327P3 contactor there seems to have been some chance of having simultaneous problem also with the contactor of the redundant pump during the period of about two months. For simplicity, the CCF risk is combined with the seond 327P3 event.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF03	
C01	ICDE Event Identifier	RO-O2-96/043	
	Short Description	Systematic error to restore power supply after containment leak test	
C03	Failure Mode	FS	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	323P1	13/11/96	C	1	17	TI	
B	323P2	13/11/96	C	1	17		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1			1
		Average multiplicity					2	

Impact Vector Assessment

Actual CCF of order 2 (complete CCF for this group).

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF04	
C01	ICDE Event Identifier	R1-RO48-93/R1-RO54-93	
	Short Description	Leakages in the mechanical seal of the axle	
C03	Failure Mode	MR	
C11	Shared Cause Factor	M	0.5
C14	Time Factor	L	0.1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	322P1	28/12/93	I	0.1	34		
B	322P2	28/12/93	W	0			
C	322P3	14/11/93	I	0.1	34	MW	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	The pumps are considered likely to have survived actual demand	1	2					2
2.								0
Net Impact Vector			2	0	0	0		2
	Average multiplicity						0	

Impact Vector Assessment

The CCF risk seems relatively small. The two incipient events, separated 6 six weeks, are considered as two failure-free TDCs.

Notice that Failure Mode = MR, i.e. to be included in the maintenance down-time.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF05	
C01	ICDE Event Identifier	R2-RO013-90	
	Short Description	Faulty logic installed due to incorrect circuit diagrams	
C03	Failure Mode	FS	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	711P1	20/05/90	C	1	16	DE	
B	711P2	20/05/90	C	1	16		
C	711P3	20/05/90	C	1	16		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	Evident triple CCF	1				1		1
2.								0
Net Impact Vector			0	0	0	1		1
		Average multiplicity					3	

Impact Vector Assessment

Actual CCF of order 3 (complete CCF for this group).

The failure mechanism is connected to overhaul, likely to be detected prior entering power operation cycle. Thus a special treatment is needed in the quantification, e.g. only relevant for the shutdown state.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF06a	
C01	ICDE Event Identifier	R3-RO014-93/R4-RO012-93	
	Short Description	Pump trip due to loss of lubrication water, cause unkown	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	01/07/93	C	1		MC	R3
B	SWAPCW-02	01/07/93	C	1			
C	SWAPCW-03	01/07/93	W	0			
D	SWAPCW-04	01/07/93	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
	Average multiplicity						2	

Impact Vector Assessment

Actual CCF of order 2. Notice the relatively short time of unavailability (11 min).

Possible unit-to-unit interaction due to simultaneous similar event at R4, see SF06b.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF06b	
C01	ICDE Event Identifier	R3-RO014-93/R4-RO012-93	
	Short Description	Pump trip due to loss of lubrication water, cause unkown	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	01/07/93	C	1		MC	R4 replicate
B	SWAPCW-02	01/07/93	C	1			
C	SWAPCW-03	01/07/93	W	0			
D	SWAPCW-04	01/07/93	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
	Average multiplicity						2	

Impact Vector Assessment

Actual CCF of order 2. Notice the relatively short time of unavailability (17 min).

Possible unit-to-unit interaction due to simultaneous similar event at R3, see SF06a.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF07a	
C01	ICDE Event Identifier	R4-RO026-91	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	17/09/91	C	1		MC	R4
B	SWAPCW-02	17/09/91	C	1			
C	SWAPCW-03	17/09/91	C	1			
D	SWAPCW-04	17/09/91	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident quadruple CCF	1					1	1
2.								0
Net Impact Vector			0	0	0	0	1	1
	Average multiplicity						4	

Impact Vector Assessment

Actual CCF of order 4 (complete CCF of the group). Notice the relatively short time of unavailability (9 min).

Possible unit-to-unit interaction due to simultaneous similar event at R3, see SF07b.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF07b	
C01	ICDE Event Identifier	R4-RO026-91	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	17/09/91	C	1		MC	R3 replicate
B	SWAPCW-02	17/09/91	C	1			
C	SWAPCW-03	17/09/91	C	1			
D	SWAPCW-04	17/09/91	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident quadruple CCF	1					1	1
2.								0
Net Impact Vector			0	0	0	0	1	1
	Average multiplicity						4	

Impact Vector Assessment

Actual CCF of order 4 (complete CCF of the group). According to RO, the disturbance at R3 was limited only to change-over to redundant lubrication water supply?

Possible unit-to-unit interaction due to simultaneous similar event at R4, see SF07a.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF08	
C01	ICDE Event Identifier	R4-RO22-93/R3-RO08-94	
	Short Description	Ageing problems in the contactor of the lubrication oil pumps	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	L	1
G5	Test Interval		
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A		07/03/94	W	0	34	TI	
B		07/03/94	W	0			
C		07/03/94	D	0.5	34		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	The pumps are considered likely to have survived actual demand	1	1					1
2.								0
Net Impact Vector			1	0	0	0		1
	Average multiplicity						0	

Impact Vector Assessment

The CCF risk seems relatively small. Because there are two lubrication oil pumps, the failure of one only reduces the reliability over mission time, thus Component Impairment Value = 'D' for Sub C seems overestimated.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF09	
C01	ICDE Event Identifier	R4-RO015-94	
	Short Description	Pump trip due to loss of lubrication water, erroneous test maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	29/07/94	C	1		TI	
B	SWAPCW-02	29/07/94	C	1			
C	SWAPCW-03	29/07/94	W	0			
D	SWAPCW-04	29/07/94	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
	Average multiplicity						2	

Impact Vector Assessment

Actual CCF of order 2. Notice the relatively short time of unavailability (5 min).

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF10	
C01	ICDE Event Identifier	R4-RO024-95	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	23/07/95	C	1		MC	
B	SWAPCW-02	23/07/95	C	1			
C	SWAPCW-03	23/07/95	W	0			
D	SWAPCW-04	23/07/95	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Evident double CCF	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
	Average multiplicity						2	

Impact Vector Assessment

Actual CCF of order 2. Notice the relatively short time of unavailability (8 min).

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF11a	
C01	ICDE Event Identifier	LOTI-180181A-1	
	Short Description	Vulnerability to high temperature trip and start-stop cycling due to inadequate bearing design, replicate SF11b	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	28 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	11TJ11D001	22/06/93	D	0.2	...	TI	LO1
B	11TJ12D001	27/07/93	D	0.2		TI	
C	12TJ51D001	27/07/93	D	0.2		TI	
D	12TJ52D001	27/07/93	D	0.2		TI	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	At most two pumps will trip before reaching manual control range	0.6	1					1
2.	Three pumps will trip ...	0.2	0.25	0.5	0.25			1
3.	All four pumps will trip ...	0.2		0.25	0.25	0.25	0.25	1
Net Impact Vector			0.65	0.15	0.1	0.05	0.05	1
		Average multiplicity					0.7	

Impact Vector Assessment

The Impact Vector assessment will be made with respect to the condition of special Small LOCA, where the HPSI signal is coming only from the low level in the pressurizer. It seems that in the other LOCAs the risk of damaging pumps is relatively small.

According to the available (extended) event description, the crucial aspect is whether the set-point of high bearing temperature will be reached before entering manual control range. There should be component-to-component variation in this respect. Due to the lack of more precise information, it is assumed that the probability is evenly distributed over the possibility of 0, 1, 2, 3 or 4 pumps tripping, i.e. 20% for each alternative, which yields to the weights for the three scenarios as defined in the above Impact Vector table.

It is believed that in the first scenario, where only two pumps or less trip before reaching the manual control range, the operators have good chances to take control of the situation, and by switching of the operating pump can avoid bearing damages. It has to emphasized that in this scenario it can be assumed substantial component-to-component variation in the temperature increase rate among the pumps.
... continues

...
In the second scenario only one pump remains operating when reaching the manual control range. The other three have tripped and stay for the moment in stand-by, because the operating pump can keep the water level. It is believed that in this scenario there is a substantial chance of damaging bearings of one pump (50%), additional chance to loose another pump (25%), but small risk to loosing more than two pumps.

In the third scenario the pumps will begin uncontrolled start-stop cycling, which can be confusing to the operators. The chances of loosing pumps is divided evenly over multiplicities from 1 to 4.

There are definitely very large uncertainty in the Impact Vector assessment in this case. The use of a time-dependent model is recommended, based on the measurements of the temperature increase and cooldown rates, cycling period and observed component-to-component variation. The operating instructions for the situation should be known in detail for a more accurate assessment. Maybe there are even experiences from the training simulator? It would be interesting to make a comparison with the assessment by the Loviisa PSA team.

Tme Factor should be 'High', is empty in the ICDE data.

Notice that this CCF had been latent from the begin of commercial operation, requiring a special treatment in the quantification.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF11b	
C01	ICDE Event Identifier	LOTI-180181A-1	
	Short Description	Replicate to SF11a	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	28 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	11TJ11D001	22/06/93	D	0.2	...	TI	LO2 replicate
B	11TJ12D001	22/06/93	D	0.2		TI	
C	12TJ51D001	22/06/93	D	0.2		TI	
D	12TJ52D001	22/06/93	D	0.2		TI	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.								0
2.								0
Net Impact Vector			0.65	0.15	0.1	0.05	0.05	1
	Average multiplicity						0.7	

Impact Vector Assessment

Identical case with the pump group of LO1, see SF11a.

Impact Vector Construction Sheet

Analyst A
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF12	
C01	ICDE Event Identifier	OL2-5009449	
	Short Description	Blockage of pump suction by plywood boards in the seawater channel	
C03	Failure Mode	FR	
C11	Shared Cause Factor	L	0.1
C14	Time Factor	L	0.1
G5	Test Interval	7 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	712P1	05/04/96	I	0.1	34		
B	712P2		W	0			
C	712P3	19/06/96	C	1	34	DE	
D	712P4		W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Scenarios structured by using a causal model (Event Tree)							0
2.								0
Net Impact Vector			1.16	0.76	6.7E-2	7.7E-3	8.0E-4	2
	Average multiplicity						0.92	

Impact Vector Assessment

The impact vector assessment is reproduced from [Pumps_CC], see the attached Event Tree model (Sheet = 'SF12-EventTree'):

Impact vector assessment for the blocking events of 712-pumps by plywood boards is based on the use of event tree to structure the impact scope of the failure mechanism and coupling between the two sea water (SW) channels (divisions containing pump pair P1/P3 and P2/P4, respectively):

- The scope may concern both divisions with 50% chances due to the intake change-over tests after annual overhaul, or other scenarios in connection to overhaul
- The likelihood of the large amount of floating plywood boards is assessed to be only a fraction of 20%
- The coupling of the CCF mechanism is connected to the simultaneity by which the existing plywood boards would gather with the flow, get wetted and bogged with the suction flow. The coupling factor is dependent on the amount of plywood boards

This reasoning is used to calculate the split fractions for the scenarios (Event Tree branches).

For each branch of the Event Tree, the impact vector elements are generated based on engineering judgment, assuming that if blocking occurs, both SW channels are investigated, which prevents recurrence during same operating cycle. The normalization of the assessment concerns two demand/test cycles in order to take into account the possibility that the impact may be separated by time between the two divisions, i.e. affect them during disjoint demand/test intervals. The relatively low values of the elements of higher order reflect the benefit from the short time between demands and tests (one week per pump).

More specifically, the impact vector elements are assessed in the following way for the event tree branches (in other branches, except BrNo = 4, 6 and 8, the effective coupling between safety divisions is assessed to be so weak that possible failure are limited to one division and the root cause then removed, i.e. no recurrence during the same operating cycle; this means that from the total impact mass, one of the two units is placed to element 0):

1) In case of small amount of plywood boards in one SW channel, it is assumed that the chances are PS = 2/3 for having single failure instead of reduced flow as a first symptom

2) In case of large amount of plywood boards in one SW channel, it is assumed that the chances are PL = 2/10 for having double failure, and alternatively a singe failure but no warning symptom

3) The impact between divisions is considered independent. Based on BrNo = 1 the likelihood of not getting reduced flow as first warning is (1-2/3)^2, which makes about 10%, i.e. chances of single failure is about 90%. The likelihood of multiple failure is considered negligible in this case

4) In case of small amount of plywood boards in both SW channels and strong coupling, the impacts per division are considered crudely independent and possible during same demand/test interval. The chances of failure in both divisions are calculated as PS^2, and in one division only as 2*PS*(1-PS). Compare to BrNo = 1.

5) In this case, the likelihood of double failure is reduced as compared to BrNo = 2, because there are about 50% chances that the problem is first revealed in the division with small amount of plywood

6) In case of large amount of plywood boards in one and small amount in other SW channel and strong coupling, the impacts per division are considered again crudely independent and possible during same demand/test interval. The chances of triple failure are calculated as PS*PL, of double failure as PS*(1-PL) + (1-PS)*PL. Compare to BrNo = 1 and 2.

7) In this cases the conditional impact vector is crudely same as in BrNo = 2, because the problem is likely to affect either of the two divisions first, but unlikely to affect both during same demand/test interval

8) In case of large amount of plywood boards in both SW channels and strong coupling, the impacts per division are again considered crudely independent and possible during same demand/test interval. The chances of quadruple failure are calculated as PL^2, triple failure as 2*PL*(1-PL), and double failure as (1-PL)^2. Compare to BrNo = 2. Furthermore, it is assessed that there are chances of 50% that the first symptom is not detection of reduced flow but a single failure, which is different as compared to other branches

The weighted impact vector is obtained from the branch estimates through weighting by split fractions.

In overall, the conditional likelihood of higher order failure is relatively small: usually the ratio between high order and single failure probability is about 1%. It can thus be concluded that the conditional CCF risk connected to plywood boards is relatively low. Generally, it is not recommended to include this kind low contributor in CCF data requiring laborious evaluation. Here it is taken under consideration due to lack of more significant CCF event in order to include at least one case for the test exchange purpose.

Impact vector assessment for the plywood blocking events of 712-pumps at OL2.
712P1 on 05.04.1996
712P3 on 19.06.1996

Construction work in SW channels	Work scope	Amount of plywood	Coupling factor between divisions	BrNo	Split fraction	Impact vector elements					Notes
						0	1	2	3	4	
	One division	Small	N/A				*PS*	*PL*			
	0.5	0.8		1	0.4	1.33	0.67				
		Large	N/A								
		0.2		2	0.1	1	0.8	0.2			
	Both divisions	Small in both divisions	Weak								
	0.5	0.8	0.9	3	0.36	1.1	0.9				
			Strong								
			0.1	4	0.04	1.11	0.44	0.44			
		Large in one division	Weak								
		0.1	0.8	5	0.04	1	0.9	0.1			
			Strong								
			0.2	6	0.01	1	0.267	0.6	0.133		
		Large in both divisions	Weak								
		0.1	0.6	7	0.03	1	0.8	0.2			
			Strong								
			0.4	8	0.02	0.5	0.5	0.64	0.32	0.04	
					1	1.16	0.76	6.7E-2	7.7E-3	8.0E-4	
						Weighted impact vector					

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF01	
C01	ICDE Event Identifier	RO-O1-88/018	
	Short Description	Systematic error to restore power supply after maintenance	
C03	Failure Mode	MC	
C11	Shared Cause Factor	H	1
C14	Time Factor		
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	323P1	14/09/88	C	1	34	MC	
B	323P2	14/09/88	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Both 323 P1 and P2 would fail to start automatically on demand	1			1			1
2.								0
Net Impact Vector			0	0	1			1
	Average multiplicity						2	

Impact Vector Assessment

The isolation breaker for both 323 P1 and P2 being not restored in the closed state in front of nuclear heat-up of the reactor, the automatic start of both core spray pumps was not possible. The probability for fast operator action and successful restoration of the breakers during a real demand has not been assessed.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF02	
C01	ICDE Event Identifier	RO-O2-96/015	
	Short Description	Contactor failure due to inadequate dimensioning	
C03	Failure Mode	FS	
C11	Shared Cause Factor		
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	327P3	22/03/96	C	1	35	TI	
B	327P4	22/03/96	I	0.1	14		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Only 327 P3 would fail on demand	0.9		1				1
2.	Both 327 P3 and P4 would fail on demand	0.1			1			1
Net Impact Vector			0	0.9	0.1			1
	Average multiplicity						1.1	

Impact Vector Assessment

Comment on impairment vector: [I] has been used for 327 P4 due to the replacement of this type of contactors/EG relays for many components in several systems in the plant. Considering the assessment of the net impact vector, operating experiences from the Swedish plants indicate that EG-relays in general have experienced both significant ageing problems and mechanical seizing/jamming of some internal parts. The probability for contactor/relay failure is to be considered relatively high. A failure impairs the start of the concerned pump. The probabilty for concurrent contactor/relay failure for 327 P4 is assessed w = 5% - 10%. The conservative value w = 0,1 has been used in the construction of the impact vector.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF03	
C01	ICDE Event Identifier	RO-O2-96/043	
	Short Description	Systematic error to restore power supply after containment leak test	
C03	Failure Mode	FS	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	323P1	13/11/96	C	1	17	TI	
B	323P2	13/11/96	C	1	17		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Both 323 P1 and P2 would fail to start automatically on demand	1			1			1
2.								0
Net Impact Vector			0	0	1			1
		Average multiplicity					2	

Impact Vector Assessment

The isolation breaker for both 323 P1 and P2 being not restored in the closed state after pressure test of the reactor containment, the automatic start of both core spray pumps was not possible. The probability for fast operator action and successful restoration of the breakers during a real demand has not been assessed.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF04	
C01	ICDE Event Identifier	R1-RO48-93/R1-RO54-93	
	Short Description	Leakages in the mechanical seal of the axle	
C03	Failure Mode	MR	
C11	Shared Cause Factor	M	0.5
C14	Time Factor	L	0.1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	322P1	28/12/93	I	0.1	34		
B	322P2	28/12/93	W	0			
C	322P3	14/11/93	I	0.1	34	MW	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	Both pumps would have fulfilled their function during an actual	1	2					2
2.								0
3.								0
Net Impact Vector			2	0	0	0		2
		Average multiplicity					0	

Impact Vector Assessment

Even if a small risk for CCF exists, the system solution (via system 356 and even 345) provided to drain leaks from the pumps shroud surrounding each pump and its motor unit is highly redundant and diversified. Although impaired, the pumps function has been assessed successful during actual demands.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF05	
C01	ICDE Event Identifier	R2-RO-013-90	
	Short Description	Faulty logic installed due to incorrect circuit diagrams	
C03	Failure Mode	FS	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	711P1	20/05/90	C	1	16	DE	
B	711P2	20/05/90	C	1	16		
C	711P3	20/05/90	C	1	16		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	711 P1 - P3 fail to start on demand	1				1		1
2.								0
Net Impact Vector			0	0	0	1		1
	Average multiplicity						3	

Impact Vector Assessment

Due to a modification error, the logic of system 711 (component cooling system) was partly disabled. The consequence was that during certain situations, the automatic start/re-start and manual start from the main control room of all three pumps was blocked.

Impact Vector Construction Sheet

Analyst B

Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF06a	
C01	ICDE Event Identifier	R3-RO014-93/R4-RO012-93	
	Short Description	Pump trip due to loss of lubrication water, cause unkown	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	01/07/93	C	1		MC	R3
B	SWAPCW-02	01/07/93	C	1			
C	SWAPCW-03	01/07/93	W	0			
D	SWAPCW-04	01/07/93	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both SWAPCW-01 and -02 stop on low lubrication water flow	0.9			1			1
2.	SWAPCW-01, -02 and -03 stop on low lubrication water flow	0.05				1		
3.	All four SWAPCW-pumps stop on low lubrication water flow	0.05					1	1
Net Impact Vector			0	0	0.9	0.05	0.05	1
	Average multiplicity						2.15	

Impact Vector Assessment

SWAPCW-01 and -02 belong both to system 715 A train. Three different water sources are available for the water lubrication of the pumps. Change of water source for lubrication requires however operator action. In the construction of the impact vector it has been assumed that the alignements to the water sources for lubrication of the pumps belonging to train A, respectively train B, is the same during most of the operational time. Thus a probability for common cause failure between the trains is assessed to exist due to operational practicesand design. The probability for disturbances in both train A and train B has thus been conservatively assessed as w = 0,05. OBS! The design of the lubrication water source for SWAPCW-pumps has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B

Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF06b	
C01	ICDE Event Identifier	R3-RO014-93/R4-RO012-93	
	Short Description	Pump trip due to loss of lubrication water, cause unkown	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	01/07/93	C	1		MC	R4 replicate
B	SWAPCW-02	01/07/93	C	1			
C	SWAPCW-03	01/07/93	W	0			
D	SWAPCW-04	01/07/93	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both SWAPCW-01 and -02 stop on low lubrication water flow	0.9			1			1
2.	SWAPCW-01, -02 and -03 stop on low lubrication water flow	0.05				1		
3.	All four SWAPCW-pumps stop on low lubrication water flow	0.05					1	1
Net Impact Vector			0	0	0.9	0.05	0.05	1
	Average multiplicity						2.15	

Impact Vector Assessment

SWAPCW-01 and -02 belong both to system 715 A train. Three different water sources are available for the water lubrication of the pumps. Change of water source for lubrication requires however operator action. In the construction of the impact vector it has been assumed that the alignements to the water sources for lubrication of the pumps belonging to train A, respectively train B, is the same during most of the operational time. Thus a probability for common cause failure between the trains is assessed to exist due to operational practicesand design. The probability for disturbances in both train A and train B has thus been conservatively assessed as w = 0,05. OBS! The design of the lubrication water source for SWAPCW-pumps has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF07a	
C01	ICDE Event Identifier	R4-RO026-91	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	17/09/91	C	1		MC	R4
B	SWAPCW-02	17/09/91	C	1			
C	SWAPCW-03	17/09/91	C	1			
D	SWAPCW-04	17/09/91	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All four 715-pumps stop during realignment of the lubrication flow	1					1	1
2.								0
Net Impact Vector			0	0	0	0	1	1
	Average multiplicity						4	

Impact Vector Assessment

The duration of the manual realignment of the lubrication flow to the 715-pumps (both train A and train B) from industry water to demineralised water was about 9 minutes. During this time all four 715-pumps were stopped. OBS! The design of the lubrication water source for 715-pumps (SWAPCW-pumps) has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF07b	
C01	ICDE Event Identifier	R4-RO026-91	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	17/09/91	C	1		MC	R3 replicate
B	SWAPCW-02	17/09/91	C	1			
C	SWAPCW-03	17/09/91	C	1			
D	SWAPCW-04	17/09/91	C	1			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All four 715-pumps stop during realignment of the lubrication flow	1					1	1
2.								0
Net Impact Vector			0	0	0	0	1	1
	Average multiplicity						4	

Impact Vector Assessment

The duration of the manual realignment of the lubrication flow to the 715-pumps (both train A and train B) from industry water to demineralised water was about 9 minutes. During this time all four 715-pumps were stopped. OBS! The design of the lubrication water source for 715-pumps (SWAPCW-pumps) has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF08	
C01	ICDE Event Identifier	R4-RO22-93/R3-RO08-94	
	Short Description	Ageing problems in the contactor of the lubrication oil pumps	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	L	0.1
G5	Test Interval		
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A		07/03/94	I	0.01	34	TI	
B		07/03/94	I	0.01			
C		07/03/94	D	0.1	34		

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3		Element sum
1.	All 334-pumps would survive on demand, including 334 P3	0.99	1					1
2.	334 P3 fails to run on demand period	0.01		1				1
Net Impact Vector			0.99	0.01	0	0		1
		Average multiplicity					0.01	

Impact Vector Assessment

Comment for Component events: Based on exhaustive replacement at the Ringhals plant of internal part in contactors belonging to EG relays, it is proposed to classify 334 P1 and P2 as impaired. The value I = 0,01 is proposed based on the fact that each main pump has two lubrication pumps. Based on the same facts it is proposed to set D = 0,1. Operating experience demonstrates relatively frequent failures in contactors similar to the involved contactors on the lubrication pumps to 334 P1 - P3 (see for example R4-RO-22/1993), the probability for concurrent failure is assessed for two lubrication pumps (ie impairing the function of one 334-pump) as w = 0,01. The assessment is made that 4-fold concurrent failure of four lubrication pumps belonging to two of 334-P1 - P3 is very remote.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF09	
C01	ICDE Event Identifier	R4-RO015-94	
	Short Description	Pump trip due to loss of lubrication water, erroneous test maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	29/07/94	W	1		TI	
B	SWAPCW-02	29/07/94	W	1			
C	SWAPCW-03	29/07/94	C	0			
D	SWAPCW-04	29/07/94	C	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	SWAPCW-03 and -04 stopped spuriously	0.99			1			1
2.	All SWAPCW-pumps stop spuriously	0.01					1	1
Net Impact Vector			0	0	0.99	0	0.01	1
	Average multiplicity						2.02	

Impact Vector Assessment

Comment to Component events: The spurious manual short closing of 134 V2 during operability readiness control (DKV) resulted in loss of NPSH for lubrication pumps for SWAPCW-03 and -04.These pumps belong to train B of system 715. Due to the potential to also close shortly 134 V, a probability existed to loose NPSH to train A lubrication pumps. The LER does not provide any information about the communication between the main control room and the field operator that can put ligth on the assessment of the probability for such spurious closing of both valves. Lacking further information it is assessed that w = 0,01 for the having low lubrication flow on all four 715-pumps. OBS! The design of the lubrication water source for 715-pumps (SWAPCW-pumps) has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF10	
C01	ICDE Event Identifier	R4-RO024-95	
	Short Description	Pump trip due to loss of lubrication water, erroneous valve maneuver	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor		
G5	Test Interval	30 days	
G5-2	Test Staggering		

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	SWAPCW-01	23/07/95	C	1		MC	
B	SWAPCW-02	23/07/95	C	1			
C	SWAPCW-03	23/07/95	W	0			
D	SWAPCW-04	23/07/95	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	SWAPCW-01 and -02 stopped spuriously	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
	Average multiplicity						2	

Impact Vector Assessment

SWAPCW-01 and -02 stopped on low lubrication water flow. No further comment except that the design of the lubrication water source for 715-pumps (SWAPCW-pumps) has been modified during the late nineties in order to prevent experienced failures.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF11a	
C01	ICDE Event Identifier	LOTI-180181A-1	
	Short Description	Vulnerability to high temperature trip and start-stop cycling due to inadequate bearing design, replicate SF11b	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	e	
G5	Test Interval	28 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	11TJ11D001	22/06/93	D	0.5		TI	LO1
B	11TJ12D001	27/07/93	D	0.5		TI	
C	12TJ51D001	27/07/93	D	0.5		TI	
D	12TJ52D001	27/07/93	D	0.5		TI	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All HPSI pumps fulfill their function during a running demand > 4 hr	0.5	1					1
2.	One HPSI pump fails during a running demand > 4 hr	0.3		1				
3.	Two HPSI pumps fail during a running demand > 4 hr	0.15			1			
4.	Three HPSI pumps fail during a running demand > 4 hr	0.04				1		
5.	All HPSI pumps fail during a running demand > 4 hr	0.01					1	1
Net Impact Vector			0.5	0.3	0.15	0.04	0.01	1
		Average multiplicity					0.76	

Impact Vector Assessment

The assessment of the impact vector is difficult due to the lack of information about possible operational strategies in case of LOCA events. Whether or not some of the HPSI pumps will be manually operated on/off to allow the cooling down of the bearings before restarted. Obviously the repeated pump startups could overload the pump motors. The weights utilised in the construction of the impact vector are consequently based on best estimates without any pretention of deeper robustness.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF11b	
C01	ICDE Event Identifier	LOTI-180181A-1	
	Short Description	Replicate to SF11a	
C03	Failure Mode	FR	
C11	Shared Cause Factor	H	1
C14	Time Factor	e	
G5	Test Interval	28 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	11TJ11D001	22/06/93	D	0.5		TI	LO2 replicate
B	11TJ12D001	22/06/93	D	0.5		TI	
C	12TJ51D001	22/06/93	D	0.5		TI	
D	12TJ52D001	22/06/93	D	0.5		TI	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All HPSI pumps fulfill their function during a running demand > 4 hr	0.5	1					1
2.	One HPSI pump fails during a running demand > 4 hr	0.3		1				
3.	Two HPSI pumps fail during a running demand > 4 hr	0.15			1			
4.	Three HPSI pumps fail during a running demand > 4 hr	0.04				1		
5.	All HPSI pumps fail during a running demand > 4 hr	0.01					1	1
Net Impact Vector			0.5	0.3	0.15	0.04	0.01	1
		Average multiplicity					0.76	

Impact Vector Assessment

The assessment of the impact vector is difficult due to the lack of information about possible operational strategies in case of LOCA events. Whether or not some of the HPSI pumps will be manually operated on/off to allow the cooling down of the bearings before restarted. Obviously the repeated pump startups could overload the pump motors. The weights utilised in the construction of the impact vector are consequently based on best estimates without any pretention of deeper robustness.

Impact Vector Construction Sheet

Analyst B
Version 2, 03 April 2003

Principal Event Data

	NAFCS Index	SF12	
C01	ICDE Event Identifier	OL2-5009449	
	Short Description	Blockage of pump suction by plywood boards in the seawater channel	
C03	Failure Mode	FR	
C11	Shared Cause Factor	L	0.1
C14	Time Factor	L	0.1
G5	Test Interval	7 days	
G5-2	Test Staggering	Staggered	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
A	712P1	05/04/96	I	0.1	34		
B	712P2		W	0			
C	712P3	19/06/96	C	1	34	DE	
D	712P4		W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	All 712- pumps fulfill their function during a running demand > 4 hr	0.778	1					1
2.	One 712-pump fails during a running demand > 4 hr	0.2		1				
3.	Two 712-pumps fail during a running demand > 4 hr	0.02			1			
4.	Three 712-pumps fail during a running demand > 4 hr	0.001				1		
5.	All 712-pumps fail during a running demand > 4 hr	0.001					1	1
Net Impact Vector			0.778	0.2	0.02	0.001	0.001	1
		Average multiplicity					0.247	

Impact Vector Assessment

The event that occurred in June 1996 indicates a reduction of the flow from 712 P3 from normally 115 kg/s to 92 kg/s. The report does not provide information whether several pieces of plywood board were found or not in relation to the event. In the construction of the impact vector it has been assessed that only one piece was found. Furthermore, it is difficult to assess the impact of the flow reduction in one pump for the real consequence on the system level. It is here judged that the technical specifications were not fulfilled for 712 P3, although the pump itself was failure free. The weights utilised in the construction of the impact vector are consequently based on best estimates without any pretention of deeper robustness.

NACFS - Impact Vector Construction
Nordic Pumps

CCF Event List

Index	C01 CCF event identifier	Unit	System	Year
SF01	RO-O1-88/018	O1	323 Core Spray System	88
SF02	RO-O2-96/015	O2	327 Auxiliary Feed Water	96
SF03	RO-O2-96/043	O2	323 Core Spray System	96
SF04	R1-RO48-93/R1-RO54-93	R1	322 Containment Spray System	93
SF05	R2-RO013-90	R2	311 Component Cooling System	90
SF06a	R3-RO014-93/R4-RO012-93	R3	715 Salt Water Pumps	93
SF06b	- " -	R4	715 Salt Water Pumps	93
SF07a	R4-RO026-91	R4	715 Salt Water Pumps	91
SF07b	- " -	R3	715 Salt Water Pumps	91
SF08	R4-RO22-93/R3-RO08-94	R4	334 Charging Pumps of ECCS	93
SF09	R4-RO015-94	R4	715 Salt Water Pumps	94
SF10	R4-RO024-95	R4	715 Salt Water Pumps	95
SF11a	LOTI-180181A-1	L1	HPSI	93
SF11b	- " -	L2	HPSI	93
SF12	OL2-5009449	T2	712 Shutdown Service Water System	96

Version control

Version 0	Partially cleaned version	28 January 2003
Version 1	Upgraded version	06 March 2003

Notes

The structure and special notations of this workbook are explained in [NAFCS-WN-TM09].

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF01	NAFCS Index
C01	RO-O1-88/018	ICDE Event Identifier
	Systematic error to restore power supply after maintenance	Short Description
C03	MC	Failure Mode
		Generic Class
G1	323 Core Spray System	System
G4	CP-LL-SB	Pump type
G6	2	Group size
C04	2	Exposed components
C11	H	Shared Cause Factor
C14	empty	Time Factor
G5	30 days	Test Interval
G5-2	Staggered	Test Staggering

1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	323P1	14/09/88	C	1		MC
B	323P2	14/09/88	C	1		

ICDE Event Description and Qualitative Classifications

C05 Event Description

During an unplanned outage, work was done on the generators. After finished work the following startup of the reactor was performed whith the two core spray pumps out of operation.The reason was to prevent the risk of cold pressurisation of the reactor vessel. During the startup procdeure - nuclear warmup - it was discovered that the isolation breakers to the pumps were not closed making the pumps inoperable and not able to start if a demand had occured. It was discovered that the breakers were not restored before the startup procedure. The startup procedure was not signed at this point.Downtime : 2h 45 min.

C07 Event Interpretation

Both pumps were made inoperable with one single failure. Due to open isolation breakers to the pumps were these unable to function in case of a demand event if required.

No comment.
Failure mechanism: breaker problem

C09	H	Root cause
C10	O	Coupling factor(s)
C12	B	Corrective actions

C13 Other

In order to minimize the risk of cold pressurazion of the reactor vessel the procedures must be followed. The procedure are described in the ordinary operation instructions for cooling down resp. nuclear startup. Both core spray pumps are manually disconnected from the busbars at reactor temperature below 100 oC. During the startup the pumps connects to the busbar at reactor temperature 85 oC. Both pumps are always tested before the reactor temperature reaches 100 oC.

CXX Additional Clarifications

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF02	NAFCS Index
C01	RO-O2-96/015	ICDE Event Identifier
	Contactor failure due to inadequate dimensioning	Short Description
C03	FS	Failure Mode
		Generic Class
G1	327 Auxiliary Feed Water	System
G4	CP-MS-SB	Pump type
G6	2	Group size
C04	2	Exposed components
C11	empty	Shared Cause Factor
C14	H	Time Factor 1
G5	30 days	Test Interval
G5-2	Staggered	Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	327P3	22/03/96	C	1	35	TI
B	327P4	22/03/96	W	0	14	

ICDE Event Description and Qualitative Classifications

C05 Event Description

The station was at power level 106% when a periodical test was performed on the P3 pump in the auxiliary and emergency feedwater system 327 on March 22, 1996. The pump failed to start due to two blown fuses. The initial cause to this was a seizing lock that locks the contactor in closed position, which made the contactor bounce several times. This caused the pump motor to get out of phase with the network which resulted in a peak current.The operation due to this event was not effected.Downtime: 4 hours 30 min

C07 Event Interpretation

This is a possible CCF event since the same type of failure occurred on the same pump within a short period of time.

No comment.
Failure mechanism: defective contactor

C09	D	Root cause
C10	HC	Coupling factor(s)
C12	B	Corrective actions

C13 Other

A new contactor will replace the failed contactor. The maintenance department will qualify new contactors of different seizes to satisfy the need of replacement of contactors of the same type in other systems at the plant. The contactor, type EG 315 is designed by ASEA.
This event is a potential CCF-event.
A similar event has happened in Oskarshamn 2, in the 713 system, contactor EG 630, see RO O2-96/17.

CXX Additional Clarifications

327 P3 is the auxiliary condensate pump to supply high pressure injection pump 327P1 in Train A. A similar fuse failure occurred on 12.01.96 due to disturbed operation of 327P3 contactor (described in RO-O2-96/03).
The consecutive events of 327P3 will be handled as recurring failure, and CCF risk due to inadequate contactor design is considered effectively in the connection of the latter event.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF03	NAFCS Index
C01	RO-O2-96/043	ICDE Event Identifier
	Systematic error to restore power supply after containment leak test	Short Description
C03	FS	Failure Mode
		Generic Class
G1	323 Core Spray System	System
G4	CP-LL-SB	Pump type
G6	2	Group size
C04	2	Exposed components
C11	H	Shared Cause Factor 1
C14	H	Time Factor 1
G5	30 days	Test Interval
G5-2	Staggered	Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	323P1	13/11/96	C	1	17	TI
B	323P2	13/11/96	C	1	17	

ICDE Event Description and Qualitative Classifications

C05 Event Description

The station was at power level 100 % when a periodical test of the two core spray pumps was planned on November 13, 1996. It was discovered that the isolation breakers to the pumps were not closed making the pumps inoperable and not able to start. During containment leak rate test, which was done after annual overhaul, this system was taken out of operation to avoid disturbances in the measurements. After the test the system was restored and taken in operation but the breakers were not closed. The operation due to this event was not effected.Downtime: 187 hours 40 min

C07 Event Interpretation

Both pumps were made inoperable with one single failure. Due to open isolation breakers to the pumps were these unable to function, in case of a demand event, if required.

No comment.
Failure mechanism: breaker problem

C09	H	Root cause
C10	O	Coupling factor(s)
C12	empty	Corrective actions

C13 Other

A human error analysis was done after the event has happened and resulted in a proposal containing several actions to prevent recurrence of the event. The safety committe decided in January 1997 to implement these proposed actions. In summary: 1. The NPP has initiated a educationprogram covering the importance of planning in order to maintain the safetybarriers. 2. The plant will also improve the timing of testprogramme due to changes in technical specification during outage and operation. 3. The experience from other utilities will also be used in this case. 4. The indication of the disconnecting switches to the pumps in the central control room will be improved .
-In order to identify the proper root cause of the event has the utility used the specific "MTO-method". For further information of this event and this method see report: Operational Experience from Swedish NPP 1996 which can be obtained from: Kärnkraftsäkerhet och Utbildning AB, P.O.Box 1039, S-61129 Nyköping, Sweden.

CXX Additional Clarifications

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF04	NAFCS Index	
C01	R1-RO48-93/R1-RO54-93	ICDE Event Identifier	
	Leakages in the mechanical seal of the axle	Short Description	
C03	MR	Failure Mode	
	BoxLkg	Generic Class	
G1	322 Containment Spray System	System	
G4	CP-LL-Int	Pump type	
G6	3	Group size	
C04	3	Exposed components	
C11	M	Shared Cause Factor	0.5
C14	L	Time Factor	0.1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	322P1	28/12/93	I	0.1		
B	322P2	28/12/93	W	0		
C	322P3	14/11/93	I	0.1		MW

ICDE Event Description and Qualitative Classifications

C05 Event Description

System in standby. First occurrence during plant start up, second during power operation. The leakage on both occasions was discovered during plant walk trough. A running leakage was observed from the secondary seal of the mechanical seal of the axle. Seal water was leaking into the pump bearings and to the shroud surrounding the pump and motor unit. The condition will reduce the availability of the pump if needed. 30 h since verified OK.
The second event was indicated as a small leak developing to a similar situation as above in 12 days.
Time to repair 11:18 h and 12:22 h

C07 Event Interpretation

The Ccf coupling is weak in this case as no material problem or maintenance work has been identified.

Comment: This seems to be FS (nominal conditions may not be reached.
Failure mechanism: seal problem

C09	I	Root cause
C10	empty	Coupling factor(s)
C12	G	Corrective actions

C13 Other

This is a rather normal failure that could occur by coincidence in two different pump at the same time. Any material defects have not been observed. Maintenance on mechanical seal ??

CXX Additional Clarifications

The observed leaks are monitored (these pumps are normally in standby), repair-critical in this case. The event description in R1-RO54-93 tell that the incipient leak of 322P1 was detected already on 15.12.1993, was followed up, regarded repair-critical on 27.12.1993, and repaired on 28.12.1993.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF05	NAFCS Index
C01	R2-RO013-90	ICDE Event Identifier
	Faulty logic installed due to incorrect circuit diagrams	Short Description
C03	FS	Failure Mode
		Generic Class
G1	311 Component Cooling System	System
G4	CO-LL-Int	Pump type
G6	3	Group size
C04	3	Exposed components
C11	H	Shared Cause Factor 1
C14	H	Time Factor 1
G5	30 days	Test Interval
G5-2		Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	711P1	20/05/90	C	1	16	DE
B	711P2	20/05/90	C	1	16	
C	711P3	20/05/90	C	1	16	

ICDE Event Description and Qualitative Classifications

C05 Event Description

Component Cooling is normally operating with one pump. The event occurred during a plant refuelling outage so residual heat removal from fuel ponds was affected. The fault in the logic circuit was detected during a normal pump change. The system is designed with a low pressure detection which will start the two standby pumps. At the normal pump change the automatic standby pump start is blocked by a key switch. At this event the two stand-by pumps started when the automatic start was blocked. Manual actions to stop the pumps resulted only in automatic restart. The third time all pumps stopped and the selected pump for operation would not start. The operators tried the other pumps with no result. The unit was without cooling pumps for 2 h 15 m. resulting in a fuel pond temperature increase of 5 degrees. The function was last verified 16 days before the event.The cause was modifications to Auxiliary Feed Water system start logic which is in the same cubicle. The drawing sheet included both the AFWS and CCS logic. Fault in the CCS wiring drawing resulted in modifications to CCS logic in the cubicle.

C07 Event Interpretation

A failure of a common component. Due to a misstake during backfitting was logic circuit for CC changed due to a faulty drawing.

No comment.
Failure mechanism: faulty logic

C09	H	Root cause
C10	O	Coupling factor(s)
C12	A	Corrective actions

C13 Other

Human error by the fitter who worked at the wrong system. By the person who didn't alter the drawings after modifications. The event also reveals defects in administration as the drawing was not correct, the sheet covered two different systems etc.

CXX Additional Clarifications

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF06	NAFCS Index	
C01	R3-RO014-93/R4-RO012-93	ICDE Event Identifier	
	Pump trip due to loss of lubrication water, cause unkown	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	715 Salt Water Pumps	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	2	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	01/07/93	C	1		MC
B	SWAPCW-02	01/07/93	C	1		
C	SWAPCW-03	01/07/93	W	0		
D	SWAPCW-04	01/07/93	W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

The unit 3 in refuelling and unit 4 full power operation. Of the Salt Water System pumps was B train was out for maintenance and both unit 3 A train pumps stopped by the incident. In unit 4 A train pumps stopped but B train was not affected. The Service Water System supply lubricating water to the pump bearings. During a switch to bearing lubrication from Deminarilzed Water System the system was out for period of 11 min (R3) and 17 min (R4) There is one Service Water storage tank for both units with an internal deviding wall. No cause for loss of lubrication water was found. The following circumstances may have contributed. At the time Water from R3 part of the tank was pumped to R4 side then flowing back over the divider. The fuel pond of R3 was temporary cooled from the storage tank and a diesel generator test run stopped at the time of the incident. The diesel is cooled by Service Water. The theory is that air mixed in the tank is the main cause.

C07 Event Interpretation

Consequences for this type of CCF is minor as redundancy in lubrication water supply is available after a short action by the operator.

No comment.
Failure mechanism: lubrication problem

C09	U	Root cause
C10	H	Coupling factor(s)
C12	C	Corrective actions

C13 Other

Technically possible to change bearings to a type not needing lubrication water. The design change has low priority as there are tree different lubrication water sources.

CXX Additional Clarifications

The same root problem affected simultaneously Division A of Ringhals 4 System 715, see SF06b.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF06b	NAFCS Index	
C01	R3-RO014-93/R4-RO012-93	ICDE Event Identifier	
	Pump trip due to loss of lubrication water, cause unkown	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	715 Salt Water Pumps	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	2	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	01/07/93	C	1		MC
B	SWAPCW-02	01/07/93	C	1		
C	SWAPCW-03	01/07/93	W	0		
D	SWAPCW-04	01/07/93	W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Replicate event at R4, see event description for R3 (SF06a)

C07 Event Interpretation

Replicate event at R4, see eventsheet for R3 (SF06a)

C09	U	Root cause
C10	H	Coupling factor(s)
C12	C	Corrective actions

C13 Other

Replicate event at R4, see eventsheet for R3 (SF06a)

CXX Additional Clarifications

The same root problem affected simultaneously Division A of Ringhals 3 System 715, see SF06a.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF07a	NAFCS Index	
C01	R4-RO026-91	ICDE Event Identifier	
	Pump trip due to loss of lubrication water, erroneous valve maneuver	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	715 Salt Water Pumps	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	4	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	17/09/91	C	1		MC
B	SWAPCW-02	17/09/91	C	1		
C	SWAPCW-03	17/09/91	C	1		
D	SWAPCW-04	17/09/91	C	1		

ICDE Event Description and Qualitative Classifications

C05 Event Description

The Plant was in refuelling with 2 of four pumps running in the Salt Water System. A disturbance in the Service Water System caused by operation of hand valves supplying auxiliary Feed Water System led to trips of the pump due to fluctuations in SWS water supply to the pump bearings, probably due to air let in by the opening of valves. During a switch to bearing lubrication from Demineraril zed Water System all pumps were inoperational for 10 m.

C07 Event Interpretation

Consequences for this type of CCF is minor as redundancy in lubrication water supply is available after a short action by the operator.

No comment.
Failure mechanism: lubrication problem

C09	P	Root cause
C10	O	Coupling factor(s)
C12	B	Corrective actions

C13 Other

CXX Additional Clarifications

The same root problem affected simultaneously sea water pumps in Ringhals 3 System 715, see SF07b.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF07b	NAFCS Index	
C01	R4-RO026-91	ICDE Event Identifier	
	Pump trip due to loss of lubrication water, erroneous valve maneuver	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	715 Salt Water Pumps	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	4	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	17/09/91	C	1		MC
B	SWAPCW-02	17/09/91	C	1		
C	SWAPCW-03	17/09/91	C	1		
D	SWAPCW-04	17/09/91	C	1		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Replicate event at R3, see eventsheet for R4 (SF07a)

C07 Event Interpretation

Replicate event at R3, see eventsheet for R4 (SF07a)

C09	P	Root cause
C10	O	Coupling factor(s)
C12	B	Corrective actions

C13 Other

Replicate event at R3, see eventsheet for R4 (SF07a)

CXX Additional Clarifications

The same root problem affected simultaneously sea water pumps in Ringhals 4 System 715, see SF07a.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF08	NAFCS Index	
C01	R4-RO22-93/R3-RO08-94	ICDE Event Identifier	
	Ageing problems in the contactor of the lubrication oil pumps	Short Description	
C03	FR	Failure Mode	
	Contcr	Generic Class	
G1	334 Charging Pumps of ECCS	System	
G4	CP-LS-Int	Pump type	
G6	3	Group size	
C04	2	Exposed components	
C11	H	Shared Cause Factor	1
C14	L	Time Factor	0.1
G5		Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A		07/03/94	W	0		TI
B		07/03/94	W	0		
C		07/03/94	D	0.5		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Pumps in the Chemical and Volume Control system double as Safety Injection Pumps. The pump bearings is oil lubricated. The oil pressure is supplied by two pumps, one running and one standby. Once a month the operator change pumps. On the first occasion the oil pump didn't stop on the other it didn't start. The cause on both occasions was a faulty catch in the motor contactor. Ageing of the plastic material caused the catch to break, jamming the mechanism. Manufacturer: ASEA type BDB 110 VDC, for EG10 and EG20 contactors.
Further information report UT 0047/94. Actions in Ringhals was to change a total of 74 catches in class 1E equipment to a catch of better design and material.
Time to corect 11 h 46 m and 50 m
Undisscovered 181,5 and 226,25 h

C07 Event Interpretation

The time between event doesn't classify the events as a CCF. The selection of wrong material in a vital part is a CCF initiator. The event show the benefit of regular changing of running equipment and the amount of equipment using identical parts.

No comment:

C09	D	Root cause
C10	H	Coupling factor(s)
C12	C	Corrective actions

C13 Other

CXX Additional Clarifications

In the case of R3, 07.03.1994, one out of two lubrication oil pumps in Sub A has to be regarded as failed to start at the monthly switchover of the oil pumps (one running, one in standby). The implication is that the reliability of continued operation of the charging pump is reduced, thus failure mode = FR. The case of R4, 06.12.1993 had only a minor implication on the operability of the charging pump (running oil pump could not be stopped by normal means), hence to be regarded as additional information about the underlying ageing problem of the contactors.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF09	NAFCS Index	
C01	R4-RO015-94	ICDE Event Identifier	
	Pump trip due to loss of lubrication water, erroneous test maneuver	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	715 Salt Water Pumps	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	4	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	30 days	Test Interval	
G5-2		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	29/07/94	C	1		TI
B	SWAPCW-02	29/07/94	C	1		
C	SWAPCW-03	29/07/94	W	0		
D	SWAPCW-04	29/07/94	W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Unit 4 full power operation. The Salt Water System pumps of B train was affected. The Service Water System supply lubricating water to the pump bearings. The system was out for period of 5 min Unit 3 system is fed by the same header did not trip pumps but the redundant lubrication water pump started.
A isolation valve in the header is automatically closed to halve open to reduce water flow in case of a pipe rupture. During the test the power supply to the valve should be disconnected by the tester. As he didn't do that, the valve closed to halve open during the test. A later plant walk through discovered the halve open valve. During the verification of valve function the valve was closed thereby losing suction head for the lubrication water pumps.

C07 Event Interpretation

Consequences for this type of CCF is minor as redundancy in lubrication water supply is available after a short action by the operator.

No comment.
Failure mechanism: insufficient suction source (causing lubrication degradation)

C09	C	Root cause
C10	H	Coupling factor(s)
C12	C	Corrective actions

C13 Other

Technically possible to change bearings to a type not needing lubrication water. The design change has low priority as there are tree different lubrication water sources.
Other findings: inadequate procedures and no verifying of function after test have been corrected

CXX Additional Clarifications

In this case the influence on the redundant block (R3) was only automatic changeover lubrication water pump, without trip of sea water pumps.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF10	NAFCS Index
C01	R4-RO024-95	ICDE Event Identifier
	Pump trip due to loss of lubrication water, erroneous valve maneuver	Short Description
C03	FR	Failure Mode
		Generic Class
G1	715 Salt Water Pumps	System
G4	CP-LL-Int	Pump type
G6	4	Group size
C04	2	Exposed components
C11	H	Shared Cause Factor
C14	empty	Time Factor
G5	30 days	Test Interval
G5-2		Test Staggering

1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	SWAPCW-01	23/07/95	C	1		MC
B	SWAPCW-02	23/07/95	C	1		
C	SWAPCW-03	23/07/95	W	0		
D	SWAPCW-04	23/07/95	W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Unit 4 power operation. The Salt Water System pumps of A train was affected. The Service Water System supply lubricating water to the pump bearings. The system was out for period of 8 min Unit 3 system is fed by the same header did not trip pumps but the redundant lubrication water pump started.
The operator didn't follow the procedure steps in order during shut down of Service Water Header causing loss of lubricating water. By closing a valve to the lubricating water pumps before switching to Deminerarlized water.

C07 Event Interpretation

Consequences for this type of CCF is minor as redundancy in lubrication water supply is available after a short action by the operator.

No comment.
Failure mechanism: loss of lubricating water

C09	H	Root cause
C10	H	Coupling factor(s)
C12	A	Corrective actions

C13 Other

Technically possible to change bearings to a type not needing lubrication water. The design change has low priority as there are tree different lubrication water sources.

CXX Additional Clarifications

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF11	NAFCS Index
C01	LOTI-180181A-1	ICDE Event Identifier
	Vulnerability to high temperature trip and start-stop cycling due to inade-quate bearing design, replicate SF11b	Short Description
C03	FR	Failure Mode
		Generic Class
G1	HPSI	System
G4	CP-HS-SB	Pump type
G6	4	Group size
C04	4	Exposed components
C11	H	Shared Cause Factor 1
C14	empty	Time Factor
G5	28 days	Test Interval
G5-2	Staggered	Test Staggering

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	11TJ11D001	22/06/93	D	0.5		TI
B	11TJ12D001	27/07/93	D	0.5		TI
C	12TJ51D001	27/07/93	D	0.5		TI
D	12TJ52D001	27/07/93	D	0.5		TI

ICDE Event Description and Qualitative Classifications

C05 Event Description

The temperature of HPSI pump motor bearings rose above 75 C (not acceptable) after 2 h scheduled test run (22TJ52D001 22.6.1993, 11TJ11D001 27.7.1993). The other redundant pumps, 4 at both units indicated similar tendency. (continues)
This phenomenon was found out because of new increased test durations. Because of it the pumps would have had to start up repeatedly at certain process conditions when the bearing temperature exceeds the protection limit. (continues)
Emergency operation initiated by the plant protection signal prevents this protective trip. However, with certain size of LOCA it is possible that the plant protection signal stays on only a short time. (continues)
Primary coolant inventory control requires that one pump feed is still needed. This leads to repeated pump startups and trips and possibly to overloading of the pump motors.

C07 Event Interpretation

Pumps could have failed during long runs with certain LOCA sizes. This failure could have taken place already years earlier. (continues)
There is a smaller probability that the pumps would have failed because of too high bearing temperatures during all kinds of long missions .

No comment.
Failure mechanism: overheating of bearings

C09	U	Root cause

C10	HC	Coupling factor(s)
C12	C	Corrective actions

C13 Other

The bearings of 11TJ11D01 were replaced by new ones in 1993. Trip limit was raised from 85 to 110 degrees C for these old kinds of bearings. (continues)
The old bearings were replaced by new kinds of bearings in 1993 for pumps 21TJ11D01 & 22TJ52D01, in 1994 for 11TJ12, 12TJ51, 21TJ12 & 22TJ51 and in 1995 for 12TJ52D01.
Pump 11TJ11D01 bearings were replaced by new kinds 20.10.1994 after failed test.

CXX Additional Clarifications

Prepared by Tuomas Mankamo, 04.03.2003, Last update: 06.03.2003
Based on the discussion with Kalle Jänkälä, 03.03.2003

The detected failure mechanism has a more substantial impact in such a Small LOCA situation, where the actuation of HPSI is based only on the pressurizer low level, while low pressure limit is not reached. This situation is discussed first. All four HPSI pumps of the unit will be initially started. The set-point of high temperature for the pump bearings would be reached in 1 – 2 hours in the actual demand condition. It is likely that the low level signal would have been vanished (in the considered type of LOCA) at that time point, i.e. the local protection can trip pumps on high bearing temperature. The pumps would start up again automatically in a few minutes, due to level decrease and reactivation of the LOCA signal, and enter frequent trip-start cycling. The pump manufacturer had guaranteed only two subsequent starts with high bearing temperature. ...

It is, however, also possible that the primary circuit temperature could have decreased to the level that the operators stop part of the pumps and take over manual control, before reaching high temperature limit of the bearings. This would save pumps entering directly trip-start cycling. Based on this aspect the component impairment values were classified as “Degraded”.

In the other LOCA situations the HPSI actuation is coming also from the low pressure signal, staying on during the mission time, disabling thus the local pump protection on high bearing temperature. It was verified that the initial temperature limit of 85 oC was overly cautious and could be increased to 110 oC. It was thus considered likely that the operators had taken well in time the control of the pumps, and by switching of the operating pump been able to avoid damage to the bearings (except in the specific type of Small LOCA as discussed first). Only one HPSI pump is needed.

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF11b	NAFCS Index
C01	LOTI-180181A-1	ICDE Event Identifier
	Replicate to SF11a	Short Description
C03	FR	Failure Mode
		Generic Class
G1	HPSI	System
G4	CP-HS-SB	Pump type
G6	4	Group size
C04	4	Exposed components
C11	H	Shared Cause Factor
C14	empty	Time Factor
G5	28 days	Test Interval
G5-2	Staggered	Test Staggering

1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	11TJ11D001	22/06/93	D	0.5		TI
B	11TJ12D001	22/06/93	D	0.5		TI
C	12TJ51D001	22/06/93	D	0.5		TI
D	12TJ52D001	22/06/93	D	0.5		TI

ICDE Event Description and Qualitative Classifications

C05 Event Description

See the event description for the replicate case at Loviisa 1, 27.07.93 (SF11a)

C07 Event Interpretation

See the replicate case at Loviisa 1, 27.07.93 (SF11a)

C09	U	Root cause
C10	HC	Coupling factor(s)
C12	C	Corrective actions

C13 Other

See the replicate case at Loviisa 1, 27.07.93 (SF11a)

CXX Additional Clarifications

See the replicate case at Loviisa 1, 27.07.93 (SF11a)

Event Description Sheet

Upgraded version, 06 March 2003

Principal Event Data

	SF12	NAFCS Index	
C01	OL2-5009449	ICDE Event Identifier	
	Blockage of pump suction by plywood boards in the seawater channel	Short Description	
C03	FR	Failure Mode	
		Generic Class	
G1	712 Shutdown Service Water System	System	
G4	CP-LL-Int	Pump type	
G6	4	Group size	
C04	2	Exposed components	
C11	L	Shared Cause Factor	0.1
C14	L	Time Factor	0.1
G5	7 days	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	712P1	05/04/96	I	0.1	34	
B	712P2		W	0		
C	712P3	19/06/96	C	1	34	DE
D	712P4		W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

Olkiluoto 2 was in full power operation. When using RHR Train C for condensation pool cooling on 1996-06-19, the flow in pump 712P3 reduced. A plywood plate of size 300x300 mm2 was found in the suction cone.
Plywood plate(s) were presumably left in maintenance work during May 1996 in the seawater channel (common to pumps 712P1/P3). Earlier similar problems at Olkiluoto 2 for 712P4 on 1986-09-30, 712P3 on 1993-07-12 and 712P1 on 1996-04-05

C07 Event Interpretation

The assessment of the impact reflects variations in the amount of plywood plates left in the sea water channel, scope with respect to one or both safety divisions affected and simultaneity in bogging with suction flow (train pair AC has a joint sea water channel, similarly pair BD). The impact is assessed to reflect the mean bogging risk over one power cycle as the refuelling outage is considered as a renewal point for this CCF mechanism.
Analysis details are explained in [Pumps-CC].

Comment: Event dates are unclear..
Failure mechanism: foreign material in suction path.

C09	P	Root cause
C10	HC	Coupling factor(s)
C12	B	Corrective actions

C13 Other

Component degradation values are not capable to describe the CCF risk for this failure mechanisms

CXX Additional Clarifications

The following text is quoted from [Pumps_CC]:

In June 1996, 712P003 was started in order to use RHR Train C for pool cooling. Substantial vibration was noticed and the flow reached only 92 kg/s and suction head 1.2 bar (should nominally be at least 115 kg/s and 1.5 bar, respectively). The pump was stopped for investigation. The diver found a plywood board of size 300x300 mm blocking the suction cone. This failure mechanism has occurred altogether four times at OL2:

712P004, 30.09.1986: Flow reduced to 80 kg/s
712P003, 12.07.1993: Flow reduced to 110 kg/s
712P001, 05.04.1996: Flow reduced to 115 kg/s
712P003, 19.06.1996: Flow reduced to 92 kg/s

The report for the event in 1993 does not describe the causes, so it is an uncertain case.
...

It is not fully known how the plywood boards have entered the sea water (SW) channel where 712-pumps are placed. The most likely explanation is the situation when SW intake is changed to condenser outlet side (normally from the inlet side). This arrangement will be done annually in the overhaul outage for testing purpose. In addition during winter when the water temperature at the inlet side drops below 2 oC, the intake of 712-pumps P1 and P3 is changed to the condenser outlet side to avoid the risk related to possible freezing of subcooled water at the inlet side. There is a sifter to prevent bigger objects entering the SW channel but the design is poor. When the sifter is lifted for cleaning, the gathered objects can fall back inside to SW channel.

Work Notes

Comments on the ICDE database for the information stored about the Finnish and Swedish pumps, feedback from the impact vector assessment

Date/Version: 07 March 2003 Version 0, TM
25 April 2003 Version 1, TM

Prepared by: Tuomas Mankamo Avaplan Oy
Jean-Pierre Bento JPB Consulting AB

These notes collect database-specific detailed comments from the Impact Vector assessment for pumps, see the event descriptions and selected fields extracted from the ICDE database in [CCF-P-Nordic-Descriptions-V1.xls]. The overall procedure followed is described in [NAFCS-PR18]. Compare also to the details of Impact Vector assessments in [CCF-P-ImpVe-Construction-AV2.xls, CCF-P-ImpVe-Construction-BV2.xls], and to the specific difficulties as documented in the logging notes for the Impact Vector assessment [NAFCS-WN-TM09].

General comments

Many of the reported cases concern parallel events in the pump groups of separate reactor blocks, constituting separate CCCGs. Some of these cases are combined into one ICDE event record, referencing to the CCCG ID for one of the affected groups. Separate event records are needed for each affected group, with proper cross-references. This comment concerns cases SF06, SF07 and SF11.

The detailed comments are grouped per plant in order to facilitate the experience feedback from lessons learned, see the following table. The final section summarizes comments on some generic problems.

Plant	**Event**	
Loviisa	SF11a/b	LOTI-180181A-1
Olkiluoto	SF12	OL2-5009449
Oskarshamn	SF01	RO-O1-88/018
	SF02	RO-O2-96/015
	SF03	RO-O2-96/043
Ringhals	SF04	R1-RO48-93/ R1-RO54-93
	SF05	R2-RO013-90
	SF06a/b	R3-RO014-93/ R4-RO012-93
	SF07a/b	R4-RO026-91
	SF08	R4-RO22-93/ R3-RO08-94
	SF10	R4-RO024-95

Loviisa

Index	C01: ICDE event ID	Proposal/comment
SF11a/b	LOTI-180181A-1	Separate ICDE event records are needed for LO1 and LO2. The event description should also be supplemented.

The design problem of the bearings and protective temperature trip was detected in parallel for the HPSI pumps of LO1 and LO2, constituting two separate CCCGs. The event description contained in the ICDE database mixes and combines the group events into one record. Two separate event records are needed for LO1 and LO2, respectively, with proper cross-references. Additional information was needed from the plant expert for the proper understanding of the case, see field CXX in [CCF-P-Nordic-Descriptions-V1.xls] Sheet SF11.

Olkiluoto

Index	ICDE event ID (C01)	Proposal/comment
SF12	OL2-5009449	Change component impairment values from WICI to IWCW. Align component event dates accordingly. The event description should also be supplemented.

The blockage events in 1988 (712P4) and 1993 (712P3) have so substantial time separation from the two component events in 1996 (712P1 and 712P3) that they should not be considered part of CCF, only reflecting the aspect of recurring problem. The proposed alignments have already been done in the Impact Vector assessment in agreement with Jari Pesonen, TVO. Additional information was needed from the plant experts for the proper understanding of the case, see field CXX in [CCF-P-Nordic-Descriptions-V1.xls] Sheet SF12.

Oskarshamn

Index	C01: ICDE event ID	Proposal/comment
SF01	RO-O1-88/018	Change failure mode from FS to MC

The 323 pumps are normally in standby, Thus monitored critical failures should be classified with failure mode MC (this is correctly indicated in ‘Detection’ field).

Index	C01: ICDE event ID	Proposal/comment
SF02	RO-O2-96/015	The date for the Train B in the component event table should be same as for Train A, i.e. change from 12.01.96 to 22.03.1996. The event description should make reference to the earlier 327P3 event on 12.01.96 to indicate the recurring character of the problem.

The event description should also be more clear in making distinction between the auxiliary condensate pumps (327 P3 and P4 in Train A and B, respectively) and the high pressure injection pumps (327P1 and P2 in Train A and B, respectively).

Index	C01: ICDE event ID	Proposal/comment
SF03	RO-O2-96/043	The date for 323P2 event should be 13.11.1996, i.e. same as for 323P1. The date 27.10.1996 is time of power supply disconnection.

Ringhals

Index	C01: ICDE event ID	Proposal/comment
SF04	R1-RO48-93/ R1-RO54-93	Change failure mode from FR to MR. Improve also event description for timing aspects, see text.

The leak failure is monitored (these pumps are normally in standby), repair-critical in this case. The event description should tell that the incipient leak of 322P1 was detected already on 15.12.1993, was followed up, regarded repair-critical on 27.12.1993, and repaired on 28.12.1993. Compare to R1-RO54-93.

Index	C01: ICDE event ID	Proposal/comment
SF05	R2-RO013-90	Latent time (16 days) is missing from the component event table, is told in the event description field (C07)

Index	C01: ICDE event ID	Proposal/comment
SF06	R3-RO014-93/ R4-RO012-93	The same root problem affected simultaneously System 715 pumps of Ringhals 3 and 4, i.e. two separate CCCGs. Replicate event records need to prepared, with proper cross-references
SF07	R4-RO026-91	

In case SF09 (R4-RO015-94) the influence on the redundant block (R3) was only automatic changeover of the lubrication water pump, without trip of sea water pumps.

Index	C01: ICDE event ID	Proposal/comment
SF08	R4-RO22-93/ R3-RO08-94	The CCF event description should be connected to R3 event. The interpretation of the contactor problems in the lubrication oil pumps should be made with respect to the operability of the charging pump (main component)

In the case of R3, 07.03.1994, one out of two lubrication oil pumps in Sub A has to be regarded as failed to start at the monthly switchover of the oil pumps (one running, one in standby). The implication is that the reliability of continued operation of the charging pump is reduced, thus failure mode = FR. The case of R4, 06.12.1993 had only a minor implication on the operability of the charging pump (running oil pump could not be stopped by normal means). Hence R4 case has to be regarded only as additional information about the underlying ageing problem of the contactors.

Generic issues

In the following cases the Time Factor is either missing from the ICDE record, or set inconsistently. See details in [CCF-P-Nordic-Descriptions-V1.xls] and [CCF-P-ImpVe-Construction-AV2.xls].

Index	C01: ICDE event ID	Proposal/comment
SF01	RO-O1-88/018	Time Factor should be 'High'
SF08	R4-RO22-93/ R3-RO08-94	
SF10	R4-RO024-95	
SF11a/b	LOTI-180181A-1	

Many generic issues have been discussed in the logging notes more comprehensively, see [NAFCS-WN-TM09]. The following recommendation will be pointed out here:

– For the pumps that are normally in standby, the monitored failures (detected in standby by instrumentation, alarms and/or frequent walk-down) shall be consistently classified with failure mode equal to

  MC: Monitored Critical

  MR: Monitored Repair-critical

  MN: Monitored Non-critical

References

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Draft 1+, 25 April 2003.

NAFCS-WN-TM09
Logging Notes of the Impact Vector Assessment for the Pump Events. Work notes by T. Mankamo and J-P. Bento, Version 1, 25 April 2003.

CCF-P-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic NPPs. Version 1, 06 March 2003.

CCF-P-ImpVe-Construction-AV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Tuomas Mankamo, Version 2, 03 April 2003.

CCF-P-ImpVe-Construction-BV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Jean-Pierre Bento, Version 2, 03 April 2003.

Pumps-CC CCF Analysis of Pumps, Olkiluoto 1 and 2 Experience 1983-1995. Work report prepared by T. Mankamo, 14 May 1997.

Work Notes

Logging Notes of the Impact Vector Assessment for the Nordic Pumps

Date/Version:	07 March 2003	Version 0	
	25 April 2003	Version 1	
Prepared by:	Tuomas Mankamo	Avaplan Oy	TM
	Jean-Pierre Bento	JPB Consulting AB	JPB

1 Assessment Process and Technical Documentation

The principal milestones are described in Table 1. The flow of assessment was changed in comparison to DG Pilot. The event descriptions were discussed between the analysts before the first assessment round in order to identify and handle the most remarkable information deficiencies. This change proved successful. The discrepancies at the first assessment round were thus reduced.

Table 1 Milestones of the Impact Vector assessment for the pumps.

Date	Description
28 January 2003	Exchange of the extracted ICDE data, discussion of questions and needed clarifications on 11 February 2003
06 March 2003	Upgraded event description material
17 March 2003	Impact Vector assessments, Version 1, exchanged
24 March 2003	Cross-comparison of the assessments, residual questions handled by e-mail and phone
03 April 2003	Impact Vector assessments, Version 2, exchanged

The technical documentation of the event descriptions, event analysis and Impact Vector assessment are in this application made fully by the use of MS-Excel, while in the DG pilot MS-Excel and MS-Word were used in combination.

Event description workbook

The event description material are arranged in the workbook [CCF-P-Nordic-Descriptions-V1.xls], each event on separate description sheet. These sheets quote selected ICDE fields from the following database tables, pertinent for the Impact Vector assessment

- CCF Event Records
- Component Event Records and
- Group Records

Basically, the ICDE data is quoted as such and modifications are limited to correcting evident mistakes or gaps. All modifications are indicated by yellow highlighting of the field cell, and explained by the comment inserted to the cell. Furthermore, field 'CXX: Additional Clarifications' is added to the end of the sheet to contain additional information obtained from

the LERs, plant incident reports and by the discussions with the plant experts. This added information is restricted to objective technical details and facts, or the interpretation/ assessment by the plant experts. Any interpretation or assessment by the analysts will not be mixed here but are presented in the Impact Vector assessment sheets. The corrections and needs of vital additional information to ICDE data are collected in a separate memorandum [NAFCS-WN-TM08].

One practical aspect is that MS-Excel is not capable to handle smoothly long text fields. Therefore longer CXX fields are split into consecutive cells separated by dashed border. Split cells are allowed only for CXX field on the description sheet in order to facilitate later transfer of the information into a relational database, e.g. MS-Access.

Impact Vector construction workbooks

Impact Vector assessments are stored in two workbooks [CCF-P-ImpVe-Construction-AV2.xls] and [CCF-P-ImpVe-Construction-BV2.xls] for Analyst A and B, respectively. The layout is similar to the Word document sheets used in the DG Pilot. Some essential event description fields are reproduced from the description workbook. The analyst can change these fields, especially the classifications for Component Impairment Values, Time Factor and Shared Cause Factor with the condition that every change is indicated and arguments explained. See the more specific instructions in these regards in [NAFCS-WN-TM10].

2 Specific Details

A characteristic feature which differs from the DG Pilot is the fact that the standby state is the normal state for only a part of the pump groups, see Table 2. The CCF mechanisms and their detection differ significantly depending on the normal state. This influences Impact Vector assessment besides of fundamental implications to the CCF quantification.

Table 2 Grouping of the pumps according to normal state.

Normal state of the pumps	Description
SB	Standby, pump operation is limited to test runs and infrequent demands
Int	Intermittently operated, typically the pumps in the group undergo a rolling operation scheme, i.e. part of time operating, part in standby
OP	Operating continuously, except maintenance and overhaul outages

The observations and remarks about assessment details and outcome, which are of general interest regarding the use of the results or methodology, are gathered in Table 3. The comparison type classes of the base and redundant assessment are defined in Table 4. It shows also the count of events for type classes: the more general insights will be discussed in Section 3. Some of the more complicated cases will be discussed in more detail in the following subsections.

Another particular feature for the pump application is that three ICDE events actually concerned replicate events of two separate CCCGs at twin reactor units. These cases SF06, SF07 and SF11 are split with proper cross-referencing in the Impact Vector assessment. It has to be emphasized that several cases represent functional and/or operator action dependencies which ought to be explicitly modeled, i.e. not well adapted to be covered by (parametric) CCF data. See Section 3 for the insights.

Table 3 Observations from the Impact Vector assessment. The highlighted indexes in the first column indicate cases, where additional information was essential to complete the ICDE event description.

Case	Normal state	Observations	Comparison Type Class
SF01	SB	Identical assessment	1
SF02	SB	Same logic, some difference in the weights	4
SF03	SB	Identical assessment	1
SF04	Int	Difficulty to understand potential consequences of the box leakage, consensus after obtaining the judgment from the plant	3
SF05	Int	Identical assessment	1
SF06a/b(1	Int	Same logic, some difference in the weights	4
SF07a/b(1	Int	Identical assessment	1
SF08	Int	Confusing that the only one out of two lubrication pumps (of the main pump) were affected, i.e. the reliability for long term operation of the main pump reduced. Consensus after discussing the arguments.	3
SF09(1	Int	Same logic, some difference in the weights	4
SF10(1	Int	Identical assessment	1
SF11a/b(1	SB	Very complicated case because the impact depends on the operator actions during demand condition. Analyst A used causal modeling, Analyst B standard scenario method. Despite of the difficult case the assessments were (already at the first round) close to each other.	6
SF12	Int	The assessment was difficult due to relatively weak impact. Analyst A used causal modeling, Analyst B standard scenario method. The assessments were already surprisingly close already at the first round. Assessment B was modified in the second round at the low order failure based on the discussion about time-spread among the observed component events.	6

Note 1: Cases that represent functional and/or operator action dependencies which ought to be explicitly modeled.

Loss of lubrication water to 715 pumps, Ringhals 3 and 4

Cases SF06, SF07, SF09 and SF10 represent operational disturbances where sea water pumps were tripped due to loss of lubrication water. The lubrication water is primarily supplied from the service water system, and alternatively from the demineralized water system. The breaks in lubrication water were caused by erroneous flow arrangements or test maneuvers, and could be recovered by the operator typically in about ten minutes.

The CCF mechanism and consequences are very specific to the plant design and ought to be explicitly modeled. The Impact Vector assessments were nevertheless done for completeness. Actually the Impact Vector assessments were relatively straightforward – the difficulty in the quantification will be mostly connected to modeling of recovery actions in actual demand condition.

In case SF10 (R4-RO024-95) the sea water pumps in 715 Train A of R4 were primarily affected (tripped). In R3 the consequence was limited to change-over of redundant lubrication pump. Therefore no CCF event is considered for 715 pumps of R3 in this case.

Trip-start cycling of pumps due to bearing temperature

This case was a very dedicated CCF mechanism, which could only be understood by getting a more detailed description from the plant expert. See details in [CCF-P-Nordic-Descriptions-V1.xls], Sheet SF11a/b.

This case belongs also to the CCF mechanisms that ought to be explicitly modeled, because the operator control actions play an important role, and because the problem was relevant only in a specific type of Small LOCA. Besides, the CCF mechanism (with constant impact) had been latent from the start of the plant operation, which needs to be taken into account in a particular way in the quantification.

Blockage of sea water pump suctions by plywood boards, Olkiluoto 1 and 2

Obtaining more information beyond the short ICDE event descriptions was necessary. It was helpful that this case had been studied already earlier by Analyst A in co-operation with the plant experts. Thus there was also available a detailed description of the failure mechanism covering all historical occurrences.

3 Summary of the Insights

The general conclusion of this pilot work underlines the worth and necessity to perform comparative assessments by two analysts in order to reach high quality CCF data.

The count of type classes from the comparison between base and redundant assessment is presented below. The insights are generally much the same as in the DG Pilot, see [NAFCS-PR10, NAFCS-WN-TM02].

Table 4 Comparison type classes (same as in the DG Pilot).

Type class	Description	Count
1	Identical assessment, evident impact	5
2	Identical assessment, follows guide example	0
3	Identical assessment, consensus reached after discussion of the arguments, typically additional clarification had to be obtained from the plant	2
4	Same hypothesis structure, differing weights	3
5	Differences in hypothesis structure, typically weak degradation cases where one of the analysts considered the chances of higher order failure	0
6	Basic differences in the assessment logic, e.g. one of the analysts used a specific causal model or parametric dependence model to support the assessment	2
		12

New insights from this application are following:

- Quite many cases represent CCF mechanisms that ought to be explicitly modeled, i.e. are not well adapted to be covered by (parametric) CCF data and models (5 out of 12 pump cases, corresponding to 8 out of 15 CCF events). The construction of Impact Vectors is still useful in these cases but should specific advices be given for the explicit modeling, and determining the relevance to other plants (so called mapping to target application)
- One of the cases (representing two CCF events) had been latent from the begin of plant operation with permanent impact. For these kinds of cases also specific advice are needed for the quantitative treatment and mapping to target application

The conducted work is restricted to the events as currently stored in the ICDE database, i.e. no completeness verification is performed. Furthermore, so called coincident multiple failures are not covered (not presented in the ICDE data). Compare to the discussion of this issue in [NAFCS-PR03].

References

CCF-P-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic NPPs. Version 1, 06 March 2003.

CCF-P-ImpVe-Construction-AV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Tuomas Mankamo, Version 2, 03 April 2003.

CCF-P-ImpVe-Construction-BV2.xls
Impact Vector Assessment for the Nordic Pump CCFs. Jean-Pierre Bento, Version 2, 03 April 2003.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2/Draft 1, 31 October 2002.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, prepared by Tuomas Mankamo, Issue 1, 31 October 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Draft 1+, 25 April 2003.

NAFCS-WN-TM02
Logging Notes of the Impact Vector Assessment in the DG Pilot. Work notes by T. Mankamo and J-P. Bento, 18 September 2002.

NAFCS-WN-TM08
Comments on the ICDE database for the information stored about the Finnish and Swedish pumps, feedback from the impact vector assessment. Work notes by J-P. Bento and T. Mankamo, Version 1, 25 April 2003.

NAFCS-WN-TM10
Instructions for the Impact Vector Construction Sheets. Work notes by T. Mankamo, 11 March 2003.

ICDECG01 Coding Guideline for Centrifugal Pumps. Draft 2.1, 12 February 2001.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
App5.7	**Impact Vector Application to MOV PR19**	**PR19**
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS
Nordisk Arbetsgrupp för CCF studier **NAFCS-PR19**

Title:	**Impact Vector Construction to Motor Operated Valves**
Author(s):	*Tuomas Mankamo*
Issued By:	
Reviewed By:	J-P Bento
Approved By:	Gunnar Johanson
Abstract:	The Impact Vectors are preliminary constructed for the Motor Operated Valves (MOVs) of the Nordic NPPs based on the current ICDE data. The redundant assessment is pending. Foreign MOV events are explored for comparison purpose.
Doc.ref:	Project reports
Distribution	WG, Project WebSite, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Outline	2002-10-14	TM
Draft 1	2003-02-10	TM
Draft 1+	2003-05-19	TM
Issue 1	2003-08-30	TM
Final	2003-08-30	GJ

Contents

Impact Vector Construction to MOVs

1. Introduction

1.1 Objective and Scope

The Impact Vector assessments are made here for the CCF events of Motor Operated Valves (MOVs) in the Nordic NPPs following the procedure developed in the course of the earlier application to diesel generators, so called DG Pilot [NAFCS-PR10]. This application is similar to the recent construction of Impact Vectors for the centrifugal pumps [NAFCS-PR18]. A special aspect in the MOV application is the inclusion of large exposed component populations (an extension of standard concept of CCF group).

The Licensee Event Reports (ROs) were used as additional information for the Swedish events.

The ICDE database was also explored for the foreign MOV CCFs for comparison purpose, see [ICDECG02, NEA/CSNI/R(2001)10].

1.2 QA and documentation

The principal QA action is constituted by the redundant assessment of the Impact Vectors (pending). The produced documents as listed in Table 1.1. See further details of the working procedure, QA and documentation in Section 2.3.

Issue 1 of the application report is changed in the text part for some enhancements. Otherwise the documentation package is same as in the spring 2003. It must be underlined that the redundant assessment of the Impact Vectors and other internal QA actions are still pending, aimed to be completed in the next phase.

Table 1.1 Documents of the application, compare to the reference list.

Document index	Title	Last update
NAFCS-PR19	Impact Vector Construction to MOVs	30-Aug-03
CCF-MOV-Nordic-Descriptions-V1.xls	CCF Event Descriptions for the Pumps in the Nordic MOVs	16-May-03
CCF-MOV-ImpVe-Construction-AV0.xls	Impact Vector Assessment for the Nordic MOV CCFs	17-May-03
CCF-MOV-ImpVe-Construction-BV#.xls	Impact Vector Assessment for the Nordic MOV CCFs (redundant assessment)	Pending
NAFCS-WN-TM13	Comments on the ICDE database for the information stored about the Finnish and Swedish MOVs, feedback from the impact vector assessment	16-May-03
NAFCS-WN-TM14	Logging Notes of the Impact Vector Assessment for the MOV Events	17-May-03

2. Nordic CCF events of MOVs

2.1 Observed valve population, coverage of ICDE data

The observed MOV population of the Nordic NPPs and general exposure data are summarized in Table 2.1. The reactor units are grouped and sorted in the order of country and then in alphabetic order. The observation times for the Swedish units are limited to selected years (table is filled partially only, because the statistical records are not complete in the ICDE database).

Table 2.1 Summary of the ICDE data for the MOVs in the Nordic NPPs (as of February 2001). The cells with missing or incomplete information are left blank.

Units	MOV groups	Remarks	Reactor years	CCCG years	CCF events
B1/B2	52	System-wise groups	24		1
F1/F2					0
F3					0
O1	11	System-wise groups	12		0
O2	16	System-wise groups	12		1
O3	18	System-wise groups	12		0
R1		EP			1
R2/R3/R4	3	EP size 6, 8 and 14	36		2
LO1/LO2					0
OL1/OL2	2	EP size 24 and 24	30		1
Sum					6

2.2 Exposed Populations

A special aspect in the MOV application is that large CCF groups so called Exposed Populations (EPs), which can extend over several systems, are allowed. EP thus extends the concept of standard CCCG. Four of the reported CCF events occurred in EP, see Table 2.1.

The assessment of Impact Vector for EP is basically same as in standard CCF group. Handling of EPs did not cause any extra difficulty in this application, because the number of affected (failed or degraded) components per CCC event was only two at the maximum. If many components in a large EP would be degraded (status not perfectly known intact or failed), the assessment of Impact Vector can get complicated, owing similarity to CCF analysis of highly redundant systems.

2.3 Failure modes

The failure modes of the MOVs are defined as follows [ICDECG02]:

- FO Failure to open
- FC Failure to close
- IL Internal leakage
- EL External leakage

Monitored critical or repair-critical failures in standby state should be treated again strictly separately from latent failures (CCFs), but the reported six CCF events do not contain any monitored ones. Compare to the discussion of this issue in the DG and pump application [NAFCS-PR10, NAFCS-PR18].

2.4 Procedure for Impact Vector construction

The scheme of the Impact Vector construction as developed in the DG Pilot is generally followed with some minor changes, practically same as in the pump application. Again the cornerstone of the QA is the redundant assessment of the Impact Vectors … pending.

The order of assessment flow was …

The current documentation includes:

- The event description material arranged in the workbook:
  [CCF-MOV-Nordic-Descriptions-V1.xls]
- Completed assessments of the two analysts for Analyst A and B, respectively:
  [CCF-MOV-ImpVe-Construction-AV0.xls] and
  [CCF-MOV-ImpVe-Construction-BV#.xls] – pending
- Logging notes of the differences and their resolution [NAFCS-WN-TM14]
- Feedback comments on the information stored to ICDE database, e.g. proposals to supplement event descriptions and align the code classifications for consistency from plant-to-plant [NAFCS-WN-TM13].

The logging notes describe in more detail the difficulties encountered in the analysis of more complicated events and the way of solving the discrepancies. The general insights and lessons learnt will be presented in Section 2.6.

2.5 Summary of the Impact Vector results

The results are summarized in App.1, including high/low bounds. All six reported CCF events are contained on the same table irrespective of the group sizes, which are very dispersed. This aspect renders not meaningful to make similar types of quantitative summary and comparisons as for the DG and pump application, see [NAFCS-PR10, NAFCS-PR18]. A possible way to draw quantitative insights would be the use of CLM for the estimation as it can combine statistics of different group sizes in a consistent way.

2.6 Summary of the engineering insights

Because of the small amount of reported CCF events for the Nordic MOVs the insights are rather limited. One particular generic issue is, however, clearly visible. A substantial part of the CCF events are caused by systematic errors such as:

- Misadjustment of torque limits
- Omission to restore component state after maintenance or test
- Use of inadequate material or spare parts in maintenance or repair

Among the six reported CCF events for the Nordic MOVs four cases can be regarded to belong to systematic errors. The share of systematic errors is similar in the whole statistics of MOVs in the ICDE database (81 events). The events related to torque limiters alone make about 30%, see [NEA/CSNI/R(2001)10].

The latent time is very essential piece of information for the implications of systematic errors. It may not be equal to test interval in many cases but can be shorter – or also longer, e.g. time between refuelling outages. Special emphasis should be paid to the determination of the latent time in the ICDE reporting, including also the description of the factors that affect the latent time. See [NAFCS-WN-TM13].

3. Foreign CCF events of MOVs

Summary statistics from [NEA/CSNI/R(2001)10] is quoted below:

Failure mode		Partial CCF	Complete CCF	All events
FO	Failure to open	14	3	17
FC	Failure to close	8	1	34?
IL	Internal leakage	1	1	1?
EL	External leakage	0	0	9?
No failure mode		1	0	4
In total		24	5	86?

Some strange mismatch in the numbers?

The read-through of the event descriptions show that – in contrast to the difficulties in the DG and pump application – the interpretation of the foreign MOV events could be sufficiently reliable based solely on the ICDE event descriptions. It seems thus possible to make Impact Vector assessments for the foreign MOV events with reasonable effort. This is in fact very desirable in order to supplement the very limited Nordic statistics – pending for continued work.

4. Concluding remarks

The inclusion of Exposed Populations did not produce extra difficulty in this application because the number of affected MOVs were at the most two in the reported cases. In general handling of Exposed Populations may lead to similar complexity as encountered in the CCF analysis of highly redundant systems.

A characteristic feature for the CCFs in MOVs is the large portion of systematic errors. The Impact Vector assessment thus calls for similar skills as HRA.

Recommendations for the next steps (in addition to the evident need to conduct redundant assessment and supplementary QA):

- Trial to use of CLM for the estimation as it can combine statistics of different group sizes in a consistent way
- Impact Vector assessment for the foreign MOV events, which seems possible with sufficient accuracy and reasonable effort – in contrast to the difficulties to undertake this work in the DG and pump application

Appendix 1: Summary Tables of the Impact Vectors

This appendix is shipped as an embedded MS-Excel file "NACFS-PR19-App1-V0.xls". Double-click the icon to open the Excel workbook.

NAFCS-PR19-App 1-V0.xls

References

NAFCS-Programme-R1
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2/Draft 1, 31 October 2002.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 31 October 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Issue 1, 29 August 2003.

ICDECG00 ICDE General Coding Guideline. Rev.3, 21 June 2000.

ICDECG02 Coding Guideline for Motor Operated Valves. Draft 2.1, 20 November 2001.

NEA/CSNI/R(2001)10
Collection and Analysis of CCFs of Motor Operated Valves. ICDE Project Report, prepared by A. Kreuser, V. Schulze and J. Tirira. 27 July 2001.

NAFCS-WN-TM13
Comments on the ICDE database for the information stored about the Finnish and Swedish MOVs, feedback from the impact vector assessment. Work notes by T. Mankamo, Version 0, 16 May 2003.

NAFCS-WN-TM14
Logging Notes of the Impact Vector Assessment for the MOV Events. Work notes by T. Mankamo, Version 0, 17 May 2003.

CCF-MOV-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic MOVs. Version 1, 16 May 2003.

CCF-MOV-ImpVe-Construction-AV0.xls
Impact Vector Assessment for the Nordic MOV CCFs. Tuomas Mankamo, Version 0, 17 May 2003.

CCF-MOV-ImpVe-Construction-BV#.xls
Impact Vector Assessment for the Nordic MOV CCFs. Redundant assessment is pending.

Abbreviations

Acronym	Description
CCCG	Common Cause Component Group
CCF	Common Cause Failure
EP	Exposed Population
TDC	Test and Demand Cycles
BWR	Boiling Water Reactor
DG	Diesel Generator
MOV	Motor Operated Valve
PWR	Pressurized Water Reactor
IAEA	International Atomic Energy Authority
ICDE	International CCF Data Exchange
EPRI	Electric Power Research Institute
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment
SKI	Swedish Nuclear Power Inspectorate
USNRC	United States Nuclear Regulatory Commission

CCF Event List

Index	C01 CCF event identifier	Unit	Year	System	Group Size	Component Impairment
SF01	RO-B2-91/008	B2	91	312 Feedwater System	2	CI
SF02	RO-O2-89/015	O2	89	323 Core Spray System	4	CIWW
SF03	R2 RO 88/08	R2	88	Residual Heat Removal System	6	CIWW ...
SF04	R3 RO 81/21	R3	81	Containment Spray System	8	DDWW ...
SF05	R4 RO 82/05	R4	82	Safety Injection System	14	CCWW ...
SF06	OL2-19004/72298	T2	87	322 Containment Spray System	24	CCWW ...

Version control

Version 0 Working draft 19 May 2003

NACFS - Impact Vector Construction
Nordic MOVs

Summary Irrespective of Group Size

				C03		*C08*	*C11*	*C14*							
				Failure	Group	Comp. Impair-	Shared Cause	Time	Impact Vector - Analyst A						Average
Index	Unit	Year	Description	mode	Type	ment	Factor	Factor	0	1	2	3	4	Sum	multiplicity
SF01	B2	91	Broken gear due to the use of inadequate fibre material	FO	CCCG	CI	H(1)	e(0)	0	1	0	0	0	1	1.00
SF02	O2	89	Valve motor loosened due to short mounting bolts	FO	CCCG	CIWW	H(1)	L(1)	0	0.95	0.05	0	0	1	1.05
SF03	R2	88	Incorrect adjustment of torque limiters due to inadequate procedure	FO	EP	CIW...	H(1)	H(1)	0	0.5	0.5	0	0	1	1.50
SF04	R3	81	Trip on torque limiter at opening, because closed by too high torque	FO	EP	DDW...	H(1)	H(1)	0.5	0	0.5	0	0	1	1.00
SF05	R4	82	Removed fuses from the contactor	FO	EP	CCW...	H(1)	H(1)	0	0	1	0	0	1	2.00
SF06	T2	87	Torque trip caused by inadequate dimensioning	FO	EP	CCW...	H(1)	H(1)	0	0	1	0	0	1	2.00

						Average
Sum Impact Vectors are not presented because the data are split over different Group Sizes	0	1	2	3	4	Sum	multiplicity

NACFS - Impact Ve
Nordic MOVs

Summary Irrespec

			Impact Vector - Analyst B						Average	
Index	Unit	Year	0	1	2	3	4	Sum	multiplicity	Comment
SF01	B2	91								
SF02	O2	89								
SF03	R2	88								
SF04	R3	81								
SF05	R4	82								
SF06	T2	87								
Sum Impact Vector			0	1	2	3	4	Sum	Average multiplicity	
data are split over c										

NACFS - Impact Ve
Nordic MOVs

Summary Irrespec

			High Bound Comparison Impact Vector						Average	Low Bound Comparison Impact Vector						Average
Index	Unit	Year	0	1	2	3	4	Sum	multiplicity	0	1	2	3	4	Sum	multiplicity
SF01	B2	91	0.91	1.08	0.01	0	0	2	1.10	0.9	1.1	0	0	0	2	1.10
SF02	O2	89	0	0.9	0.1	0	0	1	1.10	0	0.9	0.1	0	0	1	1.10
SF03	R2	88	0	0.9	0.1	0	0	1	1.10	0	0.9	0.1	0	0	1	1.10
SF04	R3	81	0.5	0	0.5	0	0	1	1.00	0.25	0.5	0.25	0	0	1	1.00
SF05	R4	82	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
SF06	T2	87	0	0	1	0	0	1	2.00	0	0	1	0	0	1	2.00
Sum Impact Vector data are split over (			0	1	2	3	4	Sum	Average multiplicity	0	1	2	3	4	Sum	Average multiplicity

NACFS - Impact Vector Construction
Nordic MOVs

List of CCF Events

Index	C01 CCF event identifier	Unit	Year	Group Size	Component Impairment
SF01	RO-B2-91/008	B2	91	2	CI
SF02	RO-O2-89/015	O2	89	4	CIWW
SF03	R2 RO 88/08	R2	88	6	CIWW ...
SF04	R3 RO 81/21	R3	81	8	DDWW ...
SF05	R4 RO 82/05	R4	82	14	CCWW ...
SF06	OL2-19004/72298	T2	87	24	CCWW ...

Version control

Version 0	Partially cleaned version	30/01/2003
Version 1	Upgraded version	16/05/2003

Notes

The structure and special notations of this workbook are same as in the pump application, see explanations in [NAFCS-WN-TM09].

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF01		NAFCS Index
C01	RO-B2-91/008		ICDE Event Identifier
	Broken gear due to the use of inadequate fibre material		Short Description
C03	FO		Failure Mode
	312 Feedwater System		System
G6		2	Group size
C04		2	Exposed components
C11	H		Shared Cause Factor
C14	empty		Time Factor
G5	84		Test Interval
G5-2	Sequential		Test Staggering

1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	312V11	15/05/1991	C	1	84	MC
B	312V14	15/05/1991	I	0.1	84	empty

ICDE Event Description and Qualitative Classifications

C05 Event Description

Power level 40%. During start up after manual shutdown it was discovered that 312V11 was inoperable. 312V11 and 312V14 are valves in the main feedwater system and they are both open during normal operation. Investigation of the valve revealed a broken gear in the valve. The gear was made of fibre and similar problems with these gears have occured previously. Therefor it was decided to change the material from fibre to bronze in the valves with fibre gears.

C07 Event Interpretation

Only 312V11 (train 1) was affected by this event. Since the gear in 312V14 (train 2) was exchanged as precautionary measure this is coded as incipient component impairment for 312V14 in accordance with the coding guidelines for MOV.

C09	I	Root cause
C10	HC	Coupling factor(s)
C12	C	Corrective actions

C13 Other

This is a recurrent failure.

CXX Additional Clarifications

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF02	NAFCS Index	
C01	RO-O2-89/015	ICDE Event Identifier	
	Valve motor loosened due to short mounting bolts	Short Description	
C03	FO	Failure Mode	
	323 Core Spray System	System	
G6	4	Group size	
C04	4	Exposed components	
C11	H	Shared Cause Factor	1
C14	L	Time Factor	0.1
G5	30	Test Interval	
G5-2	Sequential	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	312V4	05/07/1989	C	1	30	MA
B	312V5	05/07/1989	I	0.1		MA
C	312V3	05/07/1989	W	0		
D	312V6	05/07/1989	W	0		

ICDE Event Description and Qualitative Classifications

C05 Event Description

During maintenance of the pumps and valves in the emergency core cooling system, one valve failed to open (323V4). When trying to open the valve a ground contact occured.

The motor was mounted witht bolts which were too short to properly attach the motor to the valve. Eventually the motor came off and the power cable was stretched. Two phases then came in contact with ground (short circuit). When examining the redundant valves (323V3, V5 and V6) similar short bolts were discovered on 323V5. The motor however was still attached to the valve and the valve was working. 323V3 and 323V6 had long bolts and the motors were properly attached.

C07 Event Interpretation

Two motors (323V4 and V5) were mounted with bolts which were to short. Only the motor at 323V4 was loose but it was probably only a matter of time before the motor at 323V5 would loosen.

C09	H	Root cause
C10	HQ	Coupling factor(s)
C12	G	Corrective actions

C13 Other

CXX Additional Clarifications

The problem had been present from the begin of operation. The valves in the EP are external isolation valves at the containment boundary

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF03		NAFCS Index
C01	R2 RO 88/08		ICDE Event Identifier
	Incorrect adjustment of torque limiters due to inadequate procedure		Short Description
C03	FO		Failure Mode
	Residual Heat Removal System		System
G6		6	Group size
C04		2	Exposed components
C11	H		Shared Cause Factor
C14	H		Time Factor
G5	365		Test Interval
G5-2	no data		Test Staggering

	1
	1

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	8710 A	13/05/1988	C	1		DE
B	8710 B	13/05/1988	I	0.1		MA

ICDE Event Description and Qualitative Classifications

C05 Event Description

During the normal shut down procedure for refueling the MOVs are opened before start up of RH S. Valve 8701A tripped on torque after 1 s. The valve was opened manually. Later analysis of electric current showed the adjustment of the torque limiter to be incorrect. The trip function is supposed to be blocked until the disc is clear from the closed position. The limiter was observed to act too soon. By further testing in a test bench both open and close torque values was set to low. A similar set up was discovered on valve 8702B.

C07 Event Interpretation

Both valves adjusted with an insufficient procedure, resulting in one failure and one incipient failure, due to wrongly and to low adjusted torque limiters. The combination of failures of 8701A and 8702B leads to loss of suction line.

C09	P	Root cause
C10	MP	Coupling factor(s)
C12	B	Corrective actions

C13 Other

Earlier procedures did not include a bench set up of the torque limiter. All Limitorque actuators are after the incident included in a test bench set up program.

CXX Additional Clarifications

? Latent time not described

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF04		NAFCS Index	
C01	R3 RO 81/21		ICDE Event Identifier	
	Trip on torque limiter at opening, because closed by too high torque		Short Description	
C03	FO		Failure Mode	
	Containment Spray System		System	
G6		8	Group size	
C04		2	Exposed components	
C11	H		Shared Cause Factor	1
C14	H		Time Factor	1
G5	30		Test Interval	
G5-2	Sequential		Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A	9451A	08/12/1981	D	0.5	30	TI
B	9451B	08/12/1981	D	0.5	30	TI

ICDE Event Description and Qualitative Classifications

C05 Event Description

The valves 9451 A and 9451 B tripped on the torque limiter on opening during the specified functional test. After resetting the valves open on the second respectively third attempt. The system valves can be tested at full reactor power, but the reactor was at zero power at the time. The actual valves are situated in the suction lines from containment sump and function as containment isolation valves. There are two valves in each of the two trains. The actual valves were in both trains. And are during an LOCA type accident to be opened by the operators to establish recirculation by connecting the spray pumps suction line to the containment sumps. Earlier preventive maintenance had increased the closing torque to ensure a tight valve. This was done at a refueling outage 6 moths earlier. The higher closing torque requires a higher torque to open the valve. Five prior tests were successful.

C07 Event Interpretation

Maintenance routines fail, as all consequences were not clearly understood.

C09	P	Root cause
C10	MP	Coupling factor(s)
C12	B	Corrective actions

C13 Other

CXX Additional Clarifications

? Criticality of the component state: seems complete failure! Possibly considered degraded because these valve operated manually - and could be opened at 2nd and 3rd attempt.
4 trains x 2 valves = 8 in total

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF05	NAFCS Index	
C01	R4 RO 82/05	ICDE Event Identifier	
	Removed fuses from the contactor	Short Description	
C03	FO	Failure Mode	
	Safety Injection System	System	
G6	14	Group size	
C04	2	Exposed components	
C11	H	Shared Cause Factor	1
C14	H	Time Factor	1
G5	31	Test Interval	
G5-2	Staggered	Test Staggering	

Component Events

Sub	Notes	Date:Time	Impairment		Latent	Detection
A		25/05/1982	C	1	12	TI
B		25/05/1982	C	1	12	TI

ICDE Event Description and Qualitative Classifications

C05 Event Description

During monthly testing of containment isolation valves, the parallel pair of valves between containment and boron injection tank (BIT) didn't open. Investigation found removed fuses and closed breakers. The design makes it impossible to detect broken or removed fuses when the breaker is closed there were no indication. The breakers was closed the plant went to state of operation No 3. During later investigation no document during the time between know function of the valve and closing of breaker specified the removal of fuses. The operator who closed the breakers states that he probably forgot to check the fuses due to workload.
States of operation during latent failure time have been 2 and 3 Start up and Hot standby no power production.

C07 Event Interpretation

This is a typical operator mistake and no actual fault in the MOVs. The incident is reported as fuses are within the component boundaries (ICDECG02/199-02-24 p3.)

C09	P	Root cause
C10	OP	Coupling factor(s)
C12	A	Corrective actions

C13 Other

Procedures for removal of fuses or not, when red tagging a load breaker, was not documented. So if the fuses was removed or not then depending on the individual operator. The corrective actions included a documented definition of activities when red tagging a breaker.

CXX Additional Clarifications

It remains unclear whether the inoperability of the valves had been detected in a start-up test in a normal plant start-up, or had staid latent up to next scheduled periodic test.

Event Description Sheet

Upgraded version, 16 May 2003

Principal Event Data

	SF06		NAFCS Index
C01	OL2-19004/72298		ICDE Event Identifier
	Torque trip caused by inadequate dimensioning		Short Description
C03	FO		Failure Mode
	322 Containment Spray System		System
G6		24	G10 Exposed Population (G6 x S2)
C04		24	Exposed components
C11	H		Shared Cause Factor 1
C14	H		Time Factor 1
G5	30		Test Interval
G5-2	Staggered		Test Staggering

Component Events

X	Notes	Date:Time	Impairment		Latent	Detection
	322V105	03/05/1987	C	1	30	TA
	322V205	03/05/1987	C	1	30	TA
	Component event data for the intact states (W) are truncated					

ICDE Event Description and Qualitative Classifications

C05 Event Description

OL2: Refuelling outage (30.4-15.5.87). Valves V105 and 322 V205 failed to open due to torque trip in periodic tests on 3.5.1987 (03:00). Valve stiffness (box packing/stem) was assumed to be the cause for the torque trip. Lubrication of stem was done as repair-action after unsuccessful tests. In re-test (3.5) valves worked correctly. Later redimensioning calculations (1992 and 1996) showed some underdimensioning of these actuators.

C07 Event Interpretation

Combination of underdimensioning (design) of actuator/ torque limits and at the same time valve stiffness (lubricant drying/ packing friction). Note: The corrective action is coded in this case class B but also C (design modification) is applicable.

C09	D	Root cause
C10	HC	Coupling factor(s)
C12	B	Corrective actions

C13 Other

CXX Additional Clarifications

The degraded component states were present only 30 days, to be taken into account in the quantification

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF01	
C01	ICDE Event Identifier	RO-B2-91/008	
	Short Description	Broken gear due to the use of inadequate fibre material	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	e	0
G5	Test Interval	84	
G5-2	Test Staggering	Sequential	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
	312V11	15/05/1991	C	1	84	MC	
	312V14	15/05/1991	I	0.1	84	empty	

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2			Element sum
1.	Considered as plain single failure	1		1				1
2.								0
Net Impact Vector			0	1	0			1
		Average multiplicity					1	

Impact Vector Assessment

The risk of 312V14 to fail concurrently is considered small, thus negligible CCF risk.

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF02	
C01	ICDE Event Identifier	RO-O2-89/015	
	Short Description	Valve motor loosened due to short mounting bolts	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	L	1
G5	Test Interval	30	
G5-2	Test Staggering	Sequential	

Component Events

Sub	Component	Date	Impairment		Latent	Detection	Notes
	312V4	05/07/1989	C	1	30	MA	
	312V5	05/07/1989	I	0.1		MA	
	312V3	05/07/1989	W	0			
	312V6	05/07/1989	W	0			

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Only 312V4 would fail, but 312V5 would survive in a demand	0.95		1				1
2.	Both 312V4 and 312V5 would fail in a demand	0.05			1			1
Net Impact Vector			0	0.95	0.05	0	0	1
		Average multiplicity					1.05	

Impact Vector Assessment

The loosening of the motor part seems to have been quite a slow process. Thus only small risk judged for concurrent actual failure.

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF03	
C01	ICDE Event Identifier	R2 RO 88/08	
	Short Description	Incorrect adjustment of torque limiters due to inadequate procedure	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	365	
G5-2	Test Staggering	no data	

Component Events

X	Component	Date	Impairment		Latent	Detection	Notes
	8710 A	13/05/1988	C	1		DE	
	8710 B	13/05/1988	I	0.1		MA	
	...		W				
	Component event data for the intact states (W) are truncated						EP size = 6

Event Description

Scenario		Weight	Impact vector					Element sum
			0	1	2	3	4	
1.	Only 8710A would fail, but 8710B would survive in a demand	0.5		1				1
2.	Both 8710A and 8710B would fail in a demand	0.5			1			1
Net Impact Vector			0	0.5	0.5	0	0	1
		Average multiplicity					1.5	

Impact Vector Assessment

It seems about fifty-fifty changes that the other valve had also been inoperable. The event description does not give evidence to support the low impairment value for valve 8710B. Additional clarifications should be asked from the plant expert for a more accurate assessment.

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF04	
C01	ICDE Event Identifier	R3 RO 81/21	
	Short Description	Trip on torque limiter at opening, because closed by too high torque	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30	
G5-2	Test Staggering	Sequential	

Component Events

X	Component	Date	Impairment		Latent	Detection	Notes
	9451A	08/12/1981	D	0.5	30	TI	
	9451B	08/12/1981	D	0.5	30	TI	
	...		W				
	Component event data for the intact states (W) are truncated						EP size = 8

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Both valves would be successfully opened in a demand	0.5	1					1
2.	One and only one of the valves would be successfully opened	0		1				
3.	No success to open either of the valves in a demand	0.5			1			1
Net Impact Vector			0.5	0	0.5	0	0	1
		Average multiplicity					1	

Impact Vector Assessment

It seems that component impairment values are initially set to 'D' as the possibility of succeeding in repeated opening attempts are credited. Following this, the chances of success for the first valve is set to 0.5, and complete coupling is assumed between the operator action for the second valve (thus Scenario 2 obtains zero weight). Additional clarifications should be asked from the plant expert about the timing details and role of operating instructions for a more accurate assessment.

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF05	
C01	ICDE Event Identifier	R4 RO 82/05	
	Short Description	Removed fuses from the contactor	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	31	
G5-2	Test Staggering	Staggered	

Component Events

X	Component	Date	Impairment		Latent	Detection	Notes
	8801A	25/05/1982	C	1	12	TI	
	8801B	25/05/1982	C	1	12	TI	
	...		W				
	Component event data for the intact states (W) are truncated						EP size = 14

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Actual CCF of order 2	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
		Average multiplicity					2	

Impact Vector Assessment

The CCF mechanism is specific to overhaul outage and following start-up condition. Compare to 'Additional clarifications' in the event description sheet. Special treatment is needed in the quantification.

The possibility of higher order failure is not considered, because no evidence of significant possiblity that the considered systematic error could have been more extensive. Compare to the initial data about the number of exposed components C04 = 2.

Impact Vector Construction Sheet

Analyst A
Version 0, 17 May 2003

Principal Event Data

	NAFCS Index	SF06	
C01	ICDE Event Identifier	OL2-19004/72298	
	Short Description	Torque trip caused by inadequate dimensioning	
C03	Failure Mode	FO	
C11	Shared Cause Factor	H	1
C14	Time Factor	H	1
G5	Test Interval	30	
G5-2	Test Staggering	Staggered	

Component Events

X	Component	Date	Impairment		Latent	Detection	Notes
	322V105	########	C	1	30	TA	
	322V205	########	C	1	30	TA	
	...		W				
	Component event data for the intact states (W) are truncated						EP size = 24

Net Impact Vector

Scenario		Weight	Impact vector 0	1	2	3	4	Element sum
1.	Actual CCF of order 2	1			1			1
2.								0
Net Impact Vector			0	0	1	0	0	1
		Average multiplicity					2	

Impact Vector Assessment

The possibility of higher order failure is not considered, because no evidence of significant possiblity that the considered generic problem had been active for more valves, even though the initial data about the number of exposed components C04 = 24. Additional clarifications should be asked from the plant expert about the observed condition of the valves in the whole EP.

Work Notes

Comments on the ICDE database for the information stored about the Finnish and Swedish MOVs, feedback from the Impact Vector assessment

Date/Version: 16 May 2003 Version 0, TM

Prepared by: Tuomas Mankamo Avaplan Oy

These notes collect database-specific detailed comments from the Impact Vector assessment for Motor Operated Valves (MOVs), see the event descriptions and selected fields extracted from the ICDE database in [CCF-MOV-Nordic-Descriptions-V1.xls]. The overall procedure followed is described in [NAFCS-PR19]. Compare also to the details of Impact Vector assessments in [CCF-P-ImpVe-Construction-AV1.xls], and to the specific difficulties as documented in the logging notes for the Impact Vector assessment [NAFCS-WN-TM14].

General comments

Similarly as in the earlier applications to the diesel generators and centrifugal pumps, the event descriptions lack in many cases essential details for the Impact Vector assessment.

The detailed comments are grouped per plant in order to facilitate the experience feedback from lessons learned, see the following table. The final section summarizes comments on some generic problems.

Plant	Event	
Oskarshamn	SF02	RO-O2-89/015
Ringhals	SF03	R2-RO88/08
	SF04	R3-RO81/21
	SF05	R4-RO82/05

Oskarshamn

Index	C01: ICDE event ID	Proposal/comment
SF02	RO-O2-89/015	Detection should be 'TI', periodic test

According to RO the problem was detected in a periodic test.

Ringhals

Index	C01: ICDE event ID	Proposal/comment
SF03	R2-RO88/08	Latent time is missing.

The information about latent time is vital for this case, presumably one year, i.e. incorrect adjustment of the torque limit done in the previous refuelling outage.

Index	C01: ICDE event ID	Proposal/comment
SF04	R3-RO81/21	The reasoning for the component impairment values should be presented.

Criticality of the component state seems at the first glance as complete failure! Possibly considered degraded because these valve are in actual demand operated manually - and could be opened after repeated attempts.

Index	C01: ICDE event ID	Proposal/comment
SF05	R4-RO82/05	The factors determining the latent time should be explained.

It remains unclear whether the inoperability of the valves had been detected in a start-up test in a normal plant start-up, or had staid latent up to next scheduled periodic test. This is crucial information for a proper treatment of the case in quantification.

Generic issues

Because of the small amount of reported CCF events for the Nordic MOVs the insights are rather limited. One particular generic issue is, however, clearly visible. A substantial part of the CCF events are caused by systematic errors such as:

- Misadjustment of torque limits
- Omission to restore component state after maintenance or test
- Use of inadequate material or spare parts in maintenance or repair

Among the six reported CCF events for the Nordic MOVs four cases can be regarded to belong to systematic errors. The share of systematic errors is similar in the whole statistics of MOVs in the ICDE database (81 events). The events related to torque limiters alone make about 30%, see [NEA/CSNI/R(2001)10].

The latent time is very essential piece of information for the implications of systematic errors. It may not be equal to test interval in many cases but can be shorter – or also longer, e.g. time between refuelling outages. Special emphasis should be paid to the determination of the latent time in the ICDE reporting, including also the description of the factors that affect the latent time.

References

NAFCS-PR19
Impact Vector Construction to the MOVs. Topical Report NAFCS-PR18, Draft 1+, 25 April 2003.

NAFCS-WN-TM14
Logging Notes of the Impact Vector Assessment for the Pump Events. Work notes by T. Mankamo Version 0, 17 May 2003.

CCF-MOV-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic MOVs. Version 1, 16 May 2003.

CCF-MOV-ImpVe-Construction-AV0.xls
Impact Vector Assessment for the Nordic Pump CCFs. Tuomas Mankamo, Version 0, 17 May 2003.

NEA/CSNI/R(2001)10
Collection and Analysis of CCFs of Motor Operated Valves. ICDE Project Report, prepared by A. Kreuser, V. Schulze and J. Tirira. 27 July 2001.

Work Notes

Logging Notes of the Impact Vector Assessment for the Nordic MOVs

Date/Version: 17 May2003 Version 0
…

Prepared by: Tuomas Mankamo Avaplan Oy TM

1 Assessment Process and Technical Documentation

The principal milestones are described in Table 1. The flow of assessment was …

The event descriptions were discussed between the analysts before the first assessment round in order to identify and handle the most remarkable information deficiencies. The discrepancies at the first assessment round were thus reduced. …

Table 1 Milestones of the Impact Vector assessment for the pumps.

Date	Description
28 January 2003	Exchange of the extracted ICDE data, discussion of questions and needed clarifications on 11 February 2003
17 May 2003	Partially upgraded event description material and preliminary Impact Vector assessments (Version 0, Analyst A only)

The technical documentation of the event descriptions, event analysis and Impact Vector assessment are in this application made fully by the use of MS-Excel, following the same procedure as in the pump application.

Event description workbook

The event description material are arranged in the workbook [CCF-MOV-Nordic-Descriptions-V1.xls], each event on separate description sheet. These sheets quote selected ICDE fields from the following database tables, pertinent for the Impact Vector assessment

- CCF Event Records
- Component Event Records and
- Group Records

Basically, the ICDE data is quoted as such and modifications are limited to correcting evident mistakes or gaps. All modifications are indicated by yellow highlighting of the field cell, and explained by the comment inserted to the cell. Furthermore, field 'CXX: Additional Clarifications' is added to the end of the sheet to contain additional information obtained from the LERs, plant incident reports and by the discussions with the plant experts. This added

information is restricted to objective technical details and facts, or the interpretation/ assessment by the plant experts. Any interpretation or assessment by the analysts will not be mixed here but are presented in the Impact Vector assessment sheets. The corrections and needs of vital additional information to ICDE data are collected in a separate memorandum [NAFCS-WN-TM13].

One practical aspect is that MS-Excel is not capable to handle smoothly long text fields. Therefore longer CXX fields are split into consecutive cells separated by dashed border. Split cells are allowed only for CXX field on the description sheet in order to facilitate later transfer of the information into a relational database, e.g. MS-Access.

Impact Vector construction workbooks

Impact Vector assessments are stored in two workbooks [CCF-MOV-ImpVe-Construction-AV0.xls] and [CCF-P-ImpVe-Construction-BV#.xls, pending] for Analyst A and B, respectively. The layout is similar to the Word document sheets used in the DG Pilot. Some essential event description fields are reproduced from the description workbook. The analyst can change these fields, especially the classifications for Component Impairment Values, Time Factor and Shared Cause Factor with the condition that every change is indicated and arguments explained. See the more specific instructions in these regards in [NAFCS-WN-TM10].

2 Specific Details

A special aspect in the MOV application is that large CCF groups so called Exposed Populations (EPs), which can extend over several systems, are allowed, see Table 2. EP thus extends the concept of standard CCCG.

Table 2 Grouping of the pumps according to normal state.

Group type	Description
CCCG	Standard CCF Component Group inside one system, typically redundant identical components
EP	Exposed Population

A characteristic feature for the CCFs in MOVs is the large portion of systematic errors. The Impact Vector assessment thus calls for similar skills as HRA.

The observations and remarks about assessment details and outcome, which are of general interest regarding the use of the results or methodology, are gathered in Table 3. The comparison type classes of the base and redundant assessment are defined in Table 4. It shows also the count of events for type classes: the more general insights will be discussed in Section 3. Some of the more complicated cases will be discussed in more detail in the following subsections (open questions at this stage).

Table 3 Observations from the Impact Vector assessment. The highlighted indexes in the first column indicate cases, where additional information was essential to complete the ICDE event description.

Case	Group type	Observations	Comparison Type Class
SF01	CCCG		
SF02	CCCG		
SF03	EP		
SF04	EP		
SF05	EP		
SF06	EP		

Inadequate procedure for the adjustment of limit torque, Ringhals 2, 1988

Additional clarifications are desired to understand the possibility of critical misadjustment for the 2nd valve, and for the further valves in the EP. See the details of Case SF03 in [CCF-MOV-Nordic-Descriptions-V1.xls] and [CCF-MOV-ImpVe-Construction-AV0.xls].

Valves closed on too high torque, Ringhals 3, 1981

Additional clarifications are needed about the timing details and role of operating instructions. See the details of Case SF04 in [CCF-MOV-Nordic-Descriptions-V1.xls] and [CCF-MOV-ImpVe-Construction-AV0.xls].

Torque trip caused by inadequate dimensioning, Olkiluoto 2, 1987

Additional clarifications should be asked from the plant expert about the observed condition of the valves in the whole EP (size 24), beyond the two failed ones. See the details of Case SF06 in [CCF-MOV-Nordic-Descriptions-V1.xls] and [CCF-MOV-ImpVe-Construction-AV0.xls].

3 Summary of the Insights

The general conclusion of this application is ...

The count of type classes from the comparison between base and redundant assessment is presented below. The insights are generally much the same as in the DG Pilot, see [NAFCS-PR10, NAFCS-WN-TM02].

Table 4 Comparison type classes (same as in the DG Pilot).

Type class	Description	Count
1	Identical assessment, evident impact	
2	Identical assessment, follows guide example	
3	Identical assessment, consensus reached after discussion of the arguments, typically additional clarification had to be obtained from the plant	
4	Same hypothesis structure, differing weights	
5	Differences in hypothesis structure, typically weak degradation cases where one of the analysts considered the chances of higher order failure	
6	Basic differences in the assessment logic, e.g. one of the analysts used a specific causal model or parametric dependence model to support the assessment	
		0

New insights from this application are following:

- Large portion of systematic errors …
- …

The conducted work is restricted to the events as currently stored in the ICDE database, i.e. no completeness verification is performed. Furthermore, so called coincident multiple failures are not covered (not presented in the ICDE data). Compare to the discussion of this issue in [NAFCS-PR03].

References

CCF-MOV-Nordic-Descriptions-V1.xls
CCF Event Descriptions for the Pumps in the Nordic MOVs. Version 1, 16 May 2003.

CCF-MOV-ImpVe-Construction-AV0.xls
Impact Vector Assessment for the Nordic Pump CCFs. Tuomas Mankamo, Version 0, 17 May 2003.

CCF-MOV-ImpVe-Construction-BV#.xls
Impact Vector Assessment for the Nordic Pump CCFs. Redundant assessment is pending.

NAFCS-PR03
Impact Vector Method. Topical Report NAFCS-PR03, prepared by Tuomas Mankamo, Issue 2/Draft 1, 31 October 2002.

NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, prepared by Tuomas Mankamo, Issue 1, 31 October 2002.

NAFCS-PR17
Impact Vector Construction. Topical Report NAFCS-PR17, prepared by Tuomas Mankamo, Draft 1, 31 October 2002.

NAFCS-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Draft 1+, 25 April 2003.

NAFCS-WN-TM02
Logging Notes of the Impact Vector Assessment in the DG Pilot. Work notes by T. Mankamo and J-P. Bento, 18 September 2002.

NAFCS-WN-TM10
Instructions for the Impact Vector Construction Sheets. Work notes by T. Mankamo, 11 March 2003.

NAFCS-WN-TM13
Comments on the ICDE database for the information stored about the Finnish and Swedish MOVs, feedback from the impact vector assessment. Work notes by T. Mankamo, Version 0, 16 May 2003.

ICDECG02 Coding Guideline for Motor Operated Valves. Draft 2.1, 20 November 2001.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
App5.8	**A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15**	**PR15**
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title: **A Statistical Method for Uncertainty Estimation of CCF Parameters**

Author(s): Kurt Pörn
Issued by: Pörn Consulting
Reviewed by: Tuomas Mankamo
Approved by: Gunnar Johanson

Abstract: This report presents a statistical estimation model proposed to be used to estimate CCF rates and developed within the scope of the NAFCS program (Nordic Workgroup for CCF Analyses). The estimation is based on statistical evidence of common cause basic events that are expressed in the form of impact vectors. In case of events the assessment of which is uncertain a mutually exclusive set of hypotheses are assigned to alternative impact vectors. In this paper we briefly describe how this data interpretation uncertainy is treated in the statistical analysis.

The estimation model proposed is founded on a two-stage Bayesian method, similar to the method developed for the [T-Book] application. Due to the uncertainty and meagreness of CCF data special focus is put on the likelihood function and the choice of a prior distribution for the hyperparameters. The model is tentatively applied to some of the Nordic diesel generator data collected and evaluated within the scope of the NAFCS program.

Doc.ref: Project reports
Distribution: WG, Project Website, Project archive
Confidentiality Control: Public

Revision control:

Version	Date	Initial
Outline	2002-11-30	KP
Draft 1	2003-02-28	KP
Final	2003-08-12	KP

Contents

1 Introduction

In this report some basic assumptions and ideas are presented about a possible model for the estimation of CCF parameters based on statistical evidence expressed in the form of impact vectors. These ideas are discussed and applied on pilot data collected and evaluated for Nordic diesel generators [NAFCS-PR10] in the CCF quantification project within the scope of the NAFCS program (Nordic Workgroup for CCF Analyses). The CCF parameter we have focussed on is the rate of k/n-events in a n-redundant system or common cause component group (CCCG) of size n. We presuppose the existence of CCF event data covering the experience of one or more CCCGs of size n, where the interpretation or assessment uncertainty is expressed in the form of various hypotheses of alternative impact vectors. In this report we describe how the likelihood function is calculated and we also propose some alternative non-informative prior distributions of the hyperparameters.

The basic features of the concept of Impact Vector are presented in [NAFCS-PR03]. Alternative estimation efforts similar to those discussed in this report have been made by [Vaurio 1994].

2 Some basic definitions and assumptions

Let us reproduce the definitions of some basic concepts used by [Vaurio 1994]:

k/n-event = event able to fail exactly k trains in a system with n trains

$\Lambda_{k/n}$ = rate of k/n-events in a n-redundant system or CCCG

$\lambda_{k/n}$ = rate of CCF events failing specific k trains or channels in a n-redundant CCCG

$N_{k/n}(m)$ = number of k/n-events for system m in exposure time T_m

To make the concepts above more concrete let us assume a 3-redundant system consisting of components a, b and c. Then e.g. a 2/3-event is any event where exactly 2 components fail, i.e. the component group ab, ac or bc fails, while the rate of such events is $\Lambda_{2/3}$. The components of the system are assumed to be mutually homogeneous, which means that the group ab fails equally likely as ac or bc. The failure rate of these groups of specific components is $\lambda_{2/3}$. Thus we can write $\lambda_{2/3} = \lambda_{ab} = \lambda_{ac} = \lambda_{bc}$. From the assumption of homogeneity within the CCCG follows further

$$\Lambda_{k/n} = \binom{n}{k}\lambda_{k/n} \qquad (1)$$

which means that estimates of $\lambda_{k/n}$ can easily be derived from estimates of $\Lambda_{k/n}$.

Another important feature in the estimation process is the assumption of non-homogeneity between the CCCGs. Although seemingly similar systems are grouped on the basis of their type, operating mode, size and capacity there are certainly environmental, operating and maintenace conditions that make it unrealistic to assume complete homogeneity between the systems with regard to the CCF failure rate. The similarities, however, are considered so significant that the treatment of the whole population of the redundant systems considered is deemed beneficial from the statistical or informational point of view.

Recently, a comparative study in the form of a benchmark exercise has been conducted between the T-Book methodology and the German ZEDB approach for estimating component failure rates [Blombach et.al.,2003]. The study showed very clearly that different homogeneity assumptions in the two approaches have a significant impact on the result.

Throughout this paper we prefer to describe CCF vulnerabilities by using various occurrence rates such as $\Lambda_{k/n}$ and $\lambda_{k/n}$ above. From these time related CCF rates it is then relatively easy to derive various CCF probabilities needed in the system fault tree models of a PSA taking into account factors like test strategy, repair policy and system success criteria. Thus the rates $\lambda_{k/n}$ and $\Lambda_{k/n}$ are closely connected to e.g. the subgroup failure probabilities (SGFP) per demand, Peg(k|n), Psg(k|n) and Pes(k|n) respectively, defined in [NAFCS-PR04]:

Peg(k|n) = P(specific k out of n components fail while the other n-k survive)

Psg(k|n) = P(specific k components fail in a CCCG of level n)

Pes(k|n) = P(exactly some k out of n components fail while the other n-k survive)

However, these CCF probabilities can also be estimated directly, without going via failure rates, by using demand related statistical models (see Section 6). Such models require, instead of the exposure times T_m, the knowledge of the number of demands ND_m of each system in addition to the number of k/n-events.

3 Uncertainties in CCF event data

The ideal case is when the failure records are certain. Not seldom, however, there are, just like the case of independent failures, several types of uncertainties associated with the records of multiple failures and with the assessment of the multiple failures in general. Referring to [Mosleh et.al., 1988] a broad classification of the types and sources of uncertainty is as follows:

1. Statistical uncertainty due to limited sample size.

2. Uncertainty due to assumptions of the estimation model.
3. Uncertainty in data gathering, and database development.

The role of uncertainty analysis is to generate a probability distribution of the CCF frequency of interest covering all sources of uncertainty that are relevant in the current application. What is relevant depends on the intended use of the CCF parameter, i.e. the importance of an accurate description of uncertainties, and the form and content of the available database. Also, there are different methods, varying in complexity and accuracy, for handling various types of uncertainty. In the following we give some brief remarks on the different categories of uncertainty listed above.

Statistical uncertainty

Estimating the parameters of interest based on the sample data is always associated with this type of uncertainty. It is usually quantified through probability distributions of estimated parameters (Bayesian methods) or by confidence bounds (classical methods). Statistical uncertainty is treated in most of the computer codes available for parameter estimation.

Estimation model uncertainty

Among model-related uncertainties we can list the following:

(a) Difficulties to determine the testing scheme (staggered vs nonstaggered) applied at plants from which data are collected. The testing scheme has impact on the number of demands on the CCCGs. One approach accounting for this uncertainty is to select the testing strategy that results in the more conservative estimates. Another approach is to mix two distributions representing the different testing schemes.

(b) Assumption of in-homogeneity between the CCCGs even after mapping the generic impact vectors to a specific plant. This group-to-group variability is taken into account by using the two-stage Bayesian estimation method described in this report.

(c) Averaging impact vectors over multiple hypotheses leads to underestimation of the uncertainties, as described in [Pörn, 2001]. The uncertainty analysis method proposed here accounts for the impact of the multiple hypotheses approach by treating all possible combinations of hypotheses.

Data base uncertainty

(a) Incomplete failure reports and event descriptions
(b) Difficulties to identify a shared cause for multiple component failures
(c) Difficulties to specify whether a component has failed or was only degraded, and to what extent the component is impaired
(d) Difficult to state how many components in a CCCG actually failed or should fail at a real demand
(e) Periodic tests do not correspond to real demands

(f) Difficulties to assess the applicability of the sample plants to the target plant, in particular in case of systems of different redundancy level

Many of the uncertainties listed above (the list is certainly not complete) are hard to explicitly quantify. A suitable means for assessing and recording at least a part of these judgements is the impact vector method, described for example in [NAFCS-PR03]. To account for such assessment uncertainties the hypothesis method has been suggested by [Mosleh et al.,1988]. By this method the assessment probabilities or weights are assigned for a mutually exclusive set of hypotheses for each event assessed by the impact vector construction, and these probabilities are explicitly taken into account in the statistical analysis. In this paper we briefly describe how this data interpretation uncertainy can be treated.

If all available CCF data were unambiguous we could estimate the parameter $\Lambda_{k/n}$, for given k and n, by using the T-Book methodology [Pörn, 1996], just as for the estimation of independent failure rates. A characteristic feature of the T-Book approach is its ability to provide a parametric uncertainty estimate encompassing a unit-to-unit variability as well as the statistical uncertainty. Thus the components/systems of the group of interest are assumed to be related to each other, but not identical, from reliability point of view. Thus the method allows pooling of data from various systems and various plants of similar type that we want to treat together from information point of view.

4 Parameter estimation based on uncertain CCF event data

Returning to the question of CCF rates let us now look at the specific problem of estimating $\Lambda_{k/n}$ based on observed but uncertain CCF event data. We assume that the system specific rate parameters $\Lambda_{k/n}$ and $\lambda_{k/n}$ are constant in time which means that the interarrival times of corresponding CCF events are exponentially distributed. In the ideal case of having access to certain and unambiguous data it would be enough to know the observed numbers $N_{k/n}$, i.e. $N_{1/n}$ = number of single failures, $N_{2/n}$ = number of double failures etc., observed during the system exposure time T_m to estimate $\Lambda_{k/n}$. In the following two subsections we describe how the T-Book methodology has to be modified in order to take the data uncertainties into account, where the uncertainties are expressed as impact vectors.

4.1 The likelihood function

Instead of components as in the T-Book application we now look at systems of redundancy level n as the basic units for analysis. Let us assume the following statistical evidence related to k/n-events at M CCCGs of level n. After the impact vector assessment the uncertainty of the data is expressed in terms of the following set of weights or probabilities $w_i(k/n,m)$:

Event i	$w_i(m)$	Exposure time	System or CCCG
1	$w_1(k/n,1)$	T_1	System 1
2	$w_2(k/n,1)$		
.	.		
.	.		
N_1	$w_{N1}(k/n,1)$		(N_1 recorded events)
1	$w_1(k/n,2)$	T_2	System 2
2	$w_2(k/n,2)$		
.	.		
.	.		
N_2	$w_{N2}(k/n,2)$		(N_2 recorded events)
- -			
1	$w_1(k/n,M)$	T_m	System M
2	$w_2(k/n,M)$		
.	.		
.	.		
N_M	$w_{NM}(k/n,M)$		(N_M recorded events)

From the impact vectors concerning all recorded events that have occurred in M systems in total we are now focussing on the assessment probability that the event (i) is a k/n-event, i.e. $w_i(k/n,m)$; $(m=1,\ldots,M, i=1,\ldots,N_m)$. If $w_1(k/n,m) = 1$ the event (1) is completely clear leading to a likelihood $L(\theta|\nu=1)$ where ν is the number of k/n-events and θ denotes the secondary parameters describing some uncertainty distribution. If , on the other hand, $w_1(k/n,m) < 1$ we have two or more hypotheses concerning the event (1) with the probability $1 - w_1(k/n,m)$ that no k/n-event occur, $\nu = 0$. Then we can write the likelihood function for the first recorded event as a linear mixture

$$L(\theta|\nu) = w_1 \cdot L(\theta|\nu=1) + (1- w_1) \cdot L(\theta|\nu=0), \qquad (2)$$

using the brief notation w_1 instead of $w_1(k/n,m)$. The same reasoning can be done for the other recorded events of the current system. After two recorded events we have altogether four different scenarios with the following probabilities and outcomes

$w_1 \cdot w_2$	$\nu = 2$
$w_1 \cdot (1-w_2)$	$\nu = 1$
$(1-w_1) \cdot w_2$	$\nu = 1$
$(1-w_1) \cdot (1-w_2)$	$\nu = 0$

Thus the likehood function for the first two recorded events can be written

$$L(\theta|\nu) = w_1 \cdot w_2 \cdot L(\theta|\nu=2) + [w_1 \cdot (1-w_2) + (1-w_1) \cdot w_2] \cdot L(\theta|\nu=1) + (1-w_1) \cdot (1-w_2) \cdot L(\theta|\nu=0). \quad (3)$$

This procedure is continued for all events recorded for the current system. Assuming that the systems are mutually independent we get the total likelihood function as the product of the systemwise likelihoods.

4.2 A non-informative hyperprior

The non-informative distribution used in T-Code for several versions of the T-Book is [Pörn, 1990]

$$p(\alpha,\beta) = \frac{1}{\alpha\beta(\frac{\beta}{\alpha t}+1)^{½}} \quad (4)$$

[Meyer & Hennings, 1999] generalize this function by defining the following family of hyperpriors

$$p(\alpha,\beta) = \frac{1}{\alpha^u \beta^w (C\frac{\beta}{\alpha}+1)^{\tilde{w}_2}(1+D\frac{1}{\sqrt{\alpha}})^{\tilde{u}_2}} \quad (5)$$

where

$$w = 2 - \tilde{w}_1 - \tilde{w}_2$$
$$u = \frac{1}{2} + \tilde{w}_1 + \tilde{w}_2 - \tilde{u}_1/2 \quad (6)$$

By choosing appropriate values of the parameters $\tilde{u}_1, \tilde{u}_2, \tilde{w}_1$ and $\tilde{w}_2$ we get e.g. Pörn's hyperprior (eq.4), Hora & Iman (1990) and Meyer & Hennings (1999).

Applying hyperprior (eq.4) to the CCF data of the next section results in unrealistically high failure rates. A characteristic feature of these data is that their information content is very weak, which means that the choice of the hyperprior is extremely important.

Deriving the prior (eq.4) in [Pörn, 1990] we started the discussion in terms of the mean failure rate, $\mu=\alpha/\beta$, and the coefficient of variation , $\nu=1/\sqrt{\alpha}$. These parameters were assumed to be a priori independent of each other for the purpose of applying Jeffreys' rule separately to each of them. For $\mu' = \mu \cdot t$ (the expected number of events during the exposure time t) we obtained the distribution

$$p(\mu') \propto [\mu'(1+\mu')]^{-½} \quad (7)$$

Repeating the algebraic derivation of $p(\nu|\mu')$ for various values of μ' we got results that were roughly grouped as follows:

μ'	$p(\nu\|\mu')$	
$\mu' << 1$	$\cong \nu^{0}$	
$\mu' \approx 1$	$\cong \nu^{-1}$	(8)
$\mu' >> 1$	$\cong \nu^{-3/2}$	

These results say that the coefficient of variation , ν, is locally uniform for very small mean values μ', while relatively higher prior probabilities should be assigned lower values of ν for greater mean values μ'. Now our basic assumption was that μ' and ν are a priori independent. However, if μ' really were known, we could utilize the results above as a support for the choice of the non-informative distribution of ν.

In many of the applications we had in mind in case of the T-Book, $\mu' \approx 1$ is rather typical. Thus we chose the middle alternative in (eq.8) leading to the non-informative prior (eq.4). In the current situation with $\mu \cdot t << 1$ it is more relevant to choose $p(\nu) \sim$ c(onstant). Writing (eq.8) in the general form

$$p(\nu|\mu') \propto \nu^{-k(\mu')}, \tag{9}$$

where the exponent $k(\mu')$ varies as is shown above, we return to the original hyperparameters α and β and obtain the following hyperprior

$$p(\alpha,\beta) \approx p(\mu)p(\nu)\frac{1}{\alpha^{1/2}\beta^{2}} \approx \frac{1}{\alpha^{3/2-k/2}\beta(C\frac{\beta}{\alpha}+1)^{1/2}}\ , \tag{10}$$

which also can be written as a member of Meyer's and Hennings' generalized family of hyperpriors (eq.5) where $C = 1/t_a$ and t_a = the average operating time among the CCCGs.

To make the reading easier we name the models in (eq.10) as follows:

Pörn II	$k(\mu') = 0$	(for $\mu' << 1$)	
Pörn I	$k(\mu') = 1$	(for $\mu' \approx 1$)	(11)
Pörn III	$k(\mu') = 3/2$	(for $\mu' >> 1$)	

5 Application to Nordic diesel generator data

5.1 Estimate of CCF rates $\Lambda_{k|n}$

The estimation theory comprising the likelihood function and the non-informative hyperprior described in the previous section has been implemented in a computer code (T-CodeCCF). The code has been developed through modification and improvement of [T-CODE, 1997]. In particular, improved methods for multidimensional integrations have been introduced by incorporating a technique called *recursive stratified sampling* [Press & Farrar, 1990]. T-CodeCCF has tentatively been applied to some of the Nordic CCF event information concerning diesel generators (DG) that has been analysed and presented in [NAFCS-PR10]. The results obtained with T-CodeCCF are briefly presented and discussed in this section.

For the oldest plants, B1/B2 and O1/O2, where the CCCG size is 2, the DG experiences cover up to 40 CCCG years. Only latent failure modes – failure to start or failure to run – are included in this application and treated together. Based on the impact vectors of [NAFCS-PR10, Appendix 1] the following input data, collected in Table 1, are used for the estimation of the CCF rate $\Lambda_{2|2}$. Table 1 contains one line for each recorded event (i), and also one line for each CCCG for which no k/n-event has occurred. The event assessment uncertainty is expressed as probabilities or weights, $w_i(k/2,m)$, k=0,1,2, assigned to various hypotheses about the alternative k/n-events that may occur at a real demand. The exposure time T_m of each CCCG is also included.

Table 1. *The input data used in the estimation of $\Lambda_{2|2}$ for DGs with CCCG size = 2.*

Plant	*CCCG*	*CCCG-size*	*Event i*	T_m	$w_i(k/n,m)$		
"B1",	"B1-DG",	2,	"SF15",	11.,	1.,	0.,	0.
"B1",	"B1-DG",	2,	"SF17",	11.,	0.,	0.9,	0.1
"B2",	"B2-DG",	2,	"SF16",	11.,	0.,	1.,	0.
"O1",	"O1-DG",	2,	"SF20",	9.,	1.,	0.,	0.
"O1",	"O1-DG",	2,	"SF21",	9.,	0.,	0.6,	0.4
"O2",	"O2-DG",	2,	" ",	9.,	0.,	0.,	0.

The CCF rate, $\Lambda_{2|2}$, is estimated applying the models Pörn I and Pörn II. A brief summary of the results is included in Table 3 below. Taking into account the total number of events, "0.5", during 40 CCCG years and the results in Table 3 the Pörn II model seems to be the more reasonable one. A list of fractiles and a graph of the probability density function, are presented in Figure 1, Appendix 1. The extreme skewness of the distribution is readily seen. The graph shows only the rightmost part (about 10 %) of the distribution. The main part of the distribution is characterized by failure rates that are so low that they are without practical interest.

The DGs at the other Nordic plants, with CCCG size = 4, (see Table 2.1 in [NAFCS-PR10]) covering in total 151 CCCG years are treated together. Based

on the impact vectors of [NAFCS-PR10, Appendix 1] the following input data, collected in Table 2, are used for the estimation of the CCF rates $\Lambda_{k|4}$; k=2, 3, 4. The distributions obtained are summarily described in Table 3.

Table 2. *The input data used in the estimation of various CCF rates of k/n-events for DGs with CCCG size = 4.*

Plant	*CCCG*	*CCCG-size*	*Event*	T_m	$w_i(k/n,m)$				
"T2",	"T2-DG",	4,	"SF01",	15.,	0.,	0.8,	0.2,	0.,	0.
"T2",	"T2-DG",	4,	"SF08",	15.,	0.,	0.8,	0.2,	0.,	0.
"T2",	"T2-DG",	4,	"SF12",	15.,	0.779,	0.16,	0.045,	0.013,	0.003
"T1",	"T1-DG",	4,	"SF02",	15.,	0.25,	0.5,	0.25,	0.,	0.
"T1",	"T1-DG",	4,	"SF10",	15.,	0.05,	0.9,	0.05,	0.,	0.
"T1",	"T1-DG",	4,	"SF11",	15.,	0.356,	0.289,	0.198,	0.111,	0.045
"L1",	"L1-DG",	4,	"SF14",	20.,	0.,	0.7,	0.2,	0.05,	0.05
"L2",	"L2-DG",	4,	" ",	20.,	0.,	0.,	0.,	0.,	0.
"F1",	"F1-DG",	4,	" ",	9.,	0.,	0.,	0.,	0.,	0.
"F2",	"F2-DG",	4,	"SF18",	9.,	0.,	0.45,	0.5,	0.05,	0.
"F3",	"F3-DG",	4,	"SF19",	9.,	1.,	0.,	0.,	0.,	0.
"F4",	"F4-DG",	4,	" ",	9.,	0.,	0.,	0.,	0.,	0.
"O3",	"O3-DG",	4,	"SF24",	9.,	1.,	0.,	0.,	0.,	0.
"R1",	"R1-DG",	4,	" ",	9.,	0.,	0.,	0.,	0.,	0.
"R2",	"R2-DG",	4,	"SF25",	9.,	0.,	0.,	0.8,	0.1,	0.1
"R3",	"R3-DG",	4,	"SF26",	9.,	1.,	0.,	0.,	0.,	0.
"R3",	"R3-DG",	4,	"SF27",	9.,	1.,	0.,	0.,	0.,	0.
"R3",	"R3-DG",	4,	"SF29",	9.,	0.,	1.,	0.,	0.,	0.
"R4",	"R4-DG",	4,	"SF28",	9.,	1.,	0.,	0.,	0.,	0.

As in the previous case, both of the models Pörn I and Pörn II have been used to estimate the CCF failure rate $\Lambda_{2|4}$. By a similar reasoning as above we prefer Pörn I in this case. For the failure rates $\Lambda_{3|4}$ and $\Lambda_{4|4}$, estimated on the basis of very meagre statistics, Pörn II is chosen as the most appropriate model. The estimation results are briefly summarized in Table 3.

The distributions obtained are in all cases very skew, which can be seen from the fact that the mean values are greater than the upper (95%) fractiles. This skewness indicates very clearly the rare occurrence of the events we are analyzing. Further, the results in Table 3 are to a great extent dominated by the choice of the hyperprior. The mean values that are underlined are deemed to be the most appropriate ones.

According to (eq.1) there is a simple relation between the multifailure rates above, $\Lambda_{k|n}$, and the $\lambda_{k|n}$, the rate of multiple events failing specific k trains in a n-redundant system. Further, from these latter failure rates it is easy to derive the SGFP Peg(k|n), defined in section 2.

Table 3. *Some distribution characteristics of CCF rates $\Lambda_{k|n}$ for various CCCG populations and k/n-events.*

CCF events/ type of hyperprior	5 %	50 %	95 %	Mean
2/2, Pörn I	0.	0.	1.3E-1	5.58E-2
2/2, Pörn II	0.	0.	1.7E-5	1.24E-2
2/4, Pörn I	0.	0.	2.3E-2	2.26E-2
Pörn II	0.	0.	2.7E-9	5.94E-3
3/4, Pörn II	0.	0.	0.	3.92E-3
4/4, Pörn II	0.	0.	0.	2.50E-3

5.2 Estimation of SGFPs Peg and Psg

Assuming a common test interval T we can write the failure probability Peg(k|n) at the end of the interval as

$$\text{Peg}(k|n) = \lambda_{k|n} \cdot T \qquad (12)$$

Thus there is a linear relation between Peg(k|n) and the multifailure rate $\Lambda_{k|n}$, which means that it is possible to estimate the distribution of the former based on the distribution of the latter.

The probabilities Peg(k|n) can directly be used in the quantification of fault tree models. These probabilities , however, are strongly dependent of the group size due to their definition. Much more invariant are the probabilities Psg(k|n) in the sense that Psg(k|n) ≈ Psg(k|n+1) etc. To enhance the comparison of the estimation method used in this study with other estimates, e.g. the simple maximum likelihood estimates presented in [NAFCS-PR10, Figs. 2.5 and 2.6], we have chosen to compare just the probabilities Psg(k|n) for T = 336 h.

Between Psg(k|n) and Peg(k|n) we have the relation

$$\text{Psg}(k|n) = \sum_{m=k}^{n} \binom{n-k}{m-k} \cdot \text{Peg}(m|n) \qquad (13)$$

Specifically, for n=4 and k=2,3,4 this formula says :

$$\begin{aligned} Psg(2|4) &= Peg(2|4) + 2\cdot Peg(3|4) + Peg(4|4) \\ Psg(3|4) &= Peg(3|4) + Peg(4|4) \\ Psg(4|4) &= Peg(4|4) \end{aligned} \qquad (14)$$

We restrict the comparison to looking at the mean values of the probabilities on the left side of (eq.14), expressed in terms of the corresponding mean values of the probabilities on the right side. With a word of warning for uncertain results, due to the tricky numerics required in the handling of the very skew distributions, we present the following mean values:

E[Psg(2|4)] = 3.2E-4	Mankamo:	Psg(2|4) = 2.1E-4
E[Psg(3|4)] = 1.3E-4		Psg(3|4) = 7.3E-5
E[Psg(4|4)] = 9.6E-5		Psg(4|4) = 5.2E-5

(15)

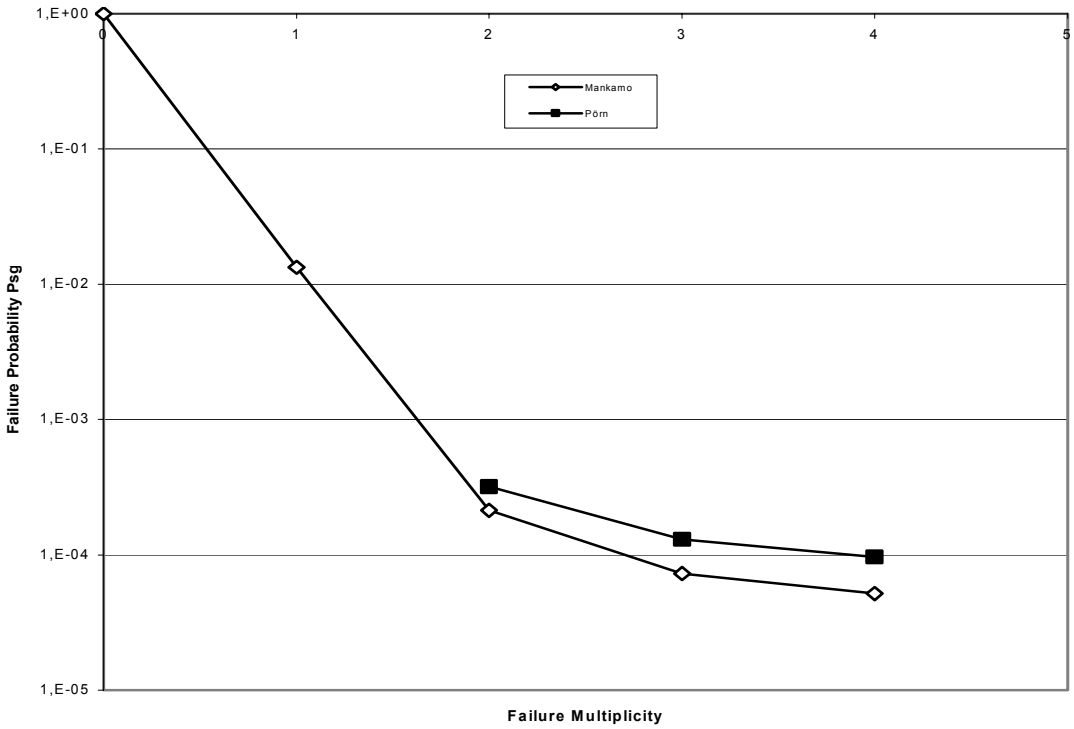


Figure 1. *Diagram comparing probabilities Psg, estimated with maximum likelihood (Mankamo) vs two-stage Bayesian method (Pörn)*

It is to be noted that the analysis above is to some extent a comparison between apples and pears. The maximum likelihood (point) estimates are based on the assumption of homogeneity between the CCCGs while the whole distributions obtained with the two-stage Bayesian estimation method are build on the assumption of non-homogeneity between the CCCGs. Thus the latter estimates take also the group-to-group variability into account. A substantial part of these distributions is, due to the skewness of the distributions, located below the maximum likelihood estimates.

6 Further discussion

The issues brought to further discussion here are largely based on the highly interesting remarks and questions raised by Tuomas Mankamo [WN-TM11] concerning an earlier draft of this report [NAFCS-PR15].

1. Coverage of Uncertainty Types

The estimation of CCF rates presented here is based on evidence expressed in the form of Impact Vectors. As TM points out the impact vector assessment relies largely on engineering judgement where the conditional probability of failure given an actual demand is assessed. The likelihood of various failure events is expressed in the form of a set of hypotheses. TM claims that there is uncertainty also in the assessment process itself , and that this type of uncertainty is not addressed in PR15. To illustrate his ideas TM makes a thinking experiment where the assessment of two CCFs ends up with identical impact vectors despite the fact that the two events are technically very different and despite the fact that the knowledge of the two cases is quite different. However, theoretically at least one could say that if the impact vectors are really determined in a logical and coherent way across the two cases it would not be possible to end up with identical impact vectors (with probabilities of hypotheses included). The greater uncertainty in the case with very unclear impact should appear with more non-zero impact vector elements and accordingly more spread hypotheses compared to the event where the impact is very evident.

2. Correlation Aspects

In my first comments on the impact vector method [Pörn, 2001] I proposed a model – for illustrative purposes - for direct estimation of the CCF probabilities Pes(k|n) in case of homogeneity between the CCCGs . This estimation model is based on a multinomial likelihood - for each demand (event) we have the impact vector telling how many components failed in the group - combined with a conjugate prior (Dirichlet) for the various probabilities Pes(k|n). Then the entire information in the impact vector of the event is used at once, not only the data for a specific k. In this multinomial-Dirichlet model there is an explicit correlation between the failure probabilities Pes(k|n), k=0,..n, in the sense that knowledge about one of these rates influences our knowledge about the others. This correlation arises from the natural condition:

$$\sum_{k=0}^{n} N_{k/n} = ND_m \qquad (16)$$

where the total number of demands, ND_m , is assumed known.

By the method proposed in this report we estimate not probabilities but a failure rate $\Lambda_{k|n}$ for given k. The estimation is based on data of success and failure events of multiplicity k by using exclusively the impact vector values of that order and the corresponding hypothesis weights. Thus the method does not explicitely take into consideration the correlation aspects between events of different multiplicity within a CCCG. On the other side, however, all failure rates $\Lambda_{k|n}$, k=1,..n, are estimated which means that all failure statistics are used in the total analysis. From the parameters $\Lambda_{k|n}$ we go further and estimate e.g. the probabilities Psg(k|n) by (eq.14), where we have an obvious correlation between Psg(k|n) for various k.

3. Comparisons

The use of the basic T-Book methodology proved to be not at all so simple as we had imagined. Numerical difficulties arose due to the weak statistical evidence that is typical for CCF failure records, leading to distributions that are extremely skew. This skewness is quite obvious in Table 3 above. The fractiles denoted by "0." are so low that it is practically meaningless to express them more accurately. The median values e.g. are telling that 50% of the distribution mass is located below very low failure rate values. The skewness property is explained by the fact that many of the CCCGs included in the population have no or very few k/n-events during the exposure time considered.

To judge the reasonableness of the distributions, and the mean values in particular, it is a good practice to make predictions about the expected number of events, E{N(k|n)}, according to the simple formula

$$E\{N(k|n)\} = E\{\Lambda_{k|n}\} \cdot T \,, \qquad (17)$$

where T is the total operating time of all CCCGs in the population. Using the underlined estimates in Table 3 and T = 40 (group size = 2) and T = 151 (group size = 4) years, respectively, result in the following predictions, which may be compared to the "observed numbers" of the CCBE of multiplicity k|n. The differences between "expected" and "observed" can be accepted taking into account that the prediction is based on the assumption of homogeneity.

Of course, one can also raise the question when it is appropriate to use the ambitious model based on the assumption of in-homogeneous populations of CCCGs. For natural reasons, in cases with very little statistics it is difficult, if not impossible, to extract possible variability between the CCCGs.

Table 4. *Predicted number of k/n-events compared to "observed" ones.*

CCF events/ Group size	E{N(k|n)}	"Observed" N(k|n)
2/2	0.50	0.50
2/4	3.41	2.44
3/4	0.59	0.32
4/4	0.38	0.20

If we leave the assumption of in-homogeneity the problem is simple. In that case simple Bayesian method with the non-informative prior $p(\lambda) = \lambda^{-1/2}$ yields the following results, among which both higher and lower mean values can be found compared to those in Table 3.

Table 5. *Some distribution characteristics of CCF rates $\Lambda_{k|n}$ for various CCCG populations and k/n-events, based on the assumption of homogeneity between the CCCGs.*

CCF events/ Group size	5 %	50 %	95 %	Mean
2/2	1.3E-3	1.7E-2	7.5E-2	2.5E-2
2/4	5.1E-3	1.7E-2	4.1E-2	1.9E-2
3/4	1.6E-4	3.4E-3	1.8E-2	5.4E-3
4/4	8.1E-5	2.7E-3	1.6E-2	4.6E-3

7 Concluding remarks

From the CCF event information used as input in this study it is readily seen that there is a certain variation of CCF rates from plant to plant, or as in this case, between the CCCGs. Such a group-to-group variability is allowed in the two-stage Bayesian estimation model developed in this study. In addition it would be possible to calculate system/group specific failure rates and even plant specific rates if there are several CCCGs at the plant under study. The estimation model would be easy to extend to cover such CCF rates.

The two-stage Bayesian method described here, allowing pooling of data over in-homogeneous CCCGs, is basically a further development of the T-Book approach. However, more resources than expected were needed for this development. The CCF statistics are usually very meagre, a matter of fact that

required a more accurate technique for multidimensional integration in the space of hyperparameters. Another problem that was focussed due to the poor statistics was the choice of a suitable non-informative hyperprior, i.e. a prior distribution of the hyperparameters (α and β describing the gamma distribution) containing very weak information.

Applying the hyperprior that has been used in the recent versions of the T-Book resulted in unrealistically high failure rates $\Lambda_{k|n}$, in particular for events of higher order k. Further analysis has shown that the cause of this problem can be found in the choice of a non-informative hyperprior. With reference to [Pörn, 1990] we take this subject into discussion where we argue for different models (Pörn I, II and III) depending on the existing amount of information. One measure of the amount of information is the expected number of events during the exposure time t. This is a form of pre-posterior analysis leading to the choice of a relevant alternative of hyperprior.

There were several reasons why the approach taken here was chosen for the pilot study. One was, as also defended by [Vaurio, 1994], the advantage of having a CCF rate which is related to time irrespective of the number of demands. It is easy to transform the failure rate to various probabilities needed in PSA taking into account the current test strategies. Another reason was the possibility to create an estimation model based on well-tried methods from the area of independent failures. To be able to have access to CCF rates that are estimated by using basically the same statistical philosophy as for independent failure rates is advantageous for PSA practitioners.

References

J. BLOMBACH, R. BUCKERMANN, L. PETTERSSON, K. PÖRN
Calculation of reliability data using two-stage Bayesian models – T-Book/ZEDB Benchmark. To be presented at Jahrestagung Kerntechnik 2003.

S.C. HORA, R.L. IMAN, (1990).
”Bayesian modeling of initiating event frequencies at nuclear power plants”, Risk Analysis vol 10 no 1 102-109.

T. MANKAMO
Impact Vector Method. Topical Report NAFCS-PR03, Issue 2, 2002-10-12.

T. MANKAMO
Model Survey and Review, Topical Report NAFCS-PR04 (Draft 3), 2001-10-24.

T. MANKAMO
Impact Vector Application to Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 2002-10-31.

T. MANKAMO
Comments on the Uncertainty Estimation. Work Notes WN-TM11, 2003-04-01.

W. MEYER, W. HENNINGS
"Prior distribution in two-stage Bayesian estimation of failure rates", Safety and Reliability, Schuëller & Kafka (eds), 1999 Balkema, Rotterdam, 893-898.

A.MOSLEH, K.N. FLEMING, G.W. PARRY, H.M. PAULA, D.H. WORLEDGE & D.M. RASMUSON
Procedures for treating common cause failures in safety and reliability studies, vol.1. US Nuclear Regulatory Commission, NUREG/CR-4780 (EPRI NP-5613), 1988.

W.H. PRESS, G.R. FARRAR
Computers in Physics, vol.4, pp.190-195, 1990.

K. PÖRN (1990).
On Empirical Bayesian Inference Applied to Poisson Probability Models, Linköping Studies in Science and Technology. Dissertations, No.234, Linköping University.

K. PÖRN (1996)
"The Two-stage Bayesian Method Used for the T-Book Application". Reliability Engineering and System Safety, Vol. 51, No.2, Febr, 1996 and SKI Report 95:10

K. PÖRN (2001)
Some Comments on the Report NAFCS-PR03: Impact Vector Method (Draft 2). Work Notes PCM01-4, 2001.

J. VAURIO
Estimation of Common Cause Failure Rates Based on Uncertain Event Data. Technical Note, Risk Analysis, Vol.14, No. 4, 1994.

T-Book, 5th edition.
Reliability Data of Components in Nordic Nuclear Power Plants. Prepared by The TUD Office and Pörn Consulting. Published by The TUD Office, SwedPower AB. (2000).

T-CODE.
A Tool for Bayesian Estimation of Component Failure Rate. User's and Methodology Manual. Pörn Consulting, 1997.

Abbreviations

Acronym	Description
CCBE	Common Cause Basic Event
CCCG	Common Cause Component Group
CCF	Common Cause Failure
DG	Diesel Generator
NAFCS	Nordisk Arbetsgrupp för CCF studier (Nordic Workgroup for CCF Analyses)
PSA	Probabilistic Safety Assessment

Appendix 1: An Example Distribution of CCF rate

GENERIC QUANTILES

.001-PERC = .1229E-14
.010-PERC = .1232E-14
.050-PERC = .1245E-14
.100-PERC = .1262E-14
.200-PERC = .1297E-14
.300-PERC = .1331E-14
.400-PERC = .1365E-14
.500-PERC = .1399E-14
.600-PERC = .1434E-14
.700-PERC = .1468E-14
.800-PERC = .1502E-14
.900-PERC = .1008E-13
.950-PERC = .1735E-04
.990-PERC = .9723E-01
.999-PERC = .1729E+01

PRIOR MEAN = .1240E-01

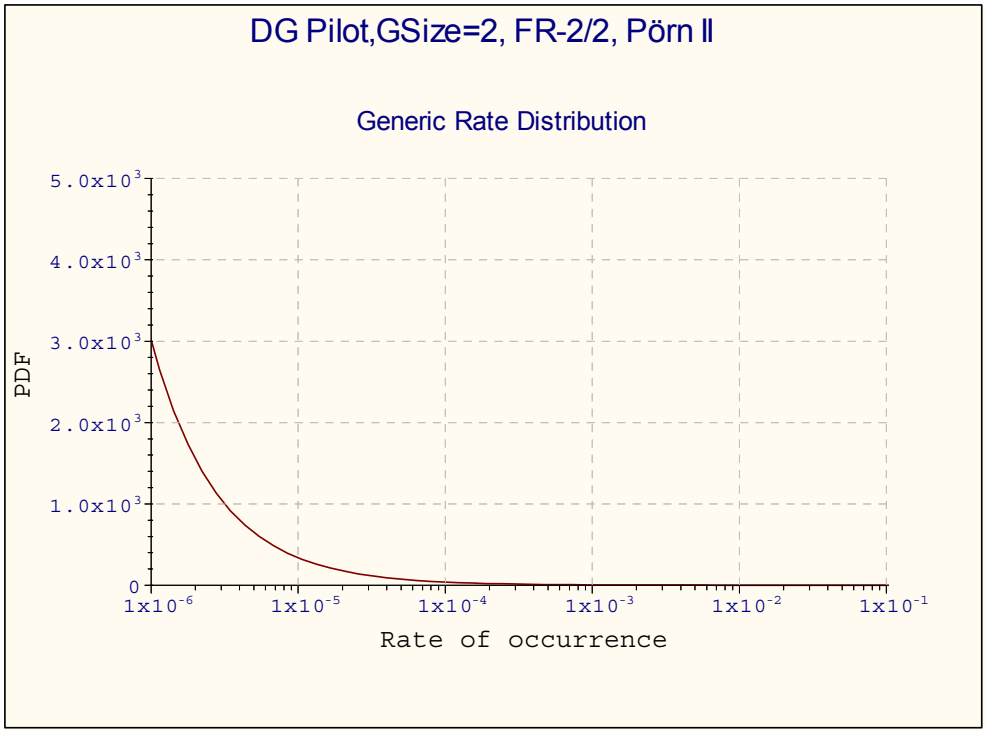


Figure 1. *Distribution of $\Lambda_{2/2}$ for failure modes "failure to run" or "failure to start" at Nordic DGs (Model Pörn II).*

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
App 6	**Literature survey PR06**	**PR06**
Appendix 7	Terms and definitions PR14	PR14
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

Title:	NAFCS: Dependency and CCF Literature Survey		
Author(s):	Per Hellström, RELCON AB		
Issued By:	Per Hellström, RELCON AB		
Reviewed By:	JPB, TM, MK		
Approved By:	Gunnar Johansson		
Abstract:	This report presents a literature survey covering both qualitative and quantitative aspects of dependencies and common cause failures		
Doc.ref:	Project reports		
Distribution	WG, Project WebSite, Project archive		
Confidentiality control:	Public??		
Revision control:	Version	Date	Initial
Created	A1	2002-04-10	PH
	A4	2003-06-26	PH
	Final	2003-06-26	GJ

List of Content

List of tables

Dependency and CCF Literature Survey

1 Introduction

This literature survey is part of the work carried out within the Nordic working group for CCF studies (NAFCS).

The general objective with the literature survey is to present information sources (books, reports, papers, standards, web sites etc) in support of:

1. Qualitative dependency analysis
2. Quantitative CCF analysis
3. Dependency modelling in PSA
4. Collection of dependent failure events
5. Treatment and evaluation of dependent failure events
6. Defence against dependencies

The following references are presented:

- NAFCS report list: All reports in the current project
- NAFCS reference list: All references made from NAFCS reports
- General references: Other reports and literature found during the survey carried out as described in section 4 (SKI, NKS, IAEA, Studsvik library, NRC).

2 NAFCS Reports

Table 1: NAFCS Reports	
No.	Title
PR01	Nordisk Arbetsgrupp för CCF Studier, Project Programme, Rev.1, 19 December 2000.
PR02	Data Survey and Review.
PR03	Impact Vector Method
PR04	Model Survey and Review
PR05	Survey on Defence against Dependent Failures, Compilation and Results of Plant Survey.
PR06	Literature Survey
PR07	Status Report. Nordic Working Group on CCF Studies
PR08	Qualitative analysis of the ICDE-database for Swedish emergency diesel generators
PR09	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs – Survey Task Report
PR10	Impact Vector Application to the Diesel Generators.
PR11	Data survey and review of the ICDE-database for Swedish emergency diesel generators
PR12	Dependency Defence Guidance
PR13	Dependency Analysis Guidance
PR14	Terms, Definitions and Abbreviations
PR15	Uncertainty Estimation of CCF Parameters
PR17	Impact Vector Construction
PR18	Impact Vector Construction for Pumps.
PR19	Impact Vector Construction for Motor Operated Valves
PR20	Defence Assessment in Data
PR21	NAFCS Summary Report

3 NAFCS Report References

This section presents documents referenced in the NAFCS reports:

Table 2: NAFCS Report References

ID	Title
Alm-HCCF	Modellering av för högredundant CCF. Sven Erick Alm, Uppsala Universitet, 27 April 2001.
CA_HredI	Instructions for CCF analysis of high redundancy systems. 2nd Version, T. Mankamo, Avaplan Oy, 22 November 1995. (Part of SKI/RA-26/96)
CCF-Benchmark	Common Cause Failure Benchmark Exercise. Prepared by A. Poucet, A. Amendola and P.C. Cacciabue, ISPRA, November 1986.
CR_ImpV2	Examples on the Relationships between Impact Vector and Component Degradation Values. Work notes, Tuomas Mankamo, Avaplan Oy, 19 November 1996.
CR_ImpVe	Expressing the impact of a CCF mechanism. Work notes, Tuomas Mankamo, Avaplan Oy, 17 September 1996.
CR_ImpVe	Expressing the impact of a CCF mechanism. Work notes, Tuomas Mankamo, Avaplan Oy, 17 September 1996.
CR_RO22x	Sammanställning av kommentarer vid RO-analys för drivdon/styrstavar (BWR). Anmärkningar, 1996-12-30. Part of SKI/RA-26/96.
CR-Alm-Review	Response on Alm's Review of Extended Common Load Model. Tuomas Mankamo, 28 November 2001.
CR-Combinatorics	Forsmark 1 and 2, evaluation of control rod failures [SPC 99 –048] – comments and remarks on the probability calculation and rod combinations. Tuomas Mankamo, Avaplan Oy, 17 August 2001.
CRDA-Agenda-011129	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs - Survey Task. Working Meeting on 29 November 2001, Stockholm
CR-SPC-99-048	Kommentarer till SPC 99-048. T. Mankamo, Avaplan Oy, 10 August 2001.
DGs-CCFA	CCF Analysis of Diesel Generators, Olkiluoto 1 and 2 Experience 1983-1997. Work report prepared by T. Mankamo, Rev. 07 April 1999.
DGTS_B92	Test strategies for standby diesel generators. IAEA Technical Committee Meeting on Advances in Reliability Analysis and PSA, Budapest, 7-11 September 1992. Proceedings
ECLM_Pub	Mankamo, T., Extended Common Load Model, A tool for dependent failure modeling in highly redundant structures. Manuscript, 15 February 1995, 10 February 2001
EPRI-NP 3967	Classification and Analysis of Reactor Operating Experience Involving Dependent Events. Prepared by K.N. Fleming and A. Mosleh, PLG 1985
F1/F2-PSA	PSA of Forsmark 1 and 2. Forsmarks Kraftgrupp AB.
HiDep	HiDep, CCF Analysis Toolbox, Version 2.4. Avaplan Oy, 2001.
HR_CCFRe	High redundancy structures, CCF models review. Work report prepared by Mankamo, T., Avaplan Oy, 31 December 1990. A companion document to SKI TR-91:6.
IAEA 50-P-7	IAEA; Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants; IAEA Safety Series 50-P-7
IAEA 50-SG-D5	IAEA; Extreme Man-Induced Events in Relation to Nuclear Power Plant Design – A Safety Guide; IAEA Safety Series 50-SG-D5; 1982
IAEA 50-SG-S11A	IAEA; Extreme Meteorological Events in Nuclear Power Siting, Excluding Tropical Cyclones – A Safety Guide; IAEA Safety Series 50-SG-S11A; 1981
IAEA 50-SG-S9	IAEA; Site Survey for Nuclear Power Plants – A Safety Guide; IAEA Safety Series 50-SG-S9; 1984
IAEA-CCF-DA	Procedure for CCF Data Analysis in PSA. IAEA-J4-97-CT-1002, Working Draft, March 1998
IAEA-J4-97-CT-1002	IAEA; Procedure for CCF Data Analysis in PSA. IAEA-J4-97-CT-1002, Working Draft, March 1998
IAEA-TECDOC-648	IAEA; Procedures for Conducting CCF Analysis in PSA; IAEA-TECDOC-648, 1992
ICDECG00 Rev 3	ICDE General Coding Guideline. Rev.3, 21 June 2000.

Table 2: NAFCS Report References	
ID	Title
ICDECG00 Rev 4	ICDE Coding Guidelines, ICDECG00, revision 4, October 2000.
ICDECG01	Coding Guideline for Centrifugal Pumps. Draft 2.1, 12 February 2001.
ICDECG02	Coding Guideline for Motor Operated Valves. Draft 2.1, 20 November 2001.
ICDE-S-EdF	Vasseur D., Voicu A., Mankamo T., Bonnet C and Dewailly J., CCF Analysis in Progress at EdF. Overview of EdF Involvement in CCF Analysis, e.g. Control Rod Application. ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, Stockholm, 12-13 June 2001.
ICDE-S-ImpVe	Mankamo, T., Impact Vectors–Construction and Linkage of CCF Data to Quantification. ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, 12-13 Stockholm, 2001.
ICDE-S-Vaurio	From Failure Rate to CCF-Rates and Basic Event Probabilities. Presentation by J.K. Vaurio, ICDE Seminar and Workshop on Qualitative and Quantitative Use of ICDE Data, Stockholm, 12–13 June 2001.
INEL-95/0035	Emergency Diesel Generator Power System Reliability 1987-1993. Prepared By G.M. Grant, et.al., February 1996.
ISBN 3-88583-015-X	Gesellschaft für Reaktorsicherheit; Deutsche Risikostudie Kernkraftwerke; Fachband 4; Einwirkungen von außen (einschließlich anlageninterner Brände); GRS; ISBN 3-88583-015-X; 1980
NEA/CSNI/R (95)11	NEA/CSNI; Knowledge Base for Emergency Core Cooling System Recirculation Reliability; NEA/CSNI/R (95)11; 1996
NEA/CSNI/R(2001)10	Collection and Analysis of CCFs of Motor Operated Valves. ICDE Project Report, prepared by A. Kreuser, V. Schulze and J. Tirira. 27 July 2001.
NEA/CSNI/R(99)2	Collection and Analysis of CCFs of Centrifugal Pumps. ICDE Project Report, prepared by ??. 29 February 2000.
NKA/RAS-470	Hirschberg, S. (Ed.), Dependencies, human interactions and uncertainties in PSA. Final Report of the NKA/RAS-470 project, NORD 1990:57 (1990).
NPSAG-CRDAs-USO	Outline for the Utility Survey. Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs. T. Mankamo, 11 September 2001.
NUREG 1407	USNRC; Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities; NUREG 1407, 1991
NUREG/CP-0104	Bohn, M.P.; Lambright, J.A.; External event analysis methods for NUREG-1150; USNRC; NUREG/CP-0104
NUREG/CR-1278	Swain, A.D.; Guttman, H.E.; Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, 1983
NUREG/CR-2815-Vol.1	Bari, R.A.; Buslik, A.J.; Cho, N.Z. Et al; Probabilistic safety analysis procedures guide. Sections 1-7 and appendices. Volume 1, Revision 1.; USNRC; NUREG/CR-2815-Vol.1-Rev.1; 1985
NUREG/CR-2815-Vol.2-	McCann, M.; Reed, J.; Ruger, C.; Shiu, K.; Teichmann, T.; Unione, A.; Youngblood, R.; Probabilistic safety analysis procedures guide, Sections 8-12. Volume 2, Rev. 1.; USNRC; NUREG/CR-2815-Vol.2-Rev.1; 1985
NUREG/CR-4550, Vol.3	Bertuccio, R.C. et.al.; Analysis of Core Damage Frequency: Surry, Unit 1, Internal Events; NUREG/CR-4550, Vol.3., Rev.1, April 1990.
NUREG/CR-4550, Vol.6	Drouin, M. T. et.al.; Analysis of Core Damage Frequency: Grand Gulf, Unit 1, Internal Events; NUREG/CR-4550, Vol.6., Rev.1, August 1989.
NUREG/CR-4780	Mosleh, K.N. Fleming, G.W. Parry, H.M. Paula, D.H. Worledge & D.M. Rasmuson, Procedures for treating common cause failures in safety and reliability studies, vol.1. US Nuclear Regulatory Commission, NUREG/CR-4780 (EPRI NP-5613), 1988.
NUREG/CR-4839	Ravindra, M.K.; Banon, H.; Methods for external event screening quantification: Risk Methods Integration and Evaluation Program (RMIEP) methods development; USNRC; NUREG/CR-4839; 1992
NUREG/CR-4840	Bohn, M.P.; Lambright, J.A.; Procedures for the external event core damage frequency analyses for NUREG-1150; USNRC; NUREG/CR-4840; 1990
NUREG/CR-5042	Kimura, C.Y.; Prassinos, P.G.; Evaluation of external hazards to nuclear power plants in the United States: Other external events; USNRC; NUREG/CR—5042-Suppl.2; 1989
NUREG/CR-	Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and

Table 2: NAFCS Report References	
ID	Title
5485	F.M.Marshall for USNRC, November 1998.
NUREG/CR-5497	CCF Parameter Estimations. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD, October 1998
NUREG/CR-5500v1	Reliability Study: Auxiliary/Emergency Feedwater System, 1987-1995. Prepared by J.P.Polowski, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.1., August 1998.
NUREG/CR-5500v2	Reliability Study: Westinghouse Reactor Protection System, 1984-1995. Prepared by S.A.Eide, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.2., April 1999.
NUREG/CR-5500v3	Reliability Study: General Electric Reactor Protection System, 1984-1995. Prepared by S.A.Eide, et.al., Idaho National Engineering and Environmental Laboratory. USNRC Report NUREG/CR-5500, Vol.3., February 1999.
NUREG/CR-6268v1	Common Cause Failure Database and Analysis System: Overview. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.1., June 1998.
NUREG/CR-6268v2	Common Cause Failure Database and Analysis System: Event Definition and Classification. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.2., June 1998.
NUREG/CR-6268v3	Common Cause Failure Database and Analysis System: Data Collection and Event Coding. Prepared by F.M.Marshall, A.Mosleh and D.M.Rasmuson. USNRC Report NUREG/CR-6268, Vol.3., June 1998.
NUREG/CR-6268v4	Common Cause Failure Database and Analysis System: CCF Software Reference Manual. Prepared by K.J. Kvarfrdt, M.J. Cebull, S.T. Wood and A.Mosleh. USNRC Report NUREG/CR-6268, Vol.1., June 1998.
O2-PSA	PSA of Oskarshamn 2. OKG Aktiebolag
Olkiluoto-PSA	PSA of Olkiluoto 1 and 2. Teollisuuden Voima Oy.
PCM01_4	Some Comments on the Report NAFCS-PR03: Impact Vector Method (Draft 2). Prepared by K.Pörn, 12 October 2001
Pumps-CC	CCF Analysis of Pumps, Olkiluoto 1 and 2 Experience 1983-1995. Work report prepared by T. Mankamo, 14 May 1997.
RESS_HiD	Mankamo, T. & Kosonen, M., Dependent failure modeling in highly redundant structures - application to BWR safety valves. SRE-Symposium 1988, Västerås, October 10-12, 1988. Enhanced manuscript published in Rel. Eng. and System Safety 35(1992)235-244
Risk Analysis, Vol.14, No. 4	Estimation of Common Cause Failure Rates Based on Uncertain Event Data. Technical Note, Risk Analysis, Vol.14, No. 4, 1994. J. Vaurio
RS-ThM 98	Relcon AB; Risk Spectrum – Theory Manual; Relcon AB, 1998
RPC 88-160	Jacobsson, P.; Sensitivity Studies on Diesel Generator and Pump CCF Data in the Swedish PSA:s; ABB Atom Report RPC 88-160, December 1988.
RPC 91-57	Defences against CCFs and generation of CCF data, pilot study for DGs, quantitative analysis. Staffan Björe, ABB Atom AB, Report RPC 91-57, 15 October 1991
RS_SweDB	BWR/Reactor shutdown systems, CCF data base, Swedish experience 1983-1995. Work report, T. Mankamo, Avaplan Oy, 30 December 1996. Part of SKI/RA-26/96.
RS_WWExp	World-wide BWR experience on CCFs affecting reactor scram function. Work report, Avaplan Oy, 30 November 1996. Part of SKI/RA-26/96.
RS-PSA99	T. Mankamo, Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Int. Topical Meeting of Probabilistic Safety Assessment PSA'99, August 22-26, 1999, Washington, D.C.
RS-ThM 94	Risk Spectrum Theory Manual. Ulf Berg, Relcon AB, Version 2.1, April 1994.
SHACAM	Mankamo, T., SHACAM, Shared Cause Model of Dependences - A review of the Multiple Greek Letter Method and a modified extension of the Beta-factor Method. Avaplan Oy, 28 March 1985.
SKI 2002:27	Knochenhauer, M, Louko, P; Guidance for External Events Analysis; SKI Report 2002:27
SKI 90:3	Johansson, G. (editor); Projekt SUPER-ASAR, Slutrapport fas II; SKI Technical Report 90:3
SKI 95:10	K. Pörn, "The Two-stage Bayesian Method Used for the T-Book Application". Reliability Engineering and System Safety, Vol. 51, No.2, Febr, 1996 and SKI Report 95:10

Table 2: NAFCS Report References	
ID	Title
SKI 96:65	Pörn, K; Skattning av brandfrekvenser per anläggning och anläggningsdel; SKI Report 96:65
SKI 97:25	Angner, A (editor); Projekt Yttre Händelser – Slutrapport; SKI Report 97:25
SKI 97:50	Knochenhauer, M, " Handbok - Komponentmodellering vid analys av yttre händelser". SKI Report 97:50; December 1997
SKI 98-09	Nyman, R, Kulig, M, Tomic, B; Identification of Common Cause Initiators in IRS Database; SKI Report 98-09, February 1998.
SKI 99:01	Pörn, K; Skattning av systemvisa utflödesfrekvenser i nordiska kärnkraftverk; SKI Report 99:01
SKI 91:6	Mankamo, T., Björe, S. & Olsson, L., CCF analysis of high redundancy systems, SRV data analysis and reference BWR application. Technical report SKI TR-91:6, Swedish Nuclear Power Inspectorate, 1991.
SKI TR-91:6	Mankamo, T., Björe, S. & Olsson, L., CCF analysis of high redundancy systems, SRV data analysis and reference BWR application. Technical report SKI TR-91:6, Swedish Nuclear Power Inspectorate, 1991.
SKI/R96:77	Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Summary report, prepared by T. Mankamo. SKI Report 96:77, December 1996
SKI/RA-26/96	CCF Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants. Work reports, prepared by T. Mankamo. SKI/RA-26/96, December 1996
SKIFS 1998:1	Statens kärnkraftinspektions föreskrifter om säkerhet i vissa kärntekniska anläggningar: Allmänna råd om tillämpningen av Statens kärnkraftinspektions föreskrifter enligt ovan, SKIFS 1998:1, 11 augusti 1998.
SPC 99-048	Forsmark 1 och 2, utvärdering av händelser för styrstavar. Mikael Heldesjö, ABB Atom AB, Rapport SPC 99-048, Rev.1, 1999-06-07
SRD R 196	Bourne, A.J., et al “Defences against common mode failures in redundancy systems – A guide for management, designers and operators”, Safety and Reliability Directorate, UKAEA, SRD R 196, January 1981.
Standard Review Plan 2.2.1-2.2.2	USNRC; Identification of Potential Hazards in Site Vicinity; Standard Review Plan 2.2.1-2.2.2, rev 2; 1981
SWR-PSA	SWR - Sicherheitsanalyse, Abschlussbericht, Teil 1. Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-102/1, Juni 1993 (in German).
T314_TrC	Mankamo, T., A pressure relief transient with pilot valve function affected by a latent CCF mechanism. Work report NKS/SIK-1(92)35, Avaplan Oy, 31 January 1994.
T-BokenR	T-Bokens data om drivdon/styrstavar (BWR). Anmärkningar, 1996-12-30. Part of SKI/RA-26/96.
T-book	T-Book, 5th edition, Reliability Data of Components in Nordic Nuclear Power Plants. Prepared by The TUD Office and Pörn Consulting. Published by The TUD Office, SwedPower AB. (2000).
TC_PASDG	Mankamo, T., A timedependent model of dependent failures, application to a pairwise symmetric structure of four components. Report NKS/SIK-1(92)13, 31 December 1993.
T-Code	T-CODE, A Tool for Bayesian Estimation of Component Failure Rate. User’s and Methodology Manual. Pörn Consulting, 1997.
TV_RSCCE	CCF analysis of BWR reactor shutdown systems, based on the operating experience at the TVO I/II in 1981-1993. Prepared by T. Mankamo, Avaplan Oy, for the Finnish Centre for Radiation and Nuclear Safety, Report STUK-YTO-TR 100, April 1996. Also part of SKI/RA-26/96.
NUREG/CR-5801	Procedures for Analysis of CCFs in PRA. Prepared by .. for USNRC, SAND91-7087, April 1993.
YVL 1.0	Safety criteria for design of nuclear power plants, STUK Regulatory Guide YVL 1.0, 12 Jan. 1996
YVL 1.5	Reporting nuclear power plant operation to the Finnish Centre for Radiation and Nuclear Safety, STUK Regulatory Guide YVL 1.5, 1 Jan. 1995
YVL 2.7	Ensuring a nuclear power plant's safety functions in provision for failures, STUK

Table 2: NAFCS Report References	
ID	Title
	Regulatory Guide YVL 2.7 , 20 May 1996
YVL 2.8	Probabilistic safety analyses (PSA), STUK Regulatory Guide YVL 2.8 , 20 Dec. 1996

4 Literature Survey

The following sources are used as input to the Literature survey:

1. Studsvik Library search for CCF literature using the key words "Common mode failures" AND “Defences” and restricting the search to the period from 1990 until 2002-06.
2. Search of SKI web list of SKI research reports 1984-June 2003.
3. Search on the Internet using Altavista search Engine and the following key words: Defence, common cause failure, redundancy, diversity
4. Search of the NRC web site using the following key words: Defence, common cause failure, redundancy, diversity
5. Search on IAEA web site and the following key words: Defence, common cause failure, redundancy, and diversity.

The A screening is made based on a check against the key areas listed above.

5 Results of the Literature Survey

5.1 Studsvik Library Search

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
Use of probabilistic safety assessment for operational safety. PSA ‘91. Proceedings of an international symposium held in Vienna, 3-7 June 1991. Vienna (Austria). IAEA. 1992. 859 p. p. 535-548.	Afzali,-A.; Mosleh,-A. (Maryland Univ., College Park, MD (United States). Materials and Nuclear Engineering Dept.),	Coupling mechanism classification for common cause failure analysis
The critical nature of dependent failures whose occurrence is not explicitly included in the event and fault tree models is well recognized. This category of dependent failures are usually defined as common cause failures. There has been a significant effort to develop procedures and models to address common cause failure phenomena and establish data sources to be used in those models. A major precursor for the occurrence of dependent failures is the presence of coupling mechanism(s). The paper discusses the concept of the coupling mechanism, introduces a classification system for systematic inclusion of these failure propagating mechanisms in reliability analysis, and recommends a defence methodology for elimination or reduction of coupling mechanism effects. The result of applying the above mentioned classification to the actual data and the conclusions reached are also reported. (author). 8 refs, 1 fig., 2 tabs.		
Probabilistic safety assessment and management. Beverly Hills, CA (USA). 4-7 Feb 1991. SAND—90-0828C	Parry,-G.W. (NUS Corp., Gaithersburg, MD (USA)); Paula,-H.M. (JBF Associates, Knoxville, TN (USA)); Rasmuson,-D. (Nuclear Regulatory Commission, Washington, DC (USA)); Whitehead,-D. (Sandia National Labs., Albuquerque, NM (USA))	Data needs for common cause failure analysis

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
The procedures guide for common cause failure analysis published jointly by USNRC and EPRI requires a detailed historical event analysis. Recent work on the further development of the cause-defense picture of common cause failures introduced in that guide identified the information that is necessary to perform the detailed analysis in an objective manner. This paper summarizes these information needs.		
Sixteenth water reactor safety information meeting. Volume 1: Plenary session, Decontamination and decommissioning, License renewal, Human factors, generic issues, Risk analysis/PRA applications, Innovative concepts for increased safety of advanced power reactors. Mar 1989. 561 p. P. 405-416. NUREG/CP—0097-Vol.1	Mitchell,-D.B.; Parry,-G.W.; Paula,-H.M.; Whitehead,-D.W.; Rasmuson,-D.M. (Sandia National Labs., Albuquerque, NM (USA))	NRC research in common-cause failures
The status and recent history of common-cause failure (CCF) research are briefly reviewed. Current NRC research in the area of CCFs is described with emphasis on the remaining problem areas. These include deficiencies in data and the need to more completely understand the characteristics of CCFs. The concepts and relationships of root cause, coupling mechanisms, and defensive mechanisms are discussed. Key definitions and some in-depth analysis of these concepts are included. An overview of the recent research to be published is presented. This research includes the following (1) the cause-defense methodology for analyzing CCFs, (2) guidelines for identifying potential CCFs as part of a nuclear power plant walkdown and procedures review, and (3) requirements for an industry-wide data base, including documentation of failure events and additional component failure and failure mode data requirements to support future PRAs.		
Transactions of the 10th international conference on structural mechanics in reactor technology. Los Angeles, CA (USA). American Association for Structural Mechanics in Reactor Technology. 1989. 199 p. p. 37-46	Ballard,-G.M	The use of engineering judgement in dependent failure analysis
The recognition that dependent failures of engineering components and systems are a major contributor to the risk from nuclear power plant is now well established. The subject of common cause failure or common mode failure, to use two of the alternative titles in common use, had been treated by engineers as rather nebulous and perhaps a figment of the safety analyst's imagination. Fortunately, or perhaps unfortunately, incidents during NPP operation have demonstrated quite clearly that dependent failures are real and significant. Thus, although there is still resistance in some quarters, both plant designers and operators, and safety analysts have had to find an acceptable method of incorporating this issue in plant safety cases. This is not an easy problem as the considerable volume of recent papers on the subject has demonstrated. The subject starts with an air of unreality and is frequently continued by complex mathematical manipulations that seem to bear little relationship to the engineering characteristics of the plant. If real progress is to be made in improving plant defenses against dependent failures there is an urgent need for dependent failure analysis (DFA) to be more systematic and understandable. The recent Procedures Guide published by the USNRC was a major step forward and one in which the UKAEA Safety and Reliability Directorate was very glad to collaborate. However, while this guide helps to systematize DFA particularly with regard to qualitative analysis, it does not manage to tie the quantitative analysis effectively to engineering design and operation; it still leaves it as a rather mathematical exercise. SRD has been trying to bridge this gap between mathematics and engineering in DFA and this paper summarizes some of the developments along that path.		

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
Kerntechnik-1987. (May 1995). V. 60(2-3). P. 105-109	Breiling,-G. (ABB Reaktor GmbH, Mannheim (Germany)); Oehmgen,-T. (Kernkraftwerk Unterweser, PreussenElektra AG, Stadland (Germany)),	Determination of input data for probabilistic safety assessment
The application of probabilistic safety assessment in decision processes depends to a great extent on the quality of the input data. The plant specific acquisition of these data must be performed in a way which allows a reliable prediction of system failures in the future. Comfortable computer tools are available to facilitate data processing and to make use of data that are already available via the computerized plant information system. The correct classification of failure occurrences with respect to the PSA relevant failure modes requires thorough evaluation of all information available in maintenance records, test reports, and licensing event reports. The flow of information relevant to future data acquisition must be properly organized. The application of generic common cause failure data requires careful evaluation of the underlying failure causes and of the level of defence achieved in the plant under consideration to prevent too pessimistic analysis result. (orig.).		
„“, Nuclear-Power-Engineering. (Feb 1995). V. 16(1). P. 67-72.	Li-Zhaohuan (Academia Sinica, Beijing, BJ (China). Inst. Of Atomic Energy),	Estimation of defense tactics effectiveness against CCFs
Common cause failures (CCFs) can seriously reduce system reliability, increase occurrence frequency of accident sequences in probabilistic safety assessment and influence the operation safety. The extensive researches have been widely taken all over the world in recent decade years. A great many of analytical models had been established. But most of works involved the discussion and quantification of CCFs, very few of them concerned the defense tactics. A model, called reduction matrix, for estimation of effectiveness of defense tactics against common cause failure is established. It is based on the component failure data base and engineering judgment as well as intersection operation in fuzzy sets. A practical example is introduced to show the use of the developed model.		
NUREG/CR—6303, 1994	Preckshot,-G.G. (Lawrence Livermore National Lab., CA (United States))	Method for performing diversity and defense-in-depth analyses of reactor protection systems
The purpose of this NUREG is to describe a method for analyzing computer-based nuclear reactor protection systems that discovers design vulnerabilities to common-mode failure. The potential for common-mode failure has become an important issue as the software content of protection systems has increased. This potential was not present in earlier analog protection systems because it could usually be assumed that common-mode failure, if it did occur, was due to slow processes such as corrosion or premature wear-out. This assumption is no longer true for systems containing software. It is the purpose of the analysis method described here to determine points of a design for which credible common-mode failures are uncompensated either by diversity or defense-in-depth.		

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
Proceedings of the sixteenth reactor operations international topical meeting. La Grange Park, IL (United States). American Nuclear Society, Inc. 1993. 436 p. P. 157-161.	Sullivan,-K. (Brookhaven National Laboratory, Upton, NY (United States)),	Fire protection of safe shutdown capability at commercial nuclear power plants
The comprehensive industrial safety standards and codes that exist today have evolved from lessons learned through past experience, research results, and improvements in technological capabilities. The current requirements for fire safety features of commercial nuclear power stations operated in the U.S. are a notable example of this practice. Although fire protection has always been an important design requirement, from the aftermath of a serious fire that occurred in 1975 at the Browns Ferry plant, it was learned that the life safety and property protection concerns of the major fire insurance underwriters may not sufficiently encompass nuclear safety issues, particularly with regard to the potential for fire damage to result in the common mode failure of redundant trains of systems, and composites important to the safe shutdown of the reactor. Following its investigations into the Browns Ferry fire, the Nuclear Regulatory Commission (NRC) promulgated guidance documents, which ultimately developed into mandatory regulations, necessary to assure the implementation of a fire protection program that would address nuclear safety concerns. The new criteria that evolved, contain prescriptive design features, as well as personnel and administrative requirements the Commission determined to be necessary to provide a defense-in-depth level of protection against the hazards of fire and its associated effects on safety related equipment. These criteria are primarily contained in Appendix R of Title 10 to the Code of Federal Regulations (10 CFR 50).		
China Nuclear Information Centre, Beijing, BJ (China). Aug 1991	Li-Zhaohuan (China Inst. Of Atomic Energy, Beijing (China)),	xi common cause failure model and method for defense effectiveness estimation
Two issues have been dealt. One is to develop an event based parametric model called xi-CCF model. Its parameters are expressed in the fraction of the progressive multiplicities of failure events. By these expressions, the contribution of each multiple failure can be presented more clearly. It can help to select defense tactics against common cause failures. The other is to provide a method which is based on the operational experience and engineering judgement to estimate the effectiveness of defense tactics. It is expressed in terms of reduction matrix for a given tactics on a specific plant in the event by event form. The application of practical example shows that the model in cooperation with the method can simply estimate the effectiveness of defense tactics. It can be easily used by the operators and its application may be extended		
„ Korea Atomic Energy Research Institute, Taejon (Korea, Republic of), Aug 2000 81 p. KAERITR16282000	Cheon,-Se-Woo; Park,-Jong-Kyun; Lee,-Ki-Young; Kwon,-Ki-Choon; Lee,-Jang-Soo; Kim,-Jang-Yeo	Guidelines on the defense-in-depth and diversity planning and analysis in digital instrumentation and control systems
Digital instrumentation and control (I and C) systems are becoming an ever-increasing part in I and C systems of nuclear power plants due to such features such as versatility, flexibility, and reduced sizes. The digital technology introduces a possibility that common-cause or common-mode failures (CCF or CMF) may cause redundant safety systems to fail in such a way that there is loss of safety function. A special form of CMF analysis called 'defense-in-depth and diversity' (D-in-D and D) analysis has been developed to identify possible common-mode failure vulnerabilities and to support a specific licensing action in digital systems. There are two main stages in D-in-D and D activities: both plan and analysis. The purposes of this technical report are I) to review background of D-in-D and D and some of important issues in digital D-in-D and D, ii) to provide guidelines for a vendor to prepare planning and/or analysis documents on D-in-D and D, and iii) to provide guidelines for an evaluator to review applicant's D-in-D and D planning and/or analysis documents, to ensure that the requirements of the D-in-D and D for digital I and C systems are followed. Most of guidelines suggested in this report were based on NUREG/CR-6303 which was published in 1994. The report will be helpful for a vendor to prepare and for an evaluator to review both D-in-D and D planning or analysis documents for digital I and C systems such as the KNGR project.		

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
Power-Engineering (Jul 1999) v. 10(1) p. 45-57	Lee,-C.-S.; Park,-C.-E.; Lee,-S.-I.; Choi,-H.-R.; Lee,-G.-C.; Choi,-C.-J,	An evaluation of defence-in-depth and diversity design against common mode failure plant protection system for Korean Next Generation Reactor
An extensive analysis has been performed qualitatively and quantitatively to evaluate the intrinsic capability of the KNGR design in coping with design bases events concurrent with Common Mode Failure (CMF) in digital Plant Protection System (PPS). A best-estimate analysis methodology has been developed and utilized since design base events concurrent with CMF in digital PPS are categorized as beyond design bases events. Due to diverse means not affected by CMF and a sufficient available over-power margin in KNGR design, the event consequences are well within the acceptance criteria for the design bases events with CMF. (author).		
International Atomic Energy Agency (IAEA) technical committee meeting on advanced technologies for improving availability and reliability of current and future water cooled nuclear power plants Argonne, IL (United States) 8-11 Sep 1997	Wyman,-R.H.; Johnson,-G.L	Defense against common-mode failures in protection system design
The introduction of digital instrumentation and control into reactor safety systems creates a heightened concern about common-mode failure. This paper discusses the concern and methods to cope with the concern. Common-mode failures have been a ‘’fact-of-life’’ in existing systems. The informal introduction of defense-in-depth and diversity (D-in-D ampersand D)-coupled with the fact that hardware common-mode failures are often distributed in time-has allowed systems to deal with past common-mode failures. However, identical software operating in identical redundant systems presents the potential for simultaneous failure. Consequently, the use of digital systems raises the concern about common-mode failure to a new level. A more methodical approach to mitigating common-mode failure is needed to address these concerns. Purposeful introduction of D-in-D ampersand D has been used as a defense against common-mode failure in reactor protection systems. At least two diverse systems are provided to mitigate any potential initiating event. Additionally, diverse displays and controls are provided to allow the operator to monitor plant status and manually initiate engineered safety features. A special form of common-mode failure analysis called ‘’defense-in-depth and diversity analysis’’ has been developed to identify possible common-mode failure vulnerabilities in digital systems. An overview of this analysis technique is provided		
China institute of atomic energy annual report (1992) Beijing (China) China Ocean Press 1993 236 p. P. 106-107	Li-Zhaohua	„Model for estimation of defense tactics effectiveness against common cause failure
Nuclear-Power-Engineering. (Feb 1997). V. 18(1). P. 82-85, 96	Li-Zhaohuan (Academia Sinica, Beijing, BJ (China). Inst. Of Atomic Energy),	Swimming pool reactor reliability and safety analysis
A reliability and safety analysis of Swimming Pool Reactor in China Institute of Atomic Energy is done by use of event/fault tree technique. The paper briefly describes the analysis model, analysis code and main results. Meanwhile it also describes the impact of unassigned operation status on safety, the estimation of effectiveness of defense tactics in maintenance against common cause failure, the effectiveness of recovering actions on the system reliability, the comparison of occurrence frequencies of the core damage by use of generic and specific data.		

Table 3: Studsvik Library Search and literature Screening Results		
No/Ref	Authors	Title
PSAM 5: Probabilistic safety assessment and management Tokyo (Japan) Universal Academy 2000 2820 p. p. 1857-1863 Published in 4 volumes, also available on CD-ROM can be used for Windows 95/98/2000, Macintosh and UNIX. Also published in Frontiers Science Series No.34, ISSN 0915-8502	Kim,-Min-Chull; Kim,-Inn-Seock (Hanyang Univ., Seoul (Korea, Republic of	Application of decision analysis to the optimization of common cause failure defense methods
Various methods to defend against common cause failure (CCF) have been proposed in the literature. These methods can be classified into five different categories. Based on these categories, we developed a novel approach to determining an optimal CCF defense strategy. The potential CCF defense strategies are evaluated using a decision analysis method, called analytic hierarchical process (AHP). This approach was applied to two motor-driven valves for containment sump isolation in Ulchin 3 and 4 nuclear power plants of Korea to defend against CCF of the valves. The example CCF defense analysis suggests several potential CCF defense strategies in this case, and prioritizes them in terms of effectiveness based on cost, safety, and operator burden. (author)		

5.2 SKI Reports

Table 4: SKI Reports related to Dependencies		
No	Author	Title
91:06	T. Mankamo, Avaplan Oy, S. Björe and L. Olsson ABB Atom AB, Västerås, Sweden December 1992	CCF Analysis of High Redundancy Systems. Safety/relief Valve Data Analysis and Reference BWR Application
93:32	J. Olsén Kungliga tekniska högskolan, Stockholm nordisk 1993	Översikt av silproblematiken
93:39	K. Spång DNV Ingemansson AB, Göteborg, Sweden December 1993	Methodology for Artificial Aging of Electrical Components. Results of Experimental Studies
94:15	M. J. Do, A. D. Chockie Battelle Seattle Research Center, Seattle, Washington September 1994	Aging Degradation of Concrete Structures in Nuclear Power Plants
94:31	K. Pörn Pörn Consulting, Nyköping April 1995	Förstudie – Vidareutveckling av trendmodell för åldringsanalys
95:28	S. Isaksson Sveriges Provnings- och Forskningsinstitut, Borås nordisk 1995	Litteraturstudie angående brandskydd i kärnkraftverk. Del 1: Brandteknisk separation
95:79	P. Lidar Studsvik Material AB, Nyköping September 1995	International Symposium on Plant Aging and Life Prediction of Corrodible Structures – Reserapport
96:77	T. Mankamo Avaplan Oy, Espoo, Finland December 1996	Common Cause Failure Analysis of Hydraulic Scram and Control Rod Systems in the Swedish and Finnish BWR Plants
97:40	K. Spång Ingemansson Technology AB, Göteborg, Sweden October 1997	Aging of Electrical Components in Nuclear Power Plants Relationships Between Mechanical and Chemical Degradation After Artificial Aging and Dielectric Behaviour During LOCA

Table 4: SKI Reports related to Dependencies		
No	Author	Title
98:09	R. Nyman (1), M.Kulig (2), B. Tomic (2). (1) Swedish Nuclear Power Inspectorate, Stockholm, Sweden. (2) ENCONET Consulting Ges.m.b.H, Vienna, Austria.	Identification of Common Cause Initiators in IRS Database
98:11	Preliminary Survey of Events in Nuclear Power Plants 1980-1997 B. Lydell RSA Technologies, USA March 1998	Undetected Latent Failures of Safety-Related System
00:06	Ola Svenson Stockholms Universitet, Department of Psychology, SE-106 91 Stockholm, Sweden and Netherlands Institute for Advanced Study in the Humanities and Social Sciences, NL-2242 Wassenaar, The Netherlands February 2000	Accident Analysis and Barrier Function (AEB) Method. Manual for Incident Analysis
01:17	Kjell Spång, Ingemansson Technology AB Gunnar Ståhl, Westinghouse Atom Maj 2002	Kvalificering av elkomponenter I kärnkraftverk. Del A – Hantering av åldring
01:37	Kenneth Persson, PWP Consulting December 2001	Underhållsverksamhetens effektivitet och ändamålsenlighet
01:47	Erik Hollnagel[1] Vincent Gauthereau[2] [1]CSELAB Department of Computer and Information Science Linköping University [2]Quality Management Department of Industrial Engineering Linköping University June 2001	Operational Readiness Verification, Phase 1: A Study on Safety During Outage and Restart of Nuclear Power Plants
01:50	Karin Lundqvist Castor Analys AB September 2001	Rationaliseringsstrategier och säkerhet
02:04	Kjell Spång, Ingemansson Technology AB Gunnar Ståhl, Westinghouse Atom May 2002	Qualification of Electrical Components in Nuclear Power Plants. Management of Ageing
02:63	Jean-Pierre Bento JPB Consulting AB December 2002	Procedures as a Contributing Factor to Events in the Swedish Nuclear Power Plants: Analysis of a Database with Licensee Event Reports 1995-1999

5.3 NKS Reports

NKS reports matching the search expression “common cause failure” are listed in Table 5. Search made in spring 2003 at the NKS web site.

Table 5: NKS Reports matching the search expression “common cause failure”		
No/Ref	Author (s)	Title
ISBN: 87-7303-454-1 NORD 1990:57	Stefan Hirschberg (edt.) ABB Atom	RAS-470: Dependencies, human interactions and uncertainties in probabilistic safety assessment
In the context of Probabilistic Safety Assessment (PSA), three areas were investigated in a 4-year Nordic programme: dependencies with special emphasis on common cause failures, human interactions and uncertainty aspects.. The approach was centered around comparative analyses in form of Benchmark/Reference Studeis and retrospective reviews. Weak points in available PSAs were identified and recommendations were made aiming at improving consistency of the PSAs . The sensitivity of PSA-results to basic assumptions was demonstrated and the sensitivity to data assignment and to choices of methods for analysis of selected topics was investigated		
NORD	Stephen Dinsmore (edt.) Studsvik	SÄK-1: PRA uses and techniques – a Nordic perspective
Techniques for probabilistic risk analysis (PRA) are analyzed with special emphasis on their application in nuclear power plants. Methods and codes currently available for PRA analysis in the Nordic countries are evaluated and compared. Additionaly, theability to generate unique failure parameters from available plant data bases and generic data sources is examined. The subsequent application of PRA techniques as an aid in the licensing and regulatory process is discussed		
NKS-6	Urho Pulkkinen, Kaisa Simola (edt.) VTT Automation	SOS-2: Proceedings of the NKS/SOS-2 Seminar on Risk Informed Principles Bergendal 13.4-14.4 1999
NKS-3	Björn Wahlström (red.) Statens Tekniska Forskningcentral VTT Automation	SOS-1: Säkerhetsindikatorer inom kärnkraftindustrin; definitioner, användning och erfarenheter Rapport från ett seminarium på VTT den 17-18 mars 1999
Föreliggande rapport har skrivits som en del av projektet ”Riskvärdering och strategier för säkerhet, SOS-1” som drivs i nordisk kärnsäkerhetsforsknings regi under åren 1998-2001. Rapporten redogör för innehållet i ett seminarium som hölls på Statens tekniska forskningscentral (VTT) i Esbo, Finland den 17-18 mars 1999. Rapporten innehåller också en mera allmänt hållen beskrivning av säkerhetsindikatorer och hur de används inom kärnkraftindustrin som har sammanställts av Björn Wahlström. Det material deltagarna använde i sina presentationer har samlats i bilaga 3.		
NKS/RAK-1(97)R8	Björn Wahlström, Lars Gunsell Statens tekniska forskninscentral, Vattenfall Energisystem AB	RAK-1: REAKTORSÄKERHET; En beskrivning och värdering av säkerhetsarbetet i Norden.
Föreliggande rapport utgör dokumenteringen av NKS/RAK-1.1. Projektet är en del av det samnordiska forskningsprogrammet inom kärnkraftsäkerhet som har löpt under åren 1994-97. Rapporten sammanfattar på ett övergripande sätt säkerhetsarbetet, dess delar och hur delarna förhåller sig till varandra. Rapporten pekar ut sådana delar av säkerhetsarbetet, som är viktiga för helheten. Rapporten skall kunna användas som ett stöd för att värdera säkerhetsrelaterade aktiviteter på kärnkraftverken och hos myndigheterna. Nya personer i branschen skall kunna använda rapporten för att sätta sig in i hur säkerhetsarbetet bedrivs både på en mera övergripande och på en detaljnivå. Författarna hoppas att rapporten skall vara av intresse också för personer i andra branscher som är engagerade i s¨kerhetskritisk verksamhet. En tekniskt intresserad lekman bör genom rapporten kunna få en inblick i kärnkraftbranschens säkerhetstänkande.		

Table 5: NKS Reports matching the search expression “common cause failure”		
No/Ref	Author (s)	Title
NKS(97)FR1	Kjell Andersson NKS	RAK-1: Strategies for Reactor Safety
The NKS/RAK-1 project formed part of a four-year nuclear research program (1994-1997) in the Nordic countries, the NKS Programme. The project aims were to investigate and evaluate the safety work, to increase realism and reliability of the safety analysis, and to give ideas for how safety can be improved en selected areas. An evaluation of the safety work in nuclear installations in Finland and Sweden was made, and a special effort was devoted to plant modernisation and to see how modern safety standards can be met up with. A combination of more resources and higher efficiency is recommended to meet requirements from plant modernisation and plant renovations. Both the utilities and the safety authorities are recommended to □ctively follow the evolving safety for new reactors. Various approaches to estimating LOCA frequencies have been explored. In particular, a probabilistic model for pipe ruptures due to intergranular stress corrosion has been developed. A survey has been done over methodologies for intergrated sequence analysis (ISA), and different approaches have been developed and tested on foru sequences. Structured frameworks for intergration between PSA and behavioural sciences have been developed, which e.g. have improved PSA. The status of maintenance data information system has been developed.		
NKS/RAK-1(97)R3	Lennart Hammar ES-konsult AB	RAK 1.1: Seminarium om Granskning för säkerhet och kvalitet Strategi och praxis den 16-17 januari 1997 på VTT i Esbo, Finland
Seminariet hade arrangerats inom det nordiska kärnsäkerhetsprogrammets (NKS) projekt RAK-1, Strategi för reaktorsäkerhet i samarbete med Kärntekniskt Centrum vid KHT. Värd för seminariet var den finska Statens Tekniska Forskningscentral, VTT. Uppgiften för seminariet var att diskutera hur säkerheten i kärnteknisk verksamhet – konstruktion, tillverkning, produktion mm – kan förbättras genom granskning, såväl hos tillståndshavarna själva som hos deras leverantörer och viken roll myndigheternas säkerhetstillsyn kan och bör spela. Frågorna gäller vad granskningen skall omfatta, resurs- och kompetensbehoven i granskningen, hur ansvarsförhållandena skall se ut och hur motivationen för att granskas och låta sig granskas skall säkerställas. Seminariet gav en belysning av den praxis som tillämpas och hur den utvecklas vid kärnkraftverken i Finland och Sverige, hos en leverantör som ABB-Atom, och hos säkerhets- och strålskyddsmyndigheterna. Seminariet avslutades med en paneldebatt där erfarenheter och visioner för framtiden diskuterades och försök gjordes att stämma av i frågor där synen kunde skilja, bl.a. på finländsk och svensk sida. Intressanta synpunkter kom bland annat fram i frågan om synen på fristående säkerhetsgranskning och myndigheternas egentliga roll i säkerhetsarbetet med tanke på tillståndshavarnas fulla ansvar för säkerheten. Av seminariet kunde följande allmänna slutsatser dras: - Den grundläggande säkerhetsgranskningen vid kärnkraftverken är både i Finland och Sverige invävd i den verksamhet där säkerheten skapas, dvs. i konstruktion, uppbyggnad och anläggningsändringar, drift och underhåll; - Fristående säkerhetsgranskning inom kraftverken finns formellt både i Finland och Sverige men tillämpas mera rigoröst i Sverige. Seminariet gav impulser till att i Finland se närmare på om det kan finnas anledning att beakta denna skillnad; - Betydelsen av att det finns klara säkerhetsregler från myndighetens sida, för kraftföretagens egen säkerhetsgranskning och deras säkerhetsredovisning till myndigheterna, framhölls starkt från både kraftföretags- och leverantörshåll; - Myndighetsrollen i säkerhetsgranskningsarbetet belv väl klarlagd vid seminariet. Från både SKI och STUK framhölls att kraftföretagens målsättning för sin egen säkerhetsgranskning skall vara att myndigheternas säkerhetsgranskning inte skall behövas – även om det kan sägas att myndighetsgranskningen i praktiken bidrar till säkerheten. Det framgick samtidigt att en sådan målsättning skulle kunna kräva en ytterligare förstärkning av kraftföretagens fritstående granskning; - Resursbehovet för säkerhetsgranskning är en kritisk fråga, särskilt i Sverige i anslutning till de omfattande moderniserongsprojekten för de äldre anläggningarna; - Attityderna till och motivationen för granskningsarbete har avsevärd betydelse för den kvalitet som kan nås och bör beaktas mycket mera i fortsättningen.		
TemaNord 1994:614	Jan Holmberg, Kari Laakso (edt.), Esko Lehtinen, Gunnar Johanson, VTT Automation, Industrial Process Safety	SIK-1: Safety Evaluation by Living Probabilistic Safety Asssessment and Safety Indicators

Table 5: NKS Reports matching the search expression "common cause failure"		
No/Ref	Author (s)	Title
A continuous monitoring and follow-up of the risks involved in the operation of a nuclear power plant is an important part of the operational safety management. In living probabilistic safety assessment (PSA), the plant specific (PSA) is applied in daily safety work to support solving of short-term problems, and maintaining as well as enhancing safety in the long term. Well-defined safety indicators, highlighting important trends and possible recurrence of operational problems at the plant can achieve a quicker and more problem-oriented feedback of operating experience. Living (PSA) and safety indicators should be used in combination to effectively support decision making in safety related issues. The Nordic NKS/SIK-1 project also showed how a more systematic and clear basis for such decision can be formulated by the methods of decision analysis.		
NORD 1990:33	Kari Laakso (edt.), Technical Research Centre of Finland	RAS-450: Optimization of technical specifications by use of probabilistic methods – A Nordic perspective
The technical specification of nuclear power plant specifies the limits for plant operation from the safety point of view. These operational safety rules were originally defined on the basis of deterministic analyses and engineering judgement. As experience has accumulated, it has proved necessary to consider problems and make specific modifications in these rules. Developments in probabilistic safety assessment have provided a new tool to analyse, present and compare the risk effects of proposed rule modifications. The main areas covered in the projects are operational decisions in failure situations, preventive maintenance during power operation and surveillance tests of standby safety systems.		

5.4 Other sources

This section presents other references found at NRC and other websites. Also included are some interesting references that are identified in reference material available as paper copies pdf documents etc. Specific IAEA documents are presented in Table 6 and other references in Table 7.

Table 6: IAEA Search for Separation, redundancy, Diversity and Common (cause failure)	
ID	Title
IAEA TECDOC 338	Methodology for the Management of Ageing of Nuclear Power Plant Components Important to Safety, IAEA, 1992
IAEA TECDOC 648	Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA, 1992,
IAEA TECDOC 986	Implementation of Defence in Depth for Next Generation Light Water Reactors, IAEA, 1997
INSAG-10	Defence in Depth in Nuclear Safety, IAEA, 1996
INSAG-12	Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, IAEA, 1999
INSAG-4	Safety Culture, IAEA, 1991
INSAG-8	A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards, IAEA,1995
NS-G-1.2	Safety Assessment and Verification for Nuclear Power Plants, IAEA, 2001
NS-G-2.3	Modifications to Nuclear Power Plants, IAEA, 2001
Safety Reports Series No. 12	Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards – A Common Basis for Judgement, IAEA, 1998
Safety Series 106	The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, IAEA, 1992
Safety Series 50-P-1	Application of the Single Failure Criterion, A Safety Practice, IAEA, 1990
Safety Series 50-P-3	Data Collection and Record Keeping for the Management of Nuclear Power Plant Ageing, IAEA, 1991.
Safety Series No 50-SG-O12	Periodic Safety Review of Operational Nuclear Power plants, A Safety Guide, IAEA 1994

Table 7: Other sources	
ID	Title
10 CFR 50.65	Requirements for monitoring the effectiveness of maintenance at nuclear power plants. (Maintenance rule)
A. Mosleh, et. Al, INEELEXT-97-0 1327, November, 1997.	Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessments
Angela E. Summers, Ph.D., Kimberly A. Ford, and Glenn Raney, Chemical Engineering Progress, November 1999	Estimation and Evaluation of Common Cause Failures in SIS
Angela E. Summers, Ph.D., P.E, www.SIS-TECH.com, Accepted for publication in ISA Transactions	Viewpoint on ISA TR84.0.02 – Simplified Methods and Fault Tree Analysis
Aniello Amendola, Kluwer Academic Publishers, 1989, ISBN 0-7923-0268-0	Common Cause Failure Analysis in Probabilistic Safety Assessment
ANSI/ISA-84.01-1996, March 1997	Application of Safety Instrumented Systems in the process Industries
BNL-NUREG-60844, Stanislav Uryasev and Pranab Samanta, International Conference on Mathematics and Computations, Reactor Physics, and Environmental Analyses, Portland, Oregon, April 30 – May 4, 1995	Analysis of Failure Dependent Test, Repair and Shutdown Strategies for Redundant Trains
F Marshall, T Wierman, D Rasmuson, A Mosleh, conference paper INEEL/CON-99-00413	Insights about Emergency Diesel Generator Failures from the USNRC´s Common Cause Failure Database
http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/1999/ri99003.html#_1_6	Resolution of Generic Issue 145, Actions to Reduce Common-Cause Failures, October 13, 1999
IEC 60880-2, December 2000.	Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software
IEC-61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
INPO 87-024, Revision 04, July 1991.	Institute of Nuclear Power Operations, NPRDS Information Retrieval Guide
INPO 89-00 1, Revision 05, December 1994.	Institute of Nuclear Power Operations, NPRDS Reporting Guidance Manual
K.L. McElhaney, ORNL, conference paper, CONF-9707112—1	Failure Modes and Causes for Swing and Lift Type Check Valves
Mosleh , A. et al, University of Maryland Nuclear Engineering Report UMNE-92-004, Prepared for the U.S. Nuclear Regulatory Commission, August 1992.	On Quantitative Analysis of Common Cause Failure Data for Plant-Specific Probabilistic Safety Assessments
Mosleh, A., G. Parry, and A.F. Zikria, accepted for publication in Nuclear Engineering and Design, 1994.	An Approach to the Analysis of Common Cause Failure Data for Plant-Specific Application
NUREG/CR 5471, February 1993.	Enhancements to Data Collection and Reporting of Single and Multiple Failure Elements
NUREG/CR-5905, August, 1992.	Review and Development of Common Nomenclature for Naming and Labeling Schemes for Probabilistic Risk Assessment
NUREG-CR-5460, March 1990.	A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures

Table 7: Other sources	
ID	Title
Paula, H. M., Nuclear Safety, Volume 3 1, No. 2, April-June 1990	Data Base Features That are Needed to Support Common Cause Failure Analysis and Prevention: An Analyst's Perspective
RG 1.160, Rev 2 1997	Monitoring the Effectiveness of Maintenance at Nuclear Power Plants March
SAND96-0343, February 1996	Aging Management Guideline for Commercial Nuclear Power Plants – Tanks and Pools
Siu, N. and A. Mosleh, Nuclear Technology, 84 (1989) 265-28 1.	Treating Data Uncertainties in Common Cause Failure Analysis
Steven A. Atkinson, INEL-95/00275, October 1995	Achieving Safety/Risk Goals for less ATR Backup Power Upgrades
Thomas Vierman, Steven Eide and Cindy Gentillon, INEL and Dale Rasmuson, USNRC, conference paper INEEL/CON-99-00445	Common Cause Failure Analysis for Reactor Protection Systems Reliability Studies
V. P Brand, SRDA – R13, April 1996	UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems
W.E. Vesely, J. P. Vora, IAEA-SM-295/34	Quantitative Relationships between Aging Failure Data and Risk.
www.iceweb.com.au/sis/ene_checklist.htm	Sample Checklist - Estimation and Evaluation of Common Cause Failures in SIS

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
App 7	**Terms and definitions PR14**	**PR14**
Appendix 8	Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01	PR01

NAFCS
Nordisk Arbetsgrupp för CCF studier **NAFCS-PR14**

Title:	**Acronyms, Terms and Definitions**
Author(s):	*Michael Knochenhauer*
Issued By:	
Reviewed By:	Per Hellström
Approved By:	Gunnar Johanson
Abstract:	The document contains all terms and definitions used within the project.
Doc.ref:	Project reports
Distribution	WG, Project Website, Project archive
Confidentiality control:	Public

Revision control:

Version	Date	Initial
Draft 1	18 March 2003	MK
Draft 2	27 March 2003, commented by JPB and PH	MK
Draft 3	9 April 2003, commented by TM & partly revised and completed based on IAEA Safety Glossary	MK
Final	9 April 2003	

1. Acronyms

Acronym	Description
AE	Area Event
AFM	Alpha Factor Method
ALARA	As low as reasonably achievable
ASAR	As-operated Safety Analysis Report
ASME	American Society of Mechanical Engineers
ATHEANA	A technique for human error analysis in PSA
BFR	Binomial Failure Rate (Model)
BFR	Binomial Failure Rate model
BKAB	Barsebäck Kraft AB
BOKA	Barsebäck Oskarshamn Design Analysis (Barsebäck Oskarshamn konstruktionsanalys)
BWR	Boiling Water Reactor
CCBE	Common Cause Basic Event
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CCI	Common Cause Initiator
CCW	Component Cooling Water
CDF	Core Damage Frequency
CET	Containment Event Tree (level 2 PSA)
CFR	Code of Federal Regulations
CLM	Common Load Model
CMF	Common Mode Failure
CRDA	Control Rod Drive Assembly
DART	Designanalys Ringhals tryckvattenreaktorer (Ringhals PWR design analysis)
DBA	design basis accident
DCH	Direct containment heating
DG	Diesel Generator
DKV	Driftklarhetsverifiering (Operability Readiness Control)
ECCS	Emergency Core Cooling System

Acronym	Description
EE	External Event
EPRI	Electric Power Research Institute
EPV	Electromagnetic Pilot Valve
ETA	Event Tree Analysis
FKA	Forsmarks Kraftgrupp AB
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality Analysis
FSAR	Final Safety Analysis Report
FSAR	Final Safety Analysis Report
FTA	Fault Tree Analysis
GDC	General Design Criteria
GEV	Generalised extreme value distribution
GRS	Gesellschaft für Reaktorsicherheit (Germany)
HEP	Human Error Probability
HPSI	High Pressure Safety Injection
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
ICDE	International Common Cause Data Exchange
IE	Initiating event
INPO	International Nuclear Power Organisation
ISI	In-service inspection
KFB	Konstruktionsförutsättningar för byggnader
KFE	Konstruktionsförutsättningar för elektriska komponenter
KFM	Konstruktionsförutsättningar för mekaniska komponenter
KSU	Kärnkraftsäkerhet och utbildning
LER	Licensee Event Report (RO)
LOCA	Loss of Coolant Accident
LOSP	Loss of off-site power
LPSA	Living PSA
LWR	Light water reactor
MAAP	Modular Accident Analysis Program

Acronym	Description
MCP	Main Coolant Pump
MCS	Minimal Cut Set
MGL	Multiple Greek Letter (model)
MGLM	Multiple Greek Letter Model
MOV	Motor Operated Valve
MTO	Människa-teknik-organisation (Man-Machine-Organisation)
NAFCS	Nordisk Arbetsgrupp för CCF-studier (Nordic Working Group for CCF studies)
NEA	See OECD/NEA
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OECD/NEA	Nuclear Energy Agency of the Organisation for Economic Co-operation and Development
OKG	Oskarshamns Kraftgrupp AB
P&I	Process and Instrumentation (flow diagram)
PDS	Plant damage state
POT	Peak over threshold method
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Analysis Report
PSF	Performance shaping factors (in HRA)
PSG	Primary Safety Review (Primär säkerhetsgranskning)
PWR	Pressurised Water Reactor
QA	Quality Assurance
QC	Quality Control
RAB	Ringhals AB
RAW	Risk Achievement Worth
RO	Rapportervärd omständighet (Licensee Event Report)
SAR	Safety Analysis Report
SGFP	Subgroup Failure Probability
SHARP	Systematic Human Action Reliability Procedure
SKI	Statens kärnkraftinspektion (Swedish Nuclear Power Inspectorate)

Acronym	Description
SKIFS	SKI författningssamling (SKI Code of Regulation)
SLIM	Success Likelihood Index Method
SRV	Safety Relief Valve
STARK	Stanna – Tänk – Agera – Reagera – Kommunicera (Stop – Think – Act – Review – Communicate)
STF	Säkerhetstekniska förutsättningar (Technical Specifications)
STUK	Radiation and Nuclear Safety Authority of Finland
TDC	Test and Demand Cycles
TechSpecs	Technical Specifications
THERP	Techniques for Human Error Rate Prediction
TVO	Teollisuuden Voima Oy
TVO	Teollisuuden Voima Oy
USNRC	United States Nuclear Regulatory Commission
WANO	World Association of Nuclear Operators

2. Terms and Definitions

Term	Definition
Alfa factor model	Method for modelling and quantification of CCF
Area event (AE)	Initiating events occurring outside the process but within the plant. Primarily these events are internal fire, flooding and steam release. Other examples are missiles from rotating machines or exploding pressure vessels. Also see definitions of "Internal event" and "External event"
Berrys method	Method used in fire analyses in order to derive room-specific fire frequencies from a total building fire frequency.
Beta-factor model	Method for modelling and quantification of CCF
C-factor model	Method for modelling and quantification of CCF
Combined external event	Two or more external events having a non-random probability of occurring simultaneously, e.g., strong winds occurring at the same time as high sea water levels.
Common Cause Basic Event (CCBE)	Basic event in the fault tree model to represent CCFs, which affect a specific combination of components in a Common Cause Component Group (CCCG)
Common Cause Component Group (CCCG)	Group of components, usually identical or closely similar, vulnerable to CCFs. In most cases the CCCG is regarded as homogeneous and symmetric, which means that a combination of components is similarly affected by CCFs as any other combination with the same number of components in the considered CCCG.
Common Cause Failure (CCF)	Dependent failure of two or more components, where the failure states, including the possible latency time, exist within the considered time frame and originate from a shared failure mechanism. Also see definition of "Potential CCF".
Common Cause Initiator (CCI)	Event causing a transient (or requiring manual shut-down) and at the same time degrading one or more safety functions that may be needed after the transient/shut-down.
Common mode failure	Failure of two or more structures, systems or components in the same manner or mode due to a single event or cause, i.e. common mode failure is a type of common cause failure in which the structures, systems, or components fail in the same way.
Corrective maintenance	Actions that restore, by repair, overhaul or replacement, the capability of a failed structure, system or component.

Term	Definition
Defence in depth	A hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.
Dependent failure	A dependent failure is an occurrence of simultaneous non-independent component failures. Also see definition of "Simultaneous failures"
Deterministic analysis	Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value of the result. In nuclear safety, for example, this implies focusing on accident types, releases and consequences, without considering the probabilities of different event sequences.
Diversity	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure. Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), and different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide physical diversity).
Dynamic effect	Denotes causal failures occurring in connection with pipe breaks or internal pressure shocks.
External event	A principle meaning, that a component. Events unconnected with the operation of a facility or activity which could have an effect on the safety of the facility or activity. Typical examples for nuclear facilities include earthquakes, tornadoes, tsunamis, aircraft crashes, etc. Also see definitions of "Area event" and "Internal event"
Fail-safe	Componnet (or system) goes to it's safe (protecting) state in case of loss of input required for it's correct function, e.g., power.
Failure	Inability of a structure, system or component to function within acceptance criteria.
Functional dependence	Denotes dependencies that are due to system and component interconnections, e.g. process connection, control signal, power supply, cooling and lubrication
Functional Dependency Fault	A functional dependency fault is the inability of a component to perform its intended function, because of the unavailability or failure of a supporting component or system (the latter also sometimes called inter-system dependency).

Term	Definition
Impact vector	The impact vector describes the conditional probability of multiple failure, when a CCF mechanism is present in a CCCG, and with respect to the condition that an actual demand should occur in that situation. In the general case the conditional failure probability can be distributed over various multiplicity.
independent equipment	Equipment that possesses both of the following characteristics: the ability to perform its required function is unaffected by the operation or failure of other equipment; and the ability to perform its function is unaffected by the presence of the effects resulting from the postulated initiating event for which it is required to function.
Independent failure	An independent failure is an occurrence in which the probability of failure of one component is not related to the state (failed or working) of another component.
Initiating event (IE)	Excursion from the normal operation, which demands automatic or manual reactor scram or a non-delayed controlled shutdown.
Internal event	Initiating event that occurs inside the plant and within the process limits. Also see definitions of "Area event" and "External event"
Latent failure (dormant failure)	Failure state, which is not detected in normal operation but only in tests or actual demands. Also referred to as dormant failure
Living PSA (LPSA)	A PSA which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the PSA model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. Also a way of using PSA, where PSA models and results are used in a wide range of applications in the plant safety work, e.g., for follow-up of incidents, selection between design alternatives, or planning of TechSpec changes.
Minimal Cut Set (MCS)	Outcome of a fault tree analysis; a minimal and unique combinations of basic events that, if they all occur, will lead to the top event of the analysed fault tree.
Monitored failure	Failure state, which is detected in normal operation by instrumentation, alarms or other means of condition monitoring; latent time is zero or negligible
Periodic maintenance	Form of preventive maintenance consisting of servicing, parts replacement, surveillance or testing at predetermined intervals of calendar time, operating time or number of cycles.

Term	Definition
Physical Dependency	The term physical dependency is utilised to denote that several components are situated in the same room or location or are functionally dependent on equipment in another common room or location. Also see definition of "Area event".
physical separation	Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.
Planned maintenance	Form of preventive maintenance consisting of refurbishment or replacement that is scheduled and performed prior to unacceptable degradation of a structure, system or component.
Potential CCF	A potential CCF means a dependent failure case, where the CCF conditions are not fully met, e.g. some of the components are only in degraded states.
Preventive maintenance	Actions that detect, preclude or mitigate degradation of a functional structure, system or component to sustain or extend its useful life by controlling degradation and failures to an acceptable level.
Probabilistic safety assessment (PSA)	A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.
PSA Level 1	PSA Level 1 comprises the assessment of plant failures leading to the determination of core damage frequency.
PSA Level 2	PSA Level 2 includes the assessment of containment response leading, together with Level 1 results, to the determination of containment release frequencies.
PSA Level 3	PSA Level 3 includes the assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimates of public risks.
redundancy	Provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other.
Redundancy	Redundancy means that a system is equipped with capacity in excess of the basic requirement (100% capacity), e.g., 2x100 % train system has 100% redundancy in one redundant train, and a 4 x 50 % system has 100% redundancy in two redundant trains. Redundancy can be introduced by additional identical trains or by diversity.
Return period	The inverse of the frequency of an extreme event; e.g., an event with frequency 0.001/year has the return period 1000 years.

Term	Definition
Risk Achievement Worth (RAW)	An importance measure expressing how much the core damage risk, or other risk measure used, increases if the unavailability of a certain safety function is set to unity (1.0).
Self-revealing failure	Failure state, which is detected by process symptoms; latent time is zero or negligible
Simultaneous failures	Failures occurring within one demand period (test or demand interval).
Single external event	External event occurring in isolation, i.e., not at the same time as another event.
single failure	A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.
Single Failure Criterion	A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.
System interaction	Cover dependencies, which are not ordinary functional dependencies but are specific to actual demand conditions and typically not detected in normal operation or by surveillance tests. The system interactions are often called as ”subtle dependencies” or ”subtle interactions”
Validation	The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgement, than verification.
Verification	The process of determining whether the quality or performance of a product or service is as stated, as intended or as required.

Appendix	Title	Report No
Appendix 1	Dependency Defence Guidance PR12	PR12
Appendix 2	Dependency Analysis Guidance PR13	PR13
Appendix 3	How to protect against dependent failures	
Appendix 3.1	Survey of defences against dependent failures PR05	PR05
Appendix 3.2	Defence Assessment in Data PR20	PR20
Appendix 4	How to model and analyse dependent failures	
Appendix 4.1	Model Survey PR04	PR04
Appendix 4.2	Impact Vector Method PR03	PR03
Appendix 4.3	Impact Vector Construction Procedure PR17	PR17
Appendix 4.4	Pilot Application (See Impact Vector Application to Diesel Generators PR10/Appendix 5.5)	
Appendix 5	Data for dependent failures	
Appendix 5.1	Data Survey and Review PR02	PR02
Appendix 5.2	Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11	PR11
Appendix 5.3	Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08	PR08
Appendix 5.4	Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09	PR09
Appendix 5.5	Impact Vector Application to Diesels PR10	PR10
Appendix 5.6	Impact Vector Application to Pumps PR18	PR18
Appendix 5.7	Impact Vector Application to MOV PR19	PR19
Appendix 5.8	A Statistical Method for Uncertainty Estimation of CCF Parameters Uncertainties PR15	PR15
Appendix 6	Literature survey PR06	PR06
Appendix 7	Terms and definitions PR14	PR14

App 8 Nordisk Arbetsgrupp för CCF Studier, Project Programme, PR01 PR01

ES-konsult
ENERGI OCH SÄKERHET AB

PM

Datum
2000-12-19
Sida
1(5)

Författare
Gunnar Johanson

Uppdragsgivare

Projekt
Nordisk Arbetsgrupp för CCF studier
Ärende
Projekt Program
Till

Kopia till

NORDISK ARBETSGRUPP FÖR CCF STUDIER

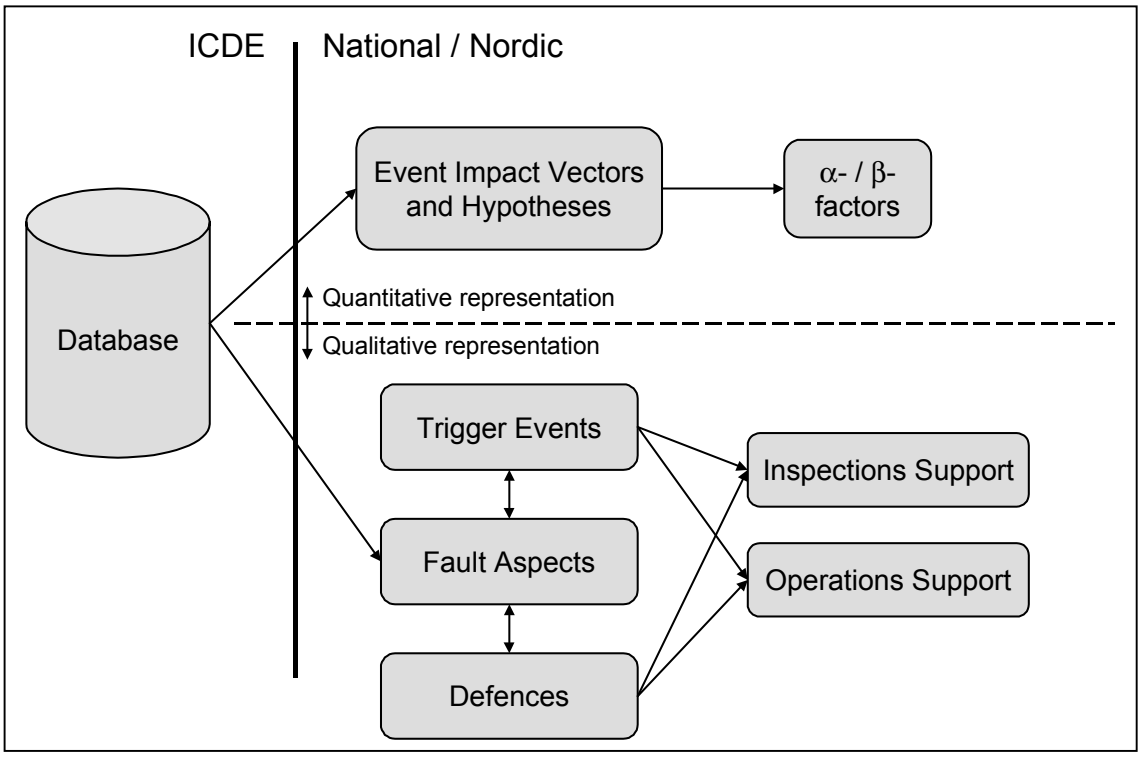
PROJECT PROGRAMME:

1 INTRODUCTION

This report present a project programme for assessment of CCF events and adoption of international data derived in the ICDE project to conditions in Sweden and Finland.

This report presents general and specific objectives for the different part of the programme in terms of task objectives, scope and limitations.

Today the international data exchanges have reached to a point, in respect to number of recorded events, that makes national in-depth assessment of CCF event meaningful.



2 PROJECT PROGRAMME

2.1 SURVEY AND REVIEW

As an initial phase of the project shall a survey be performed to provide an outlook on available experience in respect to models, data and plant operations. This activity shall verify the stated objectives with the project or shall provide background for corrections in plans and objectives.

2.1.1 MODEL SURVEY AND REVIEW

Problem statement: This survey shall examine available models and their applicability for use on the data. Several models exist and are used in the Nordic PSAs. The Basic Data Format shall be defined to allow for easy adoption to the relevant models.

Milestone deliverable: Task report

2.1.2 DATA SURVEY AND REVIEW

This survey shall examine available data sources and their applicability. Beside the ICDE exercise there are other data sources. The survey shall review other sources and provide a background for the decision on what data to be used. A possible outcome is of course that the ICDE data are shown to cover all other sources, but there are possibilities the ICDE data shall be combined with some other source. Further, the situation also differs depending on component type.

The data sources shall allow for transparency and shall allow for quality assurance of he input data.

Milestone deliverable: Task report

2.1.3 PLANT SURVEY

This survey shall provide a background to this project based on the needs and experience form the plant owners.

- Survey of plant objectives in relation to CCF defences
- Survey of plant operations/events in relation to CCF
- Survey of plant modifications in relation to CCF

Important elements of the plant survey are to carry out a dialog with the plant organisations to engage them in the issues related to this programme and to marked the outcome and use of the analysis.

The survey shall try to reach a wide spectrum of personnel from operation, design engineering, safety committees and risk assessment groups. The subjects for topical reports shall be discussed.

Deliverables:

2.2 QUANTITATIVE WORK AREAS

The quantitative work area cover activities related to the quantitative assessment of the data.

2.2.1 QUANTITATIVE MODELS

The procedure for common cause failure data analysis is intended to provide guidance on event analysis, the derivation of event statistics, and the estimation of model parameters.

- Impact vector model /methods
- Uncertainties (Qualitative , identify sources for uncertainties in terms of models and completeness)
- Guides /instructions for classification

CCF events do often contribute significantly to the PSA results and it is necessary to have the best estimates possible.

2.2.2 QUANTITATIVE CLASSIFICATION AND EVALUATION

It is important that the data analysis to be reviewable, and thereby achieve a certain level of credibility, the assumptions made through the analysis must be clearly documented. Examples can illustrate the types of decisions that must be made, and approaches used to extract the maximum amount of information from event descriptions, and to cope with lack of knowledge.

The events in a database usually involve some unique features. A description of classification rules shall be developed presenting how to deal with some commonly occurring situations and a format for documenting the analysis. The classification rules do not remove the need for subjectivity, but they lead to highlighting where and how the judgements are made.

The quantitative classification shall be applied on the available data, both preliminary and final. Plant specific information shall be recorded and consistency in classification shall be verified.

Plant specific features shall, thought transparency within the classification, be possible to consider when applying the data and in the choice of CCF - modelling approach. The approaches used must be general enough to support a variety of models, direct estimates, Alfa factors, CLM etc..

The presentation of basic CCF data will most likely be by Impact Vectors or an equivalent approach.

Any further manipulation of the data for Quantification of Alfa factors or other parameters will only be done to demonstrate the use of the data and in support for development of a software for plant specific adaptation of experience data. The software shall allow for a transparent derivation of plant specific parameters with their corresponding uncertainties.

The software shall record the quality assurance of input data carried out during the initial assessment.

2.3 QUALITATIVE WORK AREAS

Understanding the failure mechanisms is an important feature of the CCF methodology that relates to the determination of the transference of the applicability of a failure event from the plant where it occurred (original plant) to the plant of interest (the target plant).

2.3.1 QUALITATIVE MODELS

The data analysis process itself, by concentrating on failure mechanisms and possible defences, is likely to provide insights into the plant design and operation.

- Applicability aspects
- Human factors/ technical fault aspects
- CCF event defence aspects

The survey will provide proposals for topics to be analysed. The insights derived by a systematic qualitative analysis shall provide the background for experience feedback to operations/maintenance and inspections.

Depending on target group for the analysis may the format or the classification of event aspect differs, these variations must be determined and taken into account in the planning phase.

2.3.2 QUALITATIVE CLASSIFICATION

Carry out an application of qualitative classification on the available data. Assess the qualitative aspect in relation to CCF and present insight for development of defences.

2.4 MEETINGS

2.4.1 STOCKHOLM SEMINAR (JUNE 2001)

Arrangement of an international seminar and workshop to focus on the state of the art in applying and using CCF experience data to improve defences against CCF.

Objectives:

To present and discuss the aim with the International Common Cause Failure Data Exchange project - the ICDE project, for a wider audience.

To present the findings so far obtained from the International Common Cause Failure Data Exchange project.

Processing of experience and lessons learned from recorded dependent failures events for better performance of operation and of inspection of nuclear power plants.

2.4.2 WG MEETING

The Nordic-working group will carry out working groups meetings to discuss and evaluate deliverables and plans. The Steering committee will meet once per 6 month. The WG will meet more frequent.

2.5 TOPICAL REPORTS

This is a proposal for topical reports to be presented by the project. The survey and discussions with project participant will generate additional proposals to be considered. The topical reports are in addition to the task reports defined as deliverables in the previous sections.

2.5.1 HANDBOOK FOR CCF MANAGEMENT IN INSPECTIONS AND OPERATIONS

Handbook based on available experience presenting means for improving operations and inspections to prevent CCF

2.5.2 CCF DATA BOOK

Nordic data book on CCF. In the case a C-book will be presented the data book should have the same status as the T-book. The basic data format and the form of presentation (tables, software, etc.) will be decided during the quantitative model evaluation.

2.5.3 MODEL DEVELOPMENT

Report presenting the experience of the used quantitative and qualitative models used in the working group.

2.5.4 OTHER CANDIDATES FOR TOPICAL REPRTS

Several proposals exist on other candidates for topical reports. The following subjects have been mentioned but are not developed into any proposals. Proposals regarding these subjects and other will be evaluated in the WG when proposals exist.

- Recovery assessment
- Latent failures
- Cross system CCF
- Extreme weather

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se