SKI Report 2004:04

Research

Dependency Defence and Dependency Analysis Guidance

Volume 1: Summary and Guidance (Appendix 1-2)

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 1: summary and Guidance (Appendix 1-2)

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

This report concerns a study which has been conducted for the Swedish Nuclear Power Inspectorate (SKI). The conclusions and viewpoints presented in the report are those of the author/authors and do not necessarily coincide with those of the SKI.

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	

List of content

List of Figures

List of Tables

Referat

I ett kärnkraftverk med högt utbyggd redundans, domineras riskerna ofta av beroendefel, d.v.s. fel som samtidigt slår ut flera system eller systemstråk. Arbetsgruppen har haft som mål att söka stödja säkerhetsarbetet genom att studera potentiella och verkliga CCF och dra slutsatser som kan förbättra förståelsen av dessa händelser. Projektet har även kartlagt och utvärderat strategier för försvar mot olika beroenden, liksom metoder för identifiering och analys av dessa.

Resultaten från projektet presenteras i form av slutsatser och rekommendationer för tillämpning inom kärnkraftverkens drift, underhåll, inspektion och riskbedömningar. Rekommendationerna berör även bearberade statistiska data och former för modellering av beroenden i anläggningarnas PSA-studier. Denna rapport sammanfattar det arbete och den rapportering som har genomförts inom projektet från starten i mars 2001 till april 2003 då slutrapporteringen för projektet är färdig.

Projektet har samfinansierats av kraftbolag och myndigheter inom ramen för Nordiska PSA gruppens[1] verksamhet. Projektet har haft som inriktning att:

Kvalitativt - sammanställa och generera insikter från erfarenhetsdata i form av relevanta felmekanismer och effektiva skydd mot beroendefel, och dessutom att ge en inblick i möjliga säkerhetsförbättringar som kan stärka försvaret mot beroendefel och minska risken för CCF-händelser.

Kvantitativt - presentera en Nordisk CCF-databok (C-bok) i vilken kvantitativa insikter såsom ”Impact Vectors” och CCF-parametrar för olika redundansgrader redovisas. Osäkerheterna i CCF-data skall reduceras så mycket som möjligt. Med tanke på den stora riskpåverkan CCF-händelser har krävs en strukturerad kvantitativ analys resulterande i bästa möjliga skattning av realistiska och om möjligt anläggningsspecifika parametrar.

[1] Kontaktpersoner NPSAG, Göran Hultqvist/FKAB, Kalle Jänkälä/Fortum, Kajsa Eklöw/Ringhals, Ingemar Ingemarsson/Barsebäck, Risto Himanen/TVO, Ola Jonsson/OKG, Reino Virolainen/STUK och Ralph Nyman/SKI.

Abstract

The safety systems in Nordic nuclear power plants are characterised by substantial redundancy and/or diversification in safety critical functions, as well as by physical separation of critical safety systems, including their support functions. Viewed together with the evident additional fact, that the single failure criterion has been systematically applied in the design of safety systems, this means that the plant risk profile as calculated in existing PSA:s is usually strongly dominated by failures caused by dependencies resulting in the loss of more than one system sub.

The overall objective with the working group is to support safety by studying potential and real CCF events, process statistical data and report conclusions and recommendations that can improve the understanding of these events eventually resulting in increased safety. The result is intended for application in NPP operation, maintenance, inspection and risk assessments.

The NAFCS project is part of the activities of the Nordic PSA Group[2] (NPSAG), and is financed jointly by the Nordic utilities and authorities. The work is divided into one quantitative and one qualitative part with the following specific objectives:

Qualitative objectives-The goal with the qualitative analysis is to compile experience data and generate insights in terms of relevant failure mechanisms and effective CCF protection measures. The results shall be presented as a guide with checklists and recommendations on how to identify current CCF protection standard and improvement possibilities regarding CCF defences decreasing the CCF vulnerability.

Quantitative objectives-The goal with the quantitative analysis is to prepare a Nordic C-book where quantitative insights as Impact Vectors and CCF parameters for different redundancy levels are presented. Uncertainties in CCF data shall be reduced as much as possible. The high redundancy systems sensitivity to CCF events demand a well structured quantitative analysis in support of best possible and realistic CCF parameter estimates, if possible, plant specific.

[2] NPSAG contact persons, Göran Hultqvist/FKAB, Kalle Jänkälä/Fortum, Kajsa Eklöw/Ringhals, Ingemar Ingemarsson/Barsebäck, Risto Himanen/TVO, Ola Jonsson/OKG, Reino Virolainen/STUK och Ralph Nyman/SKI.

1 Project Introduction PR01

The NAFCS project is part of the activities of the Nordic PSA Group (NPSAG), which is made up jointly by the Nordic utilities and authorities. The NAFCS project is performed during the years 2001 – 2003, and the NAFCS Project Program [Ref-1] includes activities within the following fields:

- Survey and review of analysis models and data sources
- Survey of defences against dependent failures
- Analysis of Nordic CCF data from the ICDE database and other sources
- Development of impact vectors for defined components
- Estimation of CCF parameters and associated uncertainties
- Development of Dependency Defence Guidance
- Development of Dependency Analysis Guidance

The International Common-Cause Failure Data Exchange Project ("ICDE Project") constitutes essential background to the NAFCS project [Ref-19].

The following persons have been members in the project team.

Gunnar Johanson, ES konsult AB. Project leader.

Jean Pierre Bento, JPB Consulting AB,

Per Hellström, Relcon,

Michael Knochenhauer, Impera-K AB,

Tuomas Mankamo, Avaplan Oy,

Kurt Pörn Pöm, Consulting AB

1.1 Achievement of High System Reliability: Design & Plant Aspects

As a basis for achievement of high system reliability, it is required to use reliable components with proven design and operating records for the expected application and environment. Fail-safe design and passive functional modes are other examples of factors contributing to high system reliability.

It is also needed to have enough justification from testing and deterministic analyses. The above also presupposes the use of skilled and sometimes certified personnel in design, manufacturing, installation, and operation.

A system for the reporting of component failures and exchange of experience between different users of the same type of equipment and from the same manufacturer contributes further to high system reliability and availability.

The reliability possible to achieve with a single channel/train system is at the very best, supposing close adherence to the safety principles mentioned above, equivalent to a failure probability in the vicinity of 10^{-3} / demand. Such a value is generally considered not low enough for many service systems in nuclear power plants. This is even more valid for safety systems where the reliability requirements are far more demanding. The solution to reach the required reliability (safety) level is to introduce redundancies in the plant systems, complemented with a diversification of systems utilised for critical safety functions. The reliability range of different system configurations is exemplified in Figure 1-2.

1.2 Objectives

The safety systems in Nordic nuclear power plants are characterised by substantial redundancy and/or diversification in safety critical functions, as well as by physical separation of critical safety systems, including their support functions. Viewed together with the evident additional fact, that the single failure criterion has been systematically applied in the design of safety systems, this means that the plant risk profile as calculated in existing PSA:s is usually strongly dominated by failures caused by dependencies resulting in the loss of more than one system sub.

The overall objective with the working group is to support safety by studying potential and real CCF events, process statistical data and report conclusions and recommendations that can improve the understanding of these events eventually resulting in increased safety, Figure 1-1. The result is intended for application in NPP operation, maintenance, inspection and risk assessments.

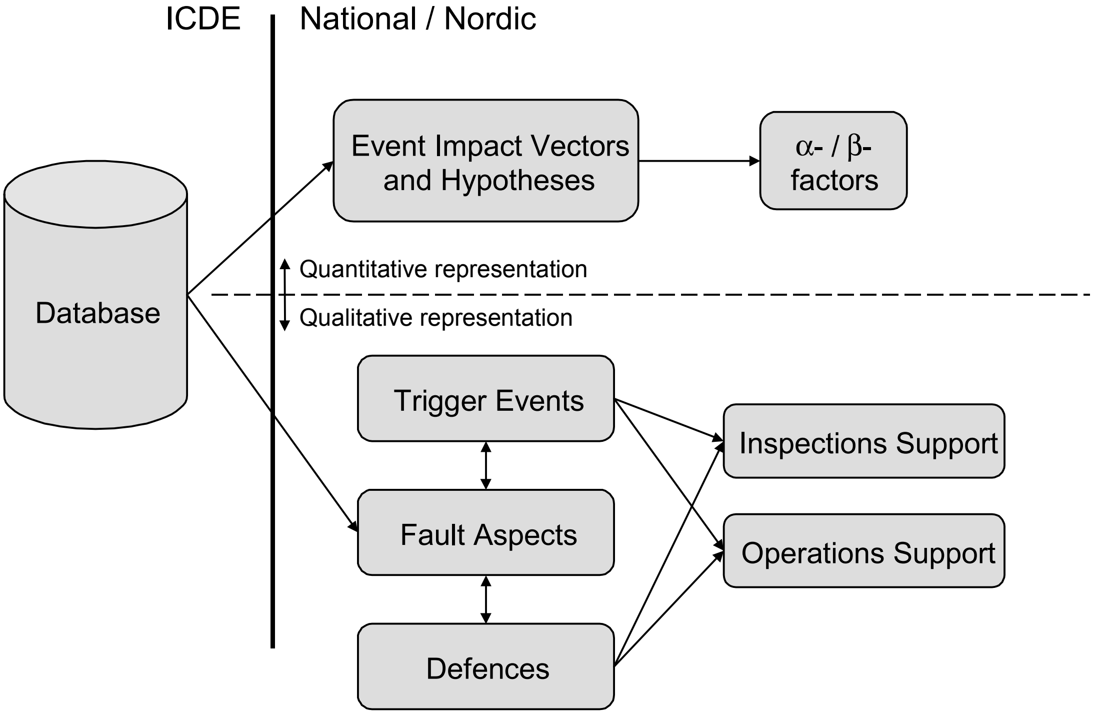


Figure 1-1. Project idea - To improve the understanding of CCF events eventually resulting in increased safety.

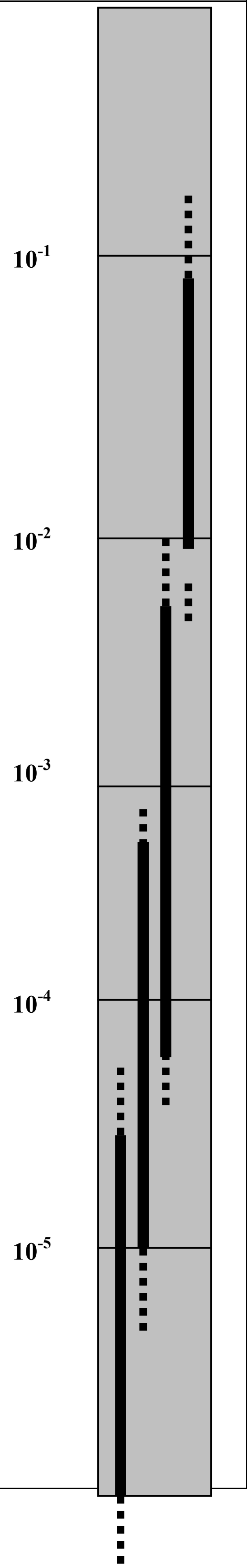
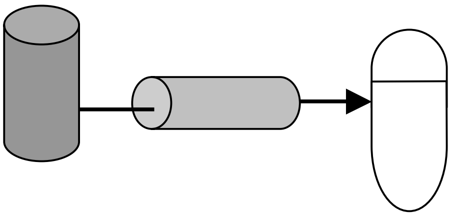
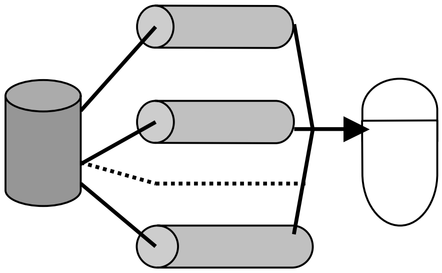
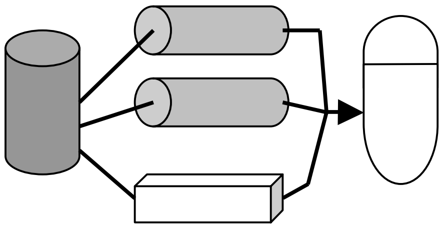
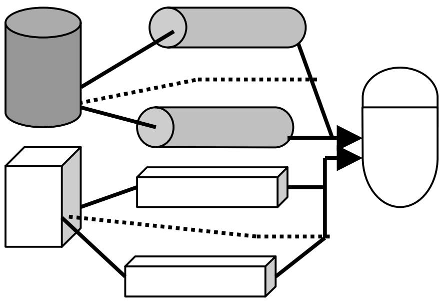
System Configuration		Defence	Failure Probability
		Technical and administrative	
Single train system		- Fail safe - Management system - Work preparation - DKV (operability readiness control) - Work practices	
Redundant system N out of m		Redundancy Separation - Functional separation - Organisational time-wise separation Stepwise introduction and test & maintenance	
Diverse system		Functional diversity	
Fully redundant and diversified systems/functions		Redundancy within diverse sections Operational diversity Software diversity	

Figure 1-2. Reliability (indicative values) of different system configurations

The work is divided into one quantitative and one qualitative part with the following specific objectives:

Qualitative objectives:

> The goal with the qualitative analysis is to compile experience data and generate insights in terms of relevant failure mechanisms and effective CCF protection measures. The results shall be presented as a guide with checklists and recommendations on how to identify current CCF protection standard and improvement possibilities regarding CCF defences decreasing the CCF vulnerability.

Quantitative objectives:

> The goal with the quantitative analysis is to prepare a Nordic C-book where quantitative insights as Impact Vectors and CCF parameters for different redundancy levels are presented. Uncertainties in CCF data shall be reduced as much as possible. The high redundancy systems sensitivity to CCF events demand a well structured quantitative analysis in support of best possible and realistic CCF parameter estimates, if possible, plant specific.

1.3 Project Scope

1.3.1 SURVEY AND REVIEW

As an initial phase of the project surveys were performed to provide an outlook on available experience in respect to models, data and plant operations. This activity was also performed to verify the stated objectives with the project or to provide background for corrections in plans and objectives.

The model survey and review examines 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.

The data survey and review examines available data sources and their applicability. Beside the ICDE exercise there are other data sources. The survey reviews other sources and provides a background for the decision on what data to be used.

The plant and regulator survey provides a background to this project based on the needs and experience from the plant owners and national regulators. Important elements of the survey has been to carry out a dialog with the organisations to engage them in the issues related to this programme and to marked the outcome and use of the analysis. The survey tried to reach a wide spectrum of personnel from operation, design engineering, safety committees and risk assessment groups.

Stockholm ICDE 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.

- 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.

The conclusions from the seminar are taken into account in the initial planning of the NAFCS project and are reported separately in OECD/NEA report (Ref-20).

1.3.2 QUANTITATIVE WORK AREAS

The quantitative work area cover activities related to the analysis of dependencies in general and quantitative assessment of dependent failures in the data. 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. CCF events do often contribute significantly to the PSA results and it is necessary to have as accurate estimates as possible. It is important that the data analysis is review able, and thereby achieve a certain level of credibility, the assumptions made through the analysis must be clearly documented.

The events in a database usually involve some unique features. A description of classification rules has been 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 has been applied on the available data. Plant specific information shall be recorded and consistency in classification shall be verified.

1.3.3 QUALITATIVE WORK AREAS

Understanding the failure mechanisms is an important feature of the CCF methodology that relates to the determination of the transfer of the applicability of a failure event from the plant where it occurred to your own plant design or organisation. The data analysis process itself, by concentrating on failure mechanisms and possible defences provides insights into the plant design and operation such as:

- Applicability aspects
- Human factors/ technical fault aspects
- CCF event defence aspects

2 Outline of project reporting

The general areas covered in the NAFCS project were outlined in the previous section.

The different reports produced, and their use in producing the two main topical reports, the Dependency Defence Guidance and the Dependency Analysis Guidance, are indicated.

A number of topical reports have been presented by the project. The relation between these report are presented in Figure 2-1.

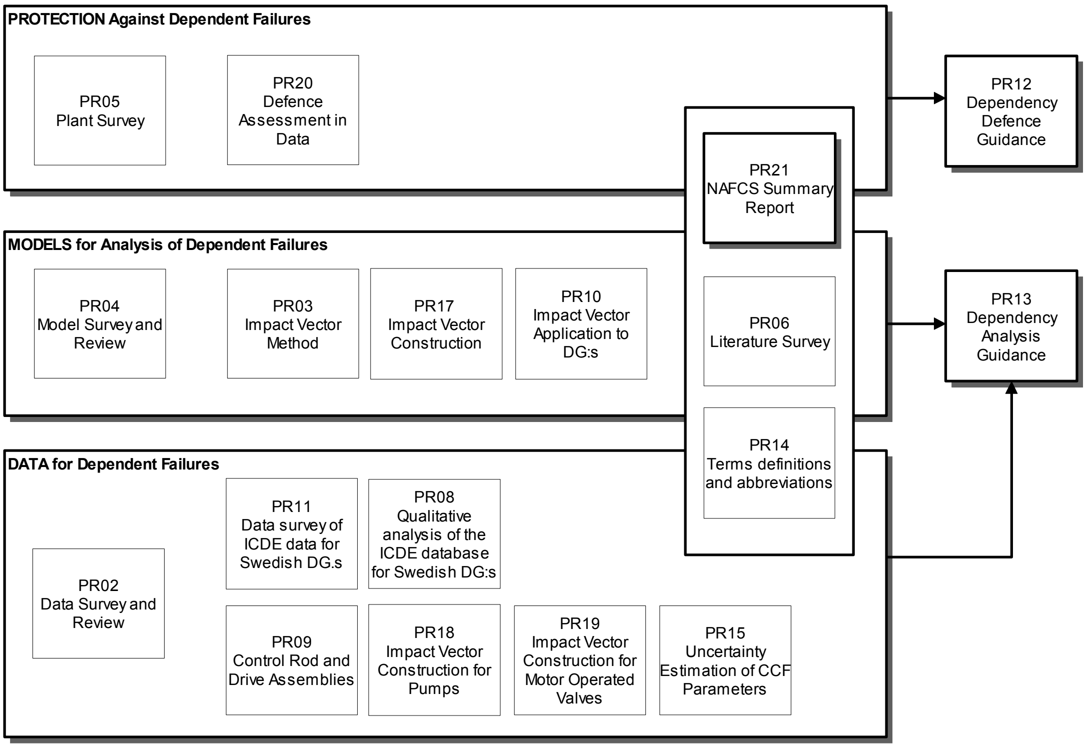

PROTECTION Against Dependent Failures
PR05 Plant Survey
PR20 Defence Assessment in Data
PR12 Dependency Defence Guidance
PR21 NAFCS Summary Report
MODELS for Analysis of Dependent Failures
PR04 Model Survey and Review
PR03 Impact Vector Method
PR17 Impact Vector Construction
PR10 Impact Vector Application to DG:s
PR06 Literature Survey
PR13 Dependency Analysis Guidance
PR14 Terms definitions and abbreviations
DATA for Dependent Failures
PR11 Data survey of ICDE data for Swedish DG.s
PR08 Qualitative analysis of the ICDE database for Swedish DG:s
PR02 Data Survey and Review
PR09 Control Rod and Drive Assemblies
PR18 Impact Vector Construction for Pumps
PR19 Impact Vector Construction for Motor Operated Valves
PR15 Uncertainty Estimation of CCF Parameters

Figure 2-1. Relation between project reports

How to protect against dependent failures

Presentation of guidance for CCF management in inspections and operations. The Guidance is based on available experience presenting means for improving operations and inspections to prevent CCF

- Dependency Defence Guidance PR12
  - Efficiency of Protective Measures
  - Work procedures for defence against dependencies
- Survey of defences against dependent failures PR05
- Defence Assessment in Data PR20

How to model and analyse dependent failures

Presentation of Model development and the development of procedures and pilot applications. The reports present the experience of the used quantitative and qualitative models used in the working group.

- Dependency Analysis Guidance PR13
- Development of quantification procedure
  - Model Survey PR04
  - Impact Vector Method PR03
  - Impact Vector Construction Procedure PR17
  - Pilot Application (Impact Vector Application to Diesel Generators PR10)

Data for dependent failures

Presentation of Data development and CCF parameters

Analysis of Nordic CCF data

- Data Survey and Review PR02
- Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11
- Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08
- Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09

Component type- specific CCF event analysis and estimation of CCF parameters

- Diesels PR10
- Pumps PR18
- MOV PR19
- Uncertainties PR15

Part I Qualitative work areas

The qualitative part of the project include survey and review followed by qualitative model development and data classification in support of development of a dependency defence guidance to be used in safety work together with the quantitative results of the project:

3 Dependency Defence Guidance PR12

The main objective with the Dependency Defence Guidance is to provide guidance on defences against dependencies in cases where redundancy is applied to achieve a high reliability in safety critical systems, especially functions and systems in nuclear power plants. The use of the guidance will contribute to lower and control the risk contribution from dependencies originating from plant design and review, construction, commissioning, operation, maintenance, testing, and modifications.

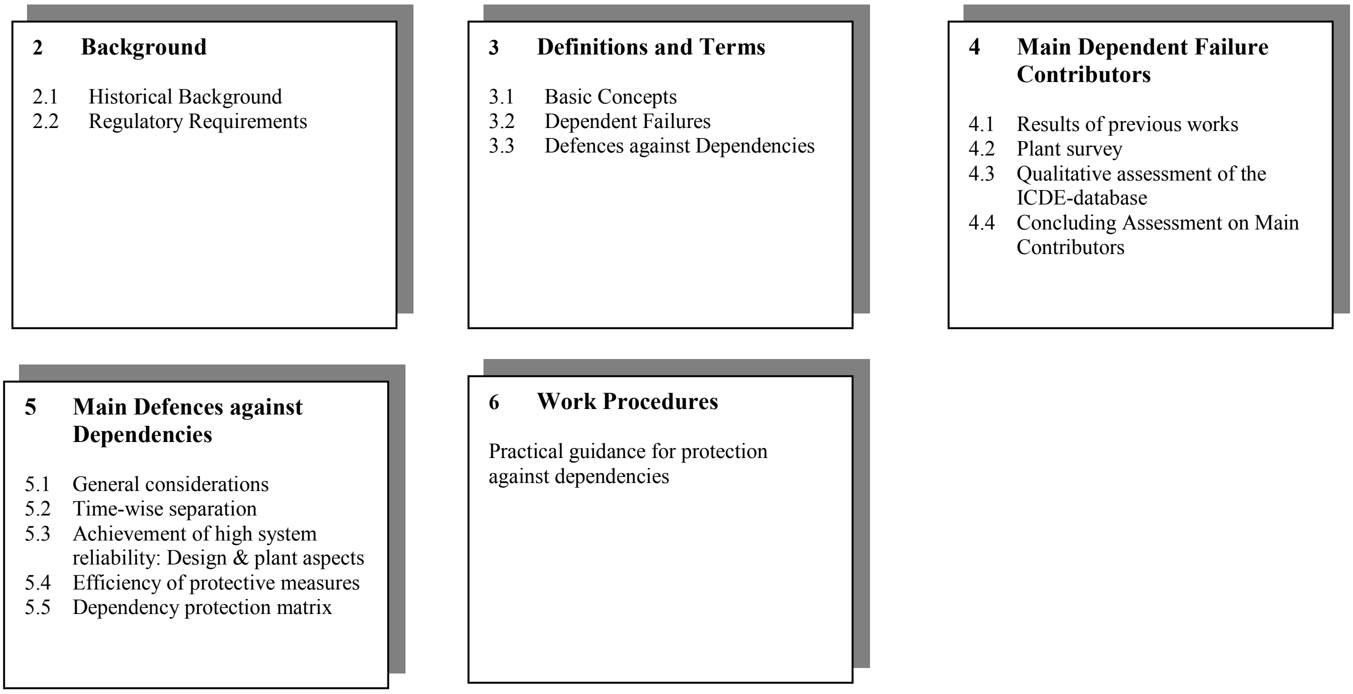
The guidance is intended for plant management and staff, as well as regulators. The complexity and importance of the dependency issues on nuclear safety may require that more specific guidance and instructions need to be developed and established for use in the utilities and regulators own organisations, e g for consideration in case of plant changes during modernisations and in inspection activities. The guidance can additionally be considered in a broader context including the development and implementation, on a national scale, of explicit guidelines and educational and training material concerning dependency defences.

It covers plant design, design review, installation, operation, maintenance, testing, and modifications. Operational experience feedback is also covered.

The Dependency Defence Guideline:

- Present dependency defences that can be utilised by the licensees as a checklist in relation with operational and other activities, and as a learning document for the whole plant staff.
- It summarises the requirements concerning defences against dependent events in Sweden and Finland.
- It gives an overview and summarises the dominating contributors to CCF.
- It includes a presentation of defence against dependent failures in system redundancies and related set of defence mechanisms.
- Give methodology guidance and describes work procedures the for efficient defences or good practice in view of dependent failures
- Give a description of the interaction of the Guideline with other NAFCS project reports.

The main sections in the dependency defence guidance are shown in the figure below.



2 Background

2.1 Historical Background
2.2 Regulatory Requirements

3 Definitions and Terms

3.1 Basic Concepts
3.2 Dependent Failures
3.3 Defences against Dependencies

4 Main Dependent Failure Contributors

4.1 Results of previous works
4.2 Plant survey
4.3 Qualitative assessment of the ICDE-database
4.4 Concluding Assessment on Main Contributors

5 Main Defences against Dependencies

5.1 General considerations
5.2 Time-wise separation
5.3 Achievement of high system reliability: Design & plant aspects
5.4 Efficiency of protective measures
5.5 Dependency protection matrix

6 Work Procedures

Practical guidance for protection against dependencies

Figure 3-1. Content of Dependency Defence Guidance

3.1 Efficiency of Protective Measures

The assessment of the efficiency of the protective measures against the occurrence of dependent failures is a delicate task, mainly due to the complicated and mutual influences of the different measures on the efficiency of each other. It is furthermore not possible to rank different phases in the life of an installation, system or component as regards to the most important phase for the protection against CCF. All phases are important and complement – are dependent upon - each other.

A manageable assessment has in practice to consider each protective measure and each plant life phase independently. This approach has been followed here as a base for an aggregated engineering judgement.

The plant survey carried out as part of the NAFCS project [NAFCS-PR05] evaluated the efficiency of different defences against dependent failures according to plant personnel. The result is shown in Table 3-1, listing without prioritisation such defences. It can be observed that a basic defence like diversity has been left out. The reason for doing so is that diversity is most likely already established.

Table 3-2 indicates the decisive impact that managerial and organisational systems have on the efficiency of protective measures against the occurrence of dependent failures. It is furthermore judged that many of these systems and practices can be robustly implemented and verified at relatively low costs. The long-term benefits of these systems and practices, if clearly supported by the upper management, are obvious for the prevention and identification of dependent failures.

The indications on efficiency and cost in the table are based mainly on engineering judgement. Of course, the efficiency and cost relation need to be investigated for a specific case, before implementation of new or improved measures.

Table 3-1: Efficient defences against unwanted dependencies (Plant survey)
Awareness about dependencies (increased)
Simple solutions
Knowledge and experience
Good safety culture
Effective feedback of experience
Review in several steps
Tests, use of information system

Table 3-2: Efficiency and costs of different preventive measures against dependencies.

Protective measure against CCF	**Efficiency**	**Implementation efforts/costs**	**Verification efforts/costs**
Diversity	High	High	[low – high]
Functional separation	High	[low – high]	[low – high]
Physical separation	High	High	[low – high]
Organisational separation			
- Stepwise installation	[low – high]	Low	Low
- Maintenance and testing	[low – high]	Low	Low
Management systems:			
- Design and design review	[low – high]	Low	Low
- Installation and commissioning	[low – high]	Low	[low – high]
- Operation	[low – high]	[low – high]	Low
- Test and maintenance programme (preventive & corrective)	[low – high]	[low – high]	Low
- Operating experience feedback (including event & failure reporting, root cause analysis, corrective action programme & implementation of corrective measures)	[low – high]	[low – high]	Low
Work organisation (including work preparation and operability readiness control)	[low – high]	Low	Low
Work practices (including respect of procedures, collective & individual self-checking)	[low – high]	Low	Low
Operational, maintenance & test procedures	[low – high]	Low	Low

3.2 Work procedures for defence against dependencies

Practical guidance for the defence and control of dependencies is provided. It would be naïve to postulate that this guidance is fully covering, although concerted efforts have been made towards this goal.

The guidance complements the presentation of the mostly technically oriented defences against dependencies in the previous section. It covers furthermore the different phases in a plant life, i.e. from design to operation. Part of the guidance is based on a plant survey that compiled proposals against dependencies mentioned by plant representatives [NAFCS-PR05]. Other parts of the guidance are based on international literature and plant experience.

The guidance on defence mechanisms and good practices is presented according to the following grouping with one table for each group:

1. Design and design review
2. Construction, installation and commissioning
3. Operation
4. Test and maintenance
5. Reporting and plant information system
6. Experience feedback
7. Other defences

4 Survey of defences against dependent failures PR05

The purpose of this report is to present the result of the plant survey carried out within the qualitative investigation on defences against dependent failures. The survey provide a background to the 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

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

There are several ways of achieving a high reliability in a safety system. 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 – many are identified as part of the plant and regulatory survey presented in this report. The most important types of separation used are: Functional, spatial and design separation (technical defences) and time separation.

Different types of time separation are administrative defences. Time separation by stepwise introduction of new equipment, staggered testing and similar need to be combined with efficient systems for testing, failure reporting and plant information. The plant information system need 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 [NAFCS-PR12.]. 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 means 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 takes 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.

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, and 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?

5 Defence Assessment in Data PR20

Proposals for defences against MTO-related CCF events are presented based on defence assessment in data. 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.

5.1 Defences against MTO related CCF

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.

As an example of the conclusions presented in the report [NAFCS-PR20] the discussion on Improvement of “self-checking” are presented here in short. In the report details are presented for the different areas mentioned above.

In a plant/company with high safety culture it is expected that each individual – notwithstanding his/her organisational level – exhibit 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.

5.2 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 [NAFCS-PR08] 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 [NAFCS-PR08].

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 [NAFCS-PR12] and [NAFCS-PR13].

Part II Quantitative work areas

6 Dependency Analysis Guidance PR13

All PSA:s have included a thorough identification and modelling of both functional and physical dependencies. The different PSA analysis tasks are tailored to identify, model and derive data for all important dependencies, e g the accident sequence analysis, the systems analysis, the analysis of common cause initiators (CCI), area events and external events analysis put special emphasis on identifying mechanisms and interactions that need dependency analysis consideration. Dependencies are in most cases considered by explicit modelling, but there is always a fraction with dependencies that either not are known, or not suited for explicit modelling. These dependencies are collectively called common cause failures (CCF) and they are in PSAs treated by CCF analysis methodology.

Figure 6-1 provides an overview of the different dependency types, and how they are considered in safety analysis.

Functional (direct or indirect) Failure of a component or operator makes another component unavailable	Explicitly unknown or chosen to be represented by Common Causes Failure Modeling	Explicitly known functional dependencies: represented by explicit modeling. Fault trees, event trees, operator actions Identification of functions: systems, structures and components, support systems, CCI analysis
Physical A common condition fails one or more other components. The condition can be caused by a failure/unavailablity of another component or initiating event. Examples: On site events (fire, flooding), Off site events (air plane crash, earthquake), Dynamic effects after LOCA, harsh environment etc.		Explicitly known physical dependencies: represented by explicit modeling. Fault trees, event tree, operator actions: Adjustment of conditional failure probabilities: Dynamic effects etc identification and modeling, area events analysis, external events analysis

Figure 6-1. Dependencies and their consideration in PSA

This means that the completeness and relevance of the identification and modelling of the various dependency categories has a strong influence on the completeness and relevance of the PSA itself.

The purpose of the Dependency Analysis Guidance is to constitute a common methodological guidance for the analysis of dependencies in Nordic PSA:s. The Guidance is meant to clarify the scope of the analysis of the various dependency categories, the interaction of the various analyses and their PSA context, as well as to provide guidance for the performance of the analysis of the various dependency categories.

The analysis of dependent failures is a comprehensive task. The sub-task "Analysis of dependent failures", which is normally found in PSA:s, will typically include only part of the analysis. In addition, parts of the analysis are usually performed as part of a number of different PSA sub-tasks, such as the analysis of initiating events, systems analysis, HRA and data analysis. In view of this split-up of the analysis, which is largely justifiable, one important aim of the Guidance is to provide an integrated description of analysis of dependent failure within a PSA.

Thus, the Dependency Analysis Guidance aims at giving a complete overview of the types of dependencies that need to be considered in a PSA and to sum up the requirements in the Nordic countries concerning analysis of dependencies. Furthermore, guidance is given for each type of dependency as how to perform the analysis. As far as possible, this is done by referring to existing handbooks and guidelines. Especially, documents developed as part of previous or on-going Nordic projects will be given as references.

The Dependency Analysis Guidance:

- Presents methodological guidance for the analysis of dependencies in Nordic PSA:s
- It summarises the requirements concerning analysis of dependent events in Sweden and Finland.
- It includes a complete identification of the basic types of dependencies (dependency category), and their mutual relationships.
- Give methodology guidance, but includes no method development. It describes the analysis methodology for each of the defined dependence categories. This includes descriptions of analysis context, input, output and documentation, as well as of the analysis methodology along with the relevant references.
- Give the term dependencies wide interpretation, and includes all external impacts or interactions, which may affect the independence of barriers.
- Give a description of the interaction of the Guidance with other NAFCS project reports.

The Guidance do not present *one* integrated approach, suited for inclusion into one "dependency analysis project", but rather present a framework for defining the various tasks needed in order to assure completeness and relevance in the analysis of dependencies. These tasks may be realised in different sub-projects, or as part of other major PSA tasks. Further, the Guidance does not include detailed information about the methods, nor practical implementation. Instead, references are given to relevant data sources, handbooks and dependency type-specific guidelines.

The Guidance is meant to describe relevant dependency categories and to clarify the scope of the analysis of the categories. It also describes the interaction of the various analyses and their PSA context, and provides some methodological guidance for the performance of the various analyses.

The discussion in the Dependency Analysis Guidance report has resulted in the definition of a number of dependence categories that need to be treated in a PSA. They are listed in Table 6-1.

Table 6-1: Summary of Dependence Categories

	Dependence category	**Description**	**Guideline chapter**
Functional	Functional Dependencies	Dependence on shared mechanical or electrical equipment, such as common support systems, power supply or control signals.	4
	Human Action Dependencies	Dependence via shared human actions: 1) Failures of consecutive actions to mitigate a transient or accident sequence 2) systematic test or maintenance errors.	5
	Subtle Dependencies	Dependencies specific to the actual demand conditions and typically not detected in normal operation or by surveillance tests.	6
Initiator	Common Cause Initiators	Initiating event, which arises from the system or component failures, or from the disturbances in the plant processes (intrinsic events).	7
	Area Events	Events occurring within the plant, but outside of plant systems and processes	8
	External Events	Events occurring outside the plant, and outside of plant systems and processes	9
	Dynamic Effects	Failures in connection dynamic effects occurring together with pipe breaks	10
CCF	Common Cause Failures	Failure of identical (or closely similar) components due to common vulnerabilities	11

In this context it may be worth pointing out, that it is impossible to make a perfect classification in the sense that the categories would both represent complete coverage and at the same be mutually exclusive, because of mixed dependence types. The aspect of complete coverage is more essential, and is judged to be fulfilled by the categories defined.

7 Analysis of Nordic CCF data from the ICDE database and other sources

7.1 Data Survey and Review PR02

A survey and description of the internationally published CCF data sources that are relevant and applicable for the Nordic PSA studies are presented.

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.

First of all the current data contents of ICDE are summarized in. The ICDE data base is regarded as preferred source of international CCF data. As complementary sources selected references are surveyed, including the following:

- NUREG reports
- EPRI reports
- ISPRA/CCF Benchmark
- Nordic specific CCF analyses

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 ICDE database is of fundamental importance. The aim is an efficient use of the ICDE data in the Nordic PSA studies.

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

Table 7-1: Current contents of ICDE database, status in December 2001.

Internationally published CCF data 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 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 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.

Risk-importance of main component types:

This survey presented 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.

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:
    - ICDE data, mapped to the conditions in the Nordic NPPs as far as possible
    - Component-type specific CCF analysis such as made for the BWR safety/relief valves and control rods/drives
    - 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.

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 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].

7.2 Data survey and review of the ICDE-database for Swedish emergency diesel generators PR11

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.

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.

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.

7.3 Qualitative analysis of the ICDE database for Swedish emergency diesel generators PR08

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. Potential corrective actions against CCF events in the Swedish emergency diesel generators are discussed.

The objectives of the 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.

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 presented observations have thus to be considered as one input in a broader discussion within the industry about potential physical and organisational barriers against 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.

7.4 Updating the CCF Analysis of Control Rod and Drive Assemblies for the Nordic BWRs PR09

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, [Ref-22] and work reports collected in the compendium SKI/RA-26/96, [Ref-23]. A compact summary exists in the form of the conference paper RS-PSA99, [Ref-25].

The survey conclusions are summarized in the form of proposed tasks for the CCF analysis update.

8 Development of quantification procedure

8.1 Model Survey PR04

The emphasis is on collecting the definitions of the CCF models, which are mostly used in the Nordic PSA studies, 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.

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.

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 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 Alpha Factor Method (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 Sub Group Failure Probabilities then into form of CCF parameters (Alpha Factors, Multiple Greek Letters) for the presentation of relative dependence level or for comparison purpose.

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.

In practical uses of the parametric CCF models, such as Alpha Factor Method, Multiple Greek Letter Method 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 or not at all correlated to the single failure probability.

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. In fact, 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.

8.2 Impact Vector Method PR03

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].

Impact vector expresses the conditional failure probability, given an observed 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 in the presence of the CCF mechanism.

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, but chances of several states exist. 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.

Topical report PR03 presents the definition, theoretical background and methodological aspects of impact vectors to support the practical instructions that are presented in separate report PR17, see next section. The method description handles the use of scenario method in different types of CCFs, including the rather usual cases, where the detection of component failures or degradations are spread in time, e.g. over consecutive staggered tests. The connections to the estimation of multiple failure probability and CCF parameters are clarified. New development includes the derivation of low and high bounds of the impact vector from the component degradation values, when these are interpreted as conditional failure probability. The low bound assumes complete independence and high bound maximum dependence between the component degradations. The component degradation values are much easier to assess in practice than the impact vector. Unfortunately, there is no generally valid one-to-one correspondence between these two entities. The bounds are determined by the basic laws of probability, and very 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).

Transferring data (impact vectors) between CCF groups of different sizes, using so called mapping down and mapping up, is also clarified. It is concluded that mapping down is a rigorous technique, based on the laws of probability. In contrary, mapping up is controversial extrapolation, requiring additional judgment about how a CCF event observed in a smaller group would affect a bigger group. Therefore, mapping up should be avoided in data pooling over CCF groups of different sizes.

The developed methodology is based on the experiences that have been cumulated in several earlier CCF analyses SKI TR-91:6, [Ref-24], SKI R-96:77, [Ref-22]. The impact vector method was initially established in the USA, see the most current reference NUREG/CR-5485, [Ref-28], which includes also an integral description of the various CCF analysis parts.

There are several specific topics that would require further elaboration:

- How to control in a consistent manner test staggering influence across event coding (ICDE data collection), event analysis (impact vector construction) and estimation/modeling/quantification. This issue is more broadly concerned with the control of time dependence in the CCF mechanisms.
- Procedures how to pool data over different group sizes without controversial mapping up, especially in the case of Exposed Populations, when the group sizes can have a large variation
- Transferring CCF data (impact vectors) to different target conditions, i.e. taking into account differences in CCF defenses, especially in test arrangements. This need is expected to be critical in the future use of foreign ICDE data, especially for the components of specific design such as safety/relief valves and control

rods/drives. Also, under which conditions to credit preventive measures taken after the occurred CCF?

- Procedures to construct a crude best estimate of impact vector based on component degradations values, and other key attributes of the CCF event. Such a "formula-driven" technique is needed as a short cut for using foreign ICDE data, because it has proven too laborious to conduct specific expert assessment of impact vectors for the foreign events. Compare to the assessment difficulties experienced in the applications to be discussed in the following sections.
- Guidance for explicit modeling of specific types of CCF mechanisms, which are not suited to be covered by parametric CCF models. A large portion of this type of CCFs were observed in the pump application [NAFCS-PR18].

8.3 Impact Vector Construction Guide PR17

The guide report PR17 provides practical, step-wise instructions for the impact vector construction. The general flow of construction is presented in Figure 8-1. 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 as contained in the ICDE data are in most cases sufficient for the impact vector construction. Compare to Figure 8-2, which shows the essential information connections. 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. Often it is most helpful to contact a plant specialist to verify correct understanding and interpretation of what happened. This was a main lesson learnt in the conducted applications to DGs, pumps and MOVs to be discussed in the following sections. It would be optimal to construct impact vectors in parallel to the ICDE data collection in order to limit the work load and to improve overall QA.

The guide discusses the interpretation of the impact vector in practical aspects, including the relationship with component degradations values and other characteristics of the CCF event (ICDE data entries such as Time Factor and Latent Time). Advices are given how to apply the scenario method in different type cases such as time spread component events. A number of fully elaborated example cases are included in the annex of the guide.

Screening advices are given to exclude "weak" CCF cases such as preventive design change at an incipient stage, after having observed the problem early without multiple components affected or with negligible impact yet in more than one component. It can be useful to include these cases in qualitative analysis, for example, to learn about efficient CCF defences, but for quantitative analysis the statistical gain would be negligible. It is thus recommended to place the weak CCF cases in a separate basket to unload the impact vector construction.

The QA practices followed in the impact vector construction are based on the American procedure NUREG/CR-6268v1, [Ref-29]. The cornerstone is redundant assessment of the impact vectors by two analysts. The followed practices and organization of the documentation is presented in the description of the DG Pilot in the next section. 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. Auditing is proposed to be carried out by the members of the NAFCS working group. In overall, 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.

The first applications proved rather laborious. It is expected that the labour requirements will reduce in the continuation due to learning effect and possibility to unburden the documentation work by moving from the use of standard office software to relational database platform. 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, as already said, facilitate improved overall QA.

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. The QA should be linked with the ICDE frame.
- Develop 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. The tools for impact vector construction and data pooling 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.
- Improve the guide of impact vector construction along with cumulating expertise from continued quantitative analysis, supplement example cases

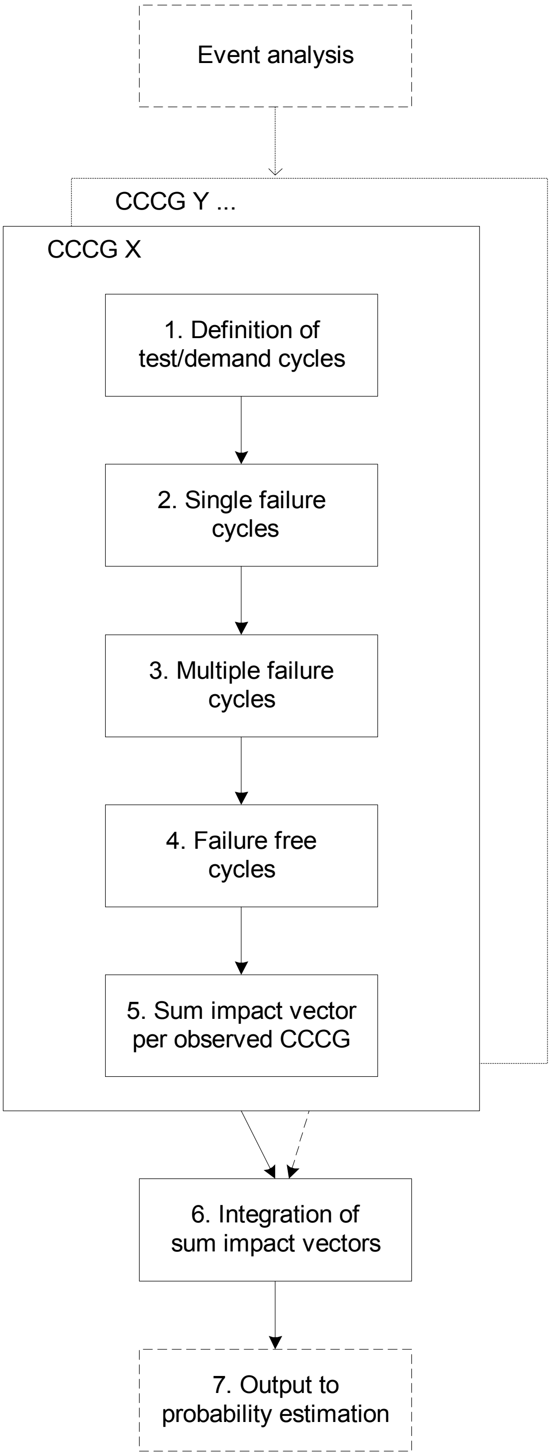

Event analysis
CCCG Y ...
CCCG X
1. Definition of test/demand cycles
2. Single failure cycles
3. Multiple failure cycles
4. Failure free cycles
5. Sum impact vector per observed CCCG
6. Integration of sum impact vectors
7. Output to probability estimation

Figure 8-1 Steps and flow of impact vector construction.

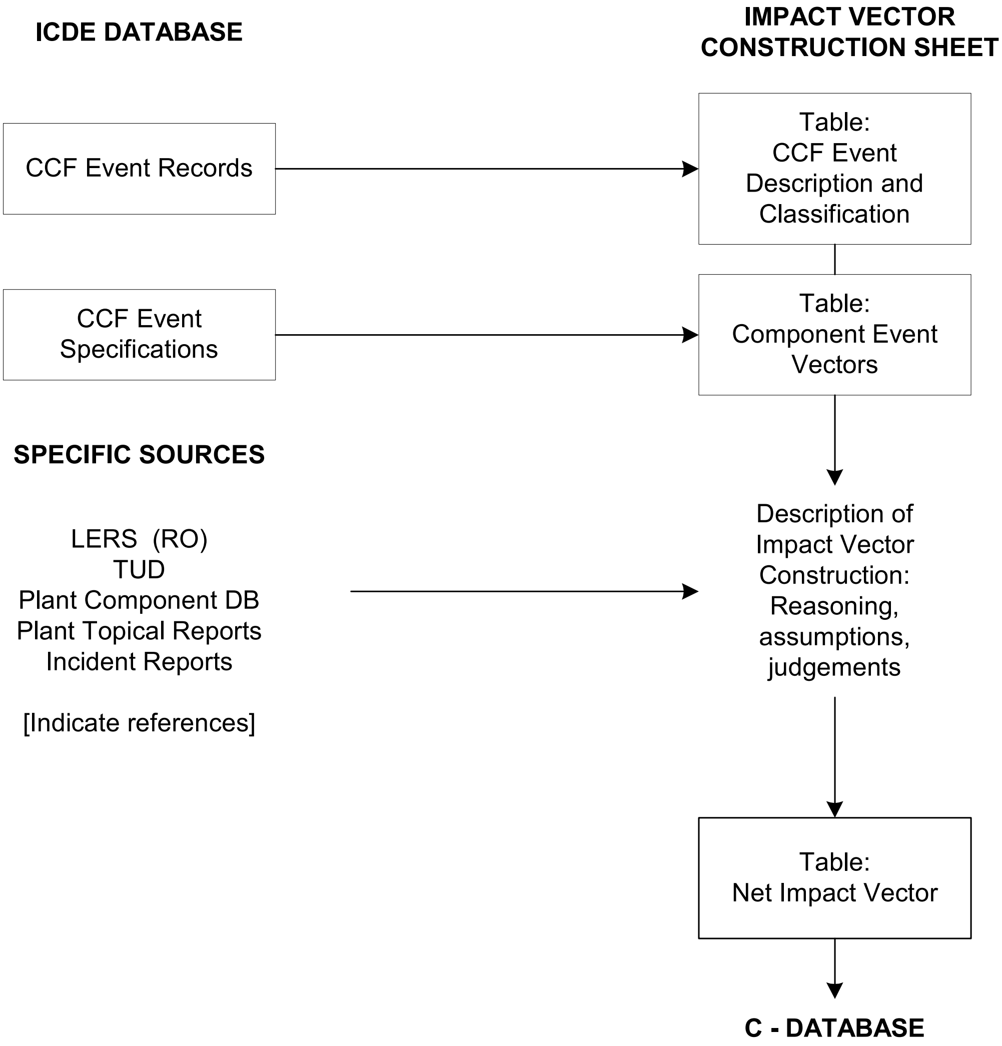


Figure 8-2 Information connections in impact vector construction.

8.4 Pilot Application, Construction of Impact Vectors for Diesel Generators, PR10

The objective of the DG pilot is to develop framework, working procedures, database structures and QA procedures for the construction of impact vectors. The insights were used for the development of the impact vector guideline, creating type examples to facilitate practical work in the continuation.

The pilot covers DG events as reported to ICDE (status in December 2001) for the Nordic NPPs. The observation period reported to ICDE for the Swedish NPPs is reduced, meaning a need to extend the coverage in the continuation. The considered data set contained 29 CCF events, which is already a reasonable amount for statistical aims. The analysis of the CCF events and impact vector construction is generally organized so that CCCG size 2 and 4 are handled separately.

The principal QA action was constituted by the redundant assessment of the impact vectors, compare to the general discussion in the previous section. For this purpose the event description parts of the impact vector sheets were submitted to the redundant analyst. The drafted method description and guide for impact vector construction and other source references as well as the Swedish ROs were made available The first versions of the redundant assessment and second round of the base assessments were exchanged. The differences were identified and grouped according to the type. The arguments behind the differences were discussed between the analysts. 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 were 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. Differences remained in many cases. However, no bias was observed between the analysts, but the differences were directed in both directions (optimistic – pessimistic). The net difference in the sum impact vector of all analysed events was in a reasonable range.

The final working documentation (archived as integral package) includes:

- Completed assessments of the two analysts.
- Logging notes of the differences and their resolution.
- 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.

The logging notes describe also in more detail the difficulties encountered in the analysis of more complicated events and the way of problem solving.

The redundant assessment of the impact vectors proved highly useful to reach good quality results. 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. However, high and low bound impact vectors were generated, providing a relatively simple and useful way for comparison aims, facilitating also qualitative uses of the foreign data.

The quantitative results of the DG pilot will be summarized in Chapter 9.

The next applications of the impact vector assessment were made for the centrifugal pumps and MOVs of the Nordic NPPs [NAFCS-PR18, -PR19]. The procedure developed in the course of the DG pilot could be largely followed. The amount of CCF events is small for pumps and MOVs. Hence, the utilization for quantitative aims is limited, see further discussion of the data aspects in Chapter 9. The specific insights from the pump application are following:

- Quite many pump 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

A special aspect in the MOV application is the inclusion of large exposed component populations (an extension of standard concept of CCF group). This did not produce extra difficulty in this application, because the number of affected MOVs was 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 regarding the CCF event analysis of DGs, pumps and MOVs:

- The quality control and review of the CCF events in the Swedish units [NAFCS-PR11] identified many additional events not reported to the ICDE database, compare to Section 7.2. Consequently, the presented results of the DG pilot can be optimistic. The ICDE database should be supplemented in these regards, and the impact vector assessment upgraded accordingly.
- Improvements and alignments of the ICDE event descriptions and classifications according to the proposals collected during the impact vector assessment
- Extension of the data coverage to more recent years, and for the Swedish units also to further earlier years, in order to obtain better statistical basis
- Further work to utilize foreign ICDE event data, compare to the discussion of this issue in the connection to the methodology and guide

8.5 Statistical Method for Uncertainty Estimation of CCF Parameters PR15

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, [0Ref-31].

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. 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.

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, 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, [Ref-32] we take this subject into discussion where we argue for different models 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, [Ref-31][2], 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.

Conclusions

Two-stage Bayesian method makes it possible to treat inhomogeneous populations of CCCGs and thereby to estimate both generic and group-specific CCF-rates. The method yields distributions that in case of meagre statistics are strongly dominated by very low CCF-rates but the mean values of which are unexpectedly high. If homogeneous populations of CCCGs are assumed simple Bayesian (one-stage) method can be used.

Recommendation for further work benchmark to compare the approach used here to alternative methods PREB (Vaurio 1994)[3] and Common Load Model.

- Direct estimation of CCF-probabilities - not via CCF-rates - by using a model that takes into account the correlation between Common Cause Basic Event of different multiplicities

9 Estimation of CCF parameters

This chapter summarizes the quantitative results of the NAFCS, the estimated CCF parameters in the form of Alpha Factors and Multiple Greek Letter Parameters. In this stage the currently used CCF data are also shown for comparison purpose. For the Swedish NPPs the CCF data compilation of SUPER-ASAR is used as reference source SUPER-ASAR, [Ref-26]. For the Olkiluoto plant the CCF data are from the current TVO PSA version [Ref-27]. For the foreign data the recent extensive compilation of the US plants in NUREG/CR-5497, [Ref-30] is used as reference source.

[2] An extension accepting more complex observations (eg. double k-out-of-n events in a single test)has been published: Vaurio, J.K.: Extensions of the uncertainty quantification of common cause failure rates. Reliability Engineering and System Safety, Vol. 78, No. 1, October 2002, pp. 63 - 70. Elsevier Science Ltd.

[3] Refers to PREB methodology (empirical Bayes), but that is not documented in [Vaurio 1994]. PREB as a procedure is best documented in: *Jänkälä, K. E. and Vaurio, J. K.: Empirical Bayes Data Analysis for Plant Specific Safety Assessment; Proc. Intl. Conf. PSA'87, Zurich, Switzerland, August 30 to September 4, 1987, pp. 281-286; Am. Nucl. Soc., Eur. Nucl. Soc. and Swiss Nucl. Soc. (Original concept in Vaurio, J. K.: On Analytic Empirical Bayes Estimation of Failure Rates, Risk Analysis, Vol. 7, No. 3 (1987) 329 338.).* Some comparisons to other methods also in PSAM5 Osaka and Esrel'04 Berlin. How PREB and the uncertainty analyses combine in the overall CCF - k/n event rate estimation for a family of plants and an individual plant was summarized in ICDE Stockholm Seminar: *Vaurio, J.K.: "From failure data to CCF-rates and basic event probabilities". Proc. ICDE Seminar and Workshop on Qualitative and Quantitative use of ICDE Data, 12-13 June 2001, Stockholm. NEA/CSNI/R(2001)8, OECD Nuclear Energy Agency, Committee on Safety of Nuclear Installations.* Now it is also available in more details: *Vaurio, J.K. and Jänkälä, K.E.: "Quantification of common cause failure rates and probabilities for standby-system fault trees using international event data sources". Proceedings of PSAM 6 Conference held in San Juan, Puerto Rico, June 23-28, 2002; Vol.1, pp.31 - 37.(Editors E.J. Bonano et al), ELSEVIER Science Ltd, Amsterdam, 2002. ISBN 0-08-044122-X.* Also a summary: *Vaurio, J.K.: Quantification and uncertainties of common cause failure rates and probabilities. Proceedings of ESREL2003 Conference, June 15-18, 2003, Maastricht, The Netherlands; Vol.2.*

In addition to tabular presentation of CCF parameters the data are also shown graphically in the form of multiple failure probabilities. For this purpose the Psg entity is used. It presents the probability of specific m components failing in the group on n components without taking into account the status of the other 'n-m' components. The benefit of using Psg entity 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 types of multiple failure probabilities. See the definitions and discussion of this issue in [NAFCS-PR04].

9.1 Impact Vector Application to Diesel Generators PR10

The presented results for the diesel generators (DGs) are point estimates for the combined data of the failure modes 'Failure to Start' and 'Failure to Run', i.e. FS and FR. Table 9-1 shows the best estimate results obtained from the average of the Impact Vector assessment by two redundant analysts. It has to be noticed that because the reporting of the CCF events in the Swedish units to ICDE database seems not complete [NAFCS-PR11], the presented estimates may be optimistic. Figure 9-1 shows also the high/low bounds that are generated. For details, see [NAFCS-PR10].

The CCF parameters recommended in SUPER-ASAR [Ref-26] are based on existing data and engineering judgement, taking into consideration major design differences, e.g., degree of separation RPC 88-160, [Ref-33].

US data are from NUREG/CR-5497 [Ref-30], and failure modes FS and FR are combined.

Table 9-1: CCF parameters for the diesel generators, combining failure modes 'Failure to Start' and 'Failure to Run'.

Source	Plant	CCF parameters for the group size of 2						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic	0.042	-	-	0.979	0.021	-	-
S-ASAR	O1	0.06	-	-	0.970	0.030	-	-
S-ASAR	B1	0.05	-	-	0.975	0.025	-	-
NUREG	US	0.061	-	-	0.969	0.0312	-	-

Source	Plant	CCF parameters for the group size of 4						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic	0.034	0.21	0.45	0.984	0.0139	1.32-3	8.14-4
S-ASAR	R1	0.06	0.64	0.94	0.977	0.013	0.001	0.009
S-ASAR	O3/F3	0.03	0.3	0.6	0.986	0.011	0.001	0.002
TVO	OL	0.080	0.109	0.209	0.960	0.0373	2.40-3	4.76-4
NUREG	US	0.100	0.747	0.571	0.964	0.0135	0.0114	0.0114

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, best estimate	5.94	8.81	2.81	0.27	0.16	18
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, best estimate	3640.44	198.81	2.81	0.27	0.16	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, best estimate		0.9839	1.39E-2	1.32E-3	8.14E-4	
Alpha Factors, low bound		0.9853	1.29E-2	1.65E-3	7.51E-5	
	0	1	2	3	4	
Psg(m|n), high bound	1	1.34E-2	2.83E-4	1.11E-4	1.04E-4	
Psg(m|n), best estimate	1	1.34E-2	1.99E-4	6.01E-5	4.27E-5	
Psg(m|n), low bound	1	1.33E-2	1.60E-4	2.55E-5	3.93E-6	

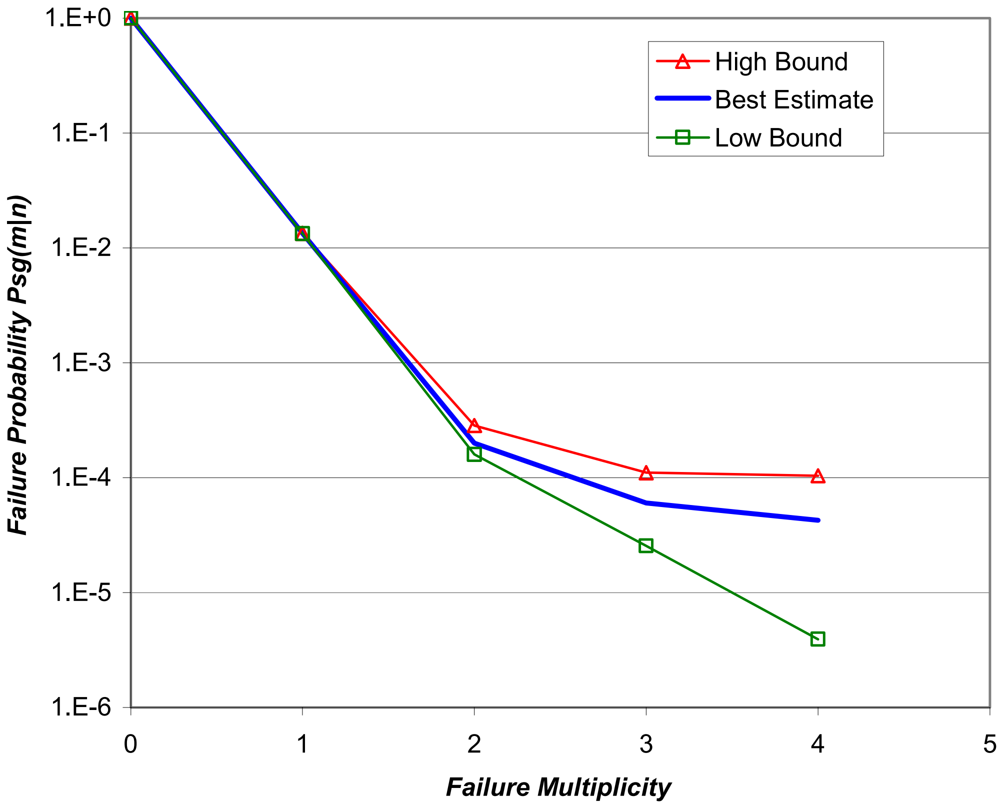


Figure 9-1 NAFCS results for the Nordic CCCG Size = 4, presented in the form of Alpha Factors and SGFPs, including the generated high/ low bounds. The diagram compares derived Psg entities [NAFCS-PR10].

9.2 Impact Vector Application to Pumps PR18

The current CCF event data in the ICDE database is rather sparse for the centrifugal pumps of the Nordic NPPs, taking into account the notion that a large part of the reported events represents functional and/or operator action dependencies to be explicitly modelled, see [NAFCS-PR18]. Besides, the CCF mechanisms and detection efficiency are much different for the pumps being normally in standby in comparison to continuously or intermittently operated pumps. These operational categories have to be treated separately. The number of reported CCF events is also dispersed over group sizes 2, 3 and 4. Meaningful point estimations can thus not be done in the same way as for the diesel generators. It should also be noticed that the pumps used in the different systems can have very varying design owing to the differences in the capacity and pressure head.

The utilization of the foreign ICDE events, for example in the form of a-priori data, proved more difficult than expected, and is pending for continued effort.

Consequently, the presentation of the CCF parameters for the pumps is restricted in this stage to the current PSA data, complied in similar lines as for the DGs in the previous section. See Table A.3.2-1 in Appendix 3 of [NAFCS-PR13].

9.3 Impact Vector Application to Motor operated valves PR19

The current CCF event data in the ICDE database is very sparse also for the MOVs of the Nordic NPPs, containing only six reported events, which are furthermore dispersed over different group sizes, see [NAFCS-PR19]. The group sizes cover a large range, because so called Exposed Populations are considered as extension to standard CCF group. Simple point estimations can thus not be done in the same way as for the diesel generators. The utilization of the foreign ICDE events, for example in the form of a-priori data, is pending for continued effort.

Consequently, the presentation of the CCF parameters for the MOVs is restricted in this stage to the current PSA data, complied in similar lines as for the DGs in the previous section. See Table A.3.3-1 in Appendix 3 of [NAFCS-PR13].

9.4 CLM parameters

For the application of Common Load Model (CLM) the best estimate results from ICDE/NAFCS are also presented in the form of CLM parameters. The nearest applications are Exposed Populations of MOVs exceeding four components. For the DGs and pumps the CLM parameter estimates are interesting as for generic insights. The estimation of CLM parameters is based the Maximum Likelihood principle [Ref-34].

Table 9-2: CLM parameter estimates based on the Impact Vector assessments for the Nordic ICDE data within NAFCS.

	CLM parameter			
Component	p_tot	p_xtr	c_co	c_cx
Diesel generator	1.4E-2	1.1E-4	0.02	0.70
Pump – generic[1	1E-3	3E-5	0.4	0.8
MOV – generic[1	1E-3	3E-5	0.4	0.8

Note 1) Generic CLM parameters are presented as placeholder data for the pumps and MOVs, pending for specific assessment.

10 Discussion

In brief the project scope can be summarized as follows.

- Survey and review: An outlook on available experience in respect to models, data and plant operation/ regulation.
- Qualitative work areas: Understanding the failure mechanisms.
- Quantitative work areas: Analysis of dependencies in general and quantitative assessment of dependent failures in the data.

The project provides an overview of models and data. A survey among plant operators and regulators has been performed to collect experience and views on the subject. This background has been used to direct the work in the qualitative and quantitative work areas.

The qualitative work provides guidance and examples on how to defend against dependent failures. The guidance and examples are derived from the experience collected from the plant operators, by interviews, and by examine the CCF event records.

The quantitative work provides tools and examples on how to assess dependencies and the failure parameters for dependent failures.

The original objectives of the project have been fulfilled. Many new problems have been identified during the work that have not been possible to solve in the framework of this project, instead these issues has been proposed for further work.

The benefit of this project can only be demonstrated after the products/reports are implemented in the training and practices of the plant owners and regulators.

As a general recommendations from the project the following proposals can be made:

- Apply the guidance documents to improve the defences and the assessment of dependencies.
- Implement a process to continuously improve the guidance documents and the supporting material.

The results also contain other recommendations for further improvements and future work, many of these recommendation needs to be assessed based on the experience of applying the guidance documents. Independent of gaining this experience the main recommendations for further work is as follows:

- Extend the impact vector assessment to cover more components available in the data (SRVs (314), check valves, batteries, level measurement, and breakers).
- Development of existing reports, based on proposal from the plant and regulator review of the draft documents - Dependency Analysis Guideline and Dependency Defense Guideline.
- Further defense assessment in data. Based on more components.
- Development of training courses related to NAFCS results, or dependency aspect, for various personnel categories.

11 References

Ref-1. NAFCS-PR01
Nordisk Arbetsgrupp för CCF Studier, Project Programme, prepared by G. Johansson, ES Konsult AB, Rev.1, 19 December 2000.

Ref-2. NAFCS-PR02
Data Survey and Review. Topical Report NAFCS-PR02, prepared by Tuomas Mankamo, Draft for Peer Review, 12 January 2002.

Ref-3. NAFCS-PR03 Impact Vector Method. Prepared by T. Mankamo, Issue 2, 31 August 2003.

Ref-4. NAFCS-PR04
Model Survey and Review. Topical Report NAFCS-PR04, prepared by Tuomas Mankamo, Draft for Peer Review, 12 January 2002.

Ref-5. NAFCS-PR05
”Survey on Defence against Dependent Failures”- Compilation and Results of Plant Survey. Per Hellström.

Ref-6. NAFCS-PR06
” Literature Survey”. Per Hellström.

Ref-7. NAFCS PR08
Bento, J.-P., “Qualitative analysis of the ICDE-database for Swedish emergency diesel generators”, , April 2002.

Ref-8. 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.

Ref-9. NAFCS-PR10
Impact Vector Application to the Diesel Generators. Topical Report NAFCS-PR10, Issue 1, 31 October 2002.

Ref-10. NAFCS-PR11
Bento, J.-P., “Data survey and review of the ICDE-database for Swedish emergency diesel generators”, April 2002.

Ref-11. NAFCS-PR12
J-P Bento, JPB Consulting, and P. Hellström, Relcon, “Redundancy Protection Guidance”, April 2003.

Ref-12. NAFCS-PR13
Mankamo, T., Knochenhauer, M., ”Dependency Analysis Guidance, Issue 1, 30 May 2003.

Ref-13. NAFCS-PR14
Knochenhauer, M., “Terms, Definitions and Abbreviations”, 9 April 2003

Ref-14. NAFCS-PR15
Pörn, K,. ” A Statistical Method for Uncertainty Estimation of CCF Parameters “ 2003-08-12

Ref-15. NAFCS-PR17
Mankamo, Tuomas. Impact Vector Construction. 10 October 2003.

Ref-16. NAFCS-PR18
Mankamo, Tuomas. Impact Vector Construction for Pumps. Issue 1, 29 August 2003.

Ref-17. NAFCS-PR19
Mankamo, Tuomas. Impact Vector Construction for Motor Operated Valves. Issue 1, 30 August 2003.

Ref-18. NAFCS-PR20
Bento, J.-P., “Defence Assessment in Data” 2003-03-26

Ref-19. ICDECG00
G. Johanson et al, ES-konsult, “ICDE General Coding Guidelines”, Rev.4, October 2000.

Ref-20. OECD/NEA/CSNI/R(2001)8: Proceedings of the ICDE workshop on qualitative and quantitative use of ICDE data. Held in Stockholm, Sweden on 12-13 June 2001

Ref-21. Mankamo, T, Jänkälä, T, Kattainen, M, Angner, A, Johansson, G and Lioubarski, A; PSA Task Guide: Analysis of Dependencies, Kola NPP Unit 2. K2PG-Dep, Issue 2, 12.04.2001.

Ref-22. 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.

Ref-23. 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.

Ref-24. 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.

Ref-25. 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.

Ref-26. SUPER-ASAR
Description of Super-ASAR CCF data for NAFCS-R13. Prepared by Michael Knochenhauer, MK03-007r0, 2003-02-07.

Ref-27. TVO-PSA Probabilistic Safety Assessment of the Olkiluoto 1 and 2, Rev.1. Teollisuuden Voima Oy, 1998.

Ref-28. NUREG/CR-5485
Guidelines on Modeling CCFs in PSA. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC, November 1998.

Ref-29. 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.

Ref-30. 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

Ref-31. J. VAURIO Estimation of Common Cause Failure Rates Based on Uncertain Event Data. Technical Note, Risk Analysis, Vol.14, No. 4, 1994.

Ref-32. K. PÖRN (1990). On Empirical Bayesian Inference Applied to Poisson Probability Models, Linköping Studies in Science and Technology. Dissertations, No.234, Linköping University.

Ref-33. 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.

Ref-34. Mankamo, T., Extended Common Load Model, A tool for dependent failure modeling in highly redundant structures. Manuscript, 15 February 1995, 10 February 2001.

Appendix 1

Dependency Defence Guidance

October 2003

Acknowledgement

The review comments and proposals for further development from Ingemar Ingemarsson, BKAB, Stefan Ericsson, RAB, C-G Mattson, RAB, Göran Hultqvist et al , FKA, Frithiof Schwartz, OKG, Ralph Nyman, SKI-RA, Lennart Carlsson, SKI-RI, Stig Erixon, SKI-RA, Lars Gunsell, SKI-RA and Bertil Morberg, SKI-RI are gratefully acknowledged.

List of Content

List of tables

List of Figures

Abbreviations

CCF	Common Cause Failure
CCI	Common Cause Initiator
CCCG	Common Cause Component Group
CFR	Code of Federal Regulation
CMF	Common Mode Failure
DKV	Driftklarhetsverifiering (Operability Readiness Control)
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
GDC	General Design Criteria
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
ICDE	International Common Cause Data Exchange
LER	Licensee Event Report (RO)
MTO	Man – Technology - Organisation
NAFCS	Nordisk Arbetsgrupp för CCF-studier (Nordic Working Group for CCF studies)
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PSA	Probabilistic Safety Assessment
PSG	Primär säkerhetsgranskning (Primary Safety Review)
QA	Quality Assurance
RO	Rapportervärd omständighet (Licensee Event Report)
SAR	Safety Analysis Report

SKI	Statens kärnkraftinspektion
SKIFS	SKI författningssamling (SKI Code of Regulation)
STARK	Stanna – Tänk – Agera – Reagera – Kommunicera (Stop – Think – Act – Review – Communicate)
STF	Säkerhetstekniska driftförutsättningar (Technical Specifications)
STUK	Radiation and Nuclear Safety Authority of Finland
TVO	Teollisuuden Voima Oy
WANO	World Association of Nuclear Operators

1 Introduction

1.1 Project Background

This Dependency Defence Guidance is the result of an effort within the Nordic Working Group on CCF Studies (NAFCS) [Ref. 1]. The NAFCS project is part of the activities of the Nordic PSA Group (NPSAG), which is a joint co-operation by the Nordic utilities and authorities for PSA recognition and development.

The NAFCS project performed during the years 2001 – 2003, includes activities within the following fields:

- Survey and review of analysis models and data sources
- Survey of defences against dependent failures
- Analysis of Nordic CCF data from the ICDE database and other sources
- Development of impact vectors for defined components
- Estimation of CCF parameters and associated uncertainties
- Development of Dependency Defence Guidance
- Development of Dependency Analysis Guidance

The International Common-Cause Failure Data Exchange Project ("ICDE Project“) constitutes essential background to the NAFCS project [Ref. 2].

The safety systems in Nordic nuclear power plants are characterised by substantial redundancy and/or diversification in safety critical functions, including their support functions. Furthermore, the redundant functions and system subdivisions have physical separation. Viewed together with the evident additional fact, that the single failure criterion has been systematically applied in the design of safety systems, this means that the plant risk profile as calculated in existing PSA:s is usually strongly dominated by failures caused by dependencies resulting in the loss of more than one system subdivision.

For the reason mentioned above, all PSA:s have included a thorough identification and modelling of both functional and physical dependencies. The different PSA analysis tasks are tailored to identify, model and derive data for all important dependencies, e g the accident sequence analysis, the systems analysis, the analysis of common cause initiators (CCI), area events and external events analysis put special emphasis on identifying mechanisms and interactions that need dependency analysis consideration. Dependencies are in most cases considered by explicit modelling, but there is always a fraction with dependencies that either not are known, or not suited for explicit modelling. These dependencies are collectively called common cause failures and they are in PSAs treated by CCF analysis methodology. [Ref. 3] provide an overview of the different dependency types, and how they are considered in safety analysis.

Table 1-1: Dependencies and their consideration in safety analysis

Dependency		Known	"Unknown"
Functional (direct or indirect)	Failure cause makes two or more components unavailable:	Connected systems, structures and components: Cooling, ventilation, signals, common parts, procedures, tools, operators etc	Common Causes Failures Causes and failure coupling mechanisms are explicitly "unknown"
Physical (direct or indirect)	A common environmental condition makes two or more components unavailable.	Area events (fire, flood), External events (air plane crash, earthquake), Dynamic effects after LOCA, environment impact.	

This means that the completeness and relevance of the identification and modelling of the various dependency categories has a strong influence on the completeness and relevance for nuclear power plant safety and safety analysis.

The key to safety is to be in control of dependencies!

1.2 Objective

The main objective with this document is to provide guidance on defences against dependencies in cases where redundancy is applied to achieve a high reliability in safety critical systems, especially functions and systems in nuclear power plants. The use of the guidance will contribute to lower and control the risk contribution from dependencies originating from plant design and review, construction, installation, commissioning, operation, maintenance, testing, and modifications.

The guidance is intended for plant management and staff, as well as regulators. The guidance includes tables with dependency defences that can be utilised by the licensees as a checklist in relation with operational and other activities, and as a learning document for the whole plant staff.

The complexity and importance of the dependency issues on nuclear safety may require that more specific guidance and instructions need to be developed and established for use in the utilities and regulators own organisations, e g for consideration in case of plant changes during modernisations and in inspection activities. The guidance can additionally be considered in a broader context including the development and implementation, on a national scale, of explicit guidelines and educational and training material concerning dependency defences.

1.3 Outline and Context of Dependency Defence Guidance

The general areas covered in the NAFCS project are:

1. Defence against dependent failures
2. Models for analysis of dependent failures
3. Data for dependent failures

Figure 1-1 shows the context of the project. The different reports produced, and their use in producing the two main topical reports, the Dependency Defence Guidance and the Dependency Analysis Guidance, are indicated.

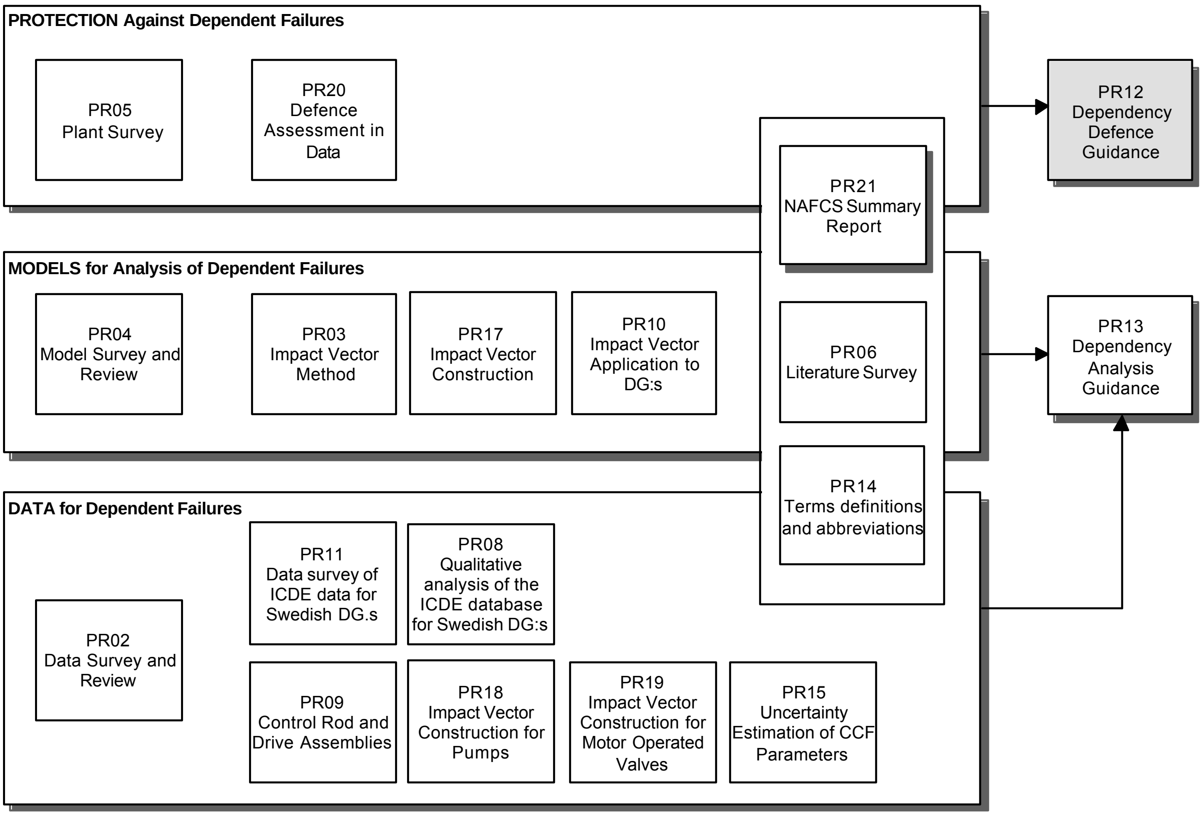
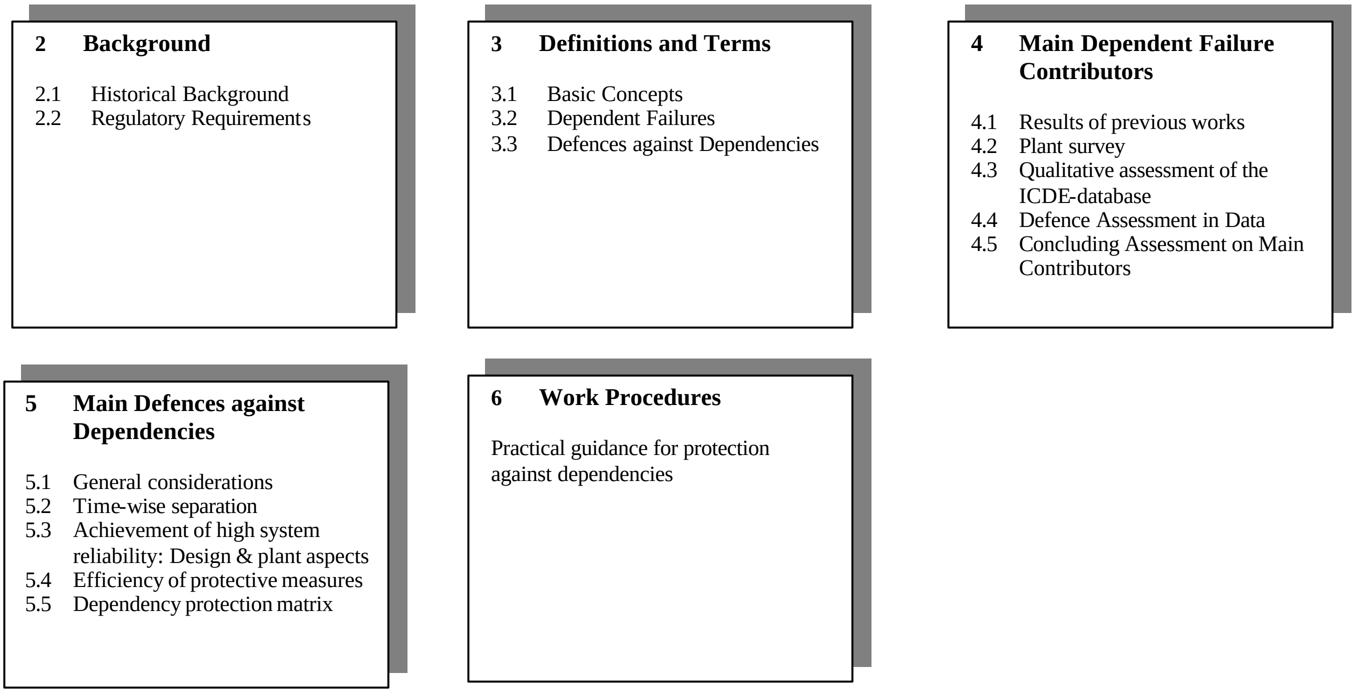

PROTECTION Against Dependent Failures
PR05 Plant Survey
PR20 Defence Assessment in Data
PR12 Dependency Defence Guidance
PR21 NAFCS Summary Report
MODELS for Analysis of Dependent Failures
PR04 Model Survey and Review
PR03 Impact Vector Method
PR17 Impact Vector Construction
PR10 Impact Vector Application to DG:s
PR06 Literature Survey
PR13 Dependency Analysis Guidance
PR14 Terms definitions and abbreviations
DATA for Dependent Failures
PR11 Data survey of ICDE data for Swedish DG.s
PR08 Qualitative analysis of the ICDE database for Swedish DG:s
PR02 Data Survey and Review
PR09 Control Rod and Drive Assemblies
PR18 Impact Vector Construction for Pumps
PR19 Impact Vector Construction for Motor Operated Valves
PR15 Uncertainty Estimation of CCF Parameters

Figure 1-1. Context of NAFCS Project

The main sections in this dependency defence guidance are shown in the figure below.



2 Background

2.1 Historical Background
2.2 Regulatory Requirements

3 Definitions and Terms

3.1 Basic Concepts
3.2 Dependent Failures
3.3 Defences against Dependencies

4 Main Dependent Failure Contributors

4.1 Results of previous works
4.2 Plant survey
4.3 Qualitative assessment of the ICDE-database
4.4 Defence Assessment in Data
4.5 Concluding Assessment on Main Contributors

5 Main Defences against Dependencies

5.1 General considerations
5.2 Time-wise separation
5.3 Achievement of high system reliability: Design & plant aspects
5.4 Efficiency of protective measures
5.5 Dependency protection matrix

6 Work Procedures

Practical guidance for protection against dependencies

Figure 1-2. Content of Dependency Defence Guidance

2 Background

2.1 Historical Background

Significant attention has historically been devoted to the analysis of dependencies and especially to common cause fa ilures, CCF, based on their potentially major contributions to the risk associated with the operation of nuclear power plants.

The requirements on high plant safety and reliability, including the due consideration of these potentially large risk contributors, are reflected in regulatory guidelines and their implementation at the plants.

WASH-1400 marked the first widespread concept and analysis of common cause failures in nuclear power plants, applying the so-called square root model. Important efforts have been spent internationally and many methods and models have been developed and used since WASH-1400, focussing on the analysis of the contribution from CCF caused by explicitly "unknown" dependencies.

One of these models, the beta factor model, gained international recognition and has been widely used. The beta factor model was later extended to the MGL (Multiple Greek Letter) model and other models were also developed to allow dependency modelling of new plant designs with safety systems built with three or more subdivisions, so called trains.

These later models have been supported with substantial resources spent on data collection and classification [Ref. 4, Ref. 5]. Classification of reported failures has lead to a better understanding of the different contributing factors behind CCF and of their relative importance. Several projects, like the ICDE project, continue the data collection and evaluation.

One area that over the years has been given less attention is how the system redundancies shall be protected against dependent failures. One exception is the work presented 1981 by the UK safety and Reliability Directorate "Defences against common mode failures in redundancy systems – A guide for management, designers and operators"[Ref. 6].

2.2 Regulatory Requirements

The regulatory requirements have been directed towards the need for redundancies and application of the principles of separation and diversity as a mean to ensure the effectiveness of these redundancies. There are also cases with explicit diversity requirements, e g for the reactivity control system.

In Finland, a state Council Decision requires systems to be safe with good redundancy, separation and diversity. STUK, the Finnish Radiation and Nuclear Safety Authority have several regulatory guides (YVL series) with requirements related to defence against dependencies. Examples are:

YVL 1.0 Safety criteria for design of nuclear power plant [Ref. 7].

YVL 1.5 Reporting nuclear power plant operation to the Finnish Centre for Radiation and Nuclear Safety. (Comment: It is required to have data collection and data processing systems and statistical trend analyses.) [Ref. 8]

YVL 2.7 Ensuring a nuclear power plant's safety functions in provision for failures [Ref. 9].

YVL 2.8 Probabilistic Safety Analyses (PSA) [Ref. 10] (Comment: Requirement for in-house PSA since 1984 and today is Living PSA also required).

STUK has furthermore regulatory guidance concerning the licensee's ability to identify CCF events and to perform training in CCF identification.

The Swedish Nuclear Power Inspectorate SKI's regulation SKIFS 1998:1[Ref. 11] contains the basic requirements on safety assessment and reporting to SKI. The requirement to perform a PSA and to consider its results is important with regard to the defence against dependencies. SKIFS 1998:1 also requires that the licensees establish a two-steps review process, which may contribute to the prevention of dependencies, for example related to the potential introduction of design failures during a plant modification. MTO activities and feedback of experience are other requirements in this area.

Similar reporting requirements as in Finland are also in place, and LERs shall be reported within a stipulated time frame and assessed by SKI.

Inspection activities are used for follow-up of plant safety issues together with review of reporting from the plants. An internal SKI document controls the safety review and different disciplines co-operate in inspection and in review activities. Thus, a high efficiency in the potential identification of missing dependency barriers is achieved.

Requirements on operability readiness control (DKV) constitute in practice an additional defence against dependencies.

However, even with the background provided above, only few examples of descriptive guidance on practical defences against dependencies have been openly published internationally.

3 Definitions and Terms

3.1 Basic Concepts

3.1.1 Defence in Depth

Defence-in-depth is a basic concept in nuclear safety applying preventive, protective and mitigating safety functions.

The safety design of nuclear power plants has, from the early beginning, been basically based on the philosophy of "defence in depth" and on specific design criteria and quality standards. The overriding intention behind the philosophy of defence in depth was to minimise the probabilities for and consequences of accidental radioactive releases into the environment. This philosophy has resulted, generally speaking, in a plant design and operation at three safety levels: preventive, protective and mitigating levels. These levels are partly overlapping. Operational and regulating systems are parts of the first level. Safety systems are parts of the second and third levels.

Stringent adherence to the philosophy of defence in depth has resulted in plants that are relatively highly tolerant toward both hardware failures and human/organisational deficiencies. The above presupposes obviously responsible organisations (licensees and regulators) exhibiting a good safety culture.

The defence in depth philosophy has in practice been realised through the application of general design safety criteria and principles as the single failure criterion, fail-safe criterion, redundancy, diversity, etc. These and other concepts are shortly explicated below.

3.1.2 Single Failure Criterion

A failure or degradation in one component or in one system shall not jeopardise the system function.

This general design criterion means that a failure or degradation in one component or in one system shall not jeopardise a safety function. In practice, this criterion has resulted in safety systems with redundancy. Redundancies are combined with diversity and separation in order to achieve a high degree of independence between the redundant equipment, and thus limit the potential impact from dependent failures.

3.1.3 Fail-Safe

A component enters a safe protecting state in case input is lost.

A fail-safe design of a system or component means that the system or component should fail to a safe mode without altering a safe plant condition, when an independent or dependent failure occurs. Application of a fail-safe design is used to assure a high reliability of certain functions, for example opening of a pneumatic valve when the air pressure is lost.

Observe that a fail-safe design is fail-safe given certain conditions, e g loss of power, but not necessarily fail-safe in other cases.

3.1.4 Redundancy

Redundancy is the existence of at least 100% back-up capacity

Redundancy is the existence of multiple components or trains of equipment, each of which intended to fulfil the intended function. Basically, a redundancy means the existence of at least 100% extra capacity to fulfil specified functional requirements. Redundancy is used to achieve high reliability in a safety system or high availability in a production or service system.

A system is considered to include redundancy only if it can operate when one or more of the trains of equipment have failed.

A system function is redundant only if two systems are back-up for each other.

Although the application of redundancy assumes that the redundant trains are independent, it is practically difficult to totally preclude some dependency and to demonstrate it.

3.2 Dependent Failures

3.2.1 Independent Failure

$$P_{system} = P(A \bullet B) = P(A) \bullet P(B)$$

An independent failure is an occurrence in which the probability of failure of one component is not related to the failure of another component.

Standard fault tree analysis makes the assumption that all events are independent as illustrated by the formula above.

The formula indicates that both components A AND B must fail in order for a system failure to occur. P(A) and P(B) are the independent probabilities of failure of A and B respectively.

3.2.2 Dependent Failure

$$P_{system} = P(A \bullet B) \neq P(A) \bullet P(B)$$

A dependent failure is an occurrence within the demand period of simultaneous component failures that are not independent. In other words a dependent failure relates to a set of events, where the combined probability cannot be expressed as the product of the failure probabilities of the individual events.

Consideration of dependent failures, both from a qualitative and quantitative perspective is especially important when $P(B|A) \succ P(B)$.

3.2.3 Functional and Intersystem Dependency Fault

The unavailability of a component to perform its intended function, because of the unavailability or failure of a supporting component, system and structure.

A functional dependency fault is the unavailability of a component to perform its intended function, because of the unavailability or failure of a supporting component or system (the latter also some times called inter system dependency). Redundancies relying on the same support system may therefore become unavailable (failed) if this common support system becomes unavailable (fails). An intermediate cooling system is one example of a system that creates an inter system dependency.

3.2.4 Physical Dependency

A physical dependency exists when redundant components can be affected by events acting at a defined location or volume.

The term of physical dependency is utilised to denote that several redundant components can be affected by events acting at a location or volume. Components can be situated in the same room or volume or are functionally dependent on equipment in another room or volume. Spatial dependency is one type of physical dependency. Physical dependencies may be critical due to the potential for external and environmental influences, also called area and external events, like fires, floods, and other environmental influences (mechanical damages, electric interference, low and high temperature etc) affecting systems, structures and components in the same location or volume. Physical separation of redundancies by placing them in different locations, or at least by distance, is an important defence against physical dependencies.

3.2.5 Common Cause Failure (CCF)

A common cause event (failure) is a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause (ICDE[1] [Ref. 2]).

A CCF is a dependent failure event where simultaneous or near simultaneous multiple failures result from a single shared cause. The shared cause can be functional or physical, for example shared power supply, internal flooding, MTO related and design fault. CCF may be seen as a subset of dependent failures. Shared causes affecting more than one component in a common cause component group (CCCG), see section 3.2.7, are modelled in a specific CCF analysis by special CCF models (see also 3.2.7). Observe that functional and physical dependencies can and normally shall be treated with explicit modelling in a PSA. The CCF analysis should only include those residual shared causes that not are explicitly modelled.

The ICDE guideline also defines a so-called ICDE event:

> *"Impairment of two or more components (with respect to performing a specific function) that exists over a relevant time interval and is the direct result of a shared cause"*

[1] International Common Cause Data Exchange - A project for collection and exchanging of information on common cause events. The project started 1994.

In the frame of the ICDE work, CCF constitute thus a subset of the ICDE-events, in addition to the fact that ICDE events encompass both complete as well as potential failures. The word *"relevant"* in the second definition refers to the time interval between two inspections or tests, or if unknown to a scheduled outage period.

3.2.6 Common Mode Failure (CMF)

A CMF is a dependent failure event, in which simultaneous or near simultaneous multiple failures occur by the same mode of failure.

A CMF example is when a set of valves fails to move from open to closed position or a pair of generators fails to start.

The most easily recognisable form of dependent failure is a CMF event. CMFs may be regarded, as a sub-set of CCF, and in systems with redundancy, the majority of CMFs will share both mode and cause of failure.

Due to the gradual historical development of the terms above, CMF has been used (from the 1960s onwards) to include all dependent failures, perhaps because it was this major type of dependent failures that was observed with the development of systems with redundancy. The term CCF has been applied in the same global manner (from the 1970s onwards) since the effect of common causes was recognised. The wider term of dependent failures has evolved in recent years to cover any failure, which is not independent, even if a shared cause is not easily identifiable.

3.2.7 Common Cause Component Group (CCCG)

A group of (usually similar) components that are considered to have a high potential of failing due to the same cause.

A common cause component group (CCCG) [Ref. 2], is an identified group of components, which is considered to be vulnerable to common cause failures

The components in a CCCG can belong to the same or to different systems.

3.2.8 Coupling Mechanism

A coupling mechanism is a way to explain how a cause propagates to involve multiple components /equipments. The three broad categories of coupling mechanisms are functional, spatial and human.

3.3 Defences against Dependencies

3.3.1 Overview

There are obvious reasons for requirements on high plant safety and reliability and more specifically for prevention of dependent failures in safety systems with redundancy:

Safety	Redundant safety critical equipment may fail simultaneously.
Availability	Unavailable equipment costs money and resources.
Cost	Failure itself may be more expensive than replacement before failure.

Most, if not all, organisational factors (QA-system, maintenance programme, modification management, experience feedback, etc) contribute, in addition to an appropriate design, construction and installation, to a high plant safety and reliability. This applies although many of these factors are not explicitly tailored for defence against dependencies in systems with redundancies.

The effect on plant safety and system reliability of deficiencies related to the above factors can be translated mathematically into a reliability expression, in our case expressed as system failure probability. The basic formula for a system with one redundant train is (beta factor):

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

P_{system} Total system failure probability

P_{train} Train failure probability

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

The formula shows that two ways exist to increase the reliability performance of a system with redundancy:

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

Design based features or administrative measures directed toward a system that reduce the potential for failure may be viewed as defences against that failure. Defences that are targeted at safeguarding the reliability of individual components act to reduce both dependent and independent failures. Certain defences are intended to 'cut', or at least reduce the strength of the coupling mechanisms between components in a potential multiple failure group and therefore act specifically to reduce the potential for dependent failure.

Defences against dependencies mean that the plant organisation needs to be in control of the component interfaces within the plant with regard to functional and physical dependencies. In addition, the analysis of plant operating experience represents one of the most efficient tools to identify those human, organisational or technical barriers that have to be reinforced in order to minimise the occurrence of CCF events. This issue is further elaborated in chapters 5 and 6.

3.3.2 Component Interfaces with the Plant

To minimize the probabilities for CCF is basically related to the robustness of the installation in regards of the components interfaces with the plants. This robustness is, in particular for safety systems, based on number of redundancies, diversity and separation, as discussed in the following sections. The components interfaces that are in focus in these discussions are the following:

- Signals to and protections of the component (activation signal, blocking signal, activation condition – logic -, component protection).
- Indication from the component (indication status, values of monitored parameters).
- Power (drive power, manoeuvre power).
- Interface with support systems (cooling, power, etc).
- MTO Interfaces (during operation, maintenance, testing and calibration, operating environment, etc).

All these interfaces represent the basic elements, which have to be protected from dependencies as illustrated in Figure 3-1 (from [Ref. 12]).

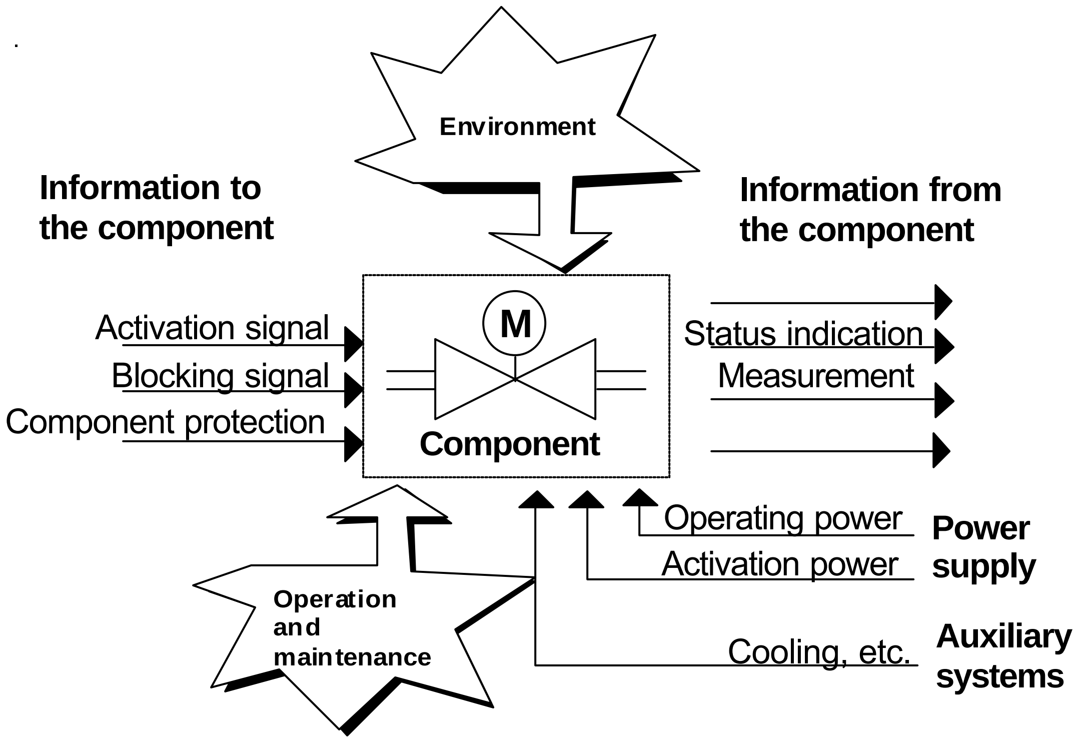


Figure 3-1. Overview of the component-plant interaction [Ref. 12].

3.3.3 Functional Separation

Functional separation means for example that two redundant trains in a safety system are not dependent on the same signal or power supply. Cases with incomplete functional separation are often inadequate solutions in technical applications where high reliability and safety are required. One important prerequisite for achieving the full benefit of the redundancy principle is thus that the redundancies of a system do not depend on common components, signals or power supplies from service systems. This condition is necessary in order to avoid that a single failure in a common service system interrupts the function of several redundancies of the safety system.

Functional separation is illustrated in Figure 3-2. The pump in train 1 has its own cooling circuit and power supply that are independent of the cooling circuit and power supply of the pump in train 2.

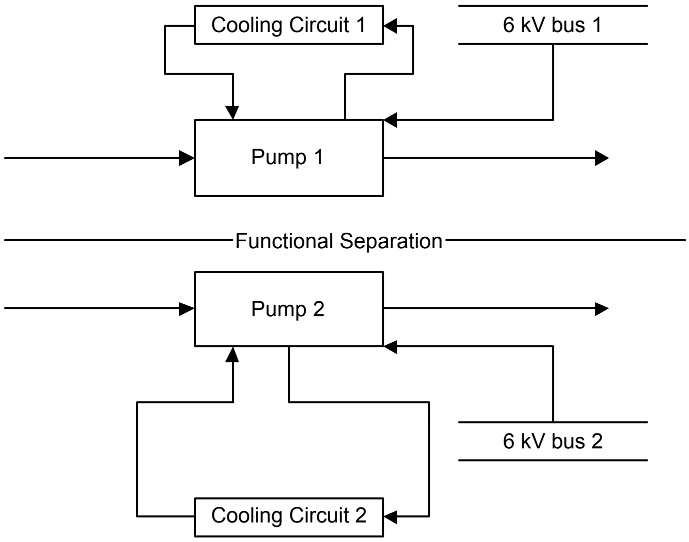


Figure 3-2. Functional Separation/Dependency

3.3.4 Physical Separation

Separation of redundant components and trains of a system is normally achieved by physical separation (distance) and protective barriers (walls, cubicles, rooms, etc). A consistent and systematic physical separation of the safety systems will effectively protect the redundancies from spatial dependencies (see section 3.2.4 for definition). The probability will thus be low that such an influence will defeat more than one train of the safety system (s).

Fail-safe design and redundancy combined with functional and physical separation are the most effective technical cornerstones of the protection against dependent failures.

Physical separation is illustrated in Figure 3-3. The pump in train 1 is physically separated from the pump in train 2 by distance and/or by walls. The design of the physical separation needs to consider all potential internal and external hazards with potential to threat redundant equipment, including its support functions.

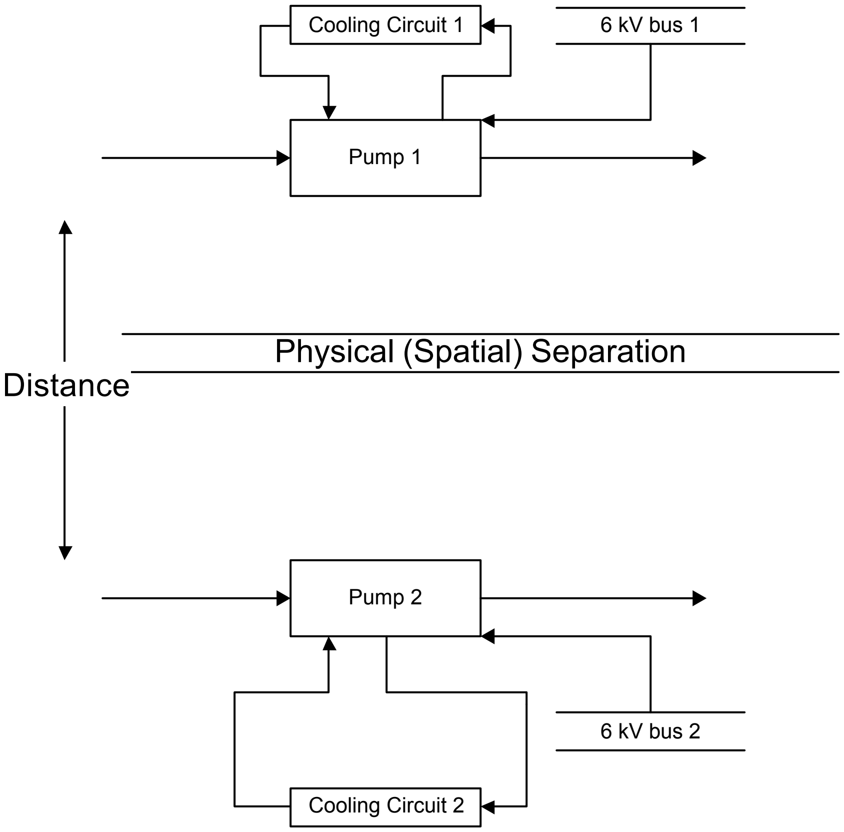


Figure 3-3. Physical and functional separation/dependency

3.3.5 Diversity and Coupling Mechanisms

The term redundancy as defined in section 3.1.4 is often used with the implicit understanding that the redundant components or trains are similar. We call this “Identical Redundancy”.

However, a redundant system can be sub-divided in two or more trains of diverse equipment with the same functional purpose, e g one motor driven pump and one turbine driven pump respectively. Equipment diversity implies thus that a system incorporates redundant components or trains of equipment, which are not identical. The extent to which the redundant items are different is referred to as the ‘level’ of diversity in the system.

Two general forms of diversity can be considered. The basic form is, as touched upon above, where the diversified systems or the diverse redundant components within a system differ in some fundamental feature, i e design, principle of operation, etc. The second is operational diversity, where redundant components are operated in different manners, e g organisation, stepwise introduction, and staggered test intervals. Full diversity is difficult to achieve, because of coupling mechanisms in hardware, operation and environment. This is illustrated in Figure 3-4.

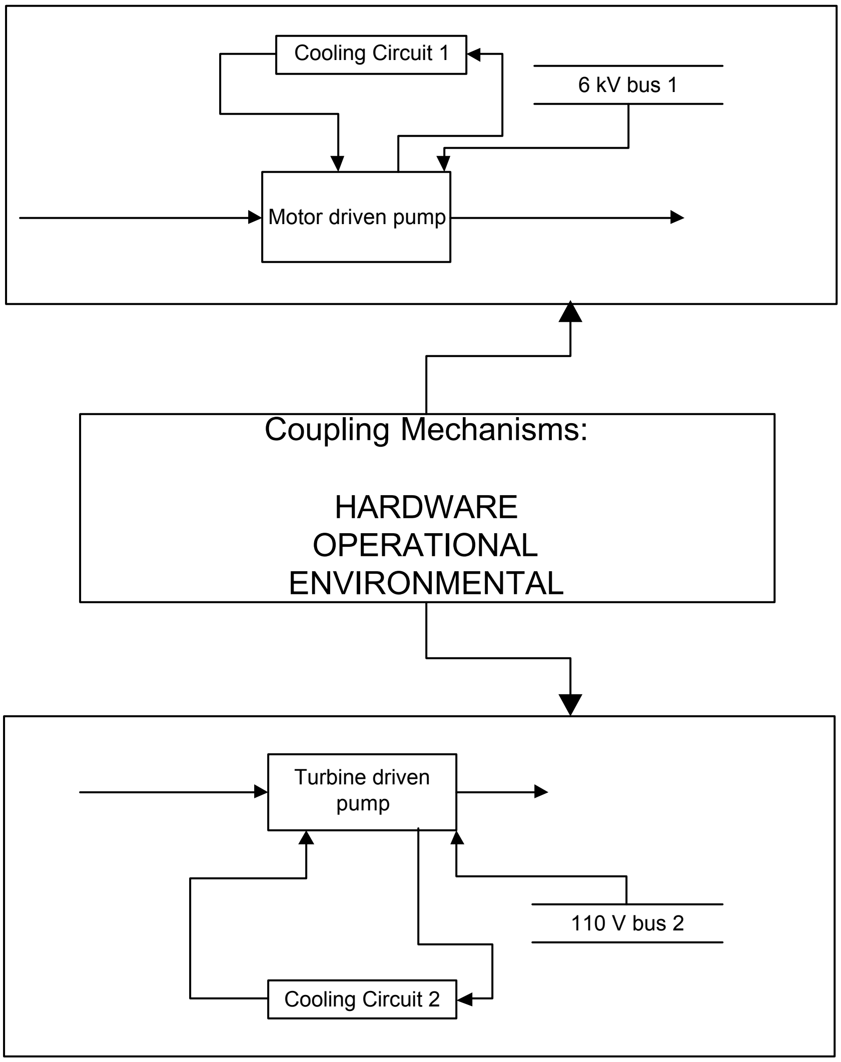


Figure 3-4. Diversity versus Coupling Mechanisms Hardware, Operation, Environmental

4 Main Contributors to Dependent Failures

Several works have been made earlier in order to identify main contributors to dependent failures, and to propose defences against their occurrence. Some international references are summarised in this section together with studies performed within the NAFCS frame.

4.1 Results of Previous Work

A comprehensive research program on dependent events was established in the early eighties by EPRI [Ref. 3 Mankamo, T., Knochenhauer, M., ”Dependency Analysis Guidance, NAFCS-PR13, October 2002.

Ref. 4]. A classification system for dependent events in support of risk and reliability evaluations was introduced. The classification system provided several basic definitions including the definitions of dependent event causes. The causes were divided into seven general classes, and each class was further subdivided. An overview of the cause classification system is shown in Table 4-1.

[Ref. 3] argues that the distribution of causes for independent and dependent failure events is similar and that a fundamental difference is that dependent events have coupling mechanisms to transmit the effect of the trigger event to two or more components. Examples of coupling mechanisms are functional dependency, physical proximity and human interactions. The key to redundancy defence should thus be to minimise the impact of the coupling mechanisms.

Table 4-1: Cause Classification [Ref. 3 Mankamo, T., Knochenhauer, M., ”Dependency Analysis Guidance, NAFCS-PR13, October 2002.

Ref. 4]

Class	Cause
Design/Manufacturing/ Construction Inadequacy	Plant Definition Requirements Inadequacy
	Design Error or Inadequacy
	Manufacturing Error or Inadequacy
	Construction Error or Inadequacy
	Other (Explain)
Procedures Inadequacy (ambiguous, incomplete, erroneous)	Defective Operational Procedure
	Defective Maintenance Procedure
	Defective Calibration/Test Procedure
	Other (Explain)
Human Actions, Plant Staff	Failure to Follow Procedure
	Misdiagnosis (followed wrong procedure)
	Accidental Action
	Other (Explain)
Maintenance	Scheduled preventive maintenance (including surveillance test and calibration)
	Forced maintenance (repair of known failure)
Abnormal Environmental Stress	Electromagnetic Inference
	Moisture (spray, flood etc)
	Fire
	Temperature (abnormally high or low)
	Radioactive Radiation (irradiation)
	Chemical Reactions
	Vibration loads
	Impact Loads
	Human-Caused External Event
	Natural events (wind, earthquake etc)
Internal (internal to component, piece-part, ambient environmental stress)	Internal to Component (Piece-Part)
	Ambient Environmental Stress
Unknown	

Looking at a breakdown by cause and event type for all components, the following observations were made [Ref. 3 Mankamo, T., Knochenhauer, M., ”Dependency Analysis Guidance, NAFCS-PR13, October 2002.

Ref. 4]:

- The most predominant cause of the independent events was internal, which accounted for nearly half of the events. Internal causes also frequently appear in the dependent event categories.
- Human related causes account for a major portion of the events and especially for the dependent events.
- Environmental stresses accounted for a small portion of the events in general and the dependent events in particular.
- A large number of events were classified as cause unknown.

NUREG/CR-6268 [Ref. 5] from 1998 is a rather recent presentation of a Common Cause Failure Database and Analysis System where the previous work from 1985 has been refined. The later reference presents an event identification and classification system including a coupling factor classification. The coupling factors are divided into three major classes: Hardware based, Operation Based and Environmental Based and a further subdivision is also presented. This coding system for coupling factors is shown in table Table 4-2.

A major contributor to dependent CCF events is, according to [Ref. 13], deficient programmatic maintenance practices. Another contributor is design problems resulting from design modifications, indicating that the modification review processes were not rigorous enough and resulted in CCF susceptibilities. The third important contributor identified in [Ref. 13] is human errors.

Table 4-2: Coupling Mechanisms and contributions to CCF events [Ref. 5]

Coupling mechanism and contribution to CCF events (fraction of total CCF)	Description
Hardware (48 %)	Hardware Design: Component part
	Hardware Designing: System Configuration
	Hardware Quality: Installation/Configuration
	Hardware Quality: Manufacturing
Operational (40%)	Operational: Maintenance/Test Schedule
	Operational: Maintenance/Test Procedure
	Operational: Maintenance/Test Staff
	Operational: Operation Procedure
	Operational: Operation Staff
Environmental (12%)	Environmental external
	Environmental internal (e g Fluid)

4.2 Plant Survey

The plant and authority survey [Ref. 14] performed within the frame of the NAFCS project, summarises discussions with both plant representatives and authority personnel on dependency contributors and best defences against them. The discussions identified the following dominating contributors to CCF:

- Ageing of equipment
- Human and organisational factors, planning errors
- Design changes, modification management.

4.3 Qualitative Assessment of the ICDE Database

A qualitative assessment of the ICDE-database for the Swedish emergency diesel generators [Ref. 15] has been performed within the NAFCS frame. The study covers events reported into the database for years 1994 – 1997, and CCF events additionally identified for years 1998 – 2001. The study has utilised the content of the so-called

MTO-database (Man – Technology – Organisation) to allow for an assessment of underlying causes contributing to CCF.

The results of this qualitative analysis indicate that 60% of the identified CCF events in the Swedish diesel generators for the years 1994 – 2001 were MTO-related and 40% were hardware failures. For the latter ageing phenomena dominated to 70%. These results are in relative good agreement with the one's presented in section 4.1.

The study results indicated that five root causes were dominating contributors to MTO-related CCF. These root causes represent, ordered by decreasing importance, deficiencies in:

- Self-checking (both individual and collective)
- Work preparation/planning
- Operability readiness control (DKV)
- Content of procedures and other documentation
- Ergonomics/design/accessibility.

4.4 Defence Assessment in Data

The report "Defence Assessment in Data" [Ref. 16] present an evaluation of MTO-related CCF events and defences against those[2]. The study covers the years 1994 – 2002. For this time period, 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.

The study focussed on the assessment of the dominating root causes behind MTO-related CCF events, as ground for proposals on general defences against these.

The overall repartition of the causal categories is illustrated in Figure 4-1. The results are, for the dominating contributors, well in line with similar results for the Swedish diesel generators.

Based on the identification of the dominating root causes, 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.

The remarkable consistency of the results obtained in the diesel generator study [Ref. 15] and in the exhaustive review of the MTO-database [Ref. 16] should ensure the efficiency and robustness of the defence proposals against, at least, MTO-related CCF events.

[2] The original intention 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.

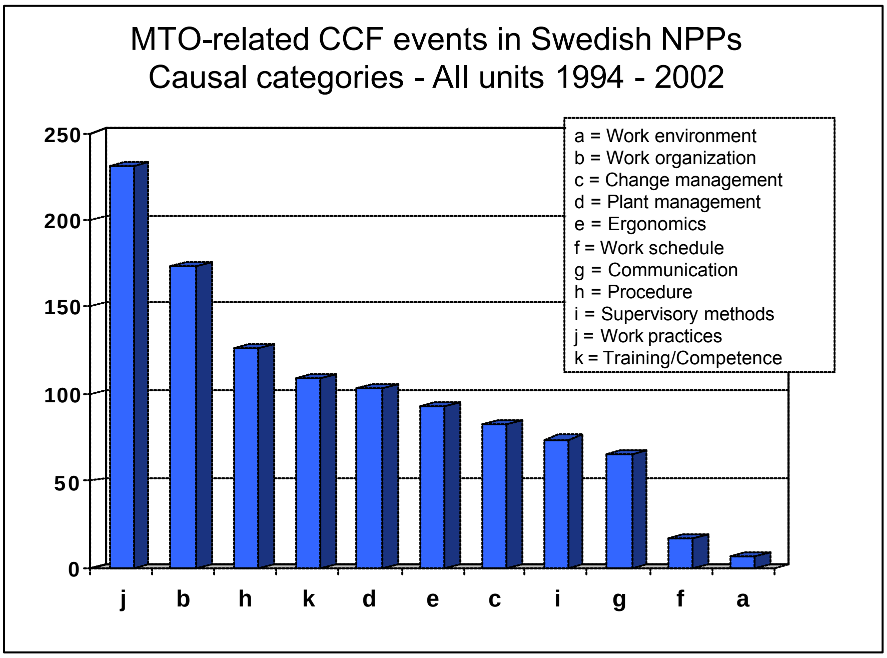


Figure 4-1. Causal categories to MTO-related CCF events in Swedish LERs.

4.5 Concluding Assessment on Main Contributors

The studies presented above together with the most recent work within ICDE and NAFCS provide homogeneous results as to the dominating contributors to CCF. These contributors are summarised in Table 4-3.

Table 4-3: Summary of main contributors to dependent failures

General category of CCF	**Main contributors**
Hardware related CCF	▪ Ageing (of electrical and mechanical equipment)
MTO related CCF	▪ Deficient individual (and also collective) self-checking (STARK) ▪ Deficient work organisation (work preparation, planning and operability readiness control) ▪ Deficient content of procedures ▪ Poor ergonomics & design in respect of accessibility for maintenance, testing & calibration.

5 Main Defences against Dependencies

5.1 General Considerations

Section 3.3.1 presented two basic principles for achieving a high reliability of systems with redundancy:

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

High reliability of individual trains can be achieved by protecting them against the failure causes while a low dependency between the trains is achieved by protecting them against functional and physical dependencies "dependent failure coupling factors".

The defence against dependent failures in system redundancies relies on a set of defence mechanisms. The latter shall not only prevent the introduction of dependent failures, they shall additionally even ensure their early detection and removal.

One basic mechanism to avoid failure of redundant equipment due to a common cause is to use separation and have different barriers / identifiers.

Separation can basically be introduced in two ways (refer to the definitions in chapter 3):

- Functional separation - diversity
- Physical separation

Functional separation and physical separation can be strong barriers, which well maintained provide effective protections against dependent failures in the system redundancies.

As mentioned in section 3.3.3, diversity encompasses operational aspects, where redundant components are operated in different manners, e g, stepwise introduction, and staggered test intervals. The latter can be viewed as introducing a separation in time (see below).

Even if the defences mentioned above are implemented, a risk will always exist that something has been overlooked. It is in this respect extremely difficult to create, and demonstrate, total separation in all aspects between redundant equipment.

There is also a monetary issue involved in the defence against dependencies. Introduction of diverse equipment requires extra equipment qualification resulting in higher costs. Installation of diverse equipment is generally more expensive than the installation of redundant non-diverse equipment. Similar equipment is less expensive than diverse. However, stepwise introduction of similar equipment will increase costs again. Quality control and exchange of experience are still very important, as much as taking advantage of stepwise introduction and other types of time-wise separation, including the possibility to detect ageing/wear out effects in trains with more operational time.

Finally an equally important part of the defence mechanisms is a high level of awareness among the plant organisations and regulators about the dependency and CCF issue. A high professionalism in operation, maintenance and testing/calibration activities is one of the most important “soft” barriers for the prevention and the detection of common cause failures in systems with redundancy. Such professionalism within the whole organisation is strongly dependent on the management involvement and of the staff motivation and education in CCF issues, redundancies and their defence.

5.2 Time-wise separation

Time-wise separation represents an administrative defence contributing to the protection against design and ageing problems. Time wise separation can be achieved by stepwise introduction of new equipment, staggered testing and similar. Time wise separation needs to be combined with efficient systems for testing, failure reporting and information collection. The plant information system needs to have enough level of detail in order for common parts to be traced. Efficient reporting is dependent on management support and recognition, of procedural guidance, and of skilled and motivated personnel.

A detailed follow-up and reporting is a prerequisite for stepwise introduction. The reasoning here is that dependencies can exist at a detailed level below the main component level (pump and valve), e g use of same oil for lubrication, or some small parts commonly manufactured (pressure gauges), even if they are utilised in different components. To prove complete diversity may therefore be difficult and require significant efforts. Sustained and systematic failure reporting, failure report evaluation and exchange of experience at different organisational levels thus constitute essential protections against the occurrence of dependent failures.

5.3 Achievement of High System Reliability: Design & Plant Aspects

As a basis for achievement of high system reliability, it is required to use reliable components with proven design and operating records for the expected application and environment. Fail-safe design and passive functional modes are other examples of factors contributing to high system reliability.

It is also needed to have enough justification from testing and deterministic analyses. The above also presupposes the use of skilled and sometimes certified personnel in design, manufacturing, installation, and operation.

A system for the reporting of component failures and exchange of experience between different users of the same type of equipment and from the same manufacturer contributes further to high system reliability and availability.

The reliability possible to achieve with a single channel/train system is at the very best, supposing close adherence to the safety principles mentioned above, equivalent to a failure probability in the vicinity of 10^{-3} / demand.

Such a value is generally considered not low enough for many service systems in nuclear power plants. This is even more valid for safety systems where the reliability requirements are far more demanding. The solution to reach the required reliability (safety) level is to introduce redundancies in the plant systems, complemented with a diversification of systems utilised for critical safety functions. The reliability range of different system configurations is exemplified in Figure 5-1.

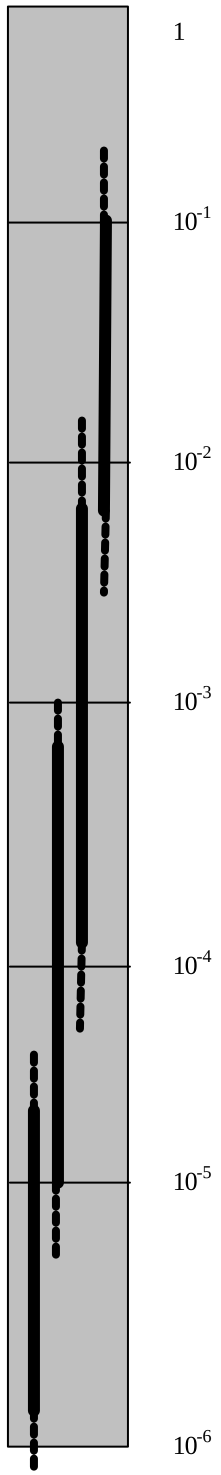
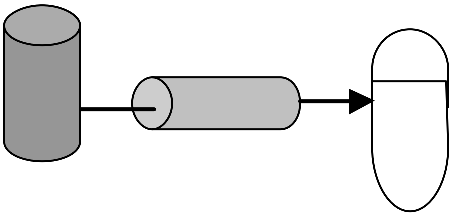
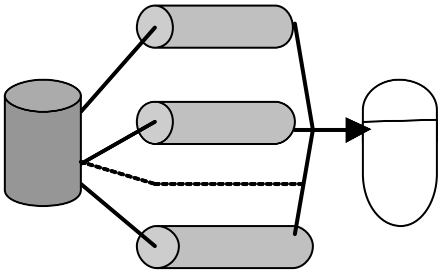
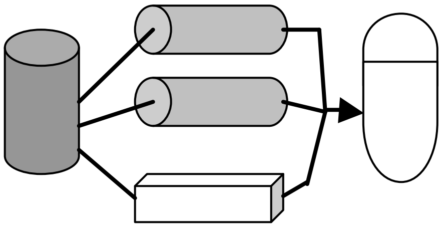
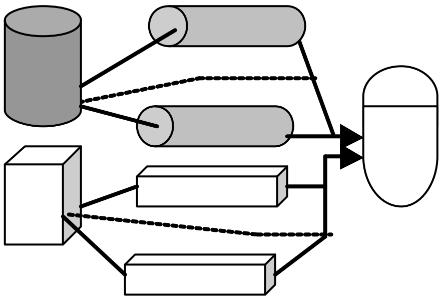
System Configuration		Defence	Failure Probability
		Technical and administrative	
Single train system		• Fail safe • Management system • Work preparation • DKV (operability readiness control) • Work practices	
Redundant system N out of m		Redundancy Separation • Functional separation • Organisational time-wise separation Stepwise introduction and test & maintenance	
Diverse system		Functional diversity	
Fully redundant and diversified systems/functions		Redundancy within diverse sections Operational diversity Software diversity	

Figure 5-1. Reliability (indicative values) of different system configurations

Empty page

Redundant equipment/systems have to be introduced in a way ensuring that any common characteristics will have a negligible impact on the overall system reliability. The goal is that the dependent failure contribution to the system failure shall be as low as possible, even if a complete independency is difficult to achieve and demonstrate.

Against this somewhat theoretical background, the following phases influence the life of equipment/systems at a nuclear power plant:

- Design and design review
- Installation and commissioning
- Operation, test and maintenance
- Plant modifications
- Operating experience feedback.

Main defences against dependencies during design, installation, test and maintenance are discussed below from a general point of view. Operation is not discussed separately. However, failure reporting, the plant information system and feedback of experience are other important parts of the defence strategy that are also discussed below.

5.3.1 Design and Design Review

Redundancy is implemented at both the function and system levels. Each system with redundancy is designed according to detailed standards and is for example required to meet the single failure criterion.

The basic physical protection against dependent failures in redundancies is the use of separation according basically to:

- Functional separation including diversity
- Physical separation

Diversity (different design principles for different redundant systems or functions and different software for the same purpose) can be seen as part of the functional separation together with time wise and organisational separation related to maintenance, testing and calibration tasks.

Procedure development and changes follow similar rules as the design of systems and equipment. Thus, procedures and other documentation have to be developed and reviewed with a special focus on the risk for dependent failures in applying or following this documentation. A careful development and regular reviews of procedures and other documentation require obviously management support and allocation of needed resources (time, personnel, etc).

Functional separation including diversity

The justification of 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. Nevertheless, it can be difficult to prove that sufficient functional separation exists. Methods used to achieve this demonstration include:

- Dependency assessment during the design and design review, or during plant modification projects.

- Use of the PSA plant model.
- Use of full-scale simulators, e g for checking of plant response in case of loss of certain bus bars.

The design process itself is secured by having adequate project management policy and instructions where dependency evaluation is explicitly required. The design process also includes requirements on internal review and preliminary safety review. Using different teams and methods to develop diverse designs can also help to secure redundancies. Another example is to have requirement on dependency consideration in contracts.

All these are administrative barriers aimed to the early identification and correction of weaknesses in the design process. Another important barrier is the review process conducted by the authorities.

International practices indicate that the principle of diversity is the most used design feature for improving the reliability of important safety functions. A safety function can accordingly be achieved by two or more safety systems based on different technical solutions and modes of action, and constituted of different components. The obvious benefit of such an arrangement is the low likelihood that a failure will commonly affect the diversified systems.

Diversity is demonstrated through physical control during the design and design review, or during plant modification projects. The review process conducted by the authorities is also important.

Physical separation

In general, separation costs money, and especially diversity in design and physical separation can initially be considered costly and resource consuming. The validation and verification costs can also be substantial.

In practice, separation by distance within the same room was used relatively often in older plants instead of physical segregation, i e closed compartments. Newer plants have relatively often adhered to a strict separation of the safety systems subdivisions. The extensive modernisation projects made recently and still on-going at the older units has resulted in a significant improvement of the physical separation in systems important for the plant safety.

Physical separation is demonstrated through assessment and verification during the design and design review, or during plant modification projects and use of PSA. The review process conducted by the authorities is also important.

5.3.2 Construction, Installation and Commissioning

Separation by the use of stepwise installation is a method to early discover and correct design weaknesses that can affect redundancies. Stepwise installation will also help in identifying ageing effects. Of course, stepwise installation is not possible in a new plant, but experience from another plant using a similar system can be taken into account. Full effectiveness of time wise separation is achieved assuming that the plant information system contains enough detailed information on change time points, as well as time points for tests and maintenance activities.

An effective failure reporting system is also needed to obtain full benefit of time wise separation as a mean to achieve a robust dependency protection.

5.3.3 Maintenance and Testing

In light of the short discussion above, time wise separation in maintenance and testing will also generally result in an increased probability for the early detection of potential CCF.

Separation of staff may further decrease the probability of dependent failures. Such a separation may however have a potential to increase the independent failure rate because of lower practical involvement and experience of the staff in related activities.

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 instrument calibration tools and tool settings before use, after use, or at scheduled regular intervals.
- Work on one train at a time.
- Limited access to redundant trains or only to parts of redundancies. Realised for example by use of key system.
- Work order for one redundancy first, then finish and go for next work order.
- Key locking of valve positions and indications to MCR (main control room).
- Complete operational readiness control (DKV) of the train after maintenance.

It is also possible to consider the safety importance of individual components in monitoring and maintenance activities. Such considerations support an efficient use of resources that can be seen as a contributor to an efficient dependency defence.

- Monitoring of equipment and individual components depending on their importance.
- Maintenance activities divided in four groups:
  1 Related to the plant's Technical Specifications (STF safety aspects)
  2 Operation (economical aspects)
  3 Important but not necessary
  4 Less important (components are allowed to fail).

  Components belonging to Group 1 are repaired according to the plant Technical Specifications. No repair priority is given to components belonging to Group 4, the work is done when time is available.

5.3.4 Failure Reporting

Internal plant practices for failure reporting mean that a judgement is made, in relation with the writing of the failure report, about the existence of potential dependencies. The judgement is then verified in steps.

An actual reporting practice (in use 2002) means that a special check mark is made on the reporting form when a CCF is suspected. No check mark is made if no CCF is suspected. Such failure report form design and procedure results in missing evidence whether the decision about CCF was made or not, in case of missing checkmark. This kind of failure reporting practice shall be avoided. The practice should be to always require an action, e g by having one check mark for independent failure and another for CCF suspected cases, or by requiring a check mark for independent failure – the basic assumption being that it is a dependent failure

Important for the robustness and use of a failure reporting system is to have a low threshold for reporting. A good safety culture is a basic prerequisite for achieving this.

5.3.5 Plant Information System

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

The plant information system has to include detailed information on all factors of importance for the plant safety in order to allow failure follow-up of critical component parts whose failure will be critical for the related component.

As earlier mentioned, the focus shall be on the risk important components. Less risk important components can be given less attention, and resources can be focussed on the high contributors. This kind of grouping can also be used in relation with maintenance and testing activities.

5.3.6 Feedback of Experience

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

- The plants have assigned personnel, so called component and system responsible, to the follow-up of specific components or/and systems.
- It is required to produce a yearly 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 representatives from different plants.
- Participation in owners group (meetings and information exchange).
- Participation in other groups meeting and work (ERFATOM, etc).

In addition, as indicated in [Ref. 15], efficient protections of safety system redundancies are management systems exhibiting a high quality improvement of:

- Experience feedback programme
- Preventive maintenance programme
- Corrective maintenance programme.

These points pertain basically to the follow-up and mitigation of ageing of both electronic and mechanical equipment.

The following areas are assessed to be cornerstones in the protection of system redundancies:

- Work practices/self-checking
- Work organisation/work preparation and operability readiness control (DKV).
- Content of procedures and other documentation utilised at the plants has to be accurate and updated (including work orders, system diagrams, etc).

The issues above should be fully reflected in the plant experience feedback programme. This presupposes in particular that the LERs should be revised whenever a replacement of similar parts on other group components has been made following inspections after failure of one component of the same group. As indicated in the mentioned study Ref. 15, replacements can even relate to other units at the same site and also to the similar components at other sites.

5.4 Efficiency of Protective Measures

The assessment of the efficiency of the protective measures against the occurrence of dependent failures is a delicate task, mainly due to the complicated and mutual influences of the different measures on the efficiency of each other. It is furthermore not possible to rank different phases in the life of an installation, system or component as regards to the most important phase for the protection against CCF. All phases are important and complement – are dependent upon - each other.

A manageable assessment has in practice to consider each protective measure and each plant life phase independently. This approach has been followed here as a base for an aggregated engineering judgement.

The plant survey carried out as part of the NAFCS project [Ref. 14] evaluated the efficiency of different defences against dependent failures according to plant personnel. The result is shown in Table 5-1, listing without prioritisation such defences. It can be observed that a basic defence like diversity has been left out. The reason for doing so is that diversity is most likely already established.

Table 5-2 indicates the decisive impact that managerial and organisational systems have on the efficiency of protective measures against the occurrence of dependent failures. It is furthermore judged that many of these systems and practices can be robustly implemented and verified at relatively low costs. The long-term benefits of these systems and practices, if clearly supported by the upper management, are obvious for the prevention and identification of dependent failures.

The indications on efficiency and cost in the table are based mainly on engineering judgement. Of course, the efficiency and cost relation need to be investigated for a specific case, before implementation of new or improved measures.

Table 5-1: Efficient defences against unwanted dependencies (Plant survey)
Awareness about dependencies (increased)
Simple solutions
Knowledge and experience
Good safety culture
Effective feedback of experience
Review in several steps
Tests, use of information system

Table 5-2: Efficiency and costs of different preventive measures against dependencies.

Protective measure against CCF	**Efficiency**	**Implementation efforts/costs**	**Verification efforts/costs**
Diversity	High	High	[low – high]
Functional separation	High	[low – high]	[low – high]
Physical separation	High	High	[low – high]
Organisational separation - Stepwise installation - Maintenance and testing	 [low – high] [low – high]	 Low Low	 Low Low
Management systems: - Design and design review - Installation and commissioning - Operation - Test and maintenance programme (preventive & corrective) - Operating experience feedback (including event & failure reporting, root cause analysis, corrective action programme & implementation of corrective measures)	 [low – high] [low – high] [low – high] [low – high] [low – high]	 Low Low [low – high] [low – high] [low – high]	 Low [low – high] Low Low Low
Work organisation (including work preparation and operability readiness control)	[low – high]	Low	Low
Work practices (including respect of procedures, collective & individual self-checking)	[low – high]	Low	Low
Operational, maintenance & test procedures	[low – high]	Low	Low

5.5 Dependency Protection Matrix

Table 5-3 describes different dependency types, the defence method, the verification method and the PSA dependency categories that are protected.

Table 5-3: Protection and verification of redundancies

Dependency type	Protection method	Verification method	Dependency Categories protected
Similar components	Diversity	- Design control - Design review - QA/QC during installation, commissioning and operation	CCF
Physical	- Physical separation and segregation	- Design control - Design review - QA/QC during installation, commissioning and operation	Area Events (on site and external events, dynamic and secondary effects)
Functional	- Engineering principles: - Functional diversity - Review of operational interfaces	- Design control - Design review - QA/QC during installation, commissioning and operation	CCI, Functional dependencies, system interactions
Management systems	- Experience feedback - Preventive maintenance - Corrective maintenance	- Internal QA-programme - Internal and external audits	CCF
Organisation related	- Work organisation	- Work preparation - Operability readiness control - Active leadership	CCF
Human related	- Management involvement - Work practices	- Active leadership - Self-checking	CCF
Ageing	- Operational practices - Maintenance programme - Experience feedback	- Trend analysis	CCF
Time	- Maintenance programme - Experience feedback	- Trend analysis	CCF
Tools (calibration and similar)	- Maintenance & calibration checks	-Internal QA-programme	CCF
Software	- Diversity - Tests - Simulator runs	- Stepwise installation & tests - Full-scope testing	CCF

6 Work procedures for defence against dependencies

This section provides practical guidance for the defence and control of dependencies. It would be naïve to postulate that this guidance is fully covering, although concerted efforts have been made towards this goal.

The guidance complements the presentation of the mostly technically oriented defences against dependencies presented in the previous section. It covers furthermore the different phases in a plant life, i.e. from design to operation. Part of the guidance is based on a plant survey that compiled proposals against dependencies mentioned by plant representatives [Ref. 14]. Other parts of the guidance are based on international literature and plant experience.

The guidance on defence mechanisms and good practices is presented according to the following grouping with one table for each group:

1. Design and design review
2. Construction, installation and commissioning
3. Operation
4. Test and maintenance
5. Reporting and plant information system
6. Experience feedback
7. Other defences

Table 6-1: Design and design review
Design and design review staff to be aware of CCF issues, both technical, organisational and human
Include CCF requirements in Project management model
Basic design requirements - Single failure analysis - Diversity in design - Spatial separation - Functional separation
Require PSA (mainly for evaluation of functional and spatial dependencies, but also for checking of other types of common characteristics)
Requirements on FMEA, FTA and HRA when purchasing equipment
Perform fire PSA to identify spatial separation deficiencies
Use PSA for checking of dependent failures
Use PSA for CCI analysis
Contract with supplier requires that CCF and dependency impacts are considered
Requirements on dependencies, failure rates and CCF rate when purchasing equipment. It is required to show that the requirements are met.
Choose components with high quality and proven design and experience
Consideration of ageing when purchasing equipment
Equipment qualification
Defence in depth in design by combination of independent review and primary safety review (PSG)
Design review shall ensure identification, minimisation of dependent failures and appropriate defences against their occurrence
Design and design review to encompass close interface with operation, maintenance, I&C departments
Design and design review to encompass operation, maintenance and test procedures
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.
Different meetings to present a modification: technical meeting and plant meeting.
Use full-scale simulator for: - Test of new design before installation - Test of system functions to identify dependent failure risks - Identification of functional dependencies - Identification of software dependencies - CCI analysis - Validation of procedures

Table 6-2: Construction, installation and commissioning
All involved persons (contractors, manufacturers, plant personnel) have knowledge about and focus on CCF issues
Perform audits, inspections and QC of component manufacturers, contractors, etc
Installation and commissioning procedures are reviewed for ensuring they do not introduce CCF
Perform systematic inspection and control after installation (especially electrical cables, I&C equipment, etc) – Check against specifications
Perform systematic testing after installation – Special test procedures for identifying potential CCF
Logic signals and actuation are tested for both operational and limiting conditions
Stepwise introduction of new equipment (to gather experience before full introduction)
Stepwise introduction of new equipment - Different ages of different redundancies

Table 6-3: Operation
Operation staff are aware of CCF issues – CCF issues are part of the staff training programme
Management attitudes promote and ensure high safety culture
An involved and powerful Safety Committee is established
CCF issues are on the agenda for shift meetings (other meetings)
Weekly meetings to inform personnel about changes (shift supervisors)
Access to redundancies is limited by administrative procedures
Access to redundancies is limited by physical procedures (different keys for accessing A, C and B, D subdivisions)
A process exists to ensure completeness, quality and validity of procedures (inclusive system instructions, drawings, copies, etc)
A policy exists how to use instructions
Check lists are circulated for new instructions (each operator shall acknowledge a new instruction)
Recurring review of procedures is performed with defined time intervals (operation, maintenance and emergency)

Table 6-4: Test and maintenance
Maintenance and I&C staffs are aware of CCF issues – CCF issues are part of the staff training programme
A process exists to ensure completeness, quality and validity of test and maintenance procedures (inclusive work orders, electrical permits, flow diagrams, logic diagrams, drawings, copies, etc)
Provide information on possible dependency/CCF risks on work permits and other administrative documents used during test and maintenance activities. Judgement by shift supervisor and approval by operation management during morning meeting
Several persons involved in activity, e g electrical permits: one writes and another reviews/approves
Judgement is made prior to the test if other redundancies can be affected by test
Time separation between tests
One redundancy is tested while the others are kept available
Maintenance of one redundant train according Technical Specifications.
Staggered testing
Different testing times (operation of diesel 1 only short time period and diesel 2 longer time, and next time shift)
Test of redundant equipment in case of unavailable component (independent if a CCF exists or not)
Check of calibration instruments before calibration of components
Check of calibration instruments after calibration tasks
Regular calibration checking
Marking of calibrated equipment
An extra operator verifies the position of manual valves that have changed position during the test
Judgement is made if other redundancies can be affected by maintenance activity
Time separation between maintenance works
One redundancy is maintained while the others are kept available
Exchange practices to make sure that a state of different ages for different redundant equipments is maintained
Motivate maintenance interval changes
Bi-cycle is used for maintenance optimisation
Operational readiness control (DKV) is strictly planned, performed and reported
All maintenance activities are recorded in the work order system
Maintenance/test interval changes are entered into the plant information system
Staff separation in test and maintenance OBS! This does not necessarily represent a good defence against CCF. Observe the risk for too little training if test occasions are few. This risk has to be related to the risk of trained personnel making the same mistake in several redundant trains.
Independent analysis of quality of deliveries important to safety (fuel for the emergency diesel generators, hydrogen, etc)
Model work (mock-up) is utilised as a mean to prevent the occurrence of CCF
All test and maintenance activities are, before closure, certified correctly performed and in accordance with the actual test and maintenance procedures (instrument and parameter readouts, electrical and instrumentation cable routing, etc)

Table 6-5: Reporting and plant information system
Plant management promotes a low reporting threshold (near-misses)
Plant management promotes and enforces high quality reporting of LERs, including the potential for CCF
Instances of miscalibrated tools are reported/logged (calibration instruments and torque keys)
Check for possible dependency impact in case of failure
Have CCF check in check lists
Check marking on failure reporting form to make check of dependency potential traceable
Morning meeting with review of failure reports and check for CCF and other systematic failures
Primary review meeting + independent evaluation of affected components and mitigating actions
PSA investigation of deviation from Technical Specifications
Perform root cause analysis of LER and report lessons learned
Follow-up reports with CCF aspects
Extra monitoring of especially important components, e g control rod drives, according to special instruction
Trend analysis of components and systems are performed and reported as a mean to identify and correct ageing effects

Table 6-6: Feedback of experience
Exchange and review of other plants LERs and scram reports
Procedure for work by system/component responsible
Participation in ERFATOM
Meetings between system responsible representatives from different plants
Meetings between component responsible representatives from different plants
Component responsible prepares yearly report with assessment of potential CCF
Risk follow-up activities
Group SAMDOK with TVO, FKG, OKG and BKAB (before also RAB) The group exchanges technical planning information. Meeting notes are distributed.
Participation in R&D projects with focus on dependencies
NOG – Nordic Owners Group

Table 6-7: Other Defences
Management and staff is confident with the content of SKIFS 1998:1
Concerned management and staff is confident with IAEA guidelines
NRC 10CFR50, and especially appendix J concerning test and maintenance is used in support of dependency protection
A CCF policy exists at the plant – Guidelines with dependency defence principles
Management promote and enforce a good safety culture and adherence to STARK
Management encourages all personnel and contractors to propose improvements of any kind

7 References

Ref. 1 **Johansson, G; NAFCS Project Programme, NAFCS-PR01, 2000-12-19**

Ref. 2 **ICDE Coding Guidelines, ICDECG00, revision 4, October 2000.**

Ref. 3 **Mankamo, T., Knochenhauer, M., "Dependency Analysis Guidance, NAFCS-PR13, October 2002.**

Ref. 4 **Classification and Analysis of Reactor Operating Experience involving Dependent Events, EPRI-NP-3967, February 1985.**

Ref. 5 **USNRC; Common Cause Failure Database and Analysis System; USNRC Report NUREG/CR-6268, Vol.1 Overview, Vol 2 Event Definition and Classification, Vol 3 Data Collection and Event CodingVol 4 CCF Software Reference Manual; USNRC NUREG/CR-6268, Vol.1-4., June 1998.**

Ref. 6 **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.**

Ref. 7 **Safety criteria for design of nuclear power plants, STUK Regulatory Guide YVL 1.0, 12 Jan. 1996**

Ref. 8 **Reporting nuclear power plant operation to the Finnish Centre for Radiation and Nuclear Safety, STUK Regulatory Guide YVL 1.5, 1 Jan. 1995**

Ref. 9 **Ensuring a nuclear power plant's safety functions in provision for failures, STUK Regulatory Guide YVL 2.7 , 20 May 1996**

Ref. 10 **Probabilistic safety analyses (PSA), STUK Regulatory Guide YVL 2.8 , 20 Dec. 1996**

Ref. 11 **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.**

Ref. 12 **Knochenhauer, M, " Handbok - Komponentmodellering vid analys av yttre händelser". SKI Report 97:50**

Ref. 13 **Bento, J.-P., "Data survey and review of the ICDE-database for Swedish emergency diesel generators", NAFCS-PR11, April 2002.**

Ref. 14 **Hellström, P., " Survey on Defence against Dependent Failures", NAFCS-PR05.**

Ref. 15 **Bento, J.-P., "Qualitative analysis of the ICDE-database for Swedish emergency diesel generators", NAFCS PR-08, April 2002.**

Ref. 16 **Bento, J.-P., "Defence Assessment in Data", NAFCS PR-20, April 2003.**

Appendix 2

Dependency Analysis Guidance

October 2003

List of Contents

List of Tables

List of Figures

Acknowledgement

Some of the descriptions of specific dependency analysis categories are based on extracts from the Guideline “Analysis of Dependencies” developed within the Kola 2 PSA [1-3]. The permission to use this material is gratefully acknowledged.

1. Introduction

1.1 Background

This Dependency Analysis Guidance is the result of an effort within the Nordic Working Group on CCF Studies (NAFCS) [1-1]. The NAFCS project is part of the activities of the Nordic PSA Group (NPSAG), which is a joint co-operation between the Nordic utilities and authorities aiming at recognition and development of PSA.

The NAFCS project is performed during the years 2001 – 2003, and includes activities within the following fields:

- Survey and review of analysis models and data sources
- Survey of defences against dependent failures
- Analysis of Nordic CCF data from the ICDE database and other sources
- Development of impact vectors for some important components:
    - diesel generator
    - pumps
    - motor operated valves
- Estimation of CCF model parameters and their uncertainties
- Development of Dependency Defence Guidance
- Development of Dependency Analysis Guidance

The International Common-Cause Failure Data Exchange Project ("ICDE Project“) constitutes essential background to the NAFCS project [1-2].

The safety systems in Nordic nuclear power plants are characterised by substantial redundancy and/or diversification in safety critical functions, including their support functions. Furthermore, these functions and system subs are physically separated. Viewed together with the evident additional fact, that the single failure criterion has been systematically applied in the design of safety systems, this means that the plant risk profile as calculated in existing PSA:s is usually strongly dominated by failures caused by dependencies resulting in the loss of more than one system sub.

For the reason mentioned above, PSA:s include a thorough identification and modelling of both functional and physical dependencies. The various PSA analysis tasks are tailored to identify, model and derive data for important dependencies. Therefore, the accident sequence analysis, the systems analysis, the analysis of common cause initiators (CCI), area events and external events all put special emphasis on identifying mechanisms and interactions that need to be considered in the dependency analysis.

This means that the completeness and relevance of the identification and modelling of the various dependency categories has a strong influence on the completeness and relevance of the PSA itself.

1.2 Aim and Scope

The purpose of this document is to provide a common methodological guidance for the analysis of dependencies in PSA:s. The Guidance is meant to clarify the scope of the analysis of the various dependency categories, the interaction of the various analyses and their PSA context, as well as to provide guidance for the performance of the analysis of the various dependency categories.

The term dependencies shall be given a wide interpretation, and includes all external impacts or interactions, which may affect the independence of barriers.

The analysis of dependent failures is a comprehensive task. The sub-task "Analysis of dependent failures", which is normally found in PSA:s, will typically include only part of the analysis. In addition, parts of the analysis are usually performed as part of a number of different PSA sub-tasks, such as the analysis of initiating events, systems analysis, HRA and data analysis. In view of this split-up of the analysis, which is largely justifiable, one important aim of this Guideline is to provide an integrated description of the analysis of dependent failure within a PSA.

Thus, the Guideline aims at giving a complete overview of the types of dependencies that need to be considered in a PSA (dependency category), and their mutual relationships, as well as to sum up the requirements in the Nordic countries concerning analysis of dependencies.

The Guideline shall give methodology guidance, but includes no method development. As far as possible, guidance on how to consider dependencies in each PSA analysis task is given by referring to existing handbooks and guidelines. Wherever possible, documents developed as part of previous or on-going Nordic projects are given as references.

The Guideline is a freestanding document, presenting methodological guidance for the analysis of dependencies in Nordic PSA:s It does not present *one* integrated approach, suited for inclusion into one "dependency analysis project", but rather a framework for defining the various tasks needed in order to assure completeness and relevance in the analysis of dependencies. These tasks may be realised in different sub-projects, or as part of other major PSA tasks.

1.3 Outline and Context of Guideline

The general areas covered in the NAFCS project as outlined in the previous section, are shown in Figure 1-1. The different reports produced, and their use in producing the two main topical reports, the Dependency Analysis Guidance, and the Dependency Defence Guidance, are indicated. More details on the project reports are given in Attachment 2.

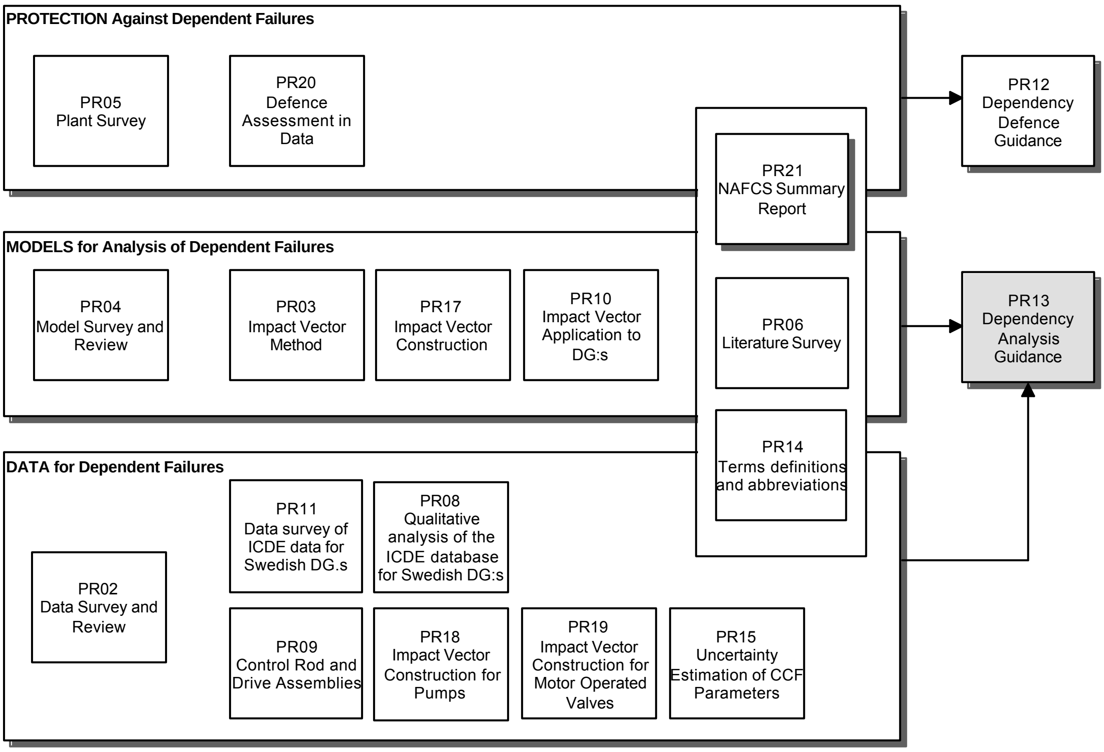

PROTECTION Against Dependent Failures
PR05 Plant Survey
PR20 Defence Assessment in Data
PR12 Dependency Defence Guidance
PR21 NAFCS Summary Report
MODELS for Analysis of Dependent Failures
PR04 Model Survey and Review
PR03 Impact Vector Method
PR17 Impact Vector Construction
PR10 Impact Vector Application to DG:s
PR06 Literature Survey
PR13 Dependency Analysis Guidance
PR14 Terms definitions and abbreviations
DATA for Dependent Failures
PR11 Data survey of ICDE data for Swedish DG.s
PR08 Qualitative analysis of the ICDE database for Swedish DG:s
PR02 Data Survey and Review
PR09 Control Rod and Drive Assemblies
PR18 Impact Vector Construction for Pumps
PR19 Impact Vector Construction for Motor Operated Valves
PR15 Uncertainty Estimation of CCF Parameters

Figure 1-1 Context of Guideline

This Dependency Analysis Guidance consists of four main parts. Chapter 1 is the introduction, which describes the background, context, aim, and scope. Chapter 2 summarises the requirements concerning analysis of dependencies in Sweden and Finland. Dependency categories and their relation to the different PSA analysis tasks are discussed in Chapter 3.. Finally, Chapters 4-11 describes the technique by which dependencies are considered in the PSA. This includes descriptions of analysis context, input, output and documentation, as well as of the analysis methodology along with the relevant references.

1.4 Assumptions and Limitations

Assumptions and limitations that are specific to some dependency category, are listed as part of the relevant chapter. In addition, the following general assumptions and limitations apply in this document:

- The interpretation of the concept of "dependency" is not literal, i.e., the focus is on safety degrading dependencies, which affect multiple safety functions.
- When describing the analysis methodology for each specific dependence category, references are made to external methodology documents as far as possible. This means that the status of these documents needs to be checked when performing an analysis.
- Although the consideration of dependencies in relation to external events is included as part of the discussion of the External Events analysis task, the methodology for specific external events is outside the scope of this Guideline.
- Dependencies originating from war impact or acts of sabotage or terrorism are outside the scope of this document.

1.5 Quality Assurance

The analysis of dependencies is one of the most important completeness and relevance issues in a PSA. This means, that the quality assurance of the analyses is proportionally important. Quality assurance as stated in PSA guidelines and method descriptions mainly covers this adequately.

There can be areas requiring special QA effort in the analysis of dependencies. For example, Section 11 describes a specific procedure of redundant CCF data analysis to enhance the quality in the interpretation and assessment of recorded events.

1.6 References

1-1. Johansson, G; NAFCS Project Programme, NAFCS-PR01, 2000-12-19

1-2. ICDE General Coding Guideline. Rev.3, 21 June 2000

1-3. Mankamo, T, Jänkälä, T, Kattainen, M, Angner, A, Johansson, G and Lioubarski, A; *PSA Task Guide: Analysis of Dependencies, Kola NPP Unit 2*. K2PG-Dep, Issue 2, 12.04.2001.

2. Requirements Concerning Analysis of Dependent Failures

2.1 Requirements in Sweden and Finland

There are no specific documents from Nordic authorities concerning the requirements put on the analysis of dependent events. However, the issue is touched upon in several authority documents, both from the design and analysis point of view.. Examples of documents containing analysis requirements are the STUK Guide YVL 2-8 [2-1], and the PSA Review Handbook of SKI [2-2].

Thus, while there are no specific requirements on how to analyse dependent events, there are expectations on the completeness and quality of the analysis and the consideration of dependencies in PSA modelling. As an example, the review criteria from the PSA Review Handbook of SKI [2-2] are listed below:

- To the extent possible, dependencies shall be treated and identified in all tasks that are part of the PSA (initiating events, systems analysis, HRA, data analysis).
- Common Cause Initiators (CCI) shall be analysed in sufficient detail in the analysis of initiating events.
- Common cause initiators (CCIs) need special concern to ensure identification of these events. The plant model itself can be an important tool for CCI identification and shall be used.
- Functional dependencies shall be explicitly modelled in the fault trees.
- Dependencies due to human errors shall be identified, evaluated and documented. They shall be treated as a kind of functional dependencies, i.e., they shall be explicitly modelled in the fault trees.
- A systematic analysis of the plant configuration shall be used to identify and group components susceptible to common causes into Common Cause Components Groups – CCCG.
- CCF type dependencies between components should be modelled both for active and passive components.
- A detailed qualitative analysis should be performed based on plant specific and generic experience data in order to identify possible safety improvements that may strengthen the protection against CCF and reduce the probability of CCF events.
- In view of the great risk importance of CCF events, data for parameters in a CCF model require a structured analysis, and it is important to make the best possible estimations of CCF parameters. If possible, plant specific data should be used as a basis for the estimation.

Furthermore, various aspects of the analysis of dependencies have been analysed in numerous Nordic research projects, as described and summed up in the Data Survey and Review [2-3] and the Model Survey and Review [2-4] reported within the NAFCS project. To some extent, these projects have defined the recommended methodology.

2.2 International Requirements

International requirements regarding the analysis of dependent failures are described in a number of procedure documents issued by the USNRC and the IAEA. It is believed that most other national procedure documents are largely based on these sources.

Specific procedures seem to exist only for CCF analysis; refer to Chapter 11 for these references. Other dependency categories are indirectly covered by various, more general PSA guidelines.

2.3 References

2-1. STUK (Finnish Radiation and Nuclear Safety Authority); *Probabilistic Safety Analysis*; STUK Report YVL2-8, December 20, 1996

2-2. SKI (Swedish Nuclear Power Inspectorate); *Tillsynshandbok PSA (PSA Review Handbook)*; SKI report 99:48

2-3. Mankamo, T; *CCF Data Survey and Review*; NAFCS-PR02

2-4. Mankamo, T; *CCF Model Survey and Review*; NAFCS-PR04

3. Description of Dependence Categories

3.1 Introduction

Safety functions and safety systems of nuclear power plant are typically characterised by a high degree of redundancy and diversity. The reliability of safety systems is further enhanced by extensive status control, supervision and maintenance programmes. As a result, multiple failures are usually required to completely fail a safety function.

Multiple independent failures of reliable equipment in soundly designed systems are usually very improbable. Therefore, any existing failure mechanism, which increases the probability of multiple failures, may have a decisive impact on the total probability of failure of the related safety function or safety system. The interactions that needs to be considered can be due to:

- functional dependencies, or
- physical dependencies.

Functional dependencies include the following types of interactions between systems, components and structures:

- Shared components; i.e., different systems/components depend on the same active or passive component for their function. Examples are shared valves, piping or water reservoirs.
- Shared auxiliary systems, i.e., different systems/components depend on the same auxiliary systems. Examples are component or room cooling systems, instrument air and power supply. System/component control is a special case under the same heading:
- Shared automatic control, i.e., different systems/components depend on the same automatic control (activation or supervision).
- Shared manual control, i.e., different systems/components depend on the same manual action.

Physical dependencies include a number of interactions where the location of systems, components and structures is of importance.

- Shared location, i.e., different systems/components are located in such a way, that they may be affected at the same time in case of certain initiating events (not necessarily restricted to location in the same room):
  - Area event impact
  - External event impact
  - Secondary impact, e g dynamic loads or other physical impact following an initiating event.

Known functional and physical dependencies can be considered by explicit modelling in the PSA.

However, there are usually residual dependencies, i.e., unknown shared causes for the unavailability/failure of systems, components and structures. These failures may have a variety of causes, including human errors during design, installation, operation or maintenance. Residual dependencies are modelled as common cause failures (CCF).

In this context it must be underlined, that the extent to which dependencies are residual/unknown, is partly dependent on the level of detail of the analysis. Thus, today's PSA models include explicit modelling of some dependencies, which were considered residual in earlier PSA versions, e.g., concerning area dependencies.

The different dependence categories defined in this document cover all of the above interactions.

3.2 Definition

The concept of dependence is related to the definition of dependent events, which can be exemplified in the case of two events. The events A and B are dependent if their probabilities fulfil the following inequality:

$$P(AB) \neq P(A) \cdot P(B)$$

Equivalently, the events A and B are independent if and only if $P(AB) = P(A) \cdot P(B)$. In the presence of dependence often, but not always, $P(AB) > P(A) \cdot P(B)$, i.e. the probability of simultaneous occurrence of the events is increased due to the dependence. An opposite situation can be relevant, for instance, in case of mutually exclusive events A and B, which implies that $P(AB) = 0$. The latter has to be considered for combinations of success and failure paths in event trees.

The analysis of dependencies is devoted to the cases where the multiple failure probability increases due to dependence. Thus, only dependencies with a negative safety impact are covered by the Guidance, i.e., where

$$P(AB) > P(A) \cdot P(B).$$

Another way to express this inequality is in terms of increased conditional failure probability, where the probability of event B given the occurrence of event A is larger than the unconditional probability of event B:

$$P(B|A) > P(B)$$

These dependencies may be due to three fundamentally different kinds of impact, each of which will be discussed in a separate section below:

- Functional dependencies,
- Initiator related dependencies (including the physical dependencies), and
- CCF dependencies

3.2.1. Functional Dependencies

In this case the first expression of the inequality is best used, i.e. $P(AB) > P(A) \cdot P(B)$. P(A) shall be read as "probability of failure of system A" and P(B) shall be read as "probability of failure of system B". Functional dependencies are described by a case where the dependency between events P(A) and P(B) lies in some kind of a shared function, i.e., the events are not independent because they share some of the failure causes.

This is clarified by expressing the dependent probability in the following way:

$$
\begin{aligned}
P(A.B) &= P((A_i + C).(B_i + C)) = P(A_i.B_i + C) \\
&\cong P(A_i).P(B_i) + P(C) \\
P(A).P(B) &= P(A_i + C).P(B_i + C) \\
&\cong P(A_i).P(B_i) + P(A_i).P(C) + P(C).P(B_i) + P(C)^2 \text{ , where}
\end{aligned}
$$

C = failure of A and B due to shared cause
A_i, B_i = failures due to independent causes.

The expressions are developed in so called Rare Event Approximation containing only 1st and 2nd order terms. Evidently P(A.B) > P(A).P(B) and the difference can be substantial because the shared cause term P(C) may dominate P(A.B).

As already discussed in some detail in the introduction to this chapter, functional dependencies involve dependence on shared equipment, systems, support functions or manual interactions. Some of these cases are very straightforward, and mainly rely on a sufficiently complete design analysis. In other cases, the functional connection is less evident, which may make the corresponding analysis quite extensive.

3.2.2. Initiator Related Dependencies (including physical dependencies)

In this case the second expression in the inequality is more useful, i.e., P(B|A) > P(B). Event A is the occurrence of initiating event A, and P(B) shall be read as the "probability of failure of system B". Thus, P(B|A) is the conditional probability of a failure of system B, given that the initiating event A has occurred. It is part of the definition of a CCI event, that system B may be needed after an initiating event of type A.

Initiator related dependencies may be of the following sorts:

- Common Cause Initiators (CCI), arising from system or component failures, or from the disturbances in plant processes, normally shortly called CCI:s.
- Area events, i.e., events occurring within the plant, but outside of plant systems and processes. The most important examples are internal fires and flooding by water or steam. However, there are also other possible area events, such as missiles from rotating equipment or exploding pressure vessels.
- External events, i.e., occurring outside the plant, and outside of plant systems and processes. They may be man-made or natural. Examples are transportation accidents in plant vicinity and various meteorological and hydrological events.
- Dynamic effects after a LOCA, i.e., failures in connection with pipe breaks. Dynamic effects may be due to pipe whip, jet impact or missiles, and may mechanically damage adjacent piping, or have other secondary impact (heat, moisture, etc.) on the function of adjacent active equipment.
- Subtle dependencies may be both functional and physical. They cover dependencies, which are specific to actual demand conditions and typically not detected in normal operation or by surveillance tests[1].

A common characteristic of these dependencies, is that they all cause a plant transient and at the same time affect the availability of safety systems. The system impact may be functional, as it is for CCI:s, or be due to an aggressive environment (moisture, heat, flame, motion, etc.).

[1] Subtle dependencies are also called ”system interactions” or ”subtle interactions”.

A further characteristic of initiator related dependencies is that, although they often also involve the development of new ways of functional dependencies between redundant equipment, this is not a prerequisite.

3.2.3. CCF Dependencies

The “standard” definition of CCF, which is also used in the ICDE project, is as follows:

> *Common Cause Failure is a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.*

In this case the first expression of the inequality is best used, i.e. $P(AB) > P(A) \cdot P(B)$. P(A) shall be read as "probability of failure of component A" and P(B) shall be read as "probability of failure of component B". In addition, it is normally assumed that components A and B are identical or closely similar. In the PSA terminology, the Common Cause Failure (CCF) is used in the special meaning for the dependent failure of identical (or closely similar) components. A group of components where the unavaílabilities/failures are vulnerable to common causes is referred to as a Common Cause Component Group (CCCG).

Note: *The restricted definition of CCF is used in this guide. The terms dependent events or dependent failures are used in a more general meaning. Compare to the standard references, e.g. [NUREG/CR-5485, Section 1.2].*

Common cause failures have a potentially large risk impact. They are also difficult to model and quantify. For this reason, these dependencies have traditionally received large attention. Several work reports within the NAFCS project deal with the evaluation and development of methods and data for CCF analysis.

3.3 Summary of Dependence Categories

The discussion in the previous sections has resulted in the definition of a number of dependence categories that need to be treated in a PSA. They are listed in Table 3-1.

Table 3-1 Summary of Dependence Categories

	Dependence category	Description	Guideline chapter
Functional	Functional Dependencies	Dependence on shared mechanical or electrical equipment, such as common support systems, power supply or control signals.	4
	Human Action Dependencies	Dependence via shared human actions: 1) Failures of consecutive actions to mitigate a transient or accident sequence 2) systematic test or maintenance errors.	5
	Subtle Dependencies	Dependencies specific to the actual demand conditions and typically not detected in normal operation or by surveillance tests (may also be a physical dependence).	6
Initiator	Common Cause Initiators	Initiating event, which arises from the system or component failures, or from the disturbances in the plant processes (intrinsic events).	7
	Area Events	Events occurring within the plant, but outside of plant systems and processes	8
	External Events	Events occurring outside the plant, and outside of plant systems and processes	9
	Dynamic Effects	Failures in connection dynamic effects occurring together with pipe breaks	10
CCF	Common Cause Failures	Failure of identical (or closely similar) components due to common vulnerabilities	11

In this context it may be worth pointing out, that it is impossible to make a perfect classification in the sense that the categories would both represent complete coverage and at the same be mutually exclusive, because of mixed dependence types. The aspect of complete coverage is more essential. It is believed that the dependency analysis tasks in this guidance completely cover all important dependencies.

3.4 Work Context in PSA

Due to the interdisciplinary character, most dependence categories must be treated in context to several PSA work tasks as indicated in Table 3-2. The PSA is assumed to include the following main tasks:

- Initiating Event Analysis
- Accident Sequence Analysis
- System Analysis
- Human Reliability Analysis
- Analysis of Dependencies (mainly CCF analysis)
- Data Analysis
- Quantification and Result Analysis
- Area events analysis (possibly conducted as separate project)

- External events analysis (possibly conducted as separate project)

The task interconnections are shown in the tables below and discussed more in detail in the chapters dealing with the dependency categories. However, this shall mainly be seen as suggestions, as the detailed task interface planning is an essential part of the work planning of every PSA.

Table 3-2 Work Context in PSA of Dependence Categories

	Dependence category	Analysis procedure or method	Work context
Functional	Functional Dependencies	Component models, FMEA Dependence matrices	System analysis, Fault Tree modelling
	Human Action Dependencies	Human Reliability Analysis	System analysis, Human Reliability Analysis, Fault Tree modelling, Event Tree modelling
	Subtle Dependencies	Analysis of operating experience, insights from other PSA studies	System analysis, Fault Tree modelling, Event Tree modelling
Initiator	Common Cause Initiators	Analysis of operating experience, insights from other PSA studies, link from functional dependencies, use of fault tree models	Initiating Event analysis, System Analysis
	Area Events	Identification of potentially safety important rooms	Quantification and Result Analysis, basic PSA
		Room specific area event frequency (initiating event)	Self-standing task
		Determine room contribution to defined plant end states	Self-standing task
	External Events	Identification of potentially relevant external events	Self-standing task
		Deterministic screening, using plant data (vulnerability and strength of safety significant buildings and structures) and event data (strength and frequency)	Self-standing task
		Determine event contribution to defined plant end states	Self-standing task
	Dynamic Effects	Physical analyses	Initiating Event analysis, pipe breaks
CCF	Common Cause Failures	Definition of CCCGs, Alpha Factor method for CCF:s	System analysis, Fault Tree modelling, Data analysis

Understanding the essential connections between analysis tasks is fundamental, and often more difficult than the methodology for a well-defined task.

Upgrading some category of the dependency analysis can require substantial additional work in existing PSA parts, in some cases even a full revision of the PSA, including documentation.

Table 3-3 Input into the analysis of dependencies

From task	Required information	Dependency analysis subtask
Determi-nistic PRA support	Structural, thermohydraulic and flow analyses for selected impact scenarios	Dynamic effects
IE analysis	Survey of the plant transients and incidents	CCI analysis
		Subtle dependencies
IE analysis, Accident sequence analysis	Protection signals to actuate each IE and generated in connection to the IE	CCI analysis
		Area events /external events
		Subtle dependencies
Systems analysis	Summary description of plant systems, simplified flow diagrams, system interfaces	Needed in all subtasks
	Functional dependence matrices	CCI analysis
		Area events /external events
		Subtle dependencies
	Dependency database	CCI analysis
		Area events /external events
		Subtle dependencies
	Candidate list of components (and failure modes) for CCCGs	CCF analysis: definition of CCCGs
	Defined CCCGs	CCI analysis: triggering events constituted by multiple component failures
	Preliminary fault trees	Subtle dependencies
Data analysis	Survey of system and component failures	CCI analysis
		Subtle dependencies

Table 3-4 Output from the analysis of dependencies

To task	Supplied information	Dependency analysis subtask
IE analysis, Accident sequence analysis	Screened list of significant CCIs	CCI analysis
	Special scenarios to be incorporated in an IE category and modelled in the event tree	Subtle dependencies
	Extensions to LOCA and transient categories; refinements in the event trees	Dynamic effects
Systems analysis	Interactions to be modelled in the fault trees	Subtle dependencies
	Defined CCCGs	CCF analysis: definition of CCCGs

4. Functional Dependencies

4.1 Definition

Functional dependencies cover system and component interconnections, which are related to process connection, control signal, power supply or other support functions such as cooling and lubrication and operator actions.

4.2 Scope

The PSA model shall include all functional dependencies that are relevant in view of the scope of the PSA. Functional dependencies may be specific for an initiating event, which means that iteration between the Initiating Event Analysis and the System Analysis is needed in order to take into account such details. As an example, protection signals for specific initiating events is a functional dependence, e.g., fire detection signals.

The correct identification of implicit system dependencies (not evident from schematics) is crucial. Thus, dependence on ambient environmental conditions is also a functional dependence, e.g., dependence on room temperature and thus on the ventilation system and on the room heating system.

4.3 Assumptions and Limitations

The specific assumptions and limitations of this task are documented as part of the System Analysis. The following items are examples of generic assumptions and limitations:

- In some plant rooms, the failure of room cooling/heating can constitute a CCI. Similarly, specific failure situations in other support systems can lead to CCIs, which are analysed separately, see Chapter 7.
- Failure of component protection is not considered as failure if it is likely that the component will survive the demand and needed mission time (will fulfil the safety function even though degraded)
- No consideration is given to functional dependencies that only have operational significance (not affecting plant response in any analysed initiating event)

4.4 Work Context and Interfaces

The identification and modelling of functional dependencies is usually included in the Systems Analysis task.

The collected data about the functional dependencies is essential information to many other tasks, especially to the analysis of CCIs, area events, external events and subtle dependencies.

4.5 Input

The input for analysis of functional dependencies is the same as to the Systems Analysis in general.

4.6 Methodology Description

The identification of functional dependencies is part of standard system analysis procedures. Thus, it is usually adequately described in method descriptions for the systems analysis task. The handbook on component modelling developed as part of the Swedish project on area events (Projekt Yttre Händelser) [4-1] can be consulted for questions related to functional dependency modelling.

Two basic issues in the identification of functional dependencies are:

- Identification of safety critical functions, systems and components
- Identification of component interfaces

Both of these issues are shortly discussed below.

4.6.1. Identification of safety critical functions, systems and components

To provide a correct risk picture, the PSA model must include all safety critical functions, systems and components – as well as a correct representation of their mutual interaction. This is an obvious requirement, which may, however, be difficult to fulfil for complex initiating event.

The definition of critical safety functions must consider all classes of initiating events and operating modes that are covered by the PSA. This means that, in addition to the safety functions traditionally included (shut-down, residual heat removal, etc.), there may be a need to consider safety functions that are needed only in connection with for example a refuelling outage or a fire (fuel pool cooling, fire detection, etc.).

The definition of safety critical systems follows logically from the definition of critical safety functions. All systems that are directly or indirectly needed in order to maintain a safety function need to be modelled in the PSA, considering the classes of initiating events and the operating modes that are covered by the PSA.

Finally, the systems analysis indicates the components that need to be modelled in the PSA.

4.6.2. Identification of relevant component interfaces

The creation of a representative component model, requires the initial definition of the expected functions of the component in connection with the safety demands being analysed. Thereafter, a systematic mapping is required of failure mechanisms that might disturb or block these functions. This requires a detailed mapping of the interaction of the component.

As part of this interaction, the component will have an exchange of information with it’s surroundings - it receives information and it supplies information. It will also normally require some kind of energy supply (electrical power, liquid fuel, compressed air, manual actions, etc.). In some cases, auxiliary functions are required (room cooling, component cooling, lubrication, etc.). The working environment of the component becomes important in connection with the analysis of area events and external events. Finally, there is the normal and situation-dependent interaction with the plant maintenance and operating personnel. Figure 4-1 summarises the interaction between a component and it's environment.

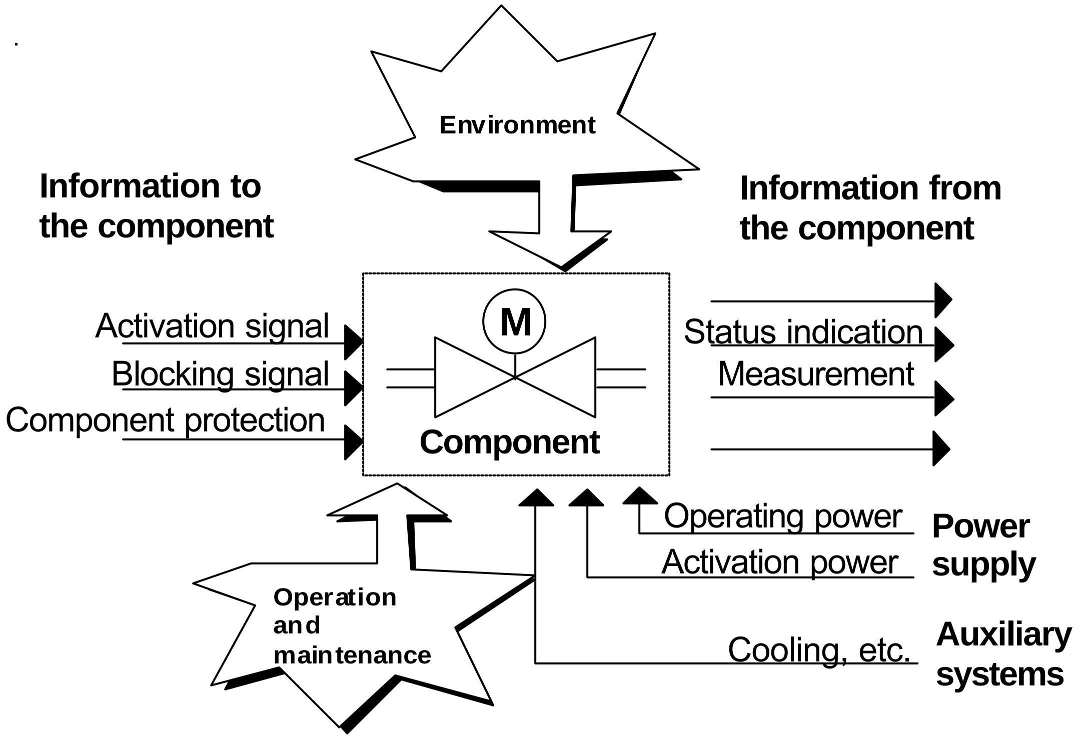


Figure 4-1 Overview of the component-plant interaction (from [4-1])

4.7 Output and Documentation

Component information tables and system dependency matrices are used to document the functional dependencies in the System Analysis reports.

In addition, it is useful to produce an integrated dependency matrix to provide an overview of the functional dependencies over all systems.

The information contained in the component information tables, protection signal tables, dependency matrices etc. is recommended to be stored in a relational database.

4.8 References

4-1. Knochenhauer, M; *Handbok – Komponentmodellering vid analys av yttre händelser*; SKI Report 97:50; December 1997.

5. Human Action Dependencies

5.1 Definition

Human action dependencies cover situations in which errors can be made in successive operations, affecting the reliability of redundant components or systems or the reliability of successive operator actions in an accident sequence after an initiator.

All operator actions with multiple human errors are susceptible to human error dependencies.

5.2 Scope

This category covers the following sub-types of dependencies:

1. Pre-initiator dependencies
   The most important human action dependencies are those of test/maintenance/calibration errors (pre-initiator errors). When a pre-initiator action is carried out for multiple similar components, there is an increased probability to repeat a pre-initiator error. In this way, systematic maintenance or testing errors can be a human action dependence.
2. Initiator dependencies
   Initiator errors, i.e., operator errors inherent to the initiating event.
3. Post-initiator dependencies
   Multiple post-initiator operator actions as recovery actions and possible preceding operator actions in the sequence can be dependent. Such dependency can be due to lack of time, reducing the time available for further operations, or due to repeated errors in successive actions. In addition, the dependencies between operator actions can appear because several different actions are accomplished by the same operator or are under supervision of the same supervisor.

All of the above dependencies are treated by the use of conditional human error probabilities, where all previous conditions are taken into account. It is not easy to show that all dependencies are considered, It is therefore recommended to perform a human error dependency check as part of the model QA.

5.3 Assumptions and Limitations

Some basic assumptions and limitations are:

- Human action dependencies usually do not include cases where the cause of a CCF event is MTO related.
- The determination of human action dependencies may always remain somewhat subjective.

5.4 Work Context and Interfaces

The analysis of human action dependencies is part of the Human Reliability Analysis.

The identification of human action dependencies is done in several PSA tasks, mainly the Initiating Event analysis, the Event Tree Analysis, the Systems Analysis, the Area Events Analysis or the External Events Analysis.

5.5 Input

The main input data needed for the analysis of pre-initiator dependencies and initiator dependencies are CCCG definitions, test/maintenance instructions, and sequencing information. Identified errors (dependencies) divide into:

- Latent errors, constituting pre-initiator dependencies, and
- Monitored or self-revealing errors, among which a part can constitute initiator dependencies

The analysis of post-initiator dependencies requests accident sequence models and operating instructions. In addition, the insights from training simulator exercises can be very useful.

5.6 Methodology Description

The dependencies introduced by human interaction as a part of the system analysis represent explicit dependencies included in the models. The human interaction dependencies can be actions related to:

- Pre-initiator human interaction, Systematic calibration or alignment errors.
- Initiator human interaction.
- Post-initiator human interaction failures in following procedures and during recovery.

If possible, dependent human actions should be combined and modelled as a single event, in case the events are completely dependent. Sometimes, there is only a partial dependence, which prevents such combination. In such case, new CCF type errors should be introduced (for pre-initiator error dependencies) or the human error probabilities for single human errors should be modified in order to reflect the dependencies (for post-initiator error dependencies).

5.6.1. Pre-initiator error dependencies

Pre-initiator error dependencies such as systematic maintenance or testing errors can be considered by the CCF modelling, as discussed in Chapter 11. Usually CCF data cover multiple failures due to maintenance or testing errors. An explicit modelling of pre-initiator error dependencies is recommended in the specific cases where their contribution falls outside the coverage of CCF models and data, e.g. due to special significance or because affecting components in different systems. For explicit modelling and quantification, NUREG/CR-1278 [5-1] presents a suitable methodology. Double counting should be avoided.

5.6.2. Initiator error dependencies

Identification of dependencies

Analysis of dependencies in initiator operator actions is determined in the Initiating Event Frequency model.

Operations performed by the control room crew or field personnel typically may have dependencies connected to the post initiator actions. Errors inherent to the Initiating Event are considered in successive actions with high or complete dependency in order to avoid excessive optimism.

Quantification of dependencies

When evaluating the post-initiator human action in a cut set, dependencies between the initiator error and the post-initiator error should be assessed by considering the cognitive situation given by the initiating event.

5.6.3. Post-initiator error dependencies

There are two categories of human errors related to post-initiator errors:

- Response-to-initiator HE
  Human error committed by an operations crew during the course of an accident while following the procedures to mitigate the situation, which is the result of failure in diagnosis or implementation. For quantification purposes, these HE:s are usually decomposed into cognitive and implementation parts.
- Recovery HE
  Human error committed by an operations crew during the course of an accident while performing actions which are, as a rule, not unequivocally included in the procedures and have as their objective the recovery of failed equipment or use of alternative means to serve the function of this equipment.

Post-initiator error dependencies are treated by re-defining dependent operator actions into a single human error.

Identification of dependencies

Analysis of dependencies in post-initiator operator actions is determined by the recoveries modelled in the reliability model. Operations performed by the control room crew or field personnel typically have dependencies. A detailed analysis of these dependencies can often be avoided by (conservatively) allowing no more than one recovery action per cut set instead of allowing consecutive recovery actions. The same rule is applicable for cut sets with preceding operator errors. In case consecutive operator actions are considered, total time requirements and availability of human resources should be taken into account. In addition, any errors in preceding actions should be present in successive actions with high or complete dependency in order to avoid excessive optimism.

Post-initiator errors should be defined at as high level as possible. This way, two or more post-initiator errors do not appear in the same cut sets, which would lead to optimistic results. The PSA results must always be reviewed to ensure that all cases (cutsets) with successive post-initiator errors are individually addressed.

Dependencies in post-initiator operator actions can be identified in many stages of the study: system analysis, fault tree modelling, event tree modelling or the HRA itself.

Quantification of dependencies

The detailed analysis of post-initiator error dependencies is avoided by allowing only one post-initiator human action in a cut set, assuming the imposed conservatism can be accepted. In an undesirable case, however, in which this cannot be accepted, the existence of dependency between preceding and latter human actions is left to the judgment of the analyst. Methods of addressing such dependencies are presented in NUREG/CR-1278 [5-1].

5.7 Output and Documentation

The documentation of the analysis of human action dependencies is part of the Human Reliability Analysis.

5.8 References

5-1. Swain, A.D.; Guttman, H.E.; *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, 1983

6. Subtle Dependencies

6.1 Definition

Subtle dependencies[2] cover dependencies, which are not ordinary functional dependencies but are specific to actual demand conditions, when the plant systems are actuated and operated under transient or emergency conditions.

Typically, subtle dependencies are not detected in normal operation or by surveillance tests. The interaction between systems or subsystems can be transmitted by the process medium, via support system routes or indirectly via operating environment, e.g. temperature, humidity, pressure waves or vibration.

Subtle dependencies are either functional or physical, but they are difficult to foresee. Identified subtle dependencies can be treated by explicit modelling, or be left to be covered by CCF factors.

6.2 Scope

The definition of subtle dependencies in a particular PSA is dependent on the scope and level of detail of some of the other PSA tasks, mainly the identification and modelling of functional dependencies and physical dependencies. As an example, impact on system functions via room heating or ventilation may be seen as a subtle dependence, but may also be explicitly modelled as a functional dependency if the analysis of functional dependencies is thorough enough.

The identification of the subtle dependencies should not be restrictive, but all types of interactions should be broadly considered and carefully documented at the identification stage irrespective of whether the continued treatment and modelling of the case is moved to another analysis task. In the case moved to another task adequate cross-referencing should be made to allow tracking of the analysis steps.

Subtle dependency events have occurred at Nordic nuclear power plants. Experiences include events affecting more components than foreseen in the design analysis like in the TVO fire, or in Ringhals when air in the 334 piping created a dependency that only could be revealed by the experience from the event itself.

6.3 Assumptions and Limitations

The basic assumptions and limitations are:

- Less significant subtle dependencies are left without explicit modelling if the parametrically modelled CCF:s overrule their estimated contributions.
- System interactions, which are functional dependencies, should be handled in the category of functional dependencies.
- If the system interaction constitutes in itself an initiating event or a CCI, it should be included in an existing initiating event group or CCI group. If this is not possible, it should be considered an additional initiating event or CCI. Similarly, if the system interaction means an effective transfer to another initiating event category, the case may be considered within the initiating event analysis task.

[2] Subtle dependencies are also called ”system interactions” or ”subtle interactions”

6.4 Work Context and Interfaces

The analysis of subtle dependencies is primarily a part of the Systems Analysis and Accident Sequence Analysis.

6.5 Input

The main input to the analysis of subtle dependencies is:

- FMEA:s for the considered systems
- Preliminary fault trees for the considered systems
- System interfaces, functional dependencies
- Incident and failure reports at the plant may include information about subtle dependencies, i.e., operating experience with (yearly) risk follow-up is an important input.
- Evaluation of events at other plants or subtle interaction modelled in other PSA:s. A relevance screening is needed for these events.
- Special data for quantification
- The checklist included in [6-1, 6-2] (described below) can be used as a start, but needs to be adapted to the specific plant being analysed.

6.6 Methodology Description

6.6.1. Identification procedure

The system analysts performs the identification of the subtle dependencies at the stage when the information about system interfaces (functional dependencies) is collected, the FMEA is made and first outlines of system fault trees are also made. In cases, where the related system is analysed by another analyst,, exchange of information between the analysts is needed to assure adequate coverage of interactions.

The following recommendations are made:

- Mark up any candidate phenomena for subtle dependencies revealed during the course of FMEA and fault tree construction, , for later systematic analysis.
- Give special attention to equipment qualification to the accident conditions. Valve actuators may not be able to operate in steam conditions caused by a primary or feed water or steam pipe break. Safety valves may not be able to operate with steam and water mixture.
- Survey plant specific operating experiences for any incidents, which carry information about subtle dependencies. It is effective to do this in parallel with the review of system operating experiences during the course of the FMEA

In conclusion, the identification of subtle dependencies largely relies on a thorough knowledge of system design and plant operating history. Evaluation of events at other plants or subtle interaction modelled in other PSA:s may also be of great use. To give some examples, the subtle interactions listed in Table 6-1 were discussed in the PSA:s for Surry and Grand Gulf [6-1, 6-2]. The plants are of PWR and BWR type, respectively:

Table 6-1 Examples of subtle interactions, from [6-1, 6-2]

Diesel generator load sequence failure	Isolation of non-essential cooling water loads
Sneak circuits following power restoration	Discharge check valve failures for cross-tied pumps
Bus switching logic problems	System failure following station blackout
Pump room cooling	Dependent events based on operating experience
Voltage droop prior to LOSP	Main feedwater availability following plant trip
Terminal blocks inside containment	Refill of dry steam generators
Isolation of all feedwater flow	Main/auxiliary feedwater commonalities
Alternate cooling systems	Power operated relief valves (PORV:s) block valve closure
Steam binding of the auxiliary feedwater pumps	Overfill of steam generators
Air binding of cooling water systems	Normal operating configuration
Steam-line break isolation circuitry	Locked door dependencies
Passive component failures	

It should be noted, that the above list was compiled by experts based on past operating experiences and PSA analyses. This was a separate task, i.e., it was not part of the two PSA:s. It seems that the analysis of subtle dependencies in the two PSA:s was restricted to a short discussion of each of the items in the list, i.e., no further identification was attempted.

6.6.2. Modelling of subtle dependencies

Some subtle dependencies are suited for explicit modelling in the fault trees. As already noted above, specific cases may be moved to be treated as functional dependence, initiating event, or CCI.

Other, less significant subtle dependencies can be left without explicit modelling if the parametrically modelled CCF:s overrule their estimated contributions, i e the CCF model will account for them. Cases, where the bounding estimate assures a negligible contribution, are screened out. The documentation shall provide the basis for exclusion of a subtle dependency from explicit treatment..

6.7 Output and Documentation

The principal subtle interaction analysis outputs are the following:

- Cases moved to functional dependencies
- Cases to be considered in initiating event or CCI analysis
- Cases to be explicitly modelled in fault trees
- Cases covered by CCF modelling

The identification step is documented on the FMEA sheets and in checklists. Cases transferred to another task for treatment and possible screening are noted in the context of documenting the identification. For explicitly modelled cases, reference is given to the fault tree analysis.

Complex cases are elaborated in the system analysis report in order to explain the details of modelling and derivation of special input data.

6.8 References

6-1. 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.

6-2. Bertuccio, R.C. et.al.; *Analysis of Core Damage Frequency: Surry, Unit 1, Internal Events*; NUREG/CR-4550, Vol.3., Rev.1, April 1990.

7. Common Cause Initiators

7.1 Definition

A Common Cause Initiator (CCI) is an event cvent 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.

7.2 Scope

The completeness of a CCI analysis is highly dependent on a sufficient scope and level of detail of the analysis, as well as on a good system knowledge and knowledge of the plant operating history among the participants in the analysis.

CCIs are in this context restricted to failures occurring inside the plant systems, such as failures in the control and protections systems, electric power supply system, service water system or other support systems. Chapter 8 and 9 handles extrinsic initiators as area events and external events respectively.

7.3 Assumptions and Limitations

The basic assumptions and limitations for the CCI analysis are:

- CCIs are selected applying the same screening criteria as for other internal initiating events
- A CCI can be included in an existing initiating event group as one potential contributor to that initiating event
- Some CCIs are already traditionally defined as distinct initiating events, like loss of main feed water, loss of off-site power and Interfacing System LOCAs
- Similarly, pipe breaks with dynamic impacts (see Section 8) and Interfacing System LOCAs can be of CCI type: they are classified into LOCA categories.
- Area events and external events, e.g. fires, flooding and missiles are treated separately.

7.4 Work Context and Interfaces

The CCI analysis is usually a part of the Initiating Events Definition and Grouping task and the Systems Analysis task, except the modelling of the plant response to an identified and important CCI, which belongs to the Accident Sequence Analysis.

7.5 Input

The main inputs to the CCI analysis are:

- FMEA:s and fault trees for the considered systems
- Local and global protection signals generated at abnormal operation
- System interfaces, functional dependencies
- Incident and failure reports which carry information about CCIs
- Special data for quantification

7.6 Methodology Description

7.6.1. Identification and screening

The identification of the CCIs is part of the Initiating Events Definition and Grouping task. The purpose is to complement the initiating event identification with plant-specific findings aiming at as comprehensive initiating event list as possible.

The identification is done by studying the support and auxiliary systems in order to find out failures that meet the selection criteria for a CCI.

Emphasis is on the failure modes, which disrupt normal operation, e.g.,

- Normally operating pumps: failure to run
- Standby pumps: inadvertent start-up
- Safety/relief valves: inadvertent opening
- Normally closed bus breaker: inadvertent opening

It is recommended to group component failures with similar effects into a CCI defined on subsystem or system level, i.e. to follow the usual grouping procedure of initiating event definition.

The failure mechanism leading to a CCI can be also a combination of a triggering event of above type and a latent failure. Typically, the control and protections systems, electric power supply system, service water system or other support systems are sources for unexpected CCIs, where the plant's transient experience not can provide information. The following are the main areas for identification of CCI:s:

Loss of process control. An analysis of the process control includes both measurement and control of process parameters. A large number of parameters supervise and control the plant, power, level, pressure, flow, temperature, humidity, etc. Loss of some parameters may cause (or require) a plant trip and functionally degrade one or more safety systems, e.g.:

- Erroneous level measurement in the reactor vessel
- Spurious isolation signals

Loss of power supply. Some failures in the power supply which may cause (or require) a plant trip and functionally degrade one or more safety systems, e.g.:

- Loss of external power
- Loss of specific ac or dc busbars

Loss of auxiliary systems. Some failures within auxiliary systems may cause (or require) a plant trip and functionally degrade one or more safety systems, e.g.:

- Loss of instrument air
- Loss of cooling water

Component failures in safety systems. Component failures in safety systems may degrade safety functions, and may also be a requirement for a plant shut-down (Technical Specification rules).

Identification of CCIs should first of all include a systematic consideration of single and multiple failures as potential triggering events in essential support systems

Consideration of multiple failures as potential triggering events for CCI can be restricted to the groups of identical or similar components, i.e. CCCGs.

Plant specific operating experiences should be surveyed for any incidents, which carry information about CCIs. This can be done most effectively in parallel when reviewing the system operating experiences for initiating event analysis and for the purpose of conducting FMEA. The survey of incidents at other plants can also be very helpful, as well as insights from analyses performed for other plants.

7.6.2. CCI Modelling

CCI:s shall be handled as initiators and modelled by specific events. Sometimes a fault tree is needed to properly take into account support or auxiliary system dependencies and to comprehensively take into account different causal mechanisms and/or to estimate their frequency. As an example, a loss or partial loss of service water may be an initiating event itself, but a model is needed to take into account all possible failure combinations that can lead to this initiating event (electric power supply to the service water system components, etc.).

Deciding the frequency of identified CCI:s is usually rather difficult, due to the limited experience background. In some cases, a fault tree analysis provides the best frequency estimation.

A review has been performed aiming at identifying actual occurrences of CCIs on the basis of international operational experience collected in the IRS database [7-1].

7.7 Output and Documentation

The principal output is a list with the CCIs , that become initiating events, and where accident sequence analysis and event tree modelling will follow.

The identification step is documented in a checklist and as defined in the Initiating Events Definition and Grouping task. Screened out cases shall be noted in the context of documenting the identification. Complex cases should be discussed in the Initiating Event Analysis or in the corresponding system analysis report, in order to explain the details of the causal modelling, special initiator characteristics and derivation of the initiator frequency.

7.8 References

7-1. Nyman, R, Kulig, M, Tomic, B; *Identification of Common Cause Initiators in IRS Database*; SKI Report 98-09, February 1998.

8. Area Events

8.1 Definition

An area event is an event occurring within the plant but outside of the process, which affects safety systems through external impact (dynamic effects or environmental conditions). The main examples of area events are internal fires and internal flooding or steam release[3]. Other possible events are missiles from rotating machinery and pressure impact from pressure vessels.

8.2 Scope

The area event analysis shall:

- identify process rooms that are important for plant safety,
- determine the risk from area events for these rooms based on the room specific area event frequency and the area event impact for the room, and
- determine rooms contribution to plant hazard state frequency

8.3 Assumptions and Limitations

No specific assumption or limitation in the context of this guide are presented

8.4 Work Context and Interfaces

Area event analyses have traditionally been separate projects, but have important interfaces with the internal events PSA, mainly the identification and modelling of functional dependencies within the Systems Analysis task. An important addition is the detailed mapping and modelling of cable routes for power and signal cables that is needed for proper consideration of functional dependencies that may propagate area event effects.

8.5 Input

The main inputs to the CCI analysis are:

- Deterministic fire, flooding, steam release, missile analysis.
- If these are not available, a simple indexing approach is recommended to carry out a (simple) risk informed assessment and successively increase scope by collecting the necessary input on component location data, cable routing data etc.

8.6 Methodology Description

The PSA model covering internal event such as transients and LOCAs describes how the plant reacts to various events. The area event analysis is carried out based on the same model. This is done in a similar way as described for the CCI, i.e.,

- either an existing scenario may be reused where the area event frequency frequency is added to the existing IE frequency,

[3] Basically, the definition also includes LOCA evens, but these are analysed as a separate category of initiating events.

- or it may be needed to add extra area event scenarios scenarios, i.e., new initiators and new event tree models.

The PSA model for internal events provides a systematic model and source of information to determine the consequences of various area events if it contains information on component location and cable routings.

The area events can be divided into two groups:

1. Events causing a plant trip but without any other affect on the plant safety features.
2. Events causing a plant trip and with impact on plant safety features (type CCI)

For type 1 no specific analysis is carried out, the area event frequency is simply added to the corresponding plant trip scenario in the internal event PSA. For type 2 the analysis is more complicated, detailed information is needed on the components and rooms related to an area event to enable a systematic identification of initiating events for area analysis.

The main steps of the Area Events Analysis correspond to the scope description above, i.e.:

- identification of process rooms that are important for plant safety,
- determination of specific area event frequency
- determination of the area event impact for the room

The final list of area events with its corresponding frequency is then transferred to the accident sequence analysis, as initiating events, for final evaluation of its core hazard state contribution. In the Accident Sequence Analysis, the event is evaluated with an existing accident sequence model with the specific conditions created by the area event taken into account.

8.7 Output and Documentation

The documentation is usually done in a separate document.

8.8 References

8-1. Angner, A (editor); *Projekt Yttre Händelser – Slutrapport;* SKI Report 97:25

8-2. Knochenhauer, M; *Handbok - Komponentmodellering vid analys av yttre händelser;* SKI Report 97:50

8-3. Pörn, K; *Skattning av brandfrekvenser per anläggning och anläggningsdel*; SKI Report 96:65

8-4. Pörn, K; *Skattning av systemvisa utflödesfrekvenser i nordiska kärnkraftverk*; SKI Report 99:01

9. External Events

9.1 Definition

In the context of PSA, external events are defined as events originating from outside the plant, but with the potential to create a PSA initiating event at the plant. They may, however, originate from within the site (e.g. local transportation accidents), or from another unit on the same site (e.g. fire spreading between plant units).

External events can occur as single events or as combinations of two or more external events. Potential combined events are 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. Combined events which may contribute significantly to the plant risk need to be identified during the analysis.

External events are grouped into natural events and man-made events. Examples of man-made external events are airplane crash and gas explosion, while coastal flooding and various extreme weather conditions are examples of natural external events.

External events have occurred at Nordic nuclear power plants. Experiences include events affecting the cooling water intake (organic material and frazil ice), events affecting ventilation (blocking of ventilation intakes by white frost), events causing loss of external grid (strong wind, salt storms, lightning), and events causing plant isolation (heavy snowfall combined with strong wind).

9.2 Scope

The frequency of external events leading to PSA initiating events is usually low. Furthermore, many external events are included in initiating events statistics for transients which are already modelled in the PSA. External events may, however, cause initiating events and at the same time affect safety systems needed, i.e., the same kind of impact as from a CCI. The scope of the analysis is limited to the identification and analysis such external events, i.e., of external event which lead to or require plant shutdown, and which additionally degrade safety systems needed after the shutdown.

9.3 Assumptions and Limitations

The assumptions and limitations are scope specific. The following are some general issues:

- External events that are due to sabotage, war impact or terrorism are not included.
- Swedish PSA:s to date have handled seismic impact in separate projects.

Finally, it should be noted that, due to their specific characteristics, Area Events are treated as a separate dependence category, see chapter 8.

9.4 Work Context and Interfaces

The analysis of external events is usually performed as a self-standing task within a plant PSA. Most of the work is largely independent of other PSA tasks.

The main interfaces with other PSA activities are in the quantification phase, where the PSA model is used. Correct PSA modelling of external events requires the same adaptations of the PSA model that are needed in order to handle Area Events, i.e., inclusion of cable routing and of location information for safety critical structures, systems and components.

The external events PSA may put some additional requirements on the model, e.g., concerning system functions that are needed in order to cope with severe weather conditions (room heating etc.).

9.5 Input

The Guidance for External Events Analysis [9-1] includes detailed discussions of input needs. Some of the important inputs are:

- Strength and frequency data for relevant external events.
- The plant FSAR and documentation related to plant design analysis projects (BOKA, DART, etc.).
  Note: FSAR information for other plant units on the same site may also be of interest.
- Previous plant redesign projects may have aimed at evaluating or improving the protection against certain external event. In such cases, the project documentation often also includes analyses of the external event or experience data.
- Descriptions of plant reaction to major external events that have occurred during the operation of the plant.
- Plant personnel with long experience of the plant and a good general knowledge of the design and operating history.
- PSA for the analysed plant (or plant unit), including information on risk significant CCI events.
- Design information regarding structural strength.
- Information regarding system requirements and system capacities in various operational situations

9.6 Methodology Description

A detailed methodology for the analysis of external events has been developed as a separate NPSAG project, and is documented in the Guidance for External Events Analysis [9-1]. The over-all structure of an analysis is shown in Figure 9-1.

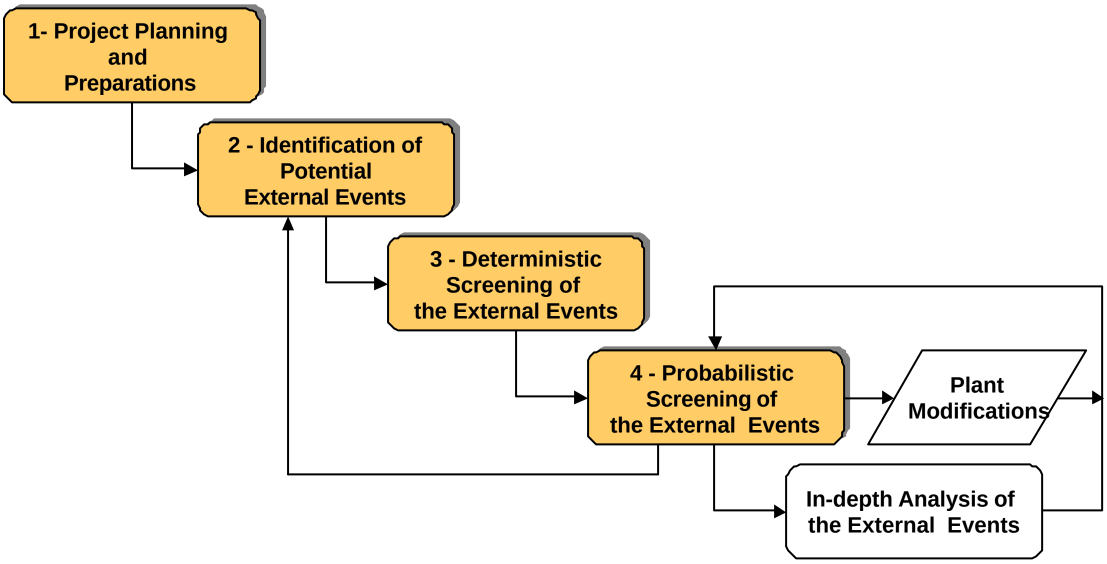

1- Project Planning and Preparations
2 - Identification of Potential External Events
3 - Deterministic Screening of the External Events
4 - Probabilistic Screening of the External Events
Plant Modifications
In-depth Analysis of the External Events

Figure 9-1 Overview of external events analysis [from 9-1]

9.7 Output and Documentation

The output from the analysis are lists of relevant external events and their frequencies, important fragility data as well as PSA model quantification results. Large parts of the results are quantitative.

The external events analysis is usually performed as a self-standing task. Therefore, it is usually documented in a separate document including the entire analysis.

9.8 References

9-1. Knochenhauer, M, Louko, P; Guidance for External Events Analysis; SKI Report 2002:27.

The following is a list of some of the important international references within the field.

9-2. 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

9-3. Bohn, M.P.; Lambright, J.A.; *External event analysis methods for NUREG-1150*; USNRC; NUREG/CP-0104

9-4. Bohn, M.P.; Lambright, J.A.; *Procedures for the external event core damage frequency analyses for NUREG-1150*; USNRC; NUREG/CR-4840; 1990

9-5. Gesellschaft für Reaktorsicherheit; *Deutsche Risikostudie Kernkraftwerke; Fachband 4; Einwirkungen von außen (einschließlich anlageninterner Brände)*; GRS; ISBN 3-88583-015-X; 1980

9-6. IAEA; *Extreme Man-Induced Events in Relation to Nuclear Power Plant Design – A Safety Guide*; IAEA Safety Series 50-SG-D5; 1982

9-7. IAEA; *Extreme Meteorological Events in Nuclear Power Siting, Excluding Tropical Cyclones – A Safety Guide*; IAEA Safety Series 50-SG-S11A; 1981

9-8. IAEA; *Site Survey for Nuclear Power Plants – A Safety Guide*; IAEA Safety Series 50-SG-S9; 1984

9-9. IAEA; *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants*; IAEA Safety Series 50-P-7

9-10. 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

9-11. 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

9-12. 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

9-13. USNRC; *Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities*; NUREG 1407, 1991

9-14. USNRC; *Identification of Potential Hazards in Site Vicinity*; Standard Review Plan 2.2.1-2.2.2, rev 2; 1981

10. Dynamic Effects

10.1 Definition

Dynamic effects of a pipe break can cause failures of safety related equipment, which are needed in the mitigation of the initiating event or which can make the initiating event worse. The focus is here on those pipe breaks, which constitute directly an initiating event, e.g. LOCA or loss of main feed water. Internal floods are otherwise considered as part of internal hazards (area events). However, the dynamic effects discussed here can also be relevant when considering particular influences of the floods.

10.2 Scope

The analysis scope for the dynamic effects should include the following categories of phenomena:

Category 1 Impacts of pipe whip, flying objects and water/steam jets in case of pipe breaks, vessel ruptures, etc.; the influences can be directed to adjacent piping components or building structures

Category 2 Flooding effects (also spreading scenarios) and consequences of increased humidity and temperature

Category 3 Distribution of isolation wool material and blocking of the recirculation flow

The motivation in covering the flooding, humidity and temperature effects is that they can substantially reduce the mitigation possibilities. It should also be noticed, that in some special cases the effects of the above categories can combine and result in a severe accident scenario.

10.3 Assumptions and Limitations

One basic assumptions and limitations is that the analysis of flooding effects are limited to cases in which the increased humidity and temperature play an important role by reducing the mitigation possibilities

10.4 Work Context and Interfaces

The analysis of dynamic effects may be performed as part of the LOCA analysis, or as a self-standing task as part of the dependency analysis task.

10.5 Input

The main needed input to the analysis of dynamic effects is:

- Containment geometrics
- Detailed information on location of piping, break locations, location of potentially affected components, isometric drawings
- Environmental specification information of vulnerable objects
- Special data for quantification

10.6 Methodology Description

10.6.1. Analysis procedure

The analysis of Category 1 effects (Impacts of pipe whip, etc.) will include the following steps:

1. Walk-rounds to identify vulnerable piping sections and equipment
2. Analysis and modelling of consequences (scenarios)
   - Stress and strength calculations for jet impingements and water loads when necessary: quantification of forces against the vulnerable objects, the durability of which should be provided by the main designer/supplier
   - Analyses of water hammers e.g. in primary to secondary leakages and in outside containment leakages
3. Frequency estimates for the initiating event and most significant consequences (scenarios)

The analysis of Category 2 effects (operating environmental) will include the following steps:

1. Identification of the dangerous piping sections and vulnerable equipment
2. Thermal hydraulic analyses to estimate the potential leak rates of water and steam
3. Analyses to evaluate the potential spreading routes of water and steam and the temperature increase and its timing in important rooms that include safety related equipment like plant protection instrumentation

The analysis of Category 3 effects (blocking of recirculation flow) will include the following steps:

1. Experimental tests of the behaviour of containment sump strainers with the insulation material
2. Experimental tests of the ECC pumps with the insulation material

In this context it should be noted, that NEA/CSNI has issued an extensive document summarizing the knowledge within this field [10-1].

10.7 Output and Documentation

The principal outputs are the following:

- Extensions to LOCA and transient categories
- Refinements to accident sequence models of LOCAs and transients
- Evaluation of containment sump operability

This task is documented as part of Initiating Event Definition and Grouping, Accident Sequence Analysis and System analysis (sump strainers).

10.8 References

10-1. NEA/CSNI; *Knowledge Base for Emergency Core Cooling System Recirculation Reliability*; NEA/CSNI/R (95)11; 1996

11. Common Cause Failures

11.1 Definition

According to ICDE definition CCF is a dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause. The dependence can arise from design error, inadequate maintenance or environmental abnormality or a combination of such shared causes. Significant CCF:s are made up coexisting failure condition of redundant components, e.g. during the period between consecutive test events or during the required mission time.

As discussed earlier the dependent failure leading to initiating event is handled as CCI. CCF:s do not constitute initiators but will affect the course of the accident sequences following a random initiator. CCF:s can be either latent prior to the demand or can occur during the mission time following the demand.

The term “CCF event” will be used especially when meaning an occurred CCF such as described in ICDE database.

11.2 Scope

The risk-significant CCF:s are mostly related to latent failure mechanisms, which can be detected only in the surveillance tests or actual demand. It should be noticed that failure mechanisms of standby components, which affect the components during the mission time, e.g. failure of the diesel generators to run during the loss of off-site power condition, are also latent failures. Simultaneous failure of the normally operating components, or on-line monitored components, use to be unlikely – but if considered significant such cases can be treated with the same general approach as ordinary latent dependent failures.

A group of components vulnerable to CCF:s is called as Common Cause Component Group (CCCG). Being a random process the dependence mechanism can affect all components in CCCG (this event is called as complete CCF) or a subset of the components. The CCF basic events of various degrees will be modelled in the fault trees by the side of the single component failures.

11.3 Assumptions and Limitations

The basic assumptions and limitations are:

- The component group constituting a CCCG is considered as internally homogeneous (symmetric)
- Component types used extensively across many systems (circuit breakers, relays, solenoid valves) constitute in principle very large CCCGs, which are usually not considered with respect to CCF risk. Sensitivity analyses are needed to evaluate the potential importance of CCF risk in such global groups
- Dependent component failures, which are directly attributed to systematic maintenance or testing errors, should normally be treated as part of the human error dependencies, and be explicitly modelled, see Chapter 5. However, if the contribution of the systematic errors is small and/or the errors are part of a more

complex dependence mechanism, they can be covered by the CCF:s of the concerned components.

- Important functional and physical dependence mechanisms should be modelled explicitly as part of the system modelling, or as a systematic error, Area Event or External Event depending of the type. In such a case, other possible CCF:s usually still have to be covered by using a parametric CCF model.
- If unit-to-unit cross-ties are credited for some systems (e.g. diesel generators) the component dependencies across unit boundaries should be taken into account
- If available, processed ICDE data should be used for the quantification.
  - Sparse plant-specific CCF data can mean large uncertainty
  - Use of generic CCF data can mean large uncertainty
- Time-dependence is often neglected or treated in a simplified way

11.4 Work Context and Interfaces

This analysis task should be sequenced in parallel to the system analysis task for the identification of CCCGs and incorporation them in the fault tree models.

As mentioned in the preceding sections, there is an important borderline between the dependent failures covered by implicit CCF modelling and those covered by explicit modelling (systematic maintenance and testing errors, Area Events, External Event, subtle interactions and CCIs). It is important that integral coverage is looked after in order to avoid both gaps and double-counting.

Preliminary (screening) calculations can be done by using generic CCF data, i.e. specific data are required as input to the final calculations.

11.5 Input

The principal input requirement concerns the identification of CCCGs, which should be based on the understanding of the system configurations created in the system analysis task. Definition of CCCGs may be a join subtask of the CCF analysis and system analysis. The quantification requires CCF parameter data as input from the data analysis task. Acquisition of CCF data can also be a part of the CCF analysis task, especially when it is not based on plant events but on generic sources.

11.6 Methodology description

The treatment of CCF:s divides into the following steps:

1. Definition of CCCGs
2. Choice of CCF model and corresponding inclusion of Common Cause Basic Events (CCBEs) into system fault trees
3. Acquisition of data for CCF model parameters and derivation of the probabilities for CCBEs

The general procedure for each step is discussed in the following subsections.

11.6.1. Definition of CCCGs

The first step is to create a preliminary list of components that are candidates for CCF modelling, i.e. they have common characteristics that make them exposed to shared causes. In this step, conservatism is necessary. The important thing is not to neglect any potential group of components without an obvious reason. In a later stage, the preliminary list can be shortened based on additional qualitative or quantitative information. The analysis should be concentrated on identifying the components in a system which share one or more of the following:

- Same design / hardware
- Same function
- Same installation
- Same maintenance personne l or operating personnel
- Same test interval
- Same procedures
- Same system or component interface
- Same location
- Same operating environment

A group of components identified in this process is referred to as a Common Cause Component Group (CCCG). A screening qualitative analysis should be made in order to assess the vulnerability of the system and it's components to CCF. In practice, the following principles guide the selection of CCCG:s:

1. Identical, functionally non-diversified, and active components used to provide a system function shall be assigned to the same CCCG.
2. Diversified components can normally be considered to be independent. However, if the diversified components have identical parts, there may be a need to break down the components into smaller parts, and model identical parts as CCCG:s.
3. Passive system parts may need to be included in the analysis, e.g., clogging of multiple pump strainers.

Consideration of special more complicated cases, e.g. CCFs among similar components in different systems, is discussed in [11-1].

More than one CCCG may be needed for a set of components to consider different functional failure modes. For example, in the case of safety/relief valves the failure to open and failure to reclose after opening are treated by two CCCGs, one for either failure mode. In some cases the number of demanded components such as safety/relief valves can depend on the type of initiating event. These cases can be handled by defining a CCCG of specific size fore each different type of initiating event, or by using a parametric CCF model, which can handle directly subgroups of the whole component group in a consistent way.

11.6.2. CCF Models

The mostly used CCF models in the Nordic PSA studies are listed in the following table (in alphabetical order) with some characterization. The models are described in more detail, including the transformations of parameters between the models in [11-1]. The earlier SUPER-ASAR project provides also useful background information about the CCF models [11-9].

CCF Model	Remarks
Alpha Factor Method	Mostly used, generally applicable model, recommended by the SUPER-ASAR project
Beta Factor Method	Limited to groups of two components except regarding the use as a crude cut-off model in larger groups
Common Load Model	Especially suitable to highly redundant systems as it has a fixed number of parameters and is subgroup invariant
Direct Estimation Method (called also as Basic Parameter Model)	Close to Alpha Factor Method: the difference is in the normalization of Alpha Factors
Multiple Greek Letter Method	Similar to Alpha Factor Method but does not lend equally well to developed estimation techniques and uncertainty analysis

When using Risk Spectrum [11-10] it is normally only needed to register the component as a member of a CCCG, and the program then automatically generates the corresponding CCBEs and calculates the CCBE probabilities based on the choice of CCF model. In case of special configurations and highly redundant systems the CCBEs have to be modelled manually into the system fault trees.

11.6.3. CCF Data

The CCF data sources can generally be grouped into the following classes in the order of preference:

1. Plant specific CCF data, which are derived from event statistics for the component type. The eventual data pooling (combining event statistics) covers components and operating conditions, which can be regarded homogeneous in a reasonable degree
2. Generic data, which are derived as industry average for the main component types and can contain variability in component design and operating conditions
3. Generic data, which are derived as overall average for different component types

The ultimate aim of the ICDE is to make possible to obtain plant specific CCF data for all important component types in the way as started with the diesel generators in the pilot application [11-3].

Generic CCF data according to the class 2 above, has thus far been common for the important main components in the PSA studies. Appendix 3 presents a compilation of Alpha Factors and corresponding Multiple Greek Letter parameters being used in the Nordic PSA studies.

Generic CCF data according to class 3 has been used in the case of lack of class 2 data for the component type. The generic data including available sources are discussed more comprehensively in [11-2].

11.7 Output and Documentation

This CCF analysis task is usually documented as a separate task, as part of Dependency Analysis, except CCF data that is documented in the Data Analysis.

11.8 References

11-1. Mankamo, T; *CCF Model Survey and Review*; NAFCS-PR04

11-2. Mankamo, T; *CCF Data Survey and Review*; NAFCS-PR02

11-3. Mankamo, T; *Impact Vector Application to Diesel Generators,* NAFCS-PR10

11-4. USNRC; *Guidelines on Modeling CCFs in PSA*. Prepared by A.Mosleh, D.M.Rasmuson and F.M.Marshall for USNRC; USNRC NUREG/CR-5485, November 1998.

11-5. USNRC; *CCF Parameter Estimations*. Prepared for USNRC by F.M.Marshall/INEL, D.M.Rasmuson/NRC and A.Mosleh/Univ.MD; USNRC NUREG/CR-5497, October 1998

11-6. USNRC; *Common Cause Failure Database and Analysis System*; USNRC Report NUREG/CR-6268, Vol.1 Overview, Vol 2 Event Definition and Classification, Vol 3 Data Collection and Event CodingVol 4 CCF Software Reference Manual; USNRC NUREG/CR-6268, Vol.1-4., June 1998.

11-7. IAEA; *Procedures for Conducting CCF Analysis in PSA*; IAEA-TECDOC-648, 1992

11-8. IAEA; *Procedure for CCF Data Analysis in PSA*. IAEA-J4-97-CT-1002, Working Draft, March 1998

11-9. Johansson, G. (editor); *Projekt SUPER-ASAR, Slutrapport fas II*; SKI Technical Report 90:3

11-10. Relcon AB; *Risk Spectrum – Theory Manual*; Relcon AB, 1998

Appendix 1 – Terms, Definitions and Acronyms

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)

Acronym	Description
ECCS	Emergency Core Cooling System
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

Acronym	Description
MAAP	Modular Accident Analysis Program
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

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”
Berry 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.
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.

Term	Definition
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	Component (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).
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.

Term	Definition
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 cutset (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.
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.

Term	Definition
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.
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.
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 (monitored)	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.

Term	Definition
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 2 – List of Project Reports in the NAFCS Project

PR01	Project Programme
PR02	Data Survey and Review
PR03	Impact Vector Method
PR04	Model Survey and Review
PR05	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	Control Rod and Drive Assemblies
PR10	Impact Vector Application to Diesel Generators
PR11	Data Survey and Review of the ICDE Database for Swedish Emergency Diesel Generators
PR12	Dependency Protection Guideline
PR13	Dependency Analysis Guideline
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

Appendix 3: CCF Data

Introduction

This appendix is aimed to summarize the quantitative results of the NAFCS, the estimated CCF parameters in the form of Alpha Factors and Multiple Greek Letter Parameters. In this stage the currently used CCF data are also shown for comparison purpose. For the Swedish NPPs the CCF data compilation of SUPER-ASAR is used as reference source [SUPER-ASAR]. For the Olkiluoto plant the CCF data are from the current TVO PSA version [TVO-PSA]. For the foreign data the recent extensive compilation of the US plants [NUREG/CR-5497] is used as reference source.

In addition to tabular presentation of CCF parameters the data are also shown graphically in the form of multiple failure probabilities. For this purpose the Psg entity is used. It presents the probability of specific m components failing in the group on n components without taking into account the status of the other 'n-m' components. The benefit of using Psg entitity 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 types of multiple failure probabilities. See the definitions and discussion of this issue in [NAFCS-PR04].

Diesel generators

The presented results for the diesel generators (DGs) are point estimates for the combined data of the failure modes ‘Failure to Start’ and ‘Failure to Run’, i.e. FS and FR. Table A3.1-1 shows the best estimate results obtained from the average of the Impact Vector assessment by two redundant analysts. Figure A3.1-1 shows also the high/low bounds that are generated. For details, see [NAFCS-PR10].

The CCF parameters recommended in SUPER-ASAR are based on existing data and engineering judgement, taking into consideration major design differences, e.g., degree of separation [RPC 88-160].

US data are from [NUREG/CR-5497], and failure modes FS and FR are combined.

Table A3.1-1 CCF parameters for the diesel generators, combining failure modes ‘Failure to Start’ and ‘Failure to Run’.

Source	**Plant**	**CCF parameters for the group size of 2**						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic	0.042	-	-	0.979	0.021	-	-
S-ASAR	O1	0.06	-	-	0.970	0.030	-	-
S-ASAR	B1	0.05	-	-	0.975	0.025	-	-
NUREG	US	0.061	-	-	0.969	0.0312	-	-

Source	**Plant**	**CCF parameters for the group size of 4**						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic	0.034	0.21	0.45	0.984	0.0139	1.32-3	8.14-4
S-ASAR	R1	0.06	0.64	0.94	0.977	0.013	0.001	0.009
S-ASAR	O3/F3	0.03	0.3	0.6	0.986	0.011	0.001	0.002
TVO	OL	0.080	0.109	0.209	0.960	0.0373	2.40-3	4.76-4
NUREG	US	0.100	0.747	0.571	0.964	0.0135	0.0114	0.0114

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, best estimate	5.94	8.81	2.81	0.27	0.16	18
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, best estimate	3640.44	198.81	2.81	0.27	0.16	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, best estimate		0.9839	1.39E-2	1.32E-3	8.14E-4	
Alpha Factors, low bound		0.9853	1.29E-2	1.65E-3	7.51E-5	
	0	1	2	3	4	
Psg(m|n), high bound	1	1.34E-2	2.83E-4	1.11E-4	1.04E-4	
Psg(m|n), best estimate	1	1.34E-2	1.99E-4	6.01E-5	4.27E-5	
Psg(m|n), low bound	1	1.33E-2	1.60E-4	2.55E-5	3.93E-6	

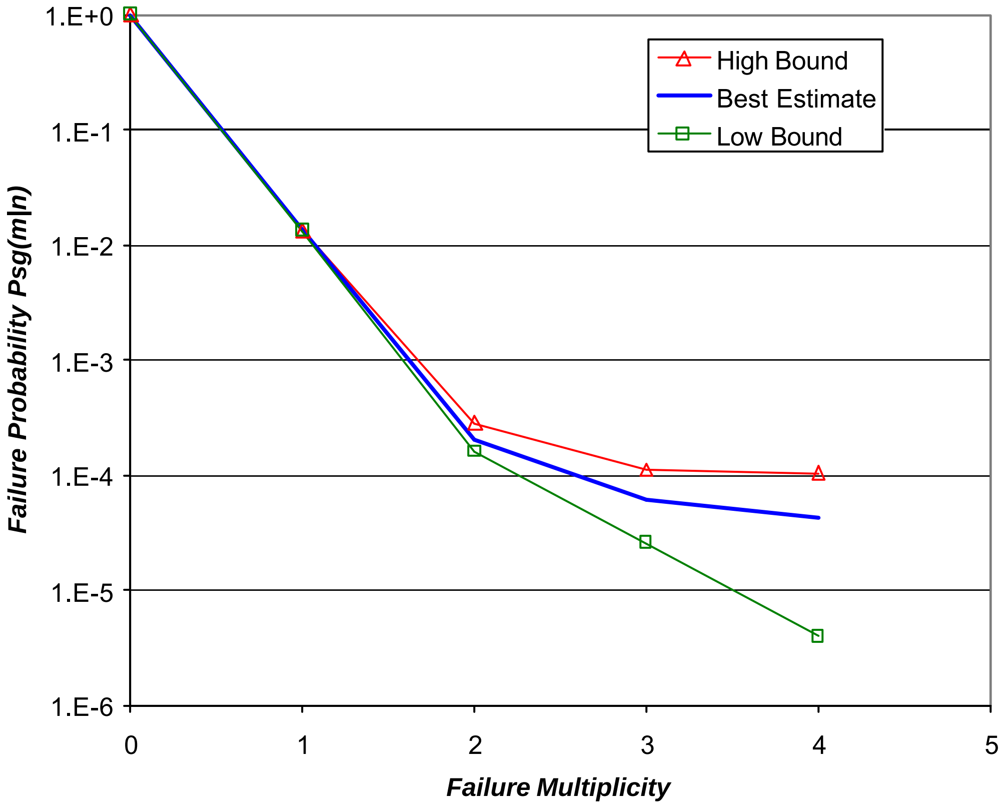


Figure A3.1-1 NAFCS results for the Nordic CCCG Size = 4, presented in the form of Alpha Factors and SGFPs, including the generated high/ low bounds. The diagram compares derived Psg entities [NAFCS-PR10].

Pumps

The current CCF event data in the ICDE database is rather sparse for the centrifugal pumps of the Nordic NPPs, taking into account the notion that a large part of the reported events represents functional and/or operator action dependencies to be explicitly modelled, see [NAFCS-PR18]. Besides, the CCF mechanisms and detection efficiency are much different for the pumps being normally in standby in comparison to continuously or intermittently operated pumps. These operational categories have to be treated separately. The number of reported CCF events is also dispersed over group sizes 2, 3 and 4. Meaningful point estimations can thus not be done in the same way as for the diesel generators. It should also be noticed that the pumps used in the different systems can have very varying design owing to the differences in the capacity and pressure head.

The utilization of the foreign ICDE events, for example in the form of a-priori data, proved more difficult than expected, and is pending for continued effort.

Consequently, the presentation of the CCF parameters for the pumps is restricted in the current stage to the following items, see Table A.3.2-1.

- SUPER-ASAR data
- TVO PSA data for two principal pump types:
    - Centrifugal pumps of the Core Spray System (323), i.e. low pressure safety injection system
    - Reciprocating pumps of the Auxiliary Feedwater System (327), i.e. high pressure safety injection system
- US data also for two selected pump types in the following systems, with best event data support:
    - High Pressure Safety Injection System of PWRs
    - Emergency Service Water System, covering both BWRs and PWRs

There are mismatches between Alpha Factors and corresponding Multiple Greek Letter Parameters for several data entries, apparently due to varying way to take into account the influence of test staggering in different sources. This aspect should be clarified in the continuation, and handled in a consistent way at different analysis stages: Impact Vector assessment, CCF parameter estimation and CCF modelling/quantification.

Table A3.2-1 CCF parameters for the pumps, applicable to failure mode ‘Failure to Start’.

Source	**Plant:System**	**CCF parameters for the group size of 2**						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic							
S-ASAR	B1/B2:321	0.03	-	-	0.985	0.015	-	-
S-ASAR	B1/B2:323 O1:321,323,327 R1:321,323	0.05	-	-	0.975	0.025	-	-
S-ASAR	B1/B2:327 O1:715	0.10	-	-	0.947	0.053	-	-
NUREG	US: PWR/HPSI	0.056	-	-	0.944	0.056		
NUREG	US: ESWS	0.036	-	-	0.964	0.036	-	-

Source	**Plant:System**	**CCF parameters for the group size of 3**						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic							
S-ASAR	O1:712	0.05	0.60	-	0.980	0.010	0.010	-
S-ASAR	B1/B2:322	0.10	0.50	-	0.956	0.027	0.027	-
S-ASAR	B1/B2:712,721 O1:322,721 R1:322,711, 712,715	0.10	0.60	-	0.958	0.021	0.021	-
NUREG	US: PWR/HPSI	0.055	0.53	-	0.945	0.026	0.030	
NUREG	US: ESWS	0.054	0.19	-	0.946	0.044	0.010	-

Source	**Plant: System**	**CCF parameters for the group size of 4**						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic							
S-ASAR	F3/O3:327	0.05	0.30	0.60	0.978	0.018	0.002	0.002
S-ASAR	F3/O3:Other	0.03	0.30	0.60	0.987	0.011	0.001	0.001
TVO-PSA	T1/T2: 323	0.105	0.27	0.57	0.951	0.041	0.0042	0.0042
TVO-PSA	T1/T2: 327	0.102	0.27	0.58	0.952	0.039	0.0041	0.0042
NUREG	US: PWR/HPSI	0.053	0.54	0.77	0.947	0.025	0.0067	0.022
NUREG	US: ESWS	0.077	0.20	0.44	0.923	0.062	0.0085	0.0067

MOVs

The current CCF event data in the ICDE database is very sparse for the MOVs of the Nordic NPPs, containing only six reported events, which are furthermore dispersed over different group sizes, see [NAFCS-PR19]. The group sizes cover a large range, because so called Exposed Populations are considered as extension to standard CCF group. Simple point estimations can thus not be done in the same way as for the diesel generators. The utilization of the foreign ICDE events, for example in the form of a-priori data, is pending for continued effort.

Consequently, the presentation of the CCF parameters for the MOVs is restricted in the current stage to the following items, see Table A.3.3-1 (US data are available also for CCCG size 3, but that is left out from the current compilation for simplicity).

- SUPER-ASAR data
- TVO PSA data for the MOVs in the injection lines of the Auxiliary Feedwater System (327), i.e. high pressure safety injection system
- US data also for a selected valve type in BWRs, with reasonable event data support, concerning high pressure injection systems of (HPCI/RCIC).

Table A3.3-1 CCF parameters for the MOVs, applicable to failure mode 'Failure to Open' and 'Failure to Close'.

Source	Plant:System	CCF parameters for the group size of 2						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic							
S-ASAR	B1/B2	0.097	-	-	0.949	0.051	-	-
NUREG	US: BWR/HPCI	0.046	-	-	0.954	0.046	-	-

Source	Plant: System	CCF parameters for the group size of 4						
		β	γ	δ	α_1	α_2	α_3	α_4
ICDE	Nordic							
S-ASAR	F3/O3	0.084	0.37	0.57	0.962	0.028	0.005	0.005
S-ASAR	O1/R1	0.135	0.63	0.85	0.948	0.028	0.005	0.019
TVO-PSA	T1/T2: 327	0.102	0.27	0.58	0.952	0.039	0.0041	0.0042
NUREG	US: BWR/HPCI	0.026	0.92	0.99	0.974	0.0021	0.0002	0.0233

CLM parameters

For the application of Common Load Model (CLM) the best estimate results from ICDE/NAFCS are also presented in the form of CLM parameters. The estimation of CLM parameters is based on the Maximum Likelihood principle [ECLM_Pub]. The correlation coefficient of the base load part (c_co) gets exceptionally small for the DGs, and can be biased by the incompleteness of reporting as for the current ICDE database.

Pending for specific assessment, generic data are used as placeholder for the pumps and MOVs. The presented generic CLM parameters correspond to so called Generic Dependence Class II, being close to dependence profile of the pumps and MOVs as in the TVO-PSA data. The concept of Generic Dependence Class is discussed in more detail in [NAFCS-PR02].

The nearest applications of CLM are Exposed Populations of MOVs exceeding four components as this model provides a seamless treatment of larger groups and pooling of statistics over different group sizes. For the DGs and pumps the CLM parameter estimates are interesting as for generic insights.

Table A3.4-1 CLM parameter estimates based on the Impact Vector assessments for the Nordic ICDE data within NAFCS.

	CLM parameter			
Component	p_tot	p_xtr	c_co	c_cx
Diesel generator	1.4E-2	1.1E-4	0.02	0.70
Pump – generic(1	1E-3	3E-5	0.4	0.8
MOV – generic(1	1E-3	3E-5	0.4	0.8

Note 1) Generic CLM parameters are presented as placeholder data for the pumps and MOVs, pending for specific assessment.

References

SUPER-ASAR
Description of Super-ASAR CCF data for NAFCS-R13. Prepared by Michael Knochenhauer, MK03-007r0, 2003-02-07.

TVO-PSA Probabilistic Safety Assessment of the Olkiluoto 1 and 2, Rev.1. Teollisuuden Voima Oy, 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

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-PR18
Impact Vector Construction to the Pumps. Topical Report NAFCS-PR18, Draft 1+, 25 April 2003.

NAFCS-PR19
Impact Vector Construction to the MOVs. Topical Report NAFCS-PR19, Draft 1+, 19 May 2003.

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.

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

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