Strål säkerhets myndigheten
Swedish Radiation Safety Authority

Author: Per Hellström

Research

2015:04

DiD-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA

Report number: 2015:04 ISSN: 2000-0456
Available at www.stralsakerhetsmyndigheten.se

SSM perspektiv

Bakgrund

Grunden för kärnkraftsäkerhet bygger enligt IAEA på ett barriärtänkande och ett djupförsvar med funktioner och system uppdelat i fem nivåer (IAEA INSAG-12).

Ramverket för hur säkerhetsanalyser ska bedrivas vid svenska kärnkraftverk regleras av SSM och inbegriper analys av en anläggnings djupförsvar. SSM ställer krav på att en anläggnings djupförsvar bland annat ska verifieras med hjälp av deterministiska och probabilistiska analyser (SSMFS 2008:1).

Hittills genomförda PSA studier redovisar dock inte idag en tydlig värdering av alla de fem definierade djupförsvarsnivåerna, speciellt djupförsvarsnivå 2 som syftar till att upprätthålla fortsatt drift av anläggningen i samband med driftsstörningar.

Det har också inträffat händelser där djupförsvarsnivå 2 har misslyckats och där det samtidigt fortplantats fel som påverkat övriga djupförsvarsnivåers förmåga att hantera händelseförloppet, t.ex. Forsmarkshändelsen med en störning på yttre nät som ledde till följdfel hos den säkerhetsklassade elförsörjningen. Denna händelse ledde till en internationell konferens benämnd DiDELSyS (Defence in Depth in Electrical Systems).

SSM:s och rapportens syfte

Syftet med projektet är att utreda i vilken utsträckning PSA på ett tydligare sätt kan beräkna och redovisa bedömningar av de fem djupförsvarsnivåerna. Arbetet innebär en inventering av möjligheterna att göra detta och utveckling av metoder för både beräkningar och resultatredovisning som stöder en riskvärdering av strukturer, system, komponenter, ingrepp och rutiner som ingår i en kärnkraftanläggnings olika djupförsvarsnivåer.

Resultat

Projektet redovisar en tolkning av IAEA:s definitioner av djupförsvaret som ger ett ramverk för koppling mot PSA. För varje djupförsvarsnivå och kombinationer av nivåer, presenteras och diskuteras metoder att värdera denna ur ett PSA-perspektiv. Ett viktigt resultat är en genomgång av de grundläggande definitionerna och grunderna för djupförsvaret så som det definieras enligt IAEA, som leder till något modifierade och vidareutvecklade beskrivningar av nivåerna som möjliggör en tydligare koppling till en utvecklad PSA analys.

Effekt på SSM:s verksamhet

Föreliggande rapport klargör gränserna mellan djupförsvaret så som det definieras enligt IAEA och i SSM:s författningssamlingar, och koppling mot mätetal som utgör indata eller resultat i en PSA studie. Denna grund kan användas till att förtydliga rapportering av händelser, anpassning av PSA-modeller för att få en mer komplett värdering av samtliga nivåer i djupförsvaret, och resultatredovisning som stöder insikter i anläggningens styrkor

och svagheter i olika händelseförlopp. På det sättet fås ett tydligare stöd i kraftbolagens och SSM:s värdering av en anläggnings befintliga djupförsvar, värdering av inträffade händelsers betydelse för djupförsvaret samt analys och värdering av anläggningsändringars påverkan på djupförsvaret.

Fortsatt verksamhet inom området

Genomgången av befintliga definitioner och de förslag som finns till modifieringar förväntas vara av värde och beaktas i framtida uppdateringar av regelverket. Det är speciellt viktigt att det genomförs aktiviteter som leder till en ökad samsyn på definitioner och förklaringsmodeller och att detta beaktas vid utvecklingen av mallar för rapportering av inträffade händelser/fel samt redovisningen och tolkningar av PSA-resultat.

Projektinformation

SSM:s handläggare: Ralph Nyman
Projektnummer: 1082-01
Diarienummer: SSM 2008/1494

Referenser till andra relaterade forskningsarbeten och rapporter:

SSM Rapport 2008:33 Risk-informed assessment of defence in depth, LOCA example.

SSM Rapport 2010:35 Probabilistic Safety Goals for Nuclear Power Plants – Phase 2-4, Final Report.

SSM Rapport 2010:36 Guidance for the Definition and Application of Probabilistic Safety Criteria.

SSM perspective

Background

The base for reactor safety, according to IAEA, builds on a set of barriers and five levels of Defence-in-Depth (IAEA INSAG-12).

The framework of how to conduct safety analyses at Swedish nuclear power plants are established by SSM, which covers the concept of Defence-in-Depth. SSM requires that the Defence-in-Depth shall be verified by deterministic and probabilistic analyses (SSMFS 2008:1).

Current PSA studies lack a clear evaluationof all Defence-in-Depth levels, in particular level 2 aiming at maintaining plant operation in case of disturbances.

There are cases where level 2 has failed and the original disturbance has affected the ability of the remaining defence levels to deal with the scenario, e.g. the Forsmark event with an external grid transient leading to cascade failure in the plants safety classified electrical power supply system. This event led to the international conference named DiDELSyS (Defence in Depth in Electrical Systems).

The aim of SSM and of the report

The objective of the project is to investigate to what extent measures and parameters of PSA can be used in order to give estimates of the five levels of Defence in Depth. This imply to make an inventory and explore the possibilities to perform calculations and present results in such a way that structures, systems, components, operator actions and procedures can be linked to DiD levels and be ranked and graded in relation to their risk contribution.

Results

The project declares an interpretation of the definitions of Defence in Depth given by IAEA which outline a framework to meet PSA. For each level of defence and combinations of levels, methods to give estimates from a PSA perspective are presented and discussed. One important result is the discussion of the basic definitions and the basis for defence-in-depth, as defined by IAEA, leading to somewhat modified and further developed definitions that support the link to a developed PSA.

Effect on SSM activities

This report clarifies the links between the defence in depth, as defined by IAEA and SSM code of statutes, and link to possible PSA measurements (input data or results from quantifications). This basis can be used in a development of event reporting, the adaptation of PSA models in support of more complete DiD levels evaluation, and development of result presentation supporting insights into plant DiD strengths and weaknesses. Such development contributes to SSMs and the utilities evaluation of the existing DiD, the importance of events in relation to the DiD and the DiD impact from plant changes.

Possible continued activities within the area

The interpretation relevant to plant safety given by the definitions of Defence in Depth on the one hand and the PSA framework on the other hand need further consideration when to perform updates of the regulations in the future. Particularly important is the establishment of activities to promote a joint perspective on definitions and models of explanation. These should constitute the foundation for future templates, report system of events and failures as well as the presentation and interpretation of PSA results.

Project information

Project responsible at SSM: Ralph Nyman
Project number: 1082-01
Diary number: SSM 2008/1494

References to other similar research projects and reports:

SSM Report 2008:33 Risk-informed assessment of defence in depth, LOCA example

SSM Report 2010:35 Probabilistic Safety Goals for Nuclear Power Plants – Phase 2-4, Final Report

SSM Report 2010:36 Guidance for the Definition and Application of Probabilistic Safety Criteria

Strål
säkerhets
myndigheten
Swedish Radiation Safety Authority

Author: Per Hellström
Strålsäkerhetsmyndigheten

2015:04

DiD-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA

Date: Januari 2015
Report number: 2015:04 **ISSN:** 2000-0456
Available at www.stralsakerhetsmyndigheten.se

This report concerns a study which has been conducted for the Swedish Radiation Safety Authority, SSM. The conclusions and viewpoints presented in the report are those of the author/authors and do not necessarily coincide with those of the SSM.

Table of Contents

List of Tables

List of Figures

Organisations

AEC	Atomic Energy Commission (responsible for US nuclear regulation until 1974 when the Nuclear Regulatory Commission was established)
ANS	American Nuclear Society
ANSI	American National Standards Institute
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Advisory Group of the IAEA
NRC	Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
SKI	Statens Kärnkraftinspektion (Swedish Nuclear Power Inspectorate, since mid 2008 SSM)
SSM	Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority)

Abbreviations

BoP	Balance of Plant
BDBA	Beyond Design Basis Accident
BWR	Boiling Water Reactor
CCDP	Conditional Core Damage Probability
CD	Core Damage
CDF	Core Damage Frequency
CFR	Code of Federal Regulation (US)
CRCP	Conditional Release Category Probability
CRP	Conditional Release Probability
DiD	Defence-in-Depth
DBA	Design Basis Accident
ECCS	Emergency Core Cooling
ET	Event Tree
FC	Fractional Contribution
FT	Fault Tree
HRA	Human Reliability Analysis
HTG	Högst Tillåtna Gränsvärde (Highest Permissible Limit)
IE	Initiating Event
INES	International Nuclear Event Scale
LBB	Leak Before Break
LER	Licensee Event Report
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LRF	Large Release Frequency
MCS	Minimal Cut Set

MFW	Main Feed Water
MSPI	Mitigating System Performance Index
NPP	Nuclear Power Plant
OK	Success state in event tree sequences
PC	Plant Condition
PDS	Plant Damage State
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
RC	Release Category
RCF	Release Category Frequency
RDF	Risk Decrease Factor
RHR	Residual Heat Removal
RIF	Risk Increase Factor
SKIFS	SKI författningssamling (SKI Code of Statutes)
SSC	Systems, Structures and Components
SSMFS	SSM författningssamling (SSM Code of Statutes)
STF	Säkerhetstekniska Driftförutsättningar (Operational Limits and Conditions, also called Technical Specifications)

Definitions

The following definitions are used in this report. They are mainly based on the IAEA Safety Glossary Terminology used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna 2007 [1].

Abnormal operation	See anticipated operational occurrence.
Accident	Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.
Accident conditions	Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents. (Examples of such deviations include a major fuel failure or a loss of coolant accident (LOCA).)
Accident management	The taking of a set of actions during the evolution of a beyond design basis accident: (a) To prevent the escalation of the event into a severe accident; (b) To mitigate the consequences of a severe accident; (c) To achieve a long term safe stable state.

Anticipated operational occurrence	An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
Beyond design basis accident	Accident conditions more severe than a design basis accident
Design basis accident	Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.
Defence-in-Depth	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions. a) To compensate for potential human and component failures; b) To maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; c) To protect workers, members of the public and the environment from harm in accident conditions in the event that these barriers are not fully effective.
Initiating event (in PSA)	An initiating event is any event that perturbs the steady state operation of the plant, if operating or the steady state operation of the decay heat removal systems during shutdown operations such that a transient is initiated in the plant. Initiating events trigger sequences of events that challenge the plant control and safety systems.
Initiating event (IAEA-TECDOC-719 [2])	An initiating event is an incident that requires automatic or operator initiated action to bring the plant into a safe and steady-state condition, where in the absence of such action the core damage states of concern can result in severe core damage. Initiating events are usually categorized in divisions of internal and external initiators, reflecting the origin of the events.

Initiating Event Satisfying Safety Goals by Probabilistic Risk Assessment by Hiromitsu Kumamoto [3]	"An initiating event is any event either internal or external to the plant that perturbs the normal operation of the plant, thereby initiating an abnormal event such as transient or loss of coolant within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could lead to an accident potentially followed by a large release of hazardous materials. For the nuclear power plant, the accident is core damage and the hazardous-material release is an early large release of radioactivity." Initiating events are identified for hazards that not can be removed. An initiating event is prevented from propagating into an accident, first by preventing the circumstances or mechanisms that can trigger an initiating event, and next by mitigating the initiating event from propagating into an initiating event that raises requirements on accident prevention and mitigation. Important aspects of initiating event prevention are: • Sufficient safety margins • Standardization • Preventive maintenance • Corrective maintenance • On-line maintenance • Change control • Prevention of human error Important aspects of initiating event mitigation are: • Normal control systems • Mitigation Systems • Interindependence • Outerindependence • Recovery • Automatic actuation • Symptom based procedures • Fail safe design • Fail soft design • Robustness Minor disturbances are dealt with through normal feedback control systems to provide tolerance for failures that might otherwise allow faults of abnormal conditions to develop into accidents. This reduces the frequency of demand on the emergency safety systems.“

Normal operation	Operation within specified operational limits and conditions.
RCPB	Reactor Coolant Pressure Boundary as defined in US10CFR50 §50.2.
RO	RO (“Rapportervärd Omständighet”) is essentially issued for all events in Category 1-3 in SSMFS 2008:1 [4]. RO in Sweden essentially corresponds to LER (Licensee Event Report) in the US.
SAR	Safety Analysis Report as defined in SSMFS 2008:1 [4] and IAEA terminology. A report that provides an overall view of how the safety of the facility is arranged in order to protect human health and the environment against nuclear accidents.

Summary

The objective of the project is to investigate to what extent PSA can be used in assessments of the Defence-in-Depth (DiD) for an existing plant, the impact on DiD from plant changes, and DiD evaluation of events. A ranking of structures, systems, and components having a role in the different DiD levels in relation to their risk contribution is sought.

The report clarifies the links between the defence-in-depth and possible PSA measurements. Specifically, it is concluded that the fundamental definitions of Defence-in-Depth from IAEA does not harmonize with results from PSA studies and a refined framework is presented. For each level of defence and combinations of levels, methods are presented and described to give estimates from a PSA perspective.

The results can be used in a development of event reporting, the adaptation of PSA models in support of evaluation of DiD levels, and development of result presentation supporting insights into plant DiD strengths and weaknesses.

Acknowledgements

The work has been financed by the Swedish Radiation Safety Authority - SSM

1. Introduction

1.1 Background

Defence-in-Depth in this report (and research project) is based on the following concept from IAEA INSAG 12 [5] which is based on IAEA INSAG 3 [6].

> *"All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure occurs it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth".*

One of the basic requirements for nuclear safety is to maintain and to develop the Defence-in-Depth (DiD). The overall aim is to prevent deviations from normal operation from occurring and, if prevention fails, to detect and limit their consequences, and to prevent any escalation to more serious conditions.

The concept of defence in depth has been guiding the design of nuclear safety for a long time and has been adopted as the leading guidance of SSM regulations; current regulation is SSMFS 2008:1 [4].

In the beginning, the Defence-in-Depth was commonly expressed in three levels: prevention, control and mitigation. The concept was later refined based on experience from incidents and accidents and from probabilistic safety assessments (PSA). These experiences demonstrated both the benefit of operating system to lower the accident frequencies (new level 2) and benefit of enhancing plant capability to limit the radioactive releases in severe accidents (new level 4), resulting in the five current DiD levels.

A loss of off-site power event took place at Forsmark in July 2006. This complex event involved several of the Defence-in-Depth levels and was a trigger for the DiDelSYS Seminar (Defence in Depth in Electrical Systems) that was organised by SKI in Stockholm 5-7 September 2007.

Shortly after the Forsmark event, the IAEA was arranging a technical meeting in Barcelona (4-8 September 2006) on the topic "Effective Combination of Deterministic Analysis and PSA in Plant Safety Management"[7], [8]. The meeting highlighted the relevance of research, how existing PSA methodology could give information on the DiD Levels, and how to risk inform decisions taking both probabilistic and deterministic aspects into consideration.

A paper by SSM [9] at the DiDelSYS Seminar presented a view of SKI on DiD as a way of maintaining a high level of safety. The presentation discussed the concept of DiD, motives to enhance safety by developing a refined DiD assessment approach, deficiencies in Forsmark 1 in view of DiD, design errors and weakness in view of regulations and activities to develop a good DiD system.

It was noted that barriers, systems and activities are not strictly assigned to one DiD level but can contribute in two or more. Deficiencies in DiD level 1 will be found as interruption of normal operation and the deficiencies in DiD level 2-4 may be hidden and not observed just from operating the plant.

The second DiD level shall prevent abnormal operation and failures to challenge the engineered safety functions. It includes all systems and activities that support this objective. The essential means could be divided into in-service-inspection, surveillance system and the normal operating systems and barriers.

The SSM motives to enhance safety by developing a refined DiD are outlined in Table 1 [9].

Table 1: Motivation for Improving DiD Levels [9].

Level	Objective	Motivation
1	Prevention of abnormal operation and failures	Strong economical motives
2	Control of abnormal operation and detection of failures	Weak economical motives and weak legal requirements (except in-service-inspection of safety classified components)
3	Control of accidents within the design basis	Strong legal requirements on design and maintenance
4	Control of severe plant conditions, including prevention of accident	Strong legal requirements on design and maintenance
5	Mitigation of radiological Consequences	Weak legal requirements on NNP role and commitments

For the development of a good DiD system, it was suggested to further investigate possible generic weaknesses in plant design and activities to maintain and enhance safety. For the utilities:

- Investigate to which extend the DiD has come into use in all safety related activities such as operation, maintenance, design modification, evaluation of events, and recurrent safety evaluations. Take appropriate actions when needed to enhance safety.

- Investigate where the fail-safe principle has not been fully used in safety systems. Take appropriate actions where non-robust short cuts have been made. Robustness in general should be addressed.
- Investigate if the organisation and processes for design modifications is suitable to take full responsibility for plant safety similar to original vendor.

For authorities:

- Investigate if further changes must be made in the regulation besides already recognised e.g. more stringent application of the requirements on diversified redundancy.
- Enhance the use of DiD to follow up plant safety performance. (DiD approach is already used in different activities e.g. evaluation of LER's, annual safety evaluations etc., but the analyses do not reach a level where concrete conclusions are drawn about the efficiency of DiD.)
- Develop methods to better measure and evaluate the efficiency of each level of the DiD.

As a PSA mainly is used to evaluate the existing NPP and prioritize changes in construction and systems, a method to interlink DiD and PSA could provide such information also in a DiD perspective [10].

There are a number of risk-informed applications where parts of the defence-in-depth are analysed and risk assessed with PSA – this is in fact one of the basic aims of PSA. PSA results can generally be seen as an assessment of the overall safety of a plant, giving information about the capability of the plant as such and of its various safety functions to handle various types of disturbances, both relatively frequent ones and disturbances that are expected to occur extremely infrequently.

A high-level description of some connections between the five levels of defence-in-depth and a PSA of level 1, 2 and 3 is shown in Figure 1 [8].

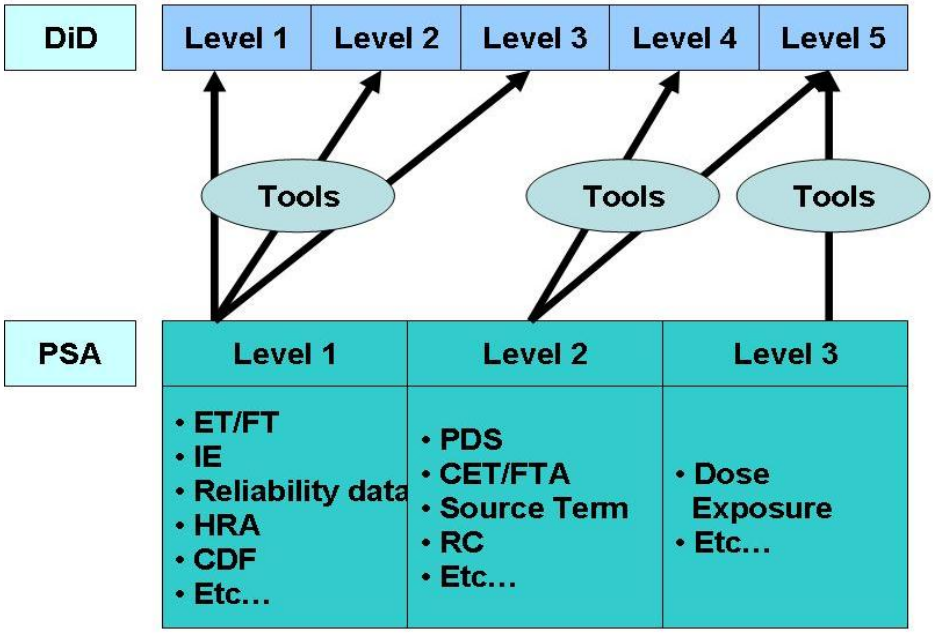

Figure 1. DiD - PSA Possible Evaluation

1.2 Objective and Scope

Given the background above, the general purpose with the DiD-PSA project is to investigate to what extent measures and parameters of PSA can be used in order to give estimates of the five levels of DiD as defined by the International Atomic Energy Agency (IAEA) based on the PSA studies for Swedish BWR and PWR plants including planned further work for these. The method should thus not imply a need for unreasonable modifications of the studies.

The evaluation should make it possible to evaluate structures, systems, components, manual actions and routines regarding risk importance for each of the five levels. The method is supposed to manage evaluation of existing plants, plant changes, and events.

1.3 Project Overview

The project has been performed in phases, starting with a survey of qualitative parameters of each level of Defence-in-Depth that should be considered in the method. This includes identification and structuring of the SSCs that belong to each DiD level and that should thus be considered for potential PSA evaluation. Next, a review was made of PSA properties (both input data and results that are or can be calculated by a PSA) and attempting to link them to the different DiD levels.

The work lead to a proposed restructured DiD framework in support of its evaluation with PSA.

A PSA model has been used in order to run calculations and develop ways of presenting the results, all in support of providing further insights on the DiD Levels.

A comment raised by SSM during this project is the need to clarify DiD principles and its terminology to be used also in the daily work. This refers to improvement of the common understanding in e.g. regulation and licensing situations and applications. The main reason for this is to clarify regulations and to translate this terminology into working-day language.

1.4 Approach in this Report

The report covers the following main parts:

- Definitions and requirements on analysis of DiD.
- Interpretation of DiD.
- Qualitative evaluation of the Defence-in-Depth, comparison of deterministic view versus PSA view on DiD.
- General discussion about quantitative evaluation with PSA.
- Elaboration on DiD evaluation and result presentation.
- Risk criteria and requirements on PSA for DiD evaluation.
- The approach for plant evaluation
- Conclusions and recommendations.

Definitions of Defence-in-Depth
The review of concepts and definitions and how those have been applied and evolved is important to fully understand the issue of DiD, and in order to develop and apply them to other contexts. A number of reports from previous work have been identified that from different aspects are relevant to this project. This section also discusses the Swedish requirements on Defence-in-Depth and on analysis of Defence-in-Depth.

Interpretation of Defence-in-Depth in relation to PSA
The process of elaborating on the definitions of Defence-in-Depth and its link to PSA models led to ideas for revised definitions and a restructured DiD framework that should be more supportive with regard to a PSA evaluation. This section presents the revised definitions and proposed restructured DiD framework.

Qualitative evaluation of Defence-in-Depth
This part discusses various deterministic frameworks and their links to the Defence-in-Depth and gives some examples on interpretation of events.

General discussion about quantitative evaluation with PSA
Quantitative PSA evaluation of DiD is discussed. This also includes a review of Swedish and international presentations of PSA results. Typical result parameters in Swedish and international PSAs are identified, described and linked to the different DiD levels.

Elaboration on DiD evaluation and result presentation.
Development of a description of DiD levels and potential corresponding PSA relations are further acknowledged in this section aiming at giving more precise definitions. Examples on result presentation providing further insights into the DiD Levels are given. These are based on test cases analyzed with RiskSpectrum.

Risk Criteria
Safety goals and risk criteria and their relations to PSA levels and DiD levels are discussed.

The approach for plant evaluation
The procedure for evaluating a plants Defence-in-Depth, evaluation of impact due to plant changes, and evaluation of events with regard to defence-in-depth is outlined. Some remarks on quality requirements on PSA for evaluation of DiD levels are provided.

Conclusions and recommendations
The report is concluded with a section summarizing findings and conclusions and providing recommendations for the further evaluation of the Defence-in-Depth and for development of reporting, analysis tools and results presentation in support of maintaining a strong Defence-in-Depth and keeping nuclear safety at levels that can be accepted by the public.

2. Defence-in-Depth Defintions

This section discusses what defence-in-depth is and the requirements for the analysis of defence-in-depth.

2.1 Basic Definitions

The IAEA document "Basic Safety Principles for Nuclear Power Plants (INSAG-3 [6], later revised as INSAG-12 [5]) discusses the implementation of a DiD concept centered on several levels of protection, including successive barriers preventing the release of radioactive material to the environment. The objectives are as follows:

- to compensate for potential human and component failures;
- to maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves; and
- to protect the public and the environment from harm in the event that these barriers are not fully effective.

The idea is that if a failure occurs it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of Defence-in-Depth.
The DiD principle thus refers to the introduction of several layers of protection between a hazard and its possible consequences. With regard to a nuclear power plants (NPP), hazards include failures that disturb plant operation and may lead to overheating of fuel, release of radioactive material or impact on the public in terms of cancer and fatalities.

The layers are composed of technical equipment, operational measures and administrative routines for protecting of the plant barriers and maintaining their efficiency, and for protecting the environment in case the barriers do not operate as planned.

The literature survey in phase 1 of the project [11] concludes that IAEA INSAG-10 [12] is the most important reference but that additional information about suitable interpretation of INSAG-10 (and thus SSMFS 2008:1 [4]) can be found in INSAG-12 [5] and IAEA Safety Reports Series No 46 [13].

Furthermore, DiD is divided in 5 levels where the first level is thought of as the first barrier against any probable release of radioactive materials. If the first level fails the next level will come into play and so forth. The different levels of DiD are described as follows in the General Recommendations

from SSMFS 2008:1 [4]. In addition, the table provides some examples of main measures.

Table 2: Definition of the Levels in the Concept of Defence-in-Depth.

Level	***Purpose***	***Main measures***	***SSCs that are the main measures***
1	Prevention of abnormal operations and failures	Robust design and high quality requirements on design, operation and maintenance	No technical plant safety systems are part of this level of defence which consists of adequate design, requirements, manufacturing, maintenance, conditioning and testing etc. that minimizes the number of potential failures and cases with abnormal operation. Also choice of site is part of this level.
2	Control of abnormal operation and detection of failures	Control and protection systems as well as surveillance and in-service inspection	Design features of the process control and monitoring systems for allowing continued operation even in the case of abnormal operation and for detection of failures. Examples: Reserve capacity and standby redundancy in Balance of Plant (BoP) systems. All kind of monitoring of plant conditions and protective measures that minimizes the risk for a failure to escalate into accident conditions and need for scram of the plant and that minimizes the probability for equipment being unavailable when called upon.
3	Control of accidents within the design basis	Technical safety functions as well as emergency operating procedures	Safety functions: Examples are reactivity control, primary water inventory control, and residual heat removal represented by technical safety systems including their monitoring and activation and related procedures and operator actions.

4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Prepared engineered measures and effective accident management at the facility	Safety functions: Examples are containment integrity control, containment atmosphere control and containment release and filtering control represented by technical safety systems including their monitoring and activation and related procedures and operator actions.
5	Mitigation of consequences of significant releases of radioactive substances	Effective co-operation with the competent authorities for protection of the public and the environment	Plant systems for monitoring the scenario give input to decisions e.g. alarming and evacuation. Choice of site is important for this DiD level.

The DiD levels and relations with PSA can also be represented by an event tree as depicted in Figure 2.

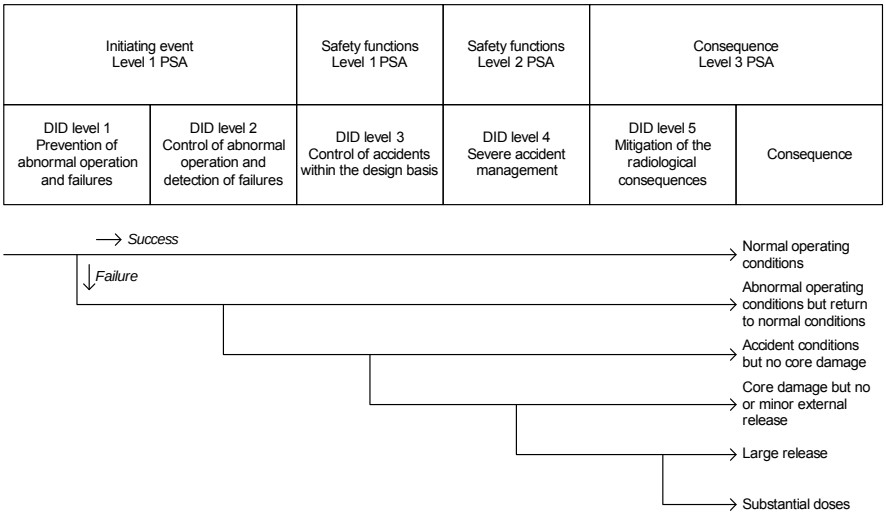

Figure 2. DiD Event Tree

The event tree in Fig. 2 represents the paths from a potential disturbance through the DiD levels, to the possible end states depending on success or failure of the DiD levels.

The initiating events cover DiD levels one and two. Failures of both levels mean that reactor protection limits are reached. There is some confusion in trying to define the interface between the PSA initiating event and DiD levels. It can be argued that the PSA initiating event is a failure of DiD level 1

and then systems to avoid scram are part of DiD level 2 and can be included in the PSA model. OK sequences without need for reactivity control, and where the plant can continue power operation will then be a special type of sequences. It can also be argued that the PSA initiating event is a failure of both DiD level 1 and 2. This is historically the way that a PSA model is constructed, with requirements for reactivity control as the first function needed to avoid core damage, and if that fails, core damage will result.

The first tree levels in DiD are particularly troublesome to relate to the PSA framework. Hence, it becomes important to scrutinize the definitions in order to fully align DiD to the PSA perspective. The definitions are further interpreted in chapter 3.

2.2 Requirements on Evaluation of DiD

The framework of how to conduct safety analyses at Swedish nuclear power plants is established by SSM. The framework covers the concept of Defence-in-Depth. Safety requirements are issued by SSM which in part are to be verified by PSA. The comprehensiveness of the PSA framework is regulated by SSM's code of statutes which requires Defence-in-Depth to be investigated with deterministic as well as with probabilistic methods.

Specifically high level requirements are presented in SSMFS 2008:1 [4], Chapter 4. Assessment and reporting of the safety of facilities, Safety analysis, 1§:

> *The capacity of a facility's barriers and defence-in-depth system to prevent nuclear accidents and mitigate the consequences in the event of an accident shall be analyzed by deterministic methods before the facility is constructed, changed and taken into operation. The analyses shall subsequently be kept up-to-date…….*
> *.....*
> *In addition to deterministic analyses in accordance with the first section, the facility shall be analyzed by probabilistic methods in order to obtain as comprehensive a view as possible of safety.*

Obtaining a safety level without dominating weaknesses is presented in the regulation as the main aim when applying probabilistic analysis for the evaluation of a facility´s design and operation.

SSMFS 2008:1 [4] also says that the DiD levels are (should be) independent and that weakness in one level cannot usually be compensated for by strength in another DiD level.

It is thus clear that the capacity of the Defence-in-Depth shall be analysed with both deterministic and probabilistic methods.

The main aim with using probabilistic analyses for the evaluation of a facility´s design and operation is to show that a plant has a certain safety level (acceptable risk below a defined target value) without dominating weaknesses (contributors to the risk for core damage/release of radioactivity).

This means that – from a PSA point of view – it does not matter what part of the DiD that makes the plant meeting the PSA objective.

2.3 Independence of DiD Levels

The general objective of defence in depth is to ensure that a single failure would not propagate to jeopardize defence in depth at subsequent levels. The independence of different levels of defence is a key element in meeting this objective. This independence between the DiD levels is also described by SSM FS 2008:1 [4] as essential in the application of the defence in depth principle and a central feature of defence-in-depth. Section 2.6 in the phase 1 report [11] concluded that achievement of complete independence is not possible. An obvious example is the plant organization, while support systems like cooling and power supply represent SSC that can violate independence between several DiD levels.

There are examples of SSCs that belong to a specific DiD level and there are also examples of SSCs that belong to several DiD levels.

Certain design principles are applied throughout the different measures representing the different levels of DiD in order to maintain a certain reliability of those. These include:

- High quality
- Fail safe design
- Automation
- Redundancy
- Defence against dependencies within a DiD level
- Defence against dependencies between DiD levels.

3. Interpretation of Defence-in-Depth

Discusses distinctions in the definition of DiD levels 1 and 2 and presents an elaborated DiD framework.

3.1 Distinction between the first DiD levels

This project has made a detailed review of the defence in depth definitions and identified a need to provide clarifications, especially for the basic definitions of the first levels of defence in depth. These clarifications are made in support of the PSA evaluation. One area discussed in the project is where the occurrence of an initiating event belongs. First the assumption was that failure of DiD level 1 results in a scram i.e. an IE. Later this assumption changed to defining the IE to occur after failure of DiD level 2, especially based on the developed framework and new definitions of DiD level 1 and 2.

However, the documents from IAEA do not convey a clear definition and the following sections will therefore depict the two interpretations. The first section convey the thoughts from phase 1 and the second section the thoughts from phase 2.

3.1.1 Interpretation from Phase 1

DiD Level 1

In accordance with IAEA Safety Reports Series No 46 [13] this DID level is achieved as long as safe normal operation subsists. This is interpreted here as preventing reactor shutdown (scram). This is a reasonable interpretation as DID Level 2 (IAEA INSAG-10 [12]) includes control of abnormal operational occurrences (events in PC2 and PC3 in ANSI/ANS 51.1-1983 [14] and 52.1-1983 [15]) and after which “the objective is to bring the plant back to normal operating conditions as soon as possible” (thus, scram may occur after an event in Level 2 but not in Level 1).

In the Swedish BWR plants, automatic partial scram and main recirculation pump speed reduction are examples of measures in DID Level 1. Examples of systems in a nuclear power plant that could be assumed to be part of the protection within this DID level are plant control system such as power control, feedwater control and pressure control systems.

This DID level could be evaluated via PSA methods if the plant models were sufficiently detailed such that different ways to cause a reactor scram could

be evaluated, the results of the evaluation would be the frequency of reactor scram for the plant.

In the current Swedish PSA studies the frequency of initiating events is mostly based on operational experiences (see e.g. the I-book [16]).

More explicitly: For frequent initiating events the initiating event frequency is normally based on operational experiences for the plant in question. For less frequent events, generic operational experiences are used. For very rare events (e.g. LOCA) industry standard frequencies are used. For Common Cause Initiators the frequency is based on fault tree analysis for systems in question using component reliabilities from the T book [17]).

To simplify, the frequency is calculated based on the number of reactor scrams in certain groups (initiating event category) that has occurred in relevant plants. Thus, no evaluation of this DID level is performed in present Swedish PSA studies that would make it possible to evaluate structures, systems, components, manual actions and routines regarding risk importance. It is reasonable to assume that the same conclusion can be drawn for all the PSA studies internationally.

It is reasonable to link potential PSA developments to improvements in operational experience evaluation. Such a potential development of the PSA studies to facilitate an evaluation of which structures, systems, components, manual actions and routines that are most likely to lead to reactor scram would have to include the following elements:

- Fault tree models of a large number of systems within the turbine plant, electrical power systems, control systems etc that are not extensively modelled in the current PSA.
- Failure mode effects analyses of these systems to evaluate which failure modes that can cause reactor scram.
- Extensive analysis of potential human errors during maintenance performed during power operation that could lead to reactor scram.

DID Level 2

In accordance with IAEA INSAG-10 [12] this DID level is achieved as long as it is possible to bring the plant back to normal operation as soon as possible after an event. It also includes preventing progression of an event to a more severe state, such that it is no longer possible to bring the plant back to normal operation as soon as possible after an event (IAEA Safety Reports Series No 46 [13]).

An event may lead to a situation where it is not possible to bring the plant back to normal operation for a long time after its occurrence even if this has no direct impact on safety (one example could be severe degradation of the

external electrical power grid in the vicinity of the plant due to external events). A further condition is thus applied for Level 2, and that is that an event is relevant in Level 2 in this project only if the event prevents restart of the plant due to the impact on safety barriers (as defined in SSMFS 2008:1 [4]).

The main barriers that are challenged by events in event class H2 (safety systems that are used to control anticipated operational occurrences, see chapter 4 for event class definitions) in accordance with SSMFS 2008:17 [21] are the fuel and the RCPB. Thus, these barriers must be in good condition such that they without damage can withstand the loads associated with the challenge posed by events in event class H2. The design of the barrier must incorporate selection of suitable material that prevents degradation including taking into account ageing of materials and use of proper fuel designs. Examples of systems in a nuclear power plant that are mainly part of the protection within this DID level are pressure relief system1 of the RCPB and the auxiliary feedwater system.

The relevant end state was defined as: Effects on safety barriers such that an operability evaluation is necessary before restart is possible.

This DID level could be evaluated via PSA methods if the PSA models incorporated an evaluation of the frequency of events after which it is not possible to bring the plant back to normal operation as soon as possible after an event. One example would be an event sequence that involves automatic depressurization of the RCPB. This can be interpreted such that the consequences are more severe than the acceptance criteria for event class H2 (in accordance with SSMFS 2008:17 [21]).

In current Swedish PSAs the evaluation normally does not include any detailed evaluation of other consequences than core damage or unacceptable releases of radioactive matter. Thus, no evaluation of this DID level is normally performed that would make it possible to evaluate structures, systems, components, manual actions and routines regarding risk importance. It is reasonable to assume that the same conclusion can be drawn for all PSA studies internationally.

Potential development of the PSA studies to make an evaluation of which structures, systems, components, manual actions and routines that are most likely to lead to consequences more severe than the acceptance criteria for event class H2 would have to include the following elements:

- Define end states other than core damage and unacceptable releases in the accident sequence analysis.

[1] In a PWR, this implies the pressure control system using the pressurizer. In a BWR, this implies the relief valves that are opened via electric signals on e.g. high reactor pressure.

- The main work would be to include a larger number of initiating events (including estimating the frequencies of occurrence for these events) to reflect different events relevant for this purpose.

In most cases, the fault trees for the plant would be sufficient also for this purpose. In some cases, additional fault trees (or extension of current fault tress) can be necessary for the purpose.

DID Level 3
The general aim of DID level 3 is to prevent core damage but also to limit accident consequences within the design basis. From a deterministic safety analysis point of view, the interpretation is that the goal is to assure that the consequences of an event in event class H3 or H4 are within the acceptance criteria of these event classes. From a probabilistic safety analysis point of view, the purpose is to assure a sufficiently low probability for core damage.

A reasonable approach to evaluate this DID level via PSA would be via evaluation of the core damage frequency and other end states. The core damage frequency and other end states are evaluated in the PSA Level 1 for Swedish nuclear power plants. Thus, an evaluation of this DID level using PSA is already being performed.

3.1.2 Interpretation from Phase 2

The phase 1 report [11] discussed the DiD concept primarily from a qualitative point of view. Potential ways of evaluating the different DiD levels with PSA were identified. Breach in DiD level 1 was identified as the point in time when an initiating event has occurred, and thus DiD level 2 should be possible to evaluate with a level 1 PSA. The time point when the initiating event, in terms of PSA, exists, can be argued. In most PSAs, need for scram and thus need for the safety functions reactivity control, water inventory control and residual heat removal, is the definition of an initiating event. However, some DiD level 2 functions are possible to model in a PSA and it is then possible to define the initiating event as the result of a failure of DiD level 1. Thus, this section elaborates on the relation between the plants SSCs and the DiD levels, and the interpretation in terms of PSA measures.

As discussed below, both the original definitions of DiD level 1 and 2 have two objectives, and division of these levels into two new levels may make it easier to use PSA in evaluating the Defence-in-Depth.

DiD Level 1
DiD level 1 “Prevention of abnormal operations and failures“ can be seen as having the following two different objectives:

Table 3: The two Objectives of DiD Level 1.

Objective	*Meaning*	*Failure*
Prevent abnormal operation	Prevention of abnormal operation is the prevention against circumstances that eventually may lead to an initiating event.	Failure will result in the existence of abnormal operation
Prevent system failures	Prevention of system failures is the prevention of circumstances that may fail system, structures and components	Failure will result in existence of potential failures in the system structures and components that form other DiD levels.

DiD Level 2

Similar to DiD level 1, DiD level 2 "Control of abnormal operation and detection of failures" have two different objectives:

Table 4: The two Objectives of DiD Level 2.

Objective	*Meaning*	*Failure*
Control of abnormal operation in case prevention of abnormal operation has failed	This can be interpreted as the plants ability to stay in operation without scram.	Initiating event that requires operation of central emergency safety features such as reactivity control, primary water inventory control and residual heat removal.
Detection of failures	Detection of potential failures serves two purposes 1) detection of a failure before it becomes critical and shows up as an abnormal operating condition 2) Detection of potentially failed equipment, e.g., in a stand-by safety system, before it becomes a real critical failure and is being challenged as part of the functions making up other DiD levels.	Existence of failed component

It is specifically noted that INSAG 10 [12] mentions that "diagnostic tools and equipment such as automatic control systems can be provided to actuate corrective actions before reactor protection limits are reached". This can be interpreted as success of level 2 and mean that the plant does not need to

scram, but failure of DiD level 2 to control abnormal operation will require a scram. However, this is quite dependent on the definition of an initiating event.

Another question is whether scram can be considered as an accident? The IAEA definition of accident conditions is a state with deviation from normal operation more severe than anticipated operational occurrences (IAEA Safety Report 23, p 71 [18]), including design basis accidents and severe accidents. Examples of such deviations include a major fuel failure or a loss of coolant accident (LOCA). NRC Glossary defines design basis accident as a postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety.

This is interpreted here such that scram is an accident condition, and any event that has lead to scram is a design basis accident, e.g. LOCA, loss of feed water, loss of turbine etc.

Note that events that require manual shutdown should not be categorised as initiating events. Manual shutdown, even in case of conditionally increased failure probability of functions needed to shut down the plant, still is to be considered as operation of the plant. The possibility of initiating events and related scenarios during low power and shutdown conditions are usually evaluated in the PSA for low power and shutdown conditions.

Failure of DiD level 2 (and level 1) can also result in failed control and safety equipment, that will become evident when functions depending on that equipment are challenged.

DiD Level 3

Engineered safety features and protection systems are provided to prevent evolution towards severe accidents and also to confine radioactive materials within the containment system. The measures taken at this level are aimed at preventing core damage in particular.

The typical measures at level 3 are the functions designed to safely shut down the plant when called upon. Active and passive engineered safety systems are used. In the short term, safety functions are actuated by the reactor protection system when needed. This can be interpreted as including both the technical systems, the monitoring and control systems, and emergency features actuation systems that will make the plant respond appropriately given a specific accident scenario.

3.2 Initiating Event Interpretation with regard to DiD Levels

To sum up the discussion about how to align the DiD perspective to PSA and especially the issue of scram, this section relates the statement that scram is the state where DiD level 3 starts. The basic document for interpretation of DiD is IAEA INSAG 10 [12] which holds the clarifying paragraph about DiD level 2:

> *Level 2 incorporates inherent plant features, such as core stability and thermal inertia, and systems to control abnormal operation (anticipated operational occurrences)… The systems to mitigate the consequences of such operating occurrences are designed according to specific criteria (such as redundancy, layout and qualification)…*
> *Diagnostic tools and equipment such as automatic control systems can be provided to actuate corrective actions before reactor protection limits are reached; examples are power operated relief valves, automatic limitation systems on reactor power and on coolant pressure, temperature or level, and process control function systems which record and announce faults in the control room.*

From IAEA INSAG 10 it is clear that DiD level 2 concerns anticipated operational occurrences. The aids to control such features are diagnostic tools as well as automatic control systems before the set limits to protect the reactor are reached. The automatic control systems are here interpreted as steam relief valves, partial scram, house turbine operation etc. Operation of such equipment can keep the plant in operation, though at lower power. Such success of DiD level 2 mean that the plant does not need to scram fully and challenge the safety systems in DiD level 3. IAEA INSAG 10 [12] provides the following definition for DiD level 3:

> *In spite of provisions for prevention, accident conditions may occur. Engineered safety features and protection systems are provided to prevent evolution towards severe accidents and also to confine radioactive materials within the containment system. The measures taken at this level are aimed at preventing core damage in particular.*

From above it is further clear that DiD Level 3 concerns accident conditions which, in turn, are defined in IAEA Safety Report no. 23 [18].

> *Accident conditions: Deviations from normal operation more severe than anticipated operational occurrences, including DBAs and severe accidents.*

As DiD level 2 concerns anticipated operational occurrences it is obvious from the above that accident conditions are not included in DiD level 2, which in turn belong to DiD level 3 (Control of accidents within the design basis). IAEA INSAG 12 [5] states that the design envelope of a NPP to protect the plant from accidents within the design basis includes the following features:

> *Design is such that abnormal developments are first met automatically by the restoration of normal conditions by means of the feedback characteristics of neutronic and process controls. These are backed up by the normal capability for shutdown, continued cooling and protection against the release of radioactive materials. Further protection is available through automatic actuation of engineered safety systems.*

These sentences are interpreted to belong to the DiD levels 1-3 in due order. It is when automatic actuation of engineered safety systems is executed that a full scram or initiating event occurs. This is further supported by the fact that the hydraulic control rod system (system 354) is considered a safety system at full scram and a control system at partial scram. To conclude, the difference between DiD Level 2 and 3 is the fact that DiD Level 2 concerns control systems and DiD Level 3 concerns safety systems. With this in mind the implication of what constitutes an initiating event needs clarification. This calls for the definition of an initiating event, which is given by IAEA TECDOC 719 [2] as follows:

> *An initiating event is an incident that requires automatic or operator initiated action to bring the plant into a safe and steady-state condition, where in the absence of such action the core damage states of concern can result in severe core damage.*

An automatically initiated action to bring the plant into a safe and steady-state condition and an automatic actuation of engineered safety systems are considered to have the same implications. The initiating events further relates to PSA by the statement given in IAEA Safety Report no. 25 [19]:

> *The starting point of the PSA is the identification of the set of initiating events which have the potential to lead to core damage if additional failures of the safety systems should occur.*

All in all, the initiating event is input to PSA of today and considers safety systems. Safety systems aim to control accidents within the design basis i.e. DiD Level 3. Safety systems are actuated when reactor protection limits are reached which is preceded by an abnormal operation control of anticipated operational occurrences i.e. DiD Level 2.

3.3 Elaborated Model of DiD Level 1 and 2

This research project has developed the original IAEA definitions into a DiD framework that emphasizes the link to the probabilistic safety assessments (PSAs) carried out as part of the safety case required for the operation of a nuclear power plant. This new framework is illustrated below.

Figure 3 below shows the relations between the different DiD levels, propagation of potential disturbances and failures through the DiD level barriers, and the PSA interpretation of failures of the DiD levels.

A potential failure can become a real failure if DiD level 1 fails to prevent a failure and DiD level 2 fails to control the failure (i.e. one of the objectives of each of DiD level 1 and 2 are not met).

The failure may be a disturbance that results in abnormal operation. This will be the case when there are failures in the normal operating systems, e.g. loss of a feed water pump. There are also other cases with disturbances, e.g. loss of offsite power, that are classified as abnormal operation. The prevention of loss of off-site power is related to the choice of site, the design of the grid and the connections to the grid.

The failure can also be in a standby system and be detected before the standby system is needed. A failure in a standby system that is not detected and repaired before the component is required to operate, means that a system function is degraded. This function may belong to systems for control of abnormal operation or systems needed to prevent core damage (DiD level 3), or to consequence mitigating systems in DiD level 4 and 5.

Abnormal operation can be controlled without need for scram, e.g. by the inherent stability of the design, or by control and safety systems that are capable of handling certain disturbances without need for shutting down the plant. This is the second part of DiD level 2. Failure of level 2 to control abnormal operation means that the DiD level 3 safety functions needed to control reactivity, control the water inventory in the primary system and control the residual heat removal function. Usually this is the initiating event in a PSA. There are some rare examples where PSAs model functions where the success of these functions mean that the reactivity control system is working.

The PSA identifies combinations of functions and related success criteria that form accident scenarios with different end states. The upper success path mean that the functions needed for safe shutdown have been successful, even if this might include possible failure combinations where a sufficient number of components are working for considering the function as successful. There will also be a number of sequences where certain systems have

failed, but other systems/functions have operated and a sufficient number of components have been successful meaning that core damage is avoided.

The strength of the DiD level 3 functions is dependent on the success of one part of the objectives for DiD level 1 and 2, described above.

Next, in case of core damage, DiD level 4 and 5 are challenged.

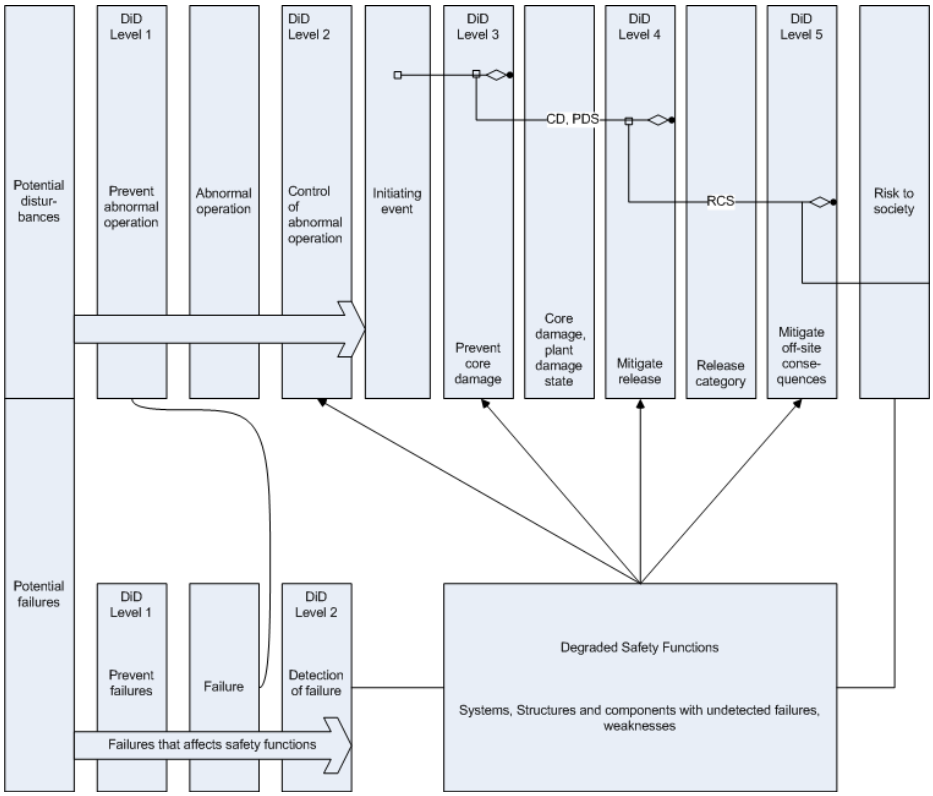

Figure 3. Relations Between DiD Levels, Objectives and PSA

The lower part of the figure illustrates that failures, degradations as a result of failure of one part of the objective of DiD level 1 and 2, affects both the normal operating system and the functions related to the succeeding DiD levels.

Observe that in this concept the original IAEA DiD level 1 and level 2 have each been split into two parts with corresponding objectives. This is a new interpretation introduced in this R&D project to match the PSA view and the link to PSA results in analyzing the different DiD levels.

The new definitions are further described in Table 5 and the new framework is also illustrated in Figure 4.

Table 5: The Extended DiD Levels Definitions.

DiD Level	Description	Examples
1:1	Quality in design, manufacturing, installation, use of redundancy, fail safe principles etc to ensure high system reliability and availability.	Use of a specific Safety Integrity Level (SIL) in design, proven design, etc
2:1	The monitoring and surveillance of the condition of SSCs in order to detect degradation and failures before they become critical, i.e. before they affect the performance of the sequential DiD levels.	Systems for continuous monitoring or regular testing of vibrations, temperature, crack growth, etc. that can identify any signs of (precursors) to equipment failures.
1:2	BoP system, other operating systems. A failure means that DiD 2.2 is needed to avoid shutdown.	Loss of offsite power, Failure of a feed water pump.
2:2	Systems for detection and control of disturbances resulting from failures in the BoP and other operating systems so that the plant can continue operation. This also includes built in robustness in terms of thermal hydraulic design.	Monitoring of feed water flow, back-up feed water pump, abnormal operation relief valves, equipment for house turbine operation. Power reduction capability – e.g. partial scram, the built in thermal hydraulic and nuclear physics behavior.
3	Safety functions for prevention of fuel (core) damage; reactivity control, water level control, pressure control and residual heat removal. Control of an accident within the design basis.	Core Spray, auxiliary feedwater, low pressure injection, high pressure injection, safety relief valves, scram system, etc
4	Safety functions for mitigation of a potential release resulting from damaged fuel. Releases above a certain level are Beyond Design Basis Accidents (BDBA).	Technical systems, mainly related to the containment – spray system, filters, containment design.
5	Emergency measures for limiting public exposure to any release resulting from a BDBA	Site location, emergency planning and preparedness, alarm systems, iodine tablets, evacuation routes etc.

The interpretation is that the new DiD levels 1:1 and 2:1 are the failure defences that limit the frequency of events in the normal operating system represented by DiD 1:2, the Balance-of-Plant (BoP) and probability of failures in the succeeding sequential DiD levels (called sequential from now on in this report), in turn resulting in the conditional probabilities of failure of the remaining DiD levels 2:2, 3, 4 and 5.

Note that DiD level 1:1 and 2:1 have somewhat different meaning for operating systems and safety systems.

- For operating systems, DiD 1:1 and 2:1, shall make sure that the frequency of events challenging DiD 1:2 is as small as possible.
- For safety systems, DiD 1:1 and 2:1, shall keep the conditional failure probability of DiD 2:2, 3, 4 and 5 as low as required.

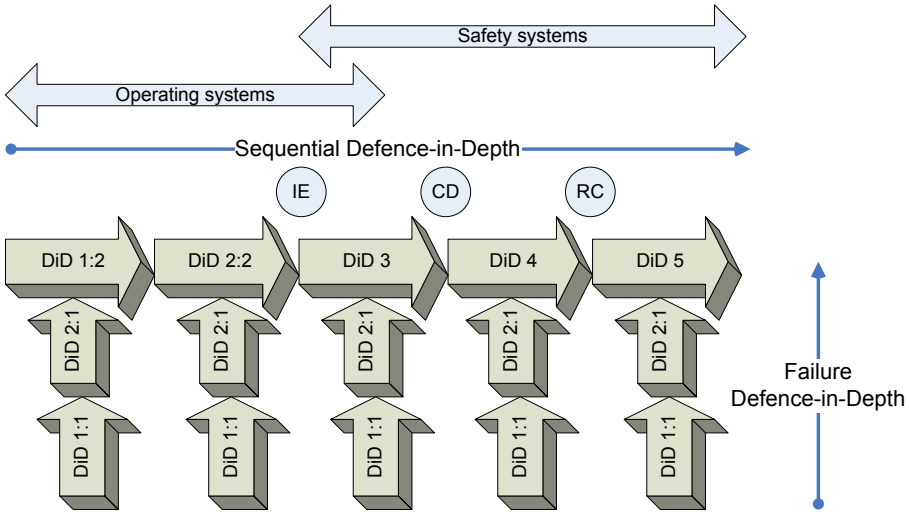

Figure 4. The failure Defence-in-Depth and the sequential Defence-in-Depth.

4. Qualitative Evaluation

Discusses different qualitative aspects and evaluations of DiD levels and provides some examples on the interpretation of events with regard to the DiD levels.

4.1 Relating DiD to INES Classification

The International Nuclear Event Scale (INES) [20] was developed jointly by IAEA and OECD/NEA in 1989. The purpose of the INES scale is to provide a means for communicating to the public in consistent terms the safety significance of an event in a nuclear installation. The INES scale classifies events in 7 levels; the upper levels (4-7) are termed accidents and the lower levels (1-3) incidents. Events which have no safety significance are classified below scale at level 0 and are termed "deviations". INES classifications are provided for example for licensee event reports in Swedish nuclear power plants. The INES scale as such is thus a means to classify an event that has occurred; the concept of defence in depth on the other hand is mainly aimed at design and development of procedures to prevent events. This is illustrated in the table below.

In the remainder of this report, the INES classification is not further discussed.

Table 6: INES Classification.

Class	*INES-Description*	*DID*	*Comment*
-	Out of scale event-No safety relevance	1	-
0	Deviation. Deviation from normal operation for which operational limits are not exceeded and which are properly managed in accordance with procedures.	2	-
1	Anomaly. Deviation from normal operation which includes deviations from (or errors in) procedures.	2	-
2	Incident. Incidents with significant failure in safety provisions but for which additional failures could have been tolerated. Local contamination/ overexposure to staff member.	3	-
3	Serious incident. Incident with significant failure in safety provisions for which no additional failures could have been tolerated. Small release to environment significant overexposure to staff member.	3	-
4	Accident without significant off-site risk. Accident with e g partial core damage. Small release to environment. Fatal injuries to staff member.	3-4.	DID Level 3 in a deterministic safety analysis includes postulated core degradation (e g Reg Guide 1.3 (BWR) /1.4 (PWR))
5	Accident with off-site risk. Accidents involving e.g. core damage. Releases up to 1000 TBq I-131. Example: TMI-2 1979.	4	Event class H5 based on 0,1 % of core inventory of Cs-137 from a 1800 MWt core; this corresponds to roughly 1000 TBq I-131.
6	Serious accident. Releases> 1000 TBq I-131.	4-5	See above.
7	Major accident. Releases of a substantial fraction of the core inventory from a large nuclear facility. Example: Chernobyl 1986.	5	

4.2 Relating DiD to Event Classification

In SSMFS 2008:17 [21] events are categorized in terms of five event classes which are denoted H1, H2, H3, H4 and H5. These classes are based on the five Plant Conditions (PC) PC1, PC2, PC3 PC4 and PC5 which are defined in ANSI/ANS 52.1-1983 [14]. Each plant condition has associated a nuclear safety criterion which consists of the frequency of occurrence reflecting a postulated expected probability concerning the performance of the reactor. The table below shows how the event classes and safety criteria are related.

Table 7: Event Class Definitions.

Event Class	Frequency(f) (year)	Description
H1	-	Normal operation
H2	$f \geq 10^{-1}$	Anticipated events
H3	$10^{-1} > f \geq 10^{-2}$	Unanticipated events
H4	$10^{-2} > f \geq 10^{-4}$	Improbable events including DBA
H5	$10^{-4} > f \geq 10^{-6}$	Highly improbable events, basis for design of severe accident mitigating systems

Events or conditions with a frequency below H5 events are called residual risks and are so unlikely that they are not needed to be considered in the safety analysis [21].

In general words, the behaviour of an operating nuclear power plant can be described in terms of a set of basic parameters such as reactivity and power distribution of the core, flow, pressure and temperature of the coolant and the status of safety-related equipment.

The values of these parameters are determined by design criteria of the power plant which are met in a normal operating state. A change from these normal state values result in an event, also known as an initiating event (IE). The majority of these events will not violate the plant nuclear safety criteria in the table above. However, events which potentially can decrease the safety and challenge control systems are supposed to be identified and their frequency of occurrence estimated. Each event is categorized into the event classes H2, H3, H4 and H5 in accordance with its frequency of occurrence.

The event class H2 covers events in a normal operating state with expected occurrences during a power plant´s life-time. The plant usually responds to H2 events by initiating safety functions such as scram.

The design principles of a NPP should be such, that safety functions can be upheld in all events including the event class improbable events H4. Hence, the design of a NPP shall be able to resist any damage to reactivity control, Reactor Coolant Pressure Boundary (RCPB), Emergency Core Cooling Systems (ECCS), Residual Heat Removing systems (RHR) and containment integrity resulting from H1 to H4 events. The systems listed are safety systems of DiD Level 3. Therefore H2 to H4 events relates to DiD Level 3.

The design should take highly improbable events (H5) into account. For example, limiting the release of radioactive substances to the environment and maintaining a water-covered core at all times [21]. It shall furthermore be possible to achieve a stable plant state in case of H5 events. This refers to systems which are active in severe accident control. Therefore, H5 events mainly relates to DiD Level 4.

One interesting conclusion from the event class definitions and their link to the defence-in-depth is that the use of event classes in the design will result in a plant with a core damage frequency less than 1E-4 per year (compared to utility PSA target values usually at 1E-5 per year). It also indicates that the plant is designed for a frequency of release less than 1E-6 per year (compared to utility PSA target values usually at 1E-7 per year). It also presupposes that a barrier strength of a factor of 100 is achievable between core damage and unacceptable release.

Another observation is that the event class definitions give guidance for DiD level risk criteria, see further section 7.

An IE as defined in the context of DiD and event classes differs in meaning when an event is regarded in a PSA analysis. In the latter case an event occurs when the plant nuclear safety criteria are violated and the safety functions are challenged. This means that events in a PSA analysis of today are only relevant for event classes H2, H3, H4 and H5. This is summarised in the table below.

Table 8: Event Class Relations to Original DiD Levels and PSA Evaluation.

Event class	Levels of DiD	PSA
H1	1, 2	No
H2	1, 2, 3	Yes
H3	3	Yes
H4	3	Yes
H5	4,5	Yes

The events in H1 and H2 will then become initial events in PSA studies whose end state will be failure of DiD Level 2. To a large extent H1-H5 events are modelled in PSA today and relevant events are defined as initiating events.

4.3 Qualitative Assessment of DiD

IAEA Safety Report Series No.46 [13] suggests a method to evaluate the DiD Levels. Although this method predominantly suggests a framework in order to evaluate DiD Levels by deterministic approaches. This framework will prove relevant also in a PSA approach. The report from IAEA describes a method of the DiD concept and its capabilities of an existing plant, including both its design features and operational measures taken to ensure safety. The general principles are displayed in the figure below. For the given objectives at each level of defence, a set of challenges is identified, and several root mechanisms leading to the challenges are specified. Finally, to the extent possible, a comprehensive list of safety provisions, which contribute to preventing the mechanisms from occurring, is provided [13].

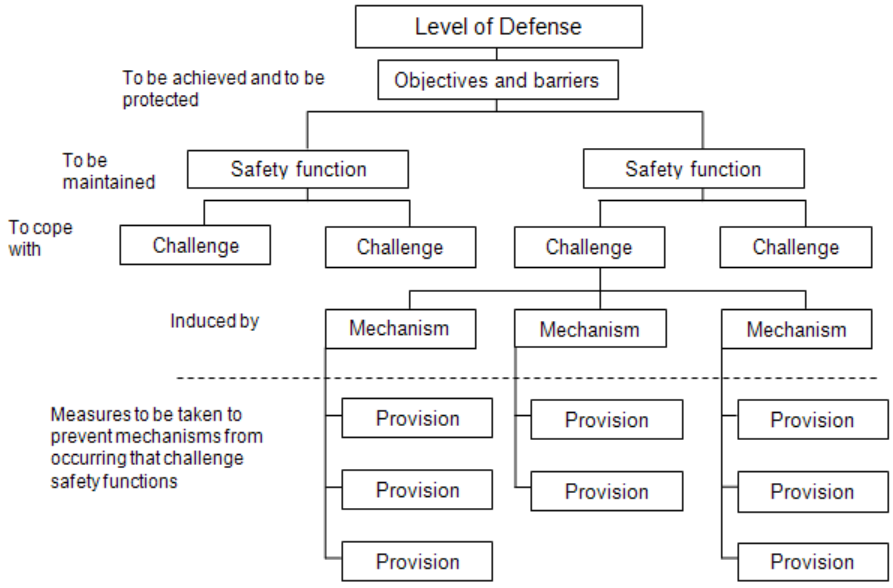

Figure 5. Structure for DiD provisions at each level of Defence.

As argued in the IAEA report the deterministic approach does not explicitly consider the probabilities of occurrence of the challenges or mechanisms. However, it is suggested that this deterministic approach could be further complemented by PSA considerations to verify an adequate level of safety as well as a balanced design. The PSA approach is particularly beneficial if the aim is to evaluate and prioritize provisions according to their contribution to risk reduction [13].

4.4 Examples of DiD Interpretation of Events

The meaning of success and failure in 5 example cases is shown below for DiD level 1-4 (original DiD level definitions):

1. Loss of Offsite power
2. Loss of feed water pump
3. Fire
4. Failure of standby equipment
5. Normal shutdown

Table 9: Example: Interpretation of Loss of Off-site Power.

DiD Level	Success	Failure
1	No Initiating event	Initiating event: Loss of Off-site power
2	Island mode operation is successful	Island mode operation fails – need for scram
3	OK sequences	CD sequences
4	Release Categories below criteria	Release Categories above criteria

Loss of offsite power is a disturbance for the plant. Depending on design, the plant may be capable of avoiding a scram if island mode operation is an option, and if this option is successful. Successful island mode operation followed by reconnection to the grid mean that DiD level 3 remains unchallenged. Failure of island mode operation will require scram and challenge DiD level 3.

Table 10: Example: Interpretation of Loss of Feed Water Pump.

DiD Level	Success	Failure
1	No loss of pump	One feed water pump fails (stops)
2	BoP control takes care of the situation, power is reduced, standby pump is started	BoP fails – need for scram
3	OK sequences	CD sequences
4	Release Categories below criteria	Release Categories above criteria

The loss of the feed water pump is a violation of DiD level 1.

Loss of one feed water pump is an event that the plant may be capable of handling without scram. The BoP design and control systems may take care of the situation by lowering the power and start of reserve pump. This can be seen as a success of DiD level 2.

Table 11: Example: Interpretation of Fire Event.

DiD Level	Success	Failure
1	No fire	Small fire
2	Fire is detected and extinguished	Large fire, automatic or manual scram, degraded safety functions.
3	OK sequences	CD sequences
4	Release Categories below criteria	Release Categories above criteria

Occurrence of a fire is a violation of DiD level 1. It means that despite good quality in equipment, good house-keeping etc., there is a fire.

The fire may be detected and extinguished without causing any harm to the plant. This can be interpreted as DiD level 2 success. A fire that grows bigger and affects operating and safety related equipment may require an automatic shutdown, or manual shutdown. The result may be a scram or controlled shutdown depending on the actual fire scenario.

Table 12: Example: Interpretation of Failure of Standby equipment.

DiD Level	Success	Failure
1	No failed equipment	Failed equipment
2	Failed equipment is detected and repaired without need for shutting down the plant	Plant is shut down with degraded barriers.
3	OK sequences	CD sequences with increased CD frequency and CCDP if the degraded barrier belongs to DiD level 3.
4	Release Categories below criteria	Release Categories above criteria. Release sequences with increased frequency and CRCP if the degraded barrier belongs to DiD level 3 or 4.

An interesting example is failure of a safety related standby equipment in DiD level 3 that is detected during test. The failed equipment is a violation of DiD level 1 that resulted in a degradation of DiD level 3.

Table 13: Example: Interpretation in case of Normal shutdown (normal operation).

DiD Level	Success	Failure
	No DiD level is challenged	

A normal shutdown, e.g. for refuelling cannot be seen as a challenge of the DiD levels.

5. Quantitative Evaluation – PSA

Gives an interesting example of quantitative DiD evaluation and discusses general aspects of PSA evaluation of defence-in-depth and how PSA software parameters are linked to the different defence-in-depth levels.

5.1 Overview

Probabilistic Safety Assessment (PSA) is an important tool to identify and evaluate strengths and weaknesses in a plant, to identify major contributors to risk and if necessary propose risk reducing measures.

INSAG 10 [12] presents PSA as an effective means of enhancing understanding of plant vulnerabilities, including complex situations due to multiple equipment and/or human failures, where the results can be used to improve defence-in-depth. PSA is mentioned as a useful tool for optimizing efforts in implementing defence-in-depth. INSAG 10 also mentions that some aspects of plant safety are difficult to assess quantitatively by probabilistic methods. The examples given are influence of plant organization and safety culture, as well as aspects such as common cause effects, reliability of software, some types of human error, and some internal and external hazards. It states that it is an essential task of deterministic plant design to limit the influence of such aspects of safety.

Current PSAs are thus used to evaluate the defence-in-depth, even if the results seldom are presented in that fashion. The focus is on core damage and large early release, and the PSA quantifies and presents core damage and release category frequencies, and usually the results are shown in terms of total frequencies and contribution from different scenarios. In many cases, conditional probabilities for core damage and release are also presented. Of course, the presented results are related to and can give information about Defence-in-Depth. However, Defence-in-Depth terminology is rarely used.

An example of DiD evaluation presented by Fleming [22] is presented in section 5.2.

Section 5.3 shortly summarizes the parts of a PSA model and what is calculated with a PSA tool, and how they relate to the DiD framework.

5.2 Fleming Example

An article by Karl Fleming and Fred Silady in Reliability Engineering and System Safety [22] presents a review of selected definitions of Defence-in-Depth covering a time period from 1967 (NRC(AEC)) through 1996 (IAEA) to 2000 (NRC), see Figure 6:

Table 1
Review of selected definitions of defense-in-depth

Author	NRC(AEC)	NRC	IAEA	NRC	NRC
Date	1967	1994	1996	1998	2000
Reference	[4–5]	[6]	[7–9]	Reg. Guide 1.174 [10]	[11]
Key elements of proposed definition	1. Prevention of initiating events 2. Engineered safety features to prevent accidents	1. Prevention of initiating events 2. Safety systems to prevent accidents	1. Prevention of abnormal operation and failures 2. Control abnormal operation and detection of failures	1. Balance between prevention and mitigation 2. No over-reliance on programmatic activities to compensate for weaknesses in plant design	*Reactor safety cornerstones* • Prevent initiating events
	3. Consequence limiting systems to prevent large releases	3. Containment to limit releases	3. Control accidents within design basis using ESF and procedures	3. System redundancy, independence, and diversity	• Mitigation systems
		4. Accident management	4. Control of severe conditions by preventing accident progression, mitigation by accident management	4. Potential common cause failures are minimize through the use of passive, and diverse active systems to support key safety functions	• Barrier integrity
		5. Reactor siting and emergency planning	5. Mitigation of radiological consequences via emergency response	5. Barriers to radionuclide release are independent 6. The potential for human errors is minimized	• Emergency preparedness *Accident prevention strategies* 1. Limit frequency of initiating events 2. Limit probability of core damage given initiating event *Accident mitigation strategies* 3. Limit releases given core damage 4. Limit public health effects given release *Tactics to implement strategies* • Safety margins • Redundancy, diversity, independence • General design criteria • Special treatment, etc.

Figure 6. Different Defence-in-Depth Definitions [22]**.**

It is quite clear that the NRC already in the 60ties had a view of defence-in-depth that was related to PSA terms.

- Prevention of initiating events
- Engineered safety features to prevent accidents
- Consequence limiting systems to prevent large releases

The article discusses the definitions, the need for incorporating risk insights into defence-in-depth, and gives critique of the current definitions.

An alternative definition of defence–in-depth comprising three major elements is proposed:

- Design defence–in-depth
- Process defence–in-depth
- Scenario defence–in-depth

Design defence-in-depth reflects all the decisions made by the designer to incorporate defence-in-depth into the physical plant.

Process defence-in-depth reflects all the decision made in the formulation of regulatory requirements associated with licensing, operating, maintaining, and inspecting the plant and in all the processes that contribute to safety. These processes cover the design, construction, operation, maintenance, testing, and inspections that ensure safe operation of the facility.

Scenario defence-in-depth reflects the development and evaluation of strategies to manage the risks of accidents, including the strategies of accident prevention and mitigation. This aspect of defence-in-depth also provides the framework for performing the deterministic and probabilistic safety evaluations which help determine how well various prevention and mitigation strategies have been implemented.

Further, it is stated that an understanding of how defence-in-depth is applied in severe accidents beyond the design basis requires the examination of a suitable spectrum of scenarios from a PSA, and that scenario defence-in-depth provides the means of identifying strategies and for evaluating their effectiveness in both deterministic and probabilistic safety evaluations. The use of PRAs to support scenario defence-in-depth is expressed in the following way [22]:

> *"The foundation of the risk management program is a living probabilistic risk assessment that identifies a reasonably complete set of accident sequences for the plant, estimates the frequencies and radiological consequences of these sequences, with a quantification and characterization of the uncertainty in these frequency and*

consequence estimates. The PRA provides important inputs to the designers and the regulators to specify the licensing basis events that lay the foundation for the safety case and establish that top level regulatory criteria are met. When taken to its fullest capability, the PRA can be used to establish system reliability targets and to evaluate changes to the plant design and operation throughout the plant life cycle. PRA has also been demonstrated its usefulness in interpreting the safety significance of reactor incidents and accidents and the results of regulatory inspections as part of the NRC accident precursor and risk-informed oversight programs."

The proposed method is based on calculating risk reduction factors for different scenario functions. The proposal by Fleming and Silady is to calculate these risk reduction factors for active and passive SSCs along the sequences. In principle this means calculation of split fraction probabilities (a conditional probability of failure of the function given the previous events in the sequence).

A useful and more general approach may be to calculate the split fraction probabilities for every function in the event tree and for every sequence. Linking of the functions to specific DiD levels will then provide insights on the strengths and weaknesses of the different DiD levels and their degree of independence.

One problem that is mentioned in the article is that uncertainties inherent in PSA results need to be considered in the evaluation. Varying the inputs may result in different results and conclusions. This means that the analyst needs to perform uncertainty / sensitivity analysis.

5.3 Quantitative PSA Measures

Table 14 summarizes typical quantitative parameters that are used as input to a PSA or calculated in a state of the art PSA, and can be part of the overall presentation of results. Their potential use for measuring the different DiD levels is indicated.

The fault tree and event tree logic is used together with the basic event data, to calculate quantitative results for the end states – consequences – in the event tree sequences. Individual results for functions and systems are sometimes presented. Normally, main contributors in terms of basic events, minimal cut sets and sequences are also presented and discussed.

Note that the focus in most cases is on CD sequences. OK sequences, and especially OK sequences when the plant remains in operation are usually not discussed in detail.

The results are usually not elaborated with regard to the implications for the DiD levels.

PSA software can be used to calculate the probabilistic characteristics for the different items of the PSA model as presented in table 15:

Table 14: Existing Quantitative PSA Parameters for Measuring DiD Levels.

Item	Quantitative parameter (s)	DiD level
Basic event	Failure rates, failure probabilities and repair rates, human actions, test intervals, time to first test, test method. It is also important to know the data behind the basic event parameters, i.e. operating time in stand-by, activated operating time, availability/unavailability, number of activations/stops, number of demands, test intervals.	1:1-2:1
Initiating event	IE frequency	1:2-2:2
System fault tree top event	System top event probability	2,3,4
Function fault tree top event	Function top event probability	2,3,4
Sequence split	Split fraction probability	2,3,4
Sequence (level 1)	Sequence frequency including IE frequency	1:2-3
	Conditional sequence probability given initiating event	3
Sequence (level 2)	Sequence frequency including IE frequency	1:2-4
	Conditional sequence probability given initiating event	3-4
	Conditional sequence probability given specific PDS	4
Consequence core damage and other sequence end states in level 1 PSA	Consequence frequency (all initiating events)	1:2-3
	Consequence frequency (specific initiating event)	1:2-3
	Conditional consequence probability given specific initiating event, all other initiating events set to zero	3

Item	Quantitative parameter (s)	DiD level
Plant damage state in level 2 PSA	Consequence frequency (all initiating events)	1:2-3
	Consequence frequency (specific initiating event)	1:2-3
	Conditional consequence probability given specific initiating event, all other initiating events set to zero	3
Release category in level 2 PSA	Release category frequencies (all initiating events)	1:2-4
	Release category frequencies (specific initiating events)	1:2-4
	Conditional release category probability given specific initiating event, all other initiating events set to zero.	3-4
	Conditional release category probability given specific plant damage state, per initiating event.	4
Consequence fatalities, cancer	Total frequency	1:2-5
	Frequency per initiating event	1:2-5
	Conditional probability given specific initiating event, specific plant damage state, specific release category.	3-5
Importance and sensitivity	Importance and sensitivity is or can be calculated in all cases. Depending on the tool and model, importance can be presented for basic events and any group of basic events.	

Table 15: Risk Spectrum Quantitative Measures for the Different PSA Model Items

PSA model items →	Basic event	MCS	FT Top event	Se-quence top event	Conse-quence top event	Comment
Probability (mean)	X	X	X	X	X	
Frequency (mean)	X	X	X	X	X	
Importance	X	X	N/A	N/A	N/A	Can be used to calculate different im-portance measures for basic events reliability parame-ters, basic events and any group of basic events
Sensitivity	X	X	N/A	N/A	N/A	Can be used to calculate sensitivity measures for basic events reliability parame-ters and basic events and any group of basic events

6. Elaboration on the Quantitative evaluation

Contains both definitions of quantitative measures of DiD Levels and results from calculations.

6.1 Overview

The proposed measures for evaluation of the defence-in-depth are either existing measures, common in ordinary PSA reports, or new measures identified in the project. The relevant conditions for each DiD Level are accounted for.

Approaches are suggested for the collection of facts and data, needed to run and build competent models, reflecting the desired DiD Level information. This includes modelling approaches and possible extensions in the PSA models but also need for adaptations of existing PSA tools.

Requirements on PSA regarding completeness, realism and level of detail of models are discussed and estimated in section 8.2.

The basis for the recommendations is the restructured DiD framework where the original DiD levels 1 and 2 are each split into two separate levels as defined in Table 5 and illustrated in Figure 7 below.

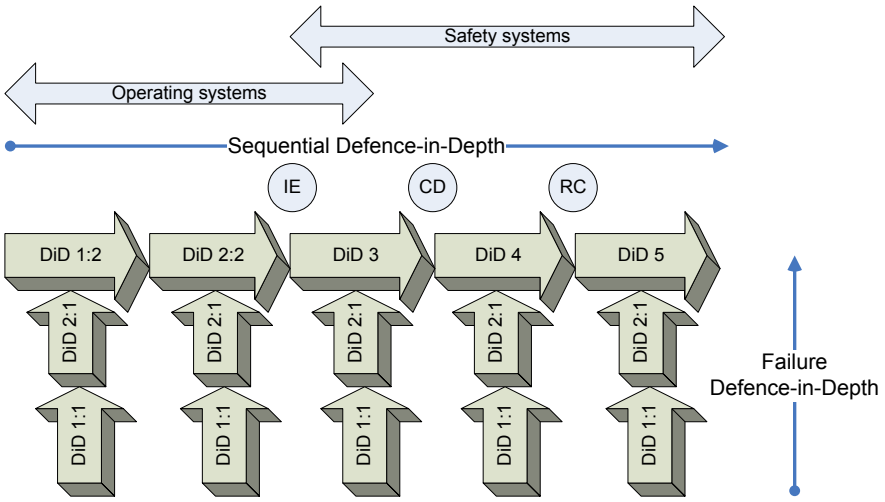

Figure 7. The Restructured DiD Framework

The figure shows that PSA results actually measure the strength of two DiD levels 1:1 and 2:1 in terms of frequencies and conditional probabilities for the failure defences:

DiD 1:1 Prevention of failures
DiD 2:1 Detection of failures (degradation).

The failure defences are measured for the sequential DiD levels:

DiD 1:2 Prevention of disturbances (failures in operating systems) – avoid abnormal operation
DiD 2:2 Control of abnormal operation – prevention of initiating events that challenges the safety functions
DiD 3 Prevention of core damage
DiD 4 Mitigation on site of radiological consequences.
DiD 5 Mitigation off site of radiological consequences.

6.2 Theoretical Framework

The framework described in previous section has a resemblance to the discussion about original DiD Level 1 and 2. Especially, the discussion about the new DiD Level 1:1 and 2:1 is to a large extent captured in the terminology of mechanisms and provisions in the method from IAEA SRS No.46 [13], see section 4.3. Whereas DiD Level 1:1 concerns the quality in design and construction this could be interpreted as referring to the control of the mechanisms. Mechanisms are defined in IAEA SRS No.46 as "specific processes or situations whose consequences might create challenges to the performance of safety functions". In PSA such situations are typically modelled as basic events. In addition, the definition of provisions; "measures to be taken to prevent mechanisms from occurring that challenge safety functions", are comparable to DiD Level 2:1. The task of DiD Level 2:1 concerns the control and surveillance of the design and construction. In short, to prevent mechanisms from degrading control and safety systems.

The framework from IAEA is mainly applicable to PSA when it comes to constructing fault trees (FT). The failure of a safety function, its inherent challenges and mechanisms, is modelled in FTs. What PSA then achieves is to put several safety functions or systems in relation and define scenarios, states and sequences where the use of safety functions will come into play. All the different safety functions are then assigned a certain PSA level, to a great extent coinciding with the definition of DiD Levels, where the end state of each PSA level results in a certain state of the NPP.

The logic of probable sequences is modelled in Event Trees (ETs) which, basically, answer the question "how do all safety functions and systems respond to different scenarios"? Therefore, to extend and complement the framework from IAEA SRS No.46 to PSA considerations, a discrete dimension of time (ordinal level) must be added as well as certain definitions of

plant conditions. A plant condition is here meant to provide information through definitions of a state relevant to safety of a NPP.

Typically, the states define the intersection between efforts relevant to safety (e.g. to avoid CD or a certain radioactive release) and, as argued before, do often coincide with the definitions of DiD Levels. Therefore, what PSA can contribute to the estimation of DiD Levels is a probabilistic estimate of the ability of full (or partial) success of the safety functions to avoid such states. To sum up, PSA can give probabilistic measures of a state which correspond to:

- Event with failure of DiD Level 1:2, events resulting in abnormal operation
- Initiating event (failure of DiD Level 1:2 and 2:2)
- Core damage (failure of DiD Level 1:2, 2:2 and 3)
- Release of radioactivity (failure of DiD Level 1:2, 2:2, 3 and 4)

The end states of each level are further possible to utilize to provide information over several levels. The result of PSA is a set of identified scenarios ending in consequences or plant states. One IE can lead to several Plant Damage States (PDS), which in turn can lead to Release Categories (RCs). Whereas all states are given frequencies it is possible to identify critical scenarios over several levels. A PDS can have contributing events from one or several IEs which could be visualized through a two-dimensional table of frequencies. In turn, a differentiated picture of contributing states to RCs could be viewed in a three-dimensional cube where it is possible to distinguish the contribution from an IE that propagates through a specific PDS.

PSA can be used to calculate the failure of DiD Levels, and also give information about the interplay of safety functions within a certain DID level. Whereas the ETs reflect sequences, those are also given probabilistic estimates. The sequences further consist of the probability of certain safety functions or systems to function. PSA provides probabilistic measures of the safety functions through FT top events. The top events from PSA as well as sequences provide information of the dynamics within a certain DID level whose relevance can be argued by the need to prioritize changes in construction and systems. Therefore, between the states the following measures can be calculated by PSA:

- Sequence frequencies
- Top event probabilities (failure of safety system)

The construction of sequences and identification of dependencies etc. requires an extensive knowledge of the system, components and usage. The availability of all components building a system is modelled in FTs, and FT models answers the question of the availability of the entire system or func-

tion. In Sweden the unavailability of safety related components in NPPs are given by the T-book [17]. The T-book provides measures or parameters to models in RiskSpectrum (or other tools) and thereby allows quantification of the basic events representing components in systems representing the different DiD levels. The choice of components and the arrangement of those (through diversity, redundancy etc) reflects the robustness of the design (1:1). It is arguable that the performance of components reflects the design and that the failure rates of such give a measure of the performance of DiD Level 1:1 and 2:1. Failures reflect the degradation of safety systems and what is named DiD Level 1:1/2:1. The original DiD Level 2 concerns "Control and protection systems as well as surveillance and in-service inspection". It is arguable that this refers to maintenance such as testing, repair etc. A general model for the steady state unavailability of the component is given by the T-book [17]:

$$Q = q_0 + \lambda s \cdot \frac{TI}{2} + (q_t + \lambda_s \cdot TI) \cdot \frac{t_r}{TI} + \lambda_d \cdot t_d + \frac{t_{FU}}{FUI}$$

where

q0 = the probability of time independent failure on demand
qt = the probability of time independent failures at tests (usually qt = q0)
λs = failure rate in standby
λd = failure rate under operation
TI = test interval
FUI = interval between preventive maintenance
tr = active repair time/down time/maximum time for corrective maintenance
td = transient time/operating time/demand time
tFU = maximum time for preventive maintenance

The total unavailability of a component (Q) reflects the probable degradation of individual components in operation and safety systems. Unavailability of a component implies a faulty condition in a system and failure of what we have named DiD Level 1:1 and 2:1. It is possible to separate DiD Level 1:1 and 2:1 in current PSA models if accepting this definition. Data analysis of the two levels could be performed by importance analysis if tagged properly, e.g. manual actions, testing and repair rates are separated from independent failure rates in standby or operation. The importance analysis conveys contributions to a consequence and could be calculated for (RiskSpectrum Theory manual):

- Individual basic events
- Groups of basic events characterised by the same attribute
- Groups of basic events that belong to the same component
- Groups of basic events that belong to the same system
- CCF groups

- Individual parameters

One of the main aims of this project is to propose ways to measure the performance of the DiD Levels with PSA. The gathered measures are presented below and illustrated in Figure 8:

1) Performance over several DiD levels through defined states
    - Relationship between states
2) Performance of a specific DiD Level
    - End state frequency
    - Relationship between the end states
3) Performance within certain DiD Level
    - Interplay between systems
    - Performance of a specific system
4) Performance under certain DiD Level
    - Failure of control activities
    - Failure of components

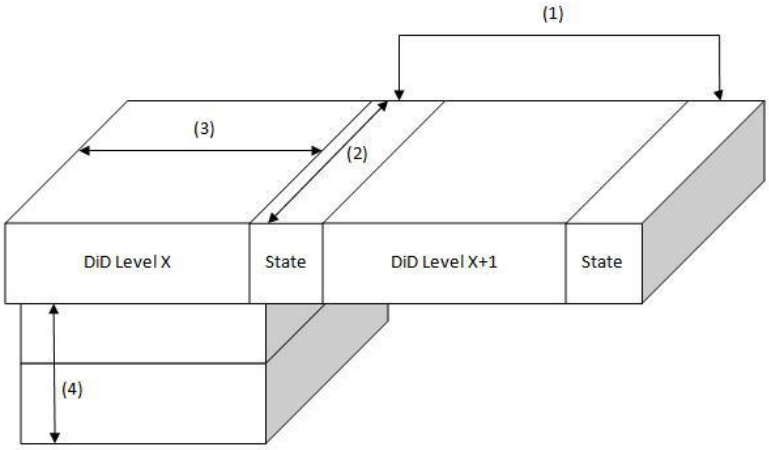

Figure 8. Measures of DiD Levels

6.3 DiD 1:2 – Prevent Abnormal Operation

The first sequential DiD level is 1:2. This means a failure in the operating systems or disturbance in interfaces from the plant to surroundings, e.g. the connection to the grid or via cooling water intake.

Success of DiD Level 1:2 means that normal operation continues uninterrupted without failures and disturbances. The disturbance means that normal operation is challenged; a condition called abnormal operation is entered.

For both DiD level 1:2 success and failure, there are no current PSA parameters that can provide information, with a few exceptions where initiating events are defined as requiring operation control functions (DiD Level 2:2) to operate, e.g. island mode operation in case of loss of offsite power.

As discussed above, the failure defences are:

- DiD 1:1 Prevention of failures
- DiD 2:1 Detection of failures (degradation).

DiD 1:1 and 2:1 for an operating system makes up DiD level 1:2.

However, disturbances and failures and maintenance activities are reported. The number of disturbances and failure events and information about their characteristics (type of equipment, number of failures, repair and replacement times, trends etc) may be used as a measure, both for absolute values and for benchmarking with other plants. See also the discussion in section 6.2 above on evaluating DiD 1:1 and 2:1.

The most straightforward implication to PSA is the quantification of new initiating events that challenge DiD Level 2:2. Data analysis and extended modelling are approaches that can be used to support such evaluation. The appendix to IAEA SS No.46 [13] presents suggestions of relevant areas to investigate. Mechanisms comparable to site seismology, hydrology, extreme meteorological conditions, release of toxic gases, aircraft impact etc. are suggested. Other mechanisms are incorrectly set up safety limits, incorrect operator action and insufficient automatic control etc. PSA encompasses many of the suggested topics today. The quantification of extreme conditions affecting construction and design is often calculated. However, the documents act as framework and summary of provisions and mechanisms of DiD Level 1 which is relevant to investigate if to broaden the scope of PSA.

Failures in construction and control mechanisms are naturally troublesome to investigate and generalize over several plants. Relevant quantitative measures to PSA are suggested to be events that cause abnormal operation control. Contribution of DiD Level 1:1 and 2:1 is then reflected in the aggregated probability of the event.

Table 16: Measures of DiD Level 1:2

Defined measures of DiD Level	Applicable measures to DiD Level 1
Relationship between states	N/A
End state frequency	Event resulting in abnormal operation
Relationship between the end states	*
Interaction between systems	**
Performance of a specific system	**
Failure of control activities	**
Failure of components	**

* To analyze the relationship between the end states of DiD Level 1 requires that all possible end states are known. As the definition of DiD Level 1 has not been used, an aggregated picture of such states is not possible to procure.

** The use of PSA to model the end state requires an initial state which, by definition, is not applicable. The root cause of an event in need of abnormal control operation is a task for deterministic analyses.

It is shown that PSA is not possible to use today in relation to DiD Level 1:2 whereas this require start and end states. The proposed extended modeling should focus on the end states of DiD Level 1:2; events resulting in abnormal operation that need to be controlled by DiD level 2:2.

Listed below are suggestions on where to find end state measures of DiD Level 1:2.

- The occurrence of fires and flooding is calculated in some analyses
- A summary of extreme external events and their consequences on control and safety systems.
- Events resulting in abnormal operation can be identified by investigating the root causes of IEs by the use of e.g. failure reports or events relevant to the definition of H2 and events categorized in accordance to SSMFS 2008:1 Category 3.
- Flow problems in turbine
- Loss of one pump in the main feed water system.
- Area event reports.

6.4 DiD 2:2 – Control of Abnormal Operation

DiD level 2:2 is challenged if DiD level 1:2 has failed.

Success of DiD level 2:2 means that the plant responds to the challenge with the normal operating system's capability to control the situation without need for shutting down – reactor protection limits are not reached - Safety systems are not challenged. Normal operation will thus continue when the

plant is capable of handling the event without need for shutting down – scram or normal controlled shutdown.

Failure of DiD Level 2:2 means a need for shutting down the plant, i.e. the occurrence of what is usually defined as an IE in PSA. The plant response to IEs is activated safety functions and systems. Therefore, DiD Level 2:2 mainly refer to operation system and how they cope with events resulting in abnormal operation.

DiD level 2:2 usually does not have corresponding PSA parameters, even if there might be some PSAs that have modelled functions that, if successful, prevent a demand for the "normal" safety functions – Reactivity control, primary system water inventory control and residual heat removal. It is likely that such events are reported and can be part of PSA applications for risk follow-up exercises.

Normal shutdown with all systems in operation is no challenge to or failure of the Defence in Depth.

The frequency of different initiating events is a measure of the sequential DiD levels 1:2 and 2:2 with respect to the plants ability to avoid that the safety functions in DiD level 3 are challenged.

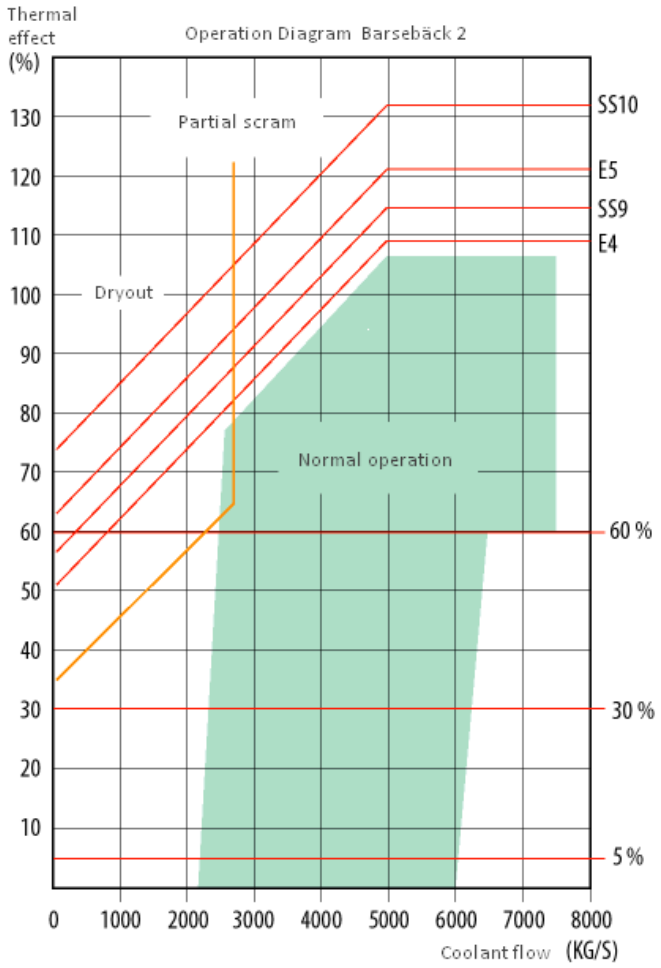

Figure 9. Operation Diagram

According to figure 9, a specific area in the relation of thermal power and coolant flow can be acknowledged as normal operation. Several systems assist in keeping normal operation within accepted limits. Automatic systems are initiated if the process exceeds certain limits (E4, SS9 etc). Another control feature is partial scram. Although the margin to initiate scram (SS9) is slim, there exist certain systems that are designed to control abnormal operation and avoid initiating events (scram).

Additional modelling of control, detection and protection systems that are part of DiD Level 2:2 is required in order to gain knowledge of the performance of this level. Principally two approaches are suggested; to investigate the root causes of an IE or to investigate scenarios and situations of abnormal operation control not included in any IE definition today.

The easiest way to investigate DiD Level 2:2 by utilizing PSA could be to examine the definitions of an IE and try to model the underlying mechanisms. Potential systems of interest are the Balance of Plant (BoP) system and the power control and supply system. The latter have the potential to handle a situation where offsite power is lost by bringing the plant to island mode operation without the need of a scram. Such scenarios are rarely modelled in PSA today. Loss of offsite power, fire and flooding are instead sometimes given a probability to result in an IE by providing an estimate, e.g. that a 60 % of all small fires cause a certain transient. Such generalisations are examples of aggregated estimates of DiD Level 2. Furthermore, a thorough revision of IE definitions is also suggested. In the Nordic countries the definitions of IEs is given in the I-book by the Swedish Nuclear Power Inspectorate (SKI) [16].

The objective of the I-book was to structure, compile and sum up data and knowledge of incidents and other occurrences known as initiating events (IE) at the Nordic nuclear power plants. These IEs are the basis for both modelling and quantification in probabilistic safety analyses (PSA). The grouping of the IEs is structured for PSA purposes to simplify the estimation of IE frequency for each IE-group and nuclear power plant (NPP), based on available operating data from Nordic BWR and PWR plants. In some cases (such as pipe breaks) international data is used [16].

The I-book has not been reissued after its second edition [16]. The reason for this is that the book had by then fulfilled one of its main aims, i.e., to provide a general definition of the IE categories to model in a PSA. The update of IE frequencies is now performed by the utilities themselves. The I-book includes trending for each group of IEs and can thus be regarded as a part of the evaluation of DiD Level 1:2 and 2:2.

The analysis of IEs conveyed in the I-book brings about a certain classification scheme. The scheme refers to effects on both operating systems and safety systems by giving examples of implications of an event to plant systems. Activation, need for restart, affected systems, blocked systems etc. are all examples of implications of an IE. The information is further useful in the forthcoming PSA as well as if to distinguish events in DiD Level 2:2 from DiD Level 3.

Separation of human actions and other causes that lead to the defined IEs is not accounted for in the I-book. However, an estimate is given that approximately 35-40% of all IEs are induced by human errors. The data is instead predominantly gathered from scram reports. A separation of human errors in report systems as well as reports of events not causing any immediate scram is therefore a suggested approach to learn more about DiD Level 2.

Naturally, not all events are considered in the I-book. The authors suggest events that could complement the study reflected by their work, which is to incorporate also the following functions [16]:

- Instrument failure e.g. level control
- Failure of pneumatic support systems
- Failure of nitrogen pressure systems
- Failure of secondary coolant systems
- Loss of deionised water supply tank caused by frost (system 733)
- Dynamic effects caused by pipe breaks
- Events during refuelling outages e.g. incorrectly loaded fuel element

The suggestions given above may constitute examples of when an automatically generated scram is not instantly necessary but instead met by the inherent resilience of the operation systems of the plant. It is therefore arguable that the examples above would serve the definition of DID Level 2:2 if they come to concern control of abnormal operation.

Figure 10 illustrates the difference in DiD Levels by their purpose and the general distinction between operation and safety systems. The figure also describes two methods to start to investigate and model DiD Level 2:2.

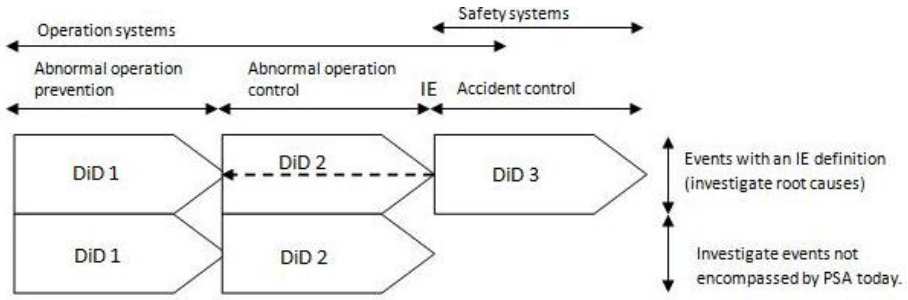

Figure 10. Illustration of DiD Levels and its Context

The control of abnormal operation does not necessarily refer to technical systems. Systems more preventive in nature and therefore more organizational in character also contribute to the strength of DiD Level 2:2, even if these also can be seen as DiD level 2:1. Suggested measures are surveillance and in-service inspection. In the case of a large LOCA there are often detectable leaks before break (LBB). Such indications mainly refer to maintenance (inspection) to be discovered. Control and safety systems require maintenance, test and repair which would serve the definition of DiD Level 2:1 (see Table 5). To quantify successful maintenance of SSCs is of course hard to achieve yet not an impossible task.

In Human Reliabilty Analysis (HRA) the distinction of initiators, pre initiators and post initiators is essential. IAEA 50-P-10 [23] gives the following definition:

Category A – Pre Initiators*: Pre-initiators consist of those actions associated with maintenance and testing that degrade system availability. They may cause failure of a component or component group or may leave components in an inoperable condition (e.g. misaligned valves). Particularly important are actions or errors that result in concurrent failure of multiple trains of safety related systems. These sources of unavailability are added to other contributions at the level of basic component or* system inputs in the fault trees. ([23] p. 11)

The definition of Category A gives the impression that this fairly well complies with the definition of DiD Level 2:2. Actions of Category A degrade control and safety systems by leaving SSCs in an improper state and thereby a faulty condition. From [23] the impression is given that DiD Level 2:2 concern all sequential DiD Levels including itself. The control and surveillance SSCs have a rather straight-forward interpretation and are easily projected to concern all DiD Levels containing technical systems.

IAEA 50-P-10 further gives a definition of Category B as follows:

Category B – Initiators: *These actions contribute to IEs or plant transients. They are generally implicit in the selection of IEs and contribute to their total frequency. An example of an IE caused by human actions is a plant trip following a mistake in a testing procedure. Such events can usually be found in the plant database, but are not always identified as having specific human causes. Because of their identification with an IE they are accounted for by adding contributions to the IE frequencies or by assuming that such frequencies already contain human-caused contributions….([23] p. 11)*

If planning to extend contemporary PSA to comprise events at DiD Level 2:2 too, Category B in HRA definitions would certainly be a source of information.

All in all, to give specific suggestion of potential measures of DiD Level 2 relevant to PSA the following areas are in need of investigation:

- The mechanisms underlying the occurrence of an IE. Input could be reported abnormal operations as a result from both human actions (HRA Category B) and control systems. (Events at DiD Level 1:2)
- The occurrence of events not in need of an instant scram (and the activation of other safety systems). An example is the loss of external power. (Events at DiD Level 2:2)

- Actions that degrade system availability (HRA Category A). (DiD Level 2:1)

Table 17: Measures of DiD Level 2:2

Defined measures of DiD Level	Applicable measures to DiD Level 2
Relationship between states	*
End state frequency	IEs
Relationship between the end states	Relation between IEs
Interaction between systems	*
Performance of a specific system	*
Failure of control activities	*
Failure of components	*

* Possible to calculate but normally not performed today.

6.4.1 Example of Mechanisms that Propagate to an IE

Area events are often modelled in relation to an IE. The occurrence of an area event such as fire is therefore not directly defined as an IE but instead it could initiate an IE. The occurrence of fire is however modelled as an IE, yet it is not included in the definition. Therefore the event of an initiated fire would be relevant to DiD Level 2:2.

Table 18: Fire Example

DiD Level	Success	Failure
1	No fire	Small fire
2	Fire is detected and extinguished	Large fire, automatic or manual scram, degraded safety functions.
3	OK sequences	CD sequences
4	Release Categories below criteria	Release Categories above criteria

A fire is naturally an event in need of control and indeed a failure of DiD Level 1:1 and 2:1 to prevent such events. The models of a fire to spread and to propagate to affect other systems are usually not as extensive as the models of PSA Level 1 and 2. Figure 11 shows an example of such a model.

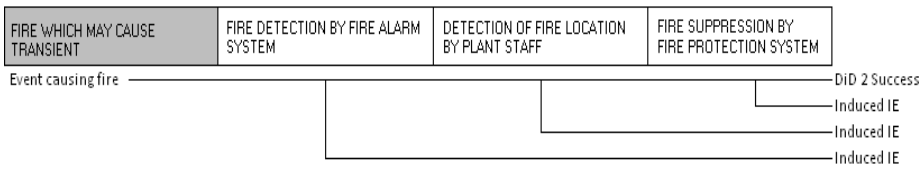

Figure 11. Event tree of Fire which may cause Transient

The model contains information and attributes that enable separation of actions relevant to human actions, repairs and maintenance and the physical systems. Calculation of importance measures of actions or events result in a differentiation of contributions from components, human actions and preventive actions.

Preventive actions such as maintenance and repair are given attributes in the model. The attributes allow for calculation of their importance to the consequence of causing, for example, a transient. The importance measure Fractional Contribution (FC) is an importance measure conveying the contribution in percent of the end state frequency.

Table 19: Result from Importance Analysis of Fire Example

Event Group	FC	RDF	RIF	Sens.	Sens. High	Sens. Low
Sys X + Y	9,45E-01	1,81E+01	4,97E+01	3,74E+00	5,76E-05	1,54E-05
Repair & Maintenance	3,90E-01	1,64E+00	4,97E+01	1,73E+00	4,07E-05	2,35E-05
Manual action	2,00E-03	1,00E+00	1,20E+00	1,00E+00	2,93E-05	2,92E-05

The importance measures calculated by RiskSpectrum PSA are Fractional Contribution (FC), Risk Decrease Factor (RDF) and Risk Increase Factor (RIF). RDF and RIF displays the result if to set the basic event group to either true or false (Frequency 0 or 1). The importance measures complement the MCS-list by indicating how important each basic event group is.

"Sens. High" and "Sens. Low" is display the result when an event group frequency is either increased or decreased by a factor 10. "Sens" is the ratio of "Sens. high" and "Sens. low". "Sens." indicates how sensitive the mean unavailability is to changes in the failure probability of each basic event.

6.5 DiD Level 3 – Prevention of Core Damage

Note that the strength of DiD level 3 (and 4 and 5) are depending on the strength of DiD level 1:2 and 2:2.

Also note that there may be failed components in safety systems being part of DiD levels 2-4, and thus safety systems may be degraded, e. g. a failure in a standby safety system, without need for shutting down. A special situation is a need to shut down the plant due to Technical specification restrictions. Such situation mean that DiD level 1:2 and 2:1 have failed - a failure exist. However, it is no failure of DiD 1:2, and thus operation continues. Normal shutdown of the plant due to Tech. Spec restrictions or due to minor disturb-

ances is no initiating event. Something extra needs to occur during the shutdown in order for an initiating event to show up and challenge safety systems.

DiD level 3 is challenged if DiD level 1.2 and 2.2 have failed. This usually implies the occurrence of an initiating event.

Success of DiD level 3 means that core damage is avoided, e.g. OK end states from a fuel damage point of view. This may include some overpressurization end states with successful cooling. The OK sequences are a mixture of sequences where all success criteria for functions in the model are met, and sequences where some criteria may not have been met, but still the result is that no core damage occurs. The OK sequences with certain degradation may be of interest to investigate further with regard to the remaining DiD barrier.

Failure of DiD level 3 means a situation with core damage, which is the end state of primary interest in a level 1 PSA. Thus, PSA level 1 parameters can be used to characterize and measure DiD level 3 and the three sequential levels 1:2-2:2-3.

The typical preventive measures in DiD Level 3 are the functions designed to safely shut down the plant when called upon. Active and passive engineered safety systems are used. In the short term, safety functions are actuated by the reactor protection system (RPS) and/or the emergency safety features actuation system (ESFAS) when needed.

The activation part can be interpreted as including both the technical systems, and the monitoring and control systems and emergency features actuation systems that will make the plant respond appropriately given a specific accident scenario.

Table 20: Measures of DiD Level 3

Defined measures of DiD Level	Applicable measures to DiD Level 3
Relationship between states	Contribution from IEs to specific PDS
End state frequency	Core Damage
Relationship between the end states	Relation between CD and Sec. Line of defense
Interaction between systems	Sequence frequencies
Performance of a specific system	System FT top events
Failure of control activities	*
Failure of components	*

* Possible to calculate. An example is given in section 6.4.1.

6.5.1 Sequence Frequencies

A sequence is a specific path in an ET. A sequence analysis gives information on the contribution to the degradation of a DiD Level in terms of identifying important event chains or paths. Sequence analyses are applicable for both PSA Level 1 and 2 and therefore give information to DiD Levels 1-3 and 1-4.

The examples in this report consider sequences in Level 1 PSA and for only one IE. The amount of sequences to consider if taking all IEs into account will grow considerably, especially if incorporating Level 2 PSA sequences as well.

The analysis could be further extended by studying the conditional probability for a sequence to occur given that the IE occurs. The conditional probability gives information of the relative importance of a specific sequence. The conditional probability is a measure of the analysis case, i.e. the barrier of PSA Level 1 (DiD Level 3).

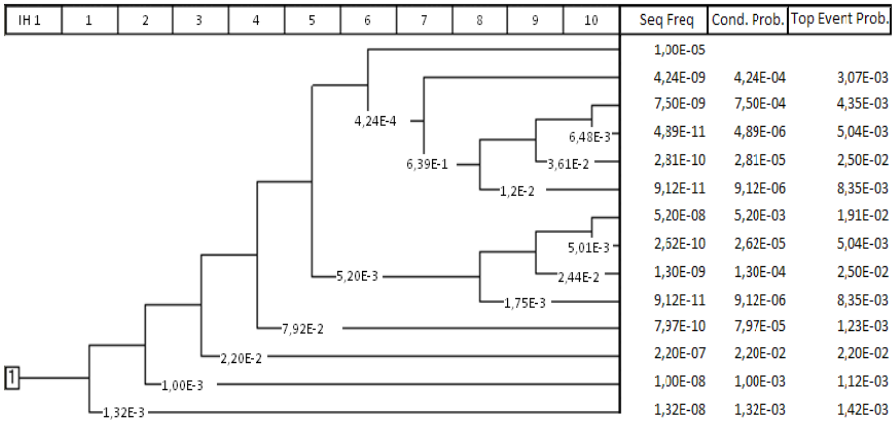

Figure 12: Event Tree with Split Fraction Probabilities

Furthermore, if sequence calculations are made, it is possible to calculate split fraction probabilities, given that all sequence results are available with sufficient accuracy. The split fraction probability in an ET is the conditional probability of a specific safety function to fail. The split fraction probabilities can provide further insights into the remaining barrier in each branch point. The split fraction probabilities are interesting because they will convey information about dependencies when compared to unconditional system fault tree top event probabilities. Figure 12 shows the frequencies of each sequence. If dividing the end state frequencies by the frequency of the IE (IE 1) the result is the conditional probability of that sequence to occur. The split fraction probability conveys the probability of system 1-10 to fail with account taken for the previous systems as well as the IE (IE=1).

Note that whole sequence usually is calculated without considering a specific timing of events. The whole sequence contains failed or successful events also after a specific node. However, split fractions can still provide some additional information on the independence between functions and DiD levels.

6.5.2 Core Damage and Relationship to Second Line of Defence

The CD frequency is traditionally displayed both in terms of total CD from all the contributing IEs but also as the frequency of specific PDSs (in case of a level 2 PSA). The frequency provides information about the strength of DiD Level 1-3.

The second line of defence is here defined as the functions having the potential to recover failure sequences to OK sequences. An example for a PWR is when the first line of defence, the auxiliary feed water system fails, and feed-and-bleed operation can be used to cool down the reactor.

The numbers in Table 21 demonstrate additional information. The CD frequencies are given in relation to a specific IE. The conditional probability will provide information about DiD level 3 specifically; what is the probability that a certain IE will propagate to CD?

Table 21: Results for Second Line of Defence.

IE	*CD*	*Second Line of Defense*	*Cond. Prob. CD*	*Cond Prob. Sec. Line of Defense*
L1	2,51E-07	7,18E-08	2,51E-02	7,18E-03
L2	2,52E-06	1,25E-06	5,73E-03	2,84E-03
L3	1,47E-06	1,94E-05	1,13E-03	1,49E-02
L4	1,87E-07	1,73E-06	9,84E-05	9,11E-04
T1	1,23E-07	7,90E-05	3,54E-06	2,28E-03
T2	4,29E-07	3,94E-04	1,37E-06	1,26E-03
T3	1,56E-06	2,18E-03	4,08E-06	5,71E-03
T4	1,84E-06	4,58E-02	2,45E-05	6,11E-01
T5	2,90E-08	8,43E-07	2,93E-05	8,52E-04
T 6	1,01E-09	5,88E-07	2,53E-05	1,47E-02
T 7	7,00E-09	4,42E-06	1,75E-05	1,11E-02
T 8	6,13E-07	3,00E-03	2,04E-04	1,00E+00
T 9	9,38E-07	9,10E-07	2,35E-02	2,28E-02
T 10	1,47E-06	4,43E-06	3,68E-03	1,11E-02

Table 21 also gives numbers on what is called (in this report), the second line of defence. When an IE occur one system may fail to perform its intended function but instead of an immediate CD, other systems can retain the

fuel integrity and give sequences ending in acceptable plant states. Sequences can be divided into at least three categories:

- OK/OK: The single sequence (usually one single sequence) where all functions are successful. The sequence will have a conditional probability close to 1.
- OK/Failure: The sequences where some success criteria are not met, yet other functions take care of the situation and CD end states are avoided.
- CD: The sequences leading to CD.

The relation between the gathered sequences ending in CD and the sequences ending in OK states with a certain degradation of system functions are displayed in figure 13. From the figure it is possible to compare the sum of frequencies leading to CD and sequences with at least one system failure. A sequence where also the second line of defence systems is strong imply higher robustness of the configuration of safety systems in DiD Level 3

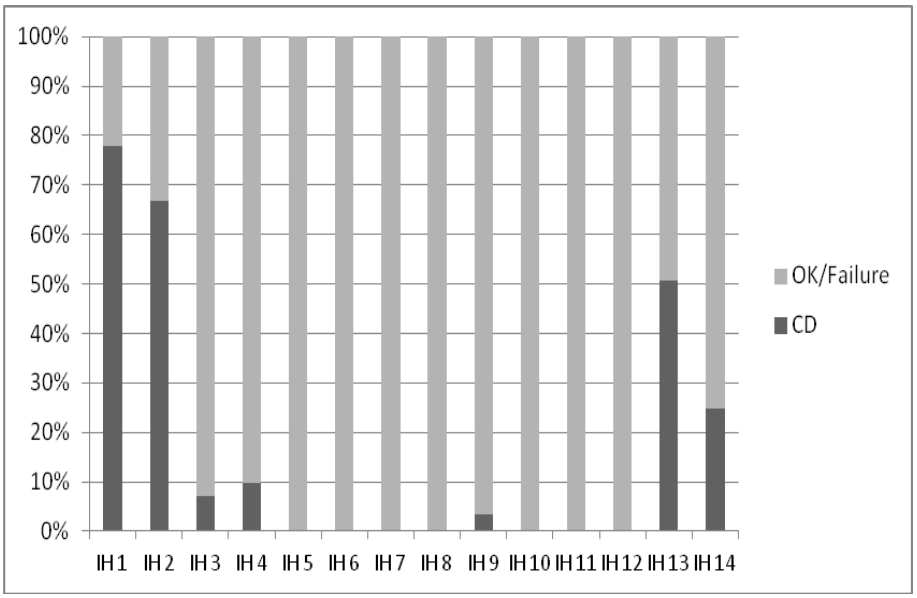

Figure 13: The relation between the sum of CD sequences and the sum of OK/Failure sequences

The frequencies and the corresponding conditional probabilities of second line of defence sequences, demonstrated in Table 21 are appealing to interpret as the strength of DiD Level 3 given that at least one system has failed. This is true if systems and functions are understood as entities to either fail or function. However, this is obviously not an accurate description of systems which may exhibit several faulty conditions and still be operable and thereby give sequences ending in OK/OK sequences. As systems in contemporary NPPs are constructed with several redundancies and success of less than all is enough (e.g. the success criteria is operation of two out of three

accumulators or two out of four spray pumps). Hence, frequencies of OK/Failure sequences are to a great extent dependent upon the model and what is encompassed by a system and function definition.

6.5.3 Contribution from IEs to Specific PDS

It is possible to extend the discussion about DiD Level 3 further. Usually, as mentioned above, the calculations may only take the total CD frequency into consideration. However, it is possible to split the term CD into smaller fragments, e.g. using the plant damage states defined in a level 2 PSA. Definitions of PDSs are related to specific attributes like the initiating event and what system have failed or operated in the sequences. From the perspective of legislation and safety goals it is often not interesting to separate the PDSs as they all contribute to the frequency of core damage and radioactive release. On the other hand, from a DiD Level perspective it is interesting to obtain an elaborated picture of possible and relative contributions to states of the plant. Measures of the contributions of all IEs to specific PDSs can provide a better basis for decision making.

Figure 14 displays results from calculations of the contribution of specific IEs to PDSs. The figures are the conditional probabilities of a PDS given the IE. Displaying the results graphically, with conditional colour formatting, provides for fast and intuitive interpretation of the results.

IE / PDS	IE 1	IE 2	IE 3	IE 4	IE 5	IE 6	IE 7	IE 8	IE 9	IE 10	IE 11	IE 12	IE 13	IE 14
PDS 1	2,51E-02													
PDS 2									3,08E-04					
PDS 3									2,55E-03					
PDS 4									3,88E-05					
PDS 5		6,05E-03	1,79E-02	1,09E-03	2,05E-03		1,24E-02		1,71E-06					
PDS 6			1,27E-01	1,74E-02	2,37E-03		1,45E-02							
PDS 7			1,75E-04	1,65E-05	4,05E-07		1,02E-05							
PDS 8		1,92E-01	5,83E-04	1,21E-04	1,18E-06		1,18E-05							
PDS 9		5,66E-02	1,67E-03	1,38E-04	1,96E-05		1,27E-04							
PDS 10			1,03E-04	6,54E-06	4,88E-07		5,31E-06							
PDS 11			2,26E-05											
PDS 12			2,05E-04	4,74E-05	3,69E-06		3,60E-05							
PDS 13					8,17E-03	1,69E-03	3,44E-02	5,44E-03	2,39E-03	1,66E-04	3,45E-05	5,72E-03	2,27E-02	1,63E-04
PDS 14					4,33E-04		1,16E-03	7,15E-03		1,09E-05	5,72E-04	5,04E-02		7,04E-05
PDS 15					3,53E-07	6,32E-04	7,99E-05	2,77E-04						
PDS 16												1,80E-07		
PDS 17					4,33E-04	0,00E+00	4,37E-03	7,15E-03					1,62E-04	
PDS 18					6,91E-03	4,04E-02	0,00E+00	1,30E-02		1,31E-05	1,06E-05	1,11E-03	9,36E-02	1,47E-01
PDS 19					2,66E-05	3,80E-05	5,80E-03	8,61E-08		1,17E-05	1,01E-05	2,06E-03	4,40E-05	1,11E-05
PDS 20					2,78E-05	1,75E-04	2,67E-04	1,02E-06		4,77E-07	7,00E-05	5,52E-04	1,07E-05	7,02E-05
PDS 21								8,82E-07						

Figure 14. The Conditional PDS Probability (state of CD) given a Specific IE

6.6 DiD Level 4 – Mitigation of Release

DiD level 4 is challenged if DiD level 1:2, 2:2 and 3 have failed. This means the existence of fuel damage sequences.

Success of DiD level 4 means that the consequence mitigating procedures and systems are successful. This does not necessarily mean that a release to the environment is completely avoided, since any fuel damage sequence will result in a radioactive release.

Failure of DiD level 2 is usually expressed as a severe plant condition with a frequency above a level that is accepted. The definition of failure and the accepted frequency varies between different countries.

The different PSA level 2 end states represent a spectrum of different magnitudes of success or failure of DiD level 4. The release sequence frequencies and the conditional probabilities of release given the initiating event or a plant damage state can provide insights into the characteristics (strengths and weaknesses) inherent to DiD level 4.

Table 22: Measures of DiD Level 4

Defined measures of DiD Level	Applicable measures to DiD Level 4
Relationship between states	Contribution from IEs via PDS to RCs Contribution from IEs to RCs
End state frequency	RC frequencies*
Relationship between the end states	Relationship between RC*
Interplay between systems	Sequence frequencies*
Performance of a specific system	System FT top events*
Failure of control activities	*
Failure of components	*

* The measures coincide with DiD Level 3 and are therefore not presented again here.

PSA Level 2 corresponds to a release frequency and thereby to DiD Level 1-4. The radioactive release in case of a PDS is further divided into release categories which are built on information of the time to release and the fraction of discharged particles, etc. Success of DiD Level 4 does not necessarily mean that no radioactive release occurs but that the mitigating procedures and systems are successful; which are reflected by the definitions of release categories.

The traditional measure of PSA Level 2, and thereby DiD level 1-4, are given by the release category (RC) frequencies. It is then possible to incorporate either all IEs or only specific ones. Figure 15 reflects the conditional probability of release categories given a specific IE which give information about DiD Level 3 to 4 together meaning that the contribution from all possible PDSs is accounted for.

IE / RC	IE 1	IE 2	IE 3	IE 4	IE 5	IE 6	IE 7	IE 8	IE 9	IE 10	IE 11	IE 12	IE 13	IE 14
RC1	1,54E-04	8,09E-06	4,10E-06	3,65E-07	8,39E-09	2,16E-09	1,21E-08	5,29E-09		2,00E-08	2,35E-06	2,27E-07	1,46E-05	2,19E-06
RC2	8,79E-06	6,55E-07	2,00E-07	4,14E-09	1,75E-09	9,81E-10	3,25E-09	9,36E-10			1,23E-06	5,73E-08	6,85E-06	1,06E-06
RC3	3,41E-04	1,86E-05	8,92E-06	7,26E-07	8,39E-09	1,95E-09	1,66E-08	6,33E-09		1,73E-08	1,53E-06	2,20E-07	8,03E-06	1,24E-06
RC4		2,50E-06	1,25E-08	1,30E-08	8,53E-09	3,80E-09	1,31E-08	5,33E-09	3,28E-07	2,68E-08	6,00E-07	1,33E-07	7,15E-06	4,43E-07
RC5									1,47E-06					
RC6									2,46E-06					
RC7	2,33E-06	9,93E-07	6,53E-07	4,92E-08	5,62E-09	2,73E-09	1,39E-08	4,88E-09		1,85E-08	1,03E-07	1,18E-07	8,93E-08	3,25E-08
RC8	2,98E-04	1,43E-05	7,29E-06	4,97E-07	8,73E-09	2,19E-09	1,27E-08	4,52E-09			5,40E-06	3,67E-07	3,20E-05	4,93E-06
RC9	1,42E-06	6,39E-07	4,28E-07	2,33E-08	3,52E-09	1,76E-09	9,06E-09	3,13E-09		1,24E-08	6,58E-08	7,70E-08	2,02E-08	1,54E-08
RC10	4,47E-04	2,18E-05	1,11E-05	8,16E-07	1,51E-08	3,48E-09	1,99E-08	7,73E-09		1,03E-08	8,05E-06	5,70E-07	4,93E-05	7,55E-06
RC11	6,13E-03	3,34E-04	1,68E-04	1,68E-05	1,82E-07	2,55E-08	2,72E-07	1,40E-07	4,11E-10	6,35E-07	1,59E-05	3,73E-06	9,70E-05	1,51E-05
RC12	1,81E-04	8,09E-05	4,81E-05	8,37E-06	5,50E-07	2,19E-07	1,03E-06	4,13E-07	5,41E-09	2,70E-06	7,33E-06	8,80E-06	3,03E-05	6,23E-06
RC13	4,08E-03	2,22E-04	1,12E-04	1,13E-05	4,03E-07	1,07E-07	4,90E-07	2,48E-07	1,55E-10	8,55E-07	1,11E-04	9,57E-06	7,40E-04	1,13E-04
RC14	1,96E-02	1,02E-03	5,04E-04	5,13E-05	1,23E-06	1,85E-07	9,50E-07	7,17E-07	0,00E+00	3,95E-06	4,10E-04	3,19E-05	2,80E-03	4,23E-04
RC15		4,84E-05	4,50E-06	2,06E-07	4,15E-08	9,94E-09	1,83E-08	2,13E-08		1,03E-08	3,68E-05	1,89E-06	2,35E-04	3,68E-05
RC16		7,27E-05	6,76E-06	3,18E-07	6,25E-08	1,50E-08	2,75E-08	3,25E-08		2,80E-08	5,53E-05	2,84E-06	3,53E-04	5,53E-05
RC17		4,73E-03	4,45E-04	2,26E-05	4,27E-06	9,84E-07	1,84E-06	2,25E-06	4,03E-09	9,88E-06	3,58E-03	1,85E-04	2,27E-02	3,58E-03

Figure 15. The Conditional RC Probability given a Specific IE (all PDS accounted for)

6.7 DiD Level 5 – Mitigation of Release Consequences

DiD Level 5 is challenged if DiD level 1, 2, 3 and 4 have failed which imply the existence of a radioactive release to the surrounding environment.

Success of DiD Level 5 does not necessarily mean that the release will not result in any fatalities or cancer cases. Success of DiD Level 5 means that consequences of release to the environment in terms of fatalities and cancer are minimized. All release sequences are a spectrum of threats to the community with various release amount and release times etc.

Considering this, it is indeed not until DiD Level 5 that the economic, environmental and effects to human lives are analyzed. Conversely, DiD Level 1-4 presents measurable plant states which are analyzed and given frequencies which to a great extent is different from the universal definitions of risk. The resulting analysis of PSA Level 3 end states are though applicable to an authentic risk definition which convey both a frequency and a consequence to property, human lives or the environment by the product of those.

PSA level 3 results in terms of frequencies of late and early fatalities and cancer cases, and conditional probabilities given the initiating event, a plant damage state or a release category can provide insights into the characteristics in terms of strengths and weaknesses in DiD level 5. PSA Level 3 has not been performed in Sweden except for minor pilot studies.

A radioactive release implies either on-site or off-site consequences. Principally, PSA Level 3 is associated with the long and short term off-site effects from airborne radioactive materials. One of the main aims in PSA Level 3 studies is to illuminate and quantify countermeasures e.g. restricted consumption, successful evacuation and intake of iodine tablets etc. The quantification of countermeasures and their effects to third party is highly dependent on time to release such as Large Early Release Frequencies (LERF) and weather conditions. Chernobyl is an example of large and early releases on top of weather conditions allowing for high plume rise resulting in long distance effects.

The use of PSA makes possible ranking from potential benefits of various countermeasures for the emergency response planning analogous to other DiD Levels. A generalized analysis of the countermeasures correspond to regular risk reduction factors or risk mitigation factors in the presence of a particular plant condition. This further implies that the end states of DiD Level 4; the set of RCs, may need clarification in terms of relevant plant conditions which could affect the analysis of DiD Level 5. Such extensions are often made between PSA Level 1 and 2 where PDS convey more information relevant to PSA Level 2 than the first definition of just CD.

In contrast to PSA Level 1 and 2 it is argued that a PSA Level 3 could be carried out independently due to its fundamentally different premises of how to conduct the analysis [24]. The use of FTs is thought not to prove relevant due to the fact that technical systems do not take part directly in the mitigation of consequences. According to IAEA-TECDOC-832 (1995) [24], a PSA Level 3 analysis shall convey countermeasures and accident sequence ranking which probably would call for ET usage. In addition, simulations of for example weather conditions, plume rise and long term environmental effects require knowledge and theory different from regular PSA studies. Taken together the conclusion becomes that much, but not all, is different in PSA Level 3 studies. Compared to the framework for how to evaluate DiD (section 6.5) most of the suggested measures are general enough to apply also to DiD Level 5. Still, quantitative measures from one state to another holds, sequence analysis is relevant and relationship between end states (scenarios resulting in disparate numbers of fatalities) become highly important.

Table 23: Measures of DiD Level 5

Defined measures of DiD Level	**Applicable measures to DiD Level 5**
Relationship between states	Contribution from IEs via PDS to RCs and their eventual effects to society. from IEs to RCs
End state frequency	Fatalities per year in relation to time to release, long/short term effects and off/on-site effects.
Relationship between the end states	Relationship between scenarios considering economic or human effects
Interaction between systems	The effect of different countermeasure
Performance of a specific system	The reliability of countermeasures
Failure of control activities	*
Failure of components	*

* The contribution from components will have very low impact and the variety of context will prove hard to capture in regular models. Therefore, measures at very low system level will probably prove irrelevant.

7. Safety Goals – Risk Criteria

Discusses risk criteria and possible interpretation for the Defence-in-Depth.

The PSA results actually measure the strength of the sequential DiD levels in terms of frequencies and conditional probabilities. These frequencies and probabilities in turn reflect the strength of the failure defence for each sequential DiD level.

Usually DiD level 2:2 (control of abnormal operation) is not modelled separately. It is represented by the initiating event frequency, which is the result of a failure in an operating system, and the plants capability to take care of this event without shutting down, i.e. DiD level 1:2 and 2:2 together. However, as already discussed, it is possible to introduce the DiD level 2:2 functions also in the PSA, thus allowing explicit consideration in the analysis.

A summary of existing and potential PSA measures of DiD levels are presented in Table 24.

Table 24: Summary of Probabilistic Measures for DiD Levels

DiD level 1-5	PSA level 3 – Society risk (fatalities and cancer)
DiD level 1-4	PSA level 2 – Source term frequencies
DiD level 1-3	PSA level 1 – Core damage frequency
DiD level 1-2	PSA Initiating event (?)
DiD level 5	Conditional probability of society risk given release
DiD level 4	Conditional probability of release given core damage
DiD level 3-4	Conditional probability of release given IE
DiD level 3	Conditional probability of core damage given IE
DiD level 2:2	Conditional probability of IE given abnormal operation
DiD level 1:2	Frequency of abnormal operation – Frequency of failures of normal operating equipment
DiD Level 1:1 and 2:1	Dependability of components in terms of the original quality and quality of surveillance/maintenance activities – represented by failure data – data investigation can identify the root causes and what went wrong.

The absolute frequencies (CDF, LRF) represents a measure of all DiD levels (1:2-3, 1:2-4, 1:2-5)

The conditional probabilities represents a measure of a single DID level or a set of DiD levels, e.g. DiD level 3 is the conditional probability of core damage given the initiating event.

The strength of each level is different, i.e. they do not have the same strength, as may be interpreted as a deterministic requirement according to section 2.2.

One interesting area is to compare safety goals with the measures that are calculated and presented in a PSA. There are general high level goals on core damage frequency or unacceptable release, and also general requirements on having a risk profile with no dominating weaknesses. The frequencies and conditional probabilities for end states in the PSA model and for individual sequences provides information on the DiD levels' contribution to the probabilistic defence against risk. However, there are currently few Swedish risk criteria on lower levels, e.g. the allowed contribution to risk from a single initiator, a single sequence except – "there shall be no dominating weaknesses".

Top level safety goals are usually defined on a high level, such as acceptable risk or acceptable risk contribution from a certain activity. This risk can be expressed for the community as a whole or as an individual risk.

Over the years, PSA safety goals have been defined for the core damage frequency and the release frequency. These are in turn based on high level risk minimizing goals that are or should be in correspondence with other man made or natural societal risks, but usually also takes into account risk psychology. The exact definitions of safety goals in PSA have varied between different countries and over time. The validity of safety goals project [25] provides a good overview of safety goals, both for nuclear risks but also a comparison with other risks, and their interpretation.

The different safety goals are defined in terms of a statement about the characteristics of a damage state and a frequency level which is seen as the target (to be below) or sometimes also the allowed upper limit.

Typical quantitative safety goals in Sweden (but not stated by SSM) are:

- For core damage frequency – less than 1E-5/y.
- For large release frequency – less than 1E-7/y (or 1E-6/y).

A screening criterion often used in the initiating events analysis is 1E-7/y. Events below this frequency are screened out.

The safety goals discussed above are subsidiary or surrogate criteria that are based on definitions on acceptable societal and individual risk.

It is obvious that the high level safety goals for core damage and release also define goals for the defence in depth. It is also possible to derive goals for

the different DiD levels and some comments for each level are given in Table 25.

One possibility is to use the event categorisation as presented in section 4.2 making a reference between the plant condition (PC) frequencies that are linked to DiD levels and to PSA. In principle, events belonging to a certain event class should have a remaining barrier so that a higher order event class frequency criterion is met. However, this is not elaborated further here. A paper by Irina Kouzmina (IAEA) at PSA11 [26] presented ideas on linking event classes to DiD levels and risk criteria.

Table 25: Comments on Possible Risk Criteria for DiD levels

DiD level 1:2 and 2:1	These levels correspond to the reliability of individual components as well as design of individual systems with regard to use of redundancies and defences against different dependencies. The reliability of functions and systems that makes up the other DiD levels needs to be adjusted to the overall goals.
DiD level 1:2	This level correspond to the frequency of disturbances in operating systems challenging DiD level 2:2. The design is built on plant condition frequencies related to defence-in-depth.
DiD level 2:2	This level corresponds together with 1:2 usually to the initiating event frequency. A measure is thus the IE frequency. This cannot be assessed in general terms but needs to be assessed for each initiating event. DiD level 1:2 and 2:2 need to have the strength (resilience) needed for the plant to have an even risk profile. Any safety goal for DiD level 1:2 and 2:2 needs to be combined with the safety goal for DiD level 3 and 4.
DiD Level 3	Failure of DiD level 1-3 corresponds to the core damage frequency. The conditional core damage probability is an assessment of DiD level 3 alone. Thus, the safety goal for the core damage frequency provides a goal for DiD level 1-3. Taking into account the initiating event frequency, it also allows an assessment of DiD level 3 alone per initiating event, by studying the conditional core damage probability given the occurrence of a specific initiating event.

DiD Level 4	Failure of DiD level 1-4 corresponds to the release frequency. The conditional release probability can be seen as an assessment of DiD level 4 alone. Thus, the safety goal for the release frequency provides a goal for DiD level 1-4. Taking into account the initiating event frequency, and the core damage frequency, it also allows an assessment of DiD level 4 alone per initiating event, by studying the conditional release probability given the occurrence of a specific initiating event and plant damage state.
DiD Level 5	PSA level 3 results can be used to measure DiD level 1-5 or level 5 alone. However, PSA level 3 is not performed in Sweden and thus PSA results cannot be used to measure DiD level 5 in Sweden.

Table 26: Linking Event Classes to PSA and DiD levels

Event Class	**Frequency(f) (year)**	**DiD level**	**PSA**	**Description**
H1	-	1, 2	No	Normal operation
H2	$f \geq 10^{-1}$	1, 2, 3	Yes	Anticipated events
H3	$10^{-1} > f \geq 10^{-2}$	3	Yes	Unanticipated events
H4	$10^{-2} > f \geq 10^{-4}$	3	Yes	Improbable events including DBA
H5	$10^{-4} > f \geq 10^{-6}$	4,5	Yes	Highly improbable events, basis for design of severe accident mitigating systems

8. Procedure for DiD Evaluation

Outlines the way of evaluating DiD levels for an existing plant, in case of plant changes and for impact from operational events. Some comments on the requirements on a PSA and PSA tool to support DiD-PSA evaluation and interpretation are also given.

8.1 Plant and Event Evaluation

In Chapter 6 the proposed measures of DiD Levels are explored by the use of an existing PSA model.

Essential to an investigation of the strength of the existing plant is to agree that it is not possible to formulate an aggregated value of the strength of a certain DiD Level. Instead the strength of a DiD Level is always to be formulated in relation to a specific event. The event can in turn propagate to new measurable end states hopefully proven to have a lower frequency.

The investigation of the propagation through end states is possible to display over several levels which in turn allows for traceability of weak DiD Levels. From figures and tables it is easy to distinguish weaknesses (and strengths) over DiD levels.

From this overview a selection of interesting events and states are made which are to be evaluated by measures within a certain level. Sequence analysis and fault tree top events will serve as measures of relevant propagating paths. Next lower level is to investigate the relevant events or failures within a certain fault tree. It is here possible to evaluate either the design (by the availability of the components) or the control in terms of maintenance, repair and human actions referring to DiD Level 1:1 and 2:1. Many PSA models hold this classification of attributes to SSC as standard. The proposed measures are therefore easy to calculate by performing importance analysis.

According to Fleming and Silady (2002) [22] it is possible to formulate a general model for describing an accident sequence in terms of the design features. Those features are separated by their character that either support prevention or mitigation of a certain event. The sequence model is organized to first identify the response of each active and passive feature by noting which systems and structures are successful and which are postulated to fail along a given accident sequence. The simple model for estimating the frequency of a release of radionuclides associated with a specific sequence could be written as follows.

$$R_j = QF_{IE}P_{Active\ SSC,j}P_{Passice\ SSC,j}r_{fuel,j}r_{PB,j}r_{cont,j}$$

R_j is the expected quantity of radioactive material released per year from sequence j;

Q, the quantity of radionuclides (for a given isotope) in the reactor core inventory;

F_{IE} , the frequency of the IE associated with sequence j;

$P_{Active\ SSC,j}$ the probability of the successful and failed active SSCs along sequence j;

$P_{Passice\ SSC,j}$ the probability of the passive structure successes and failures along sequence j;

$r_{fuel,j}$, the release fraction from the fuel, given system and structure response for sequence j;

$r_{PB,j}$, the release fraction from the PPB, given system and structure response for sequence j;

$r_{cont,j}$ j is the release fraction from the confinement, given system and structure response for sequence j.

Each probability on the right hand side of this equation depends on the events that precede it along the sequence as would be included in a competent PSA model. The partitioning of the risk into these specific terms is designed to support an evaluation of specific strategies for preventing and mitigating the risk of accident.

The analysis cases run in this project take a slightly different approach than calculating the release of radionuclides separately. Instead RCs are used which hold the same information but grouped as consequences. Indeed, by rearranging the formula above this could be used to display the logic of DiD Levels only using frequencies, and put the information of released radionuclides in the definition of RCs. The left hand side of the equation would then be the probability of a sequence to end in a specific RCj. The left hand side assigns a specific IE which is affected by several SSCs contributing to the sequence by its probability to perform its intended function.

$$RC_j = F_{IE}\prod_{SSC\,l} P_{j,l}$$

Whereas the calculations in RiskSpectrum use PDS as an intermediate state, this information could be used as the sum of all sequences ending in that particular PDS. From a particular PDS the sum of sequences relevant to a RC is further dependent on both that particular PDS and the end state (RC).

$$RC_j|PDS_i = F_{IE} \sum_{Sequence|PDS_i} \left(\prod_{SSC\,l} P_{i,j,l} \right) \sum_{Sequence|RC_j,PDS_i} \left(\prod_{SSC\,l} P_{i,j,l} \right)$$

The formula above displays the strength of DiD Level 3-4 given a specific event. The probability of active and passive SSCs could instead be assigned SSCs relevant to a specific DiD Level. Using a specific example from the calculations performed in this project it is possible to give numbers of each level as well. Each level would then give the risk reduction factor relevant to one particular IE.

$$RC_1|PDS_1 = F_{IE\,1} \sum_{Sequence|PDS_1}^{DiD\ Level\ 3} \left(\prod_{SSC\,l} P_{1,1,l} \right) \sum_{Sequence|RC_1,PDS_1}^{DiD\ Level\ 4} \left(\prod_{SSC\,l} P_{1,1,l} \right) = 1E^{-5} * 2{,}51E^{-2} * 4{,}93E^{-3} = 1{,}24E^{-9}$$

The example (figures above are for illustrative purposes) is an illustration of the strength of each DiD Level which is easily extended to DiD Level 2 as well, given appropriate PSA models exist. The frequency of the initiating event is to be interpreted as the strength of previous DiD Levels together i.e. DiD Level 1 and 2.

Results can be compared with event class frequencies and other risk criteria.

Evaluation of Plant Changes

The same approach is used as for evaluation of existing DiD levels. Results are compared before and after plant change. Similar tables can be used to show the results, both absolute and conditional values before and after change, and also the relative change in results in each cell.

Evaluation of Events

A Risk Follow-up analysis can be used to evaluate events. A research project on risk follow-up analysis methodology and possible harmonisation in the Nordic countries is reported in [27]. The approach is similar to what is presented above, yet the models are updated to reflect the occurred event scenario in the same way as in a risk follow-up application. A comparison is made of the results from the two cases: 1) without the event 2) with the event.

8.2 Requirements on PSA and PSA tools

As discussed in the previous sections, it is possible to use PSA or PSA inputs to evaluate the different DiD levels and make judgements on their strengths and weaknesses. In some cases it is needed to add new models, especially for systems representing failure of control of abnormal operation. Reporting and event evaluation may also add deeper insights into the Defence-in-Depth.

A PSA to be used in the process of evaluating the defence-in-depth should be of sufficient scope and follow current state of the art in PSA technology. A full scope PSA including all operational modes and events (i.e. internal initiating events caused by component failures and human errors, internal hazards, and external hazards) is usually required. Level 1 PSA is needed to assess compliance with DiD Level 3 and specify requirements for reliability parameters, and Level 2 PSA is needed to evaluate compliance with DiD Level 4. A quality PSA complies with contemporary PSA standards like ASME/ANS PRA Standard [28] and IAEA Safety Guides on PSA [29], [30].

The impact from less than full scope, or other limitations relative to the quality requirements addressed in the above-mentioned standards need to be discussed when an evaluation is made.

In addition to quality, DiD evaluation is supported by the way of presenting results, and then the way PSA tools are supporting a DiD-PSA presentation of result.

All the proposed measures of how to quantify DiD are possible to calculate by use of RiskSpectrum. However, no advanced support exists to collect and aggregate results.

In general, additional tools e.g. Excel are needed to perform this sort of calculations. If considering consequence analyses of PSA Level 2 there are usually thousands of analyses cases presented. To present results containing several analysis cases it would be useful to enable attributes to be assigned to consequence analysis cases. The aggregation of results would then follow a more intuitive interpretation and, in turn, the results could be processed faster.

An informative presentation of results is very useful in revealing the strengths and weaknesses in the DiD levels. This is of course limited to the DiD Levels where the PSA results can provide information. It is possible to extend the functionality in RiskSpectrum to present results graphically.

Use of tables where the contribution from IEs and conditional probabilities can be shown side by side and combined with colour marking for defined levels will emphasize strong and weak areas. Extending the consequence

analysis cases by optional attributes information relevant to certain DiD Levels could easily be aggregated and analysed.

Attributes can be added to every SSCs represented in the PSA model and indicate the possible DiD level that the SSC is related to. Importance and sensitivity analysis can then provide additional information and insights on a DiD level.

9. Conclusions

This research project started with the clear view that the PSA can be used to investigate the application of defence-in-depth. The PSA addresses

- the frequency of initiating events that challenge nuclear safety,
- the probability of failure of safety systems,
- the frequency of core damage,
- the probability of bypass or failure of the containment and the frequency of a large (early) release,
- the effectiveness of the off-site emergency response measures and the frequency of social and economic consequences.

A project result is that the original definitions of the defence in depth levels 1 and 2 provide limited support for their evaluation with PSA. A new framework of defence in depth levels is therefore proposed to provide a developed explanation model of defence-in-depth. The new model is the result of a split of each of the original DiD levels 1 and 2 (as defined in IAEA INSAG12 [5]) into two parts, as shown in figure 16 below:

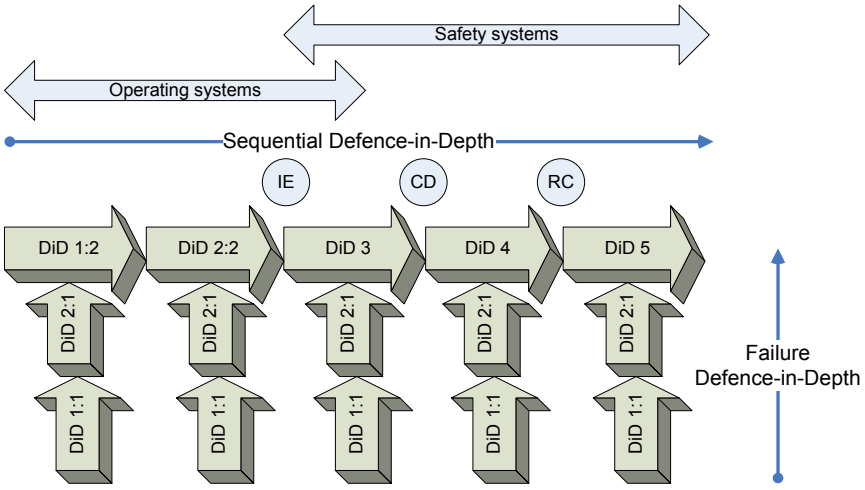

Figure 16: The New Elaborated DiD Framework

DiD 1.2 is the prevention of disturbances and DiD 2.2 is the control of disturbances. Further, this model shows that an evaluation of any individual so called sequential DiD level 1:2, 2:2, 3, 4 and 5, will essentially be an evaluation of two failure DiD levels:

- 1.1 Prevention of failures,
- 2.1 Detection of failures

Even if PSA input data and the PSA model can be used to evaluate the defence in depth, there are limitations, e.g items that not are modelled.

DiD level 3 and 4 have strong links to PSA models and results. To differentiate DiD Level 1:2-2:2 and to address DiD Level 5, extended PSA modelling is required which, in turn, calls for new definitions in the PSA framework. Further data analysis of root causes (DiD level 1.1 and 2.1) that are related to deficiencies in DiD Level 1:2 and 2:2 makes it possible to achieve a better understanding of the weaknesses and strengths of these DID levels with regard to protection against disturbances and failures. Additional modelling of the actual control and protection systems that are part of DiD level 2.2 also provides better means of evaluating this DiD level. The major systems of interest here are the Balance of Plant system and the power control and supply system.

Other additional modelling activities are related to quantification of new "top" events and to calculation of importance measures for SSCs being part of the different DiD levels

Next, to interpret at least high level measures, the visualisation of results becomes particularly important. Hence, when presenting data having several attributes the information could be used to construct tables coded by relevant colours. Using such method allow for fast and intuitive interpretation of results, both for the DiD for an existing plant, and the effects on the DiD due to plant changes and effects from events. Use of tables where the contribution from different initiating events and conditional probabilities can be shown side by side and combined with colour marking for defined levels will emphasize strong and weak areas. For PSA level 1, two dimensional tables will be enough, for PSA level 2 it may be a solution to use three-dimensional tables, see examples in Figure 14 and Figure 15.

There is a deterministic requirement for independence between DiD levels, though this report conclude that complete independence is difficult or almost impossible to achieve. Certain PSA results can be used to identify the degree of dependence between DiD levels in sequences. PSA sequence and consequence results can indicate the barrier (conditional probability) of entering from one DiD level to another. It is also in theory possible to calculate split fraction probabilities that can provide information about dependencies. Attributes can be used to tag SSCs represented in the PSA model with the DiD level they represent. Uisng these attributes in Importance and sensitivity analysis can then provide additional information and insights for the DiD levels.

It is interesting to note that the use of event classes (events leading to accident conditions) in the design indicates a plant with a core damage frequency less than 1E-4 per year. This can be compared to utility PSA target values usually at 1E-5 per year. It also indicates that the plant is designed for a frequency of release less than 1E-6 per year (compared to utility PSA target values usually at 1E-7 per year). The difference between 1E04 and 1E-6

presupposes that a barrier strength of a factor of 100 is achievable between core damage and unacceptable release.

To summarize:

- Swedish regulation SSMFS 2008:1 is basically built up around the concept of safety barriers and the defence in depth principle
- Parts of the IAEA original definitions are difficult to interpret unambiguously and they do not directly match PSA results
-
- PSA results (frequencies and conditional core damage/release probabilities for specific cases (combinations of IE, PDS, RC) can provide insights into weaknesses and strengths of DiD levels in different scenarios. However, PSA results are not explicitly presented in terms of DiD level
- A developed framework where the original DiD levels 1 and 2 are each divided into two sub-levels is proposed in support of PSA evaluation by emphasizing the link to results that are evaluated and presented in a PSA.
- PSA provides a link between Risk criteria and Defence-in-Depth (a set of DiD levels or an individual DiD level)
- Data analysis is a tool for evaluation of the "new" DiD levels 1.1, prevent failures and 2.1, detect failures.
- Modelling of specific contributors to initiating events with both the events that challenge normal operation, and the systems/components/structures that are supposed to control abnormal operation makes it possible to study the DiD level for control of abnormal operation – DiD level 2.2 according to the new definition provided in this report.
- PSA result presentation can be developed to visualize the contribution from the different DiD levels, and also dependencies.
- The event classification being the basis for the design may result in a plant with a risk that not necessarily matches the PSA risk criteria or safety goals.
- It is evident that current PSA models have limitations. These limitations are not more significant from the perspective of the current project than from the perspective of the PSA model for other use.

The interpretation of what is a relevant plant safety is based on the definitions of DiD on the one hand and the PSA framework on the other hand. Particularly important is the establishment of activities to promote a joint perspective on definitions and models of explanation. These should constitute the foundation for future templates, reporting system of events and failures as well as for the interpretation of PSA results.

10. References

[1] IAEA Safety Glossary Terminology used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna 2007.

[2] AEA TECDOC-719, “Defining Initiating Events for Purposes of Probabilistic Safety Assessment”, IAEA September 1993.

[3] Hiromitsu Kumamoto, “Satisfying Safety Goals by Probabilistic Risk Assessment”, Springer London 2007.

[4] SSMFS 2008:1, Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om säkerhet i kärntekniska anläggningar, SSM 2008-12-19

[5] IAEA INSAG-12 “Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1.” IAEA International Nuclear Safety Advisory Group 1999

[6] IAEA INSAG-3 “Basic Safety Principles for Nuclear Power Plants.” IAEA International Nuclear Safety Advisory Group 1988

[7] Reserapport från IAEA möte Effective Combination of Deterministic Analysis and PSA in Plant Safety Management”, RELCON rapport RELCON-2006113-R-002.

[8] Results of Deliberations of the IAEA Technical Meting on Effective Combination of Deterministic and Probabilistic Safety Analysis in Plant Safety Management, Technical University of Catalonia, Barcelona, Spain, 04 to 08 September 2006.

[9] Lars Gunsell, Regulation of defence in depth in view of the Forsmark event, presented at International Workshop on Defence in Depth aspects in Electrical Systems of Importance for Safety organised by SKI, Stockholm, Sweden. 5 – 7 September 2007.

[10] Per Hellström, Projektförslag till Forskningsprojekt "Värdera led i djupförsvar med hjälp av PSA, Relcon Rapport 2006113-R-001 utgåva 1, Relcon AB 2006-09-29.

[11] SEI 07-196, rev 0, SKI Research Project: Evaluation of Defence-in-Depth Using Results from PSA. Phase 1, Westinghouse Electric Sweden AB.

[12] IAEA INSAG-10 “Defence in Depth in Nuclear Safety.” IAEA International Nuclear Safety Advisory Group 1996.

[13] IAEA Safety Reports Series No 46 “Assessment of Defence in Depth for Nuclear Power Plants” IAEA 2005.

[14] ANS/ANSI-51.1-1983, Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

[15] ANS/ANSI-52.1-1983, Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

[16] SKI Report 94:12 “I-boken version 2- Inledande händelser i svenska kärnkraftverk” (Report in Swedish; “I book Version 2- Initiating events in Swedish Nuclear Power Plants”).

[17] Vattenfall TUD-kansliet T-boken Version 6 “Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer” (Report in Swedish; “T book

Version 6- Reliability Data for Components in Swedish Nuclear Power Plants”).
[18] IAEA Safety Report No 23, Accident Analysis for Nuclear Power Plants, IAEA 2002.
[19] IAEA Safety Report No 25, Review of Probabilistic Safety Assessments by Regulatory Bodies,IAEA 2002.
[20] The International Nuclear Event Scale, (INES), User's Manual, 2001 Edition, Jointly prepared by IAEA and OECD/NEA.
[21] SSMFS 2008:17 Strålsäkerhetsmyndighetens föreskrifter och allmänna råd om konstruktion och utförande av kärnkraftsreaktorer, SSM 2009-01-30.
[22] Karl N. Fleming*, Fred A. Silady, ” A risk informed defence-in-depth framework for existing and advanced Reactors”, Reliability Engineering and System Safety 78 (2002) 205–225.
[23] IAEA 50-P-10, Human reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, IAEA 1995.
[24] IAEA TECDOC-832, IPERS Guidelines for the International peer Review Service, second edition, Procedures for conducting independent peer reviews of probabilistic safety assessments, IAEA 1995.
[25] SSM 2010:36, Guidance for the Definition and Application of Probabilistic Safety Criteria.
[26] I. Kuzmina, M. El-Shanawany, M. Modro, and A. Lyubarskiy, An Approach for Holistic Consideration of Defence Depth for Nuclear Installations using Probabilistic Techniques , paper presented at ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC, March 13-17, 2011
[27] Jan-Erik Holmberg and Kim Björkman, VTT, Per Hellström, Scandpower, Research report on Methods for risk follow-up and handling of CCF events in PSA applications, VTT-R-11463-08, VTT / NPSAG 2009.
[28] ASME/ANS RA-S-2009, Standard for level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME, 2009.
[29] IAEA, Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, 2010
[30] IAEA, Safety Standards Series No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, 2010

2015:04

The Swedish Radiation Safety Authority has a comprehensive responsibility to ensure that society is safe from the effects of radiation. The Authority works to achieve radiation safety in a number of areas: nuclear power, medical care as well as commercial products and services. The Authority also works to achieve protection from natural radiation and to increase the level of radiation safety internationally.

The Swedish Radiation Safety Authority works proactively and preventively to protect people and the environment from the harmful effects of radiation, now and in the future. The Authority issues regulations and supervises compliance, while also supporting research, providing training and information, and issuing advice. Often, activities involving radiation require licences issued by the Authority. The Swedish Radiation Safety Authority maintains emergency preparedness around the clock with the aim of limiting the aftermath of radiation accidents and the unintentional spreading of radioactive substances. The Authority participates in international co-operation in order to promote radiation safety and finances projects aiming to raise the level of radiation safety in certain Eastern European countries.

The Authority reports to the Ministry of the Environment and has around 315 employees with competencies in the fields of engineering, natural and behavioural sciences, law, economics and communications. We have received quality, environmental and working environment certification.

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96

Tel: +46 8 799 40 00
Fax: +46 8 799 40 10

E-mail: registrator@ssm.se
Web: stralsakerhetsmyndigheten.se