SKI Report 2008:33

Research

Risk-informed assessment of defence in depth, LOCA example

Phase 1: Mapping of conditions and definition of quantitative measures for the defence in depth levels

Rev 0

February 2008

Jan-Erik Holmberg
Jan Nirmark

February 2007

ISSN 1104-1374
ISRN SKI-R-08/33-SE

SKI

SKI-perspective

Background

The concept of defence-in-depth (DID) is fundamental to the safety of nuclear power plants. It calls for multiple successive methods or barriers against radioactive release to the environment. DID principle is partly reflected in a probabilistic safety assessment (PSA), but not all of the DID levels are included in the models. In addition, events included in PSA are not typically labelled with DID information. PSA could however be a powerful tool to assess the status of various DID levels in an NPP.

Scope

This work is a start of a development of the PSA-methodology towards an assessment of DID levels. This research activity have included: 1) mapping of conditions that should be considered for the defence in depth levels, and 2) definition of those quantitative measures that should be used for the defence in depth levels. The work has been limited to loss-of-coolant-accidents (LOCA) and DID levels 1 and 2, i.e., prevention of abnormal operation and failures and control of abnormal operation and detection of failures. Examples are chosen both from power operation LOCAs and LOCAs during cold shutdown.

Result

The methods that are used today in PSA are applicable for evaluating defence-in-depth levels 1 and 2. Failure data can be determined through: human reliability analysis, risk-informed in-service-inspection methodology, system reliability analysis and directly from plant specific failure data for the components. Many DID activities against LOCA are not explicitly modelled in typical PSA-studies. DID activities and systems identified in this study can play a role in several DID levels, and the evaluation of the DID level must therefore be judged by the initiating event.

Effect on the SKI:s work

To extend PSA to include evaluation of each and every one of the DID levels will give a better understanding of the NPP´s strength and weaknesses out of reactor safety point of view. PSA can therefore, in this way, become an improved tool to use for both the SKI and the utilities.

Continuing work within the research field

Planning an analysis of possibilities to introduce the ideas presented in this report in a real PSA to demonstrate how the DID levels 1 and 2 can be incorporated more explicitly in PSA than in today's PSA. Another possible task is to develop a method for the presentation of results and the safety evaluation of the obtained results. By these steps of development PSA can become a tool for identifying relative and absolute weaknesses in activities for preventing or controlling abnormal events.

Project information

SKI administrator for this project has been Ralph Nyman.

SKI reference: SKI 2006/368
Project number: 2007 02 014

SKI-perspektiv

Bakgrund

Djupförsvarsprincipen är grundläggande för reaktorsäkerheten. Den kräver flerfaldiga säkerhetsarrangemang och barriärer mot radioaktiva utsläpp till omgivningarna. Djupförsvarsprincipen är delvis beaktad i probabilistisk säkerhetsanalys, men alla djupförvarsnivåer inkluderas inte i modellerna. Dessutom, är inte de händelser som ingår i PSA angivna med specifik information om djupförsvarsnivåer. PSA skulle dock kunna vara ett kraftfullt verktyg för utvärdering av de olika djupförsvarsnivåernas status i ett kärnkraftverk

Omfattning

Detta arbete är ett första steg mot en utveckling av PSA-metodik för analys av djupförsvarsnivåer. Detta uppdraget har inkluderat: 1) kartläggning av förhållanden som bör beaktas för djupförsvarsnivåer, och 2) definition av de kvantitativa mätetal som bör användas för djupförsvarsnivåerna. Arbetet har begränsats till kylmedelsförlust (LOCA) och djupförsvarsnivåerna 1 och 2, d.v.s. förebyggande av driftstörningar och fel och kontroll över driftstörningar och fel. Exempel på LOCA har valts både från effektdrift och från avställningsperioden.

Resultat

Metoderna som används i dagens PSA är tillämpliga även vid utvärdering av djupförsvarsnivåerna 1 och 2. Feldata kan bestämmas genom: Human Reliability Analysis (HRA), metoder för Risk Informed In Service Inspection (RI-ISI), systemanalys av tillförlitligheten med anläggningsspecifika data för komponenter. Många djupförsvarsaktiviteter för att förhindra LOCA modelleras inte explicit i typiska PSA- studier. Djupförsvarsaktiviteter och system som har identifierats i denna studie kan spela en roll i flera av djupförsvarsnivåerna, och utvärderingen av djupförsvarsnivåer måste därför bedömas utifrån den inledande händelsen.

Påverkan på SKI:s tillsyn

Att utvidga PSA till att inkludera utvärdering av var och en av djupförsvarsnivåerna kommer att ge en bättre förståelse av kärnkraftverkens styrkor och svagheter ur ett reaktorsäkerhetsperspektiv. PSA kan därför, på detta sätt, komma att bli ett förbättrat verktyg att använda både för SKI och för de som upprätthåller säkerheten vid kärnkraftverken.

Fortsatt arbete inom forskningsområdet

Planering och analys av möjligheter att införa rapportens idéer i en verklig PSA-studie för att demonstrera hur djupförvarsnivåerna 1 och 2 mer explicit kan inkluderas i en PSA, än de är i dagens PSA studier. En annan tänkbar uppgift är också att utveckla resultatpresentationen och säkerhetsvärderingen av erhållna resultat. Med dessa utvecklingssteg kan PSA bli ett verktyg för att identifiera relativa och absoluta svagheter i aktiviteter som syftar till att förhindra eller kontrollera onormala händelser.

Project information

Ralph Nyman har varit SKI:s handläggare i detta forskningsuppdrag

SKI referens: SKI 2006/368
Projekt nummer: 2007 02 014

SKI Report 2008:33

Research

Risk-informed assessment of defence in depth, LOCA example

Phase 1: Mapping of conditions and definition of quantitative measures for the defence in depth levels

Rev 0

February 2008

Jan Erik Holmberg - VTT
Bergmansvägen 3, Esbo
PB1000, FI-02044 VTT, Finland

Jan Nirmark - Vattenfall Power Consultant
Box 527
16216 Sweden

February 2007

Summary

The concept of defence-in-depth (DID) is fundamental to the safety of nuclear power plants. It calls for multiple successive methods or barriers against radioactive release to the environment. DID principle is partly reflected in a probabilistic safety assessment (PSA), but not all of the DID levels are included in the model. In addition, events included in PSA are not typically labelled with DID information. PSA could however be a powerful tool to assess the status of various DID levels in an NPP.

This work is a start of a development of the PSA-methodology towards an assessment of DID levels. It includes: 1) mapping of conditions that should be considered for the defence in depth levels, and 2) definition of quantitative measures that should be considered for the defence in depth levels. The work has been limited to loss-of-coolant-accidents (LOCA) and DID levels 1 and 2, i.e., prevention of abnormal operation and failures and control of abnormal operation and detection of failures. Examples are chosen both from power operation LOCAs and LOCAs during cold shutdown.

The methods that are used today in PSA are applicable for evaluating defence-in-depth levels 1 and 2. In the framework of these methodologies there are many different conditions and measures used. Failure data can be determined through: human reliability analysis (HRA), risk-informed in-service-inspection (RI-ISI) methodology, system reliability analysis and directly from plant specific failure data for the components.

Many DID activities against LOCA are not explicitly modelled in typical PSA-studies. The risk importance of in-service-inspection is analysed and quantified in RI-ISI applications but so far results from RI-ISI have not been incorporated into PSA. Very few leakage detection systems are modelled in PSA-studies. Normally leakage detection systems that is part of the automatic actuation system are modelled while leakage detection systems in DID levels 1 and 2 typically are omitted. DID activities and systems identified in this study can play a role in several DID levels, and the evaluation of the DID level must therefore be judged by the initiating event.

The next step is to implement the ideas in a real PSA to demonstrate how the DID levels 1 and 2 can be incorporated more explicitly in PSA than in today's PSA. Another task is to develop a method for the presentation of results. By these developments PSA can then become a tool for identifying relative and absolute weaknesses in activities for preventing and controlling abnormal events.

Acknowledgements

Swedish Power Nuclear Inspectorate (SKI) has sponsored the work.

Sammanfattning

Djupförsvarsprincipen är grundläggande för kärnkraftverkens säkerhet. Den kräver att det finns flerdubbla successiva metoder eller barriärer mot radioaktiva utsläpp. Djupförsvarsprincipen ingår delvis i probabilistiska säkerhetsanalyser (PSA), men alla djupförsvarsnivåer finns inte representerade i analyserna. Dessutom är inte de händelser som ingår i PSA märkta med information angående djupförsvarsnivåerna. PSA skulle emellertid kunna bli ett kraftfullt verktyg för att analysera statusen hos respektive djupförsvarsnivå i ett kärnkraftverk.

Detta arbete är en början på en utveckling av PSA metodik för utvärdering av djupförsvarsnivåer. Arbetet består i att: 1) kartläggning av förhållanden som ska beaktas för djupförsvarsnivåerna, och 2) definition av de kvantitativa mätetal som bör användas vid analys av djupförsvarsnivåer. Arbetet har begränsats till kylmedelsförlust (LOCA) och djupförsvarsnivåerna 1 och 2, d.v.s., förebyggande av driftstörningar och fel och kontroll över driftstörningar och detektering av fel. Exempel har valts både från LOCA vid normal drift och från LOCA under avställningsperioden.

Metoderna som idag används inom PSA är även tillämpliga att använda för utvärdering av djupförsvarsnivåerna 1 och 2. Inom ramen för dessa metoder finns det många olika förhållanden och mätetal. Feldata kan bestämmas genom Human Reliability Analyses (HRA), Risk-informed in-service-inspection (RI-ISI) metodik, tillgänglighetsanalys av system och direkt från anläggningsspecifika komponentdata.

Många djupförsvarsaktiviter är inte modellerade i en typisk PSA studie. Riskviktigheten för in-service-inspection analyseras och kvantifieras i RI-ISI applikationer men än så länge har inte resultat från RI-ISI införts i PSA studier. Mycket få läckagedetekteringssystem modelleras i PSA studier. Normalt sett är det bara de system som ingår i det automatiska reaktorskyddssystemet som modelleras medan de läckagedetekteringssystem som är verksamma inom djupförsvarsnivåerna 1 och 2 utelämnas. Djupförsvarsaktiviteter och system som har identifierats inom detta arbete kan vara av betydelse i flera djupförsvarsnivåer, och utvärderingen av varje nivå måste därför bedömas per inledande händelse.

Nästa steg är att införa idéerna i en befintlig PSA studie och demonstrera hur djupförsvarsnivåerna 1 och 2, mer explicit, kan inbegripas i PSA än de är i dagens PSA studier. Ett annat steg blir att utveckla resultatpresentationen. Med dessa utvecklingssteg som en fortsättning kan PSA utvecklas till att bli ett verktyg för att identifiera relativa och absoluta svagheter i aktiviteter för hantering av onormala händelser.

Erkännande

Arbetet har utförts på uppdrag av Statens Kärnkraftinspektion (SKI).

Table of contents

Abbreviations

BWR	Boiling water reactor
CDF	Core damage frequency
DBA	Design Basis Accident
DID	Defence-in-depth
DSA	Deterministic Safety Analysis
FAC	Flow-accelerated corrosion
HAZ	Heat affected zones
HRA	Human reliability analysis
IGSCC	Inter-granular stress corrosion cracking
ISI	In-service-inspection
LERF	Large early release frequency
LPSA	Living PSA
MIC	Microbiologically influenced corrosion
NDT	Non-destructive testing
NPP	Nuclear power plant
PSA	Probabilistic safety assessment
PSI	Pre-service-inspection
PWR	Pressurised-water reactor
PWSCC	Primary water stress corrosion cracking
RCPB	Reactor coolant pressure boundary
RI-ISI	Risk-informed in-service-inspection

Abbreviations of organisations

IAEA	International Atomic Energy Agency
SKI	Swedish Power Nuclear Inspectorate (Statens kärnkraftinspektion)
U.S.NRC	United States Nuclear Regulatory Commission

1 Introduction

1.1 Background

The concept of defence-in-depth (DID) is fundamental to safety of nuclear power plants. It calls for multiple successive methods or barriers to radioactive release to the environment. There are several ways to define DID [1] and there are also several definitions for safety barriers [2]. The IAEA Safety Guide INSAG-10 structures DID in five consecutive levels [3]:

> *"Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response."*

DID principle is partly reflected in a probabilistic safety assessment (PSA), but not all the levels of DID are included in the model. In addition, events included in PSA are not typically labelled with DID information. PSA could however be a powerful tool to assess the status of various DID levels in an NPP. This work is a start of a development towards risk-informed assessment of DID.

1.2 Project aim and scope

The aim of the project is to develop methods for using PSA models and results in a way that allows assessment and ranking of the structures, systems, components and operating procedures that form the defence in depth of a nuclear power plant. This whole work is divided into five phases:

1. Mapping of conditions that should be considered for the defence in depth levels.
2. Definition of quantitative measures that should be consedered for the defence in depth levels.
3. Method development and adaptation of PSA model.
4. Quantitative analyses.
5. Quantitative and qualitative safety assessment of identified aspects of defence in depth.

The first two phases is included in this project (2007). The aim is to map the conditions that should be considered when analyzing defence-in-depth level 1 and level 2 and to define quantitative measures for these conditions. This restriction is based on conception that DID level 3 to 4 are quite well handled in today's PSA-studies and DID level 5 is related the level 3 PSA, which is not a requirement in many countries. Meanwhile in DID levels 1 and 2 there are a large number of activities which not

necessarily have been modelled in PSA-studies but that may be of interest from a risk assessment point of view.

In order to effectively study and demonstrate the idea of risk-informed assessment of DID, the work has been limited to loss-of-coolant-accidents (LOCA). Examples are chosen both from power operation LOCAs and LOCAs during cold shutdown. Safety function mitigating consequences of LOCA are outside of the scope of the study.

2 Concepts

2.1 Defence-in-depth levels

IAEAs INSAG-10 guide [3] outlines the general defence in depth principles and measures used to achieve adequate safety in nuclear power plants. The basic definitions of defence in depth levels are outlined in Table 1.

Table 1. Levels in defence in depth [3] .

DID level	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

2.2 Levels of PSA and defence-in-depth

The objectives of different DID levels form a chain of consecutive barriers where an event sequence can be stopped to avoid more and more harmful consequences. This description of DID levels is straight-forward to associate with event sequence descriptions used in PSA context, since PSA is also structured in several levels with respect to consequences assessed. In level 1 PSA, the core damage risk is assessed. In level 2 PSA, the risk of radioactive release from the reactor containment is assessed and, in level 3 PSA, the environmental consequences are assessed.

As can be seen in Figure 1, there is a clear correspondence between PSA levels and levels of DID. DID levels 1 and 2 are included in the initiating events of level 1 PSA.

DID level 3 is analysed in the event trees of level 1 PSA. DID level 4 is analysed in level 2 PSA, and DID level 5 is analysed in level 3 PSA.

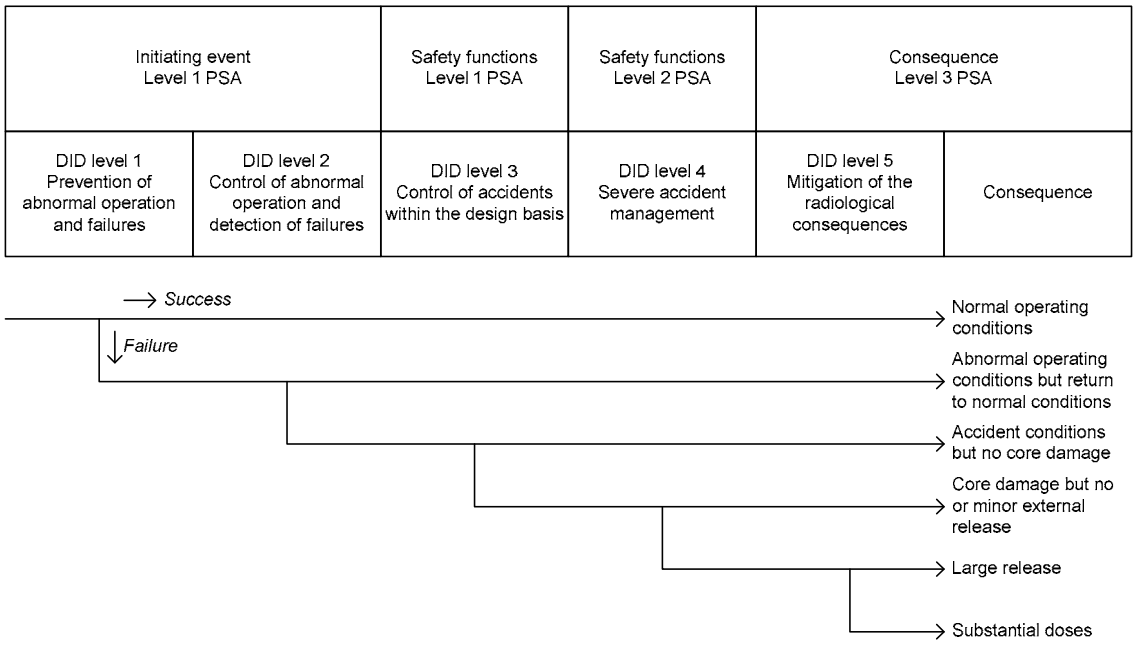

Figure 1. PSA event tree and the levels of defence-in-depth.

2.3 Defence-in-depth levels and system life cycle

While the association between objectives of the DID levels, system functions and PSA levels is rather clear, the means for DID form a more diffuse set of many different kinds of activities, principles and technical solutions. One way to structure the set of means for DID is to link them into different system (plant) life cycle phases:

- Pre-operational phases
  - design
  - manufacturing
  - installation
  - commission
- Operational phases
  - operation
  - maintenance
  - surveillance testing
- Decommission.

A system can, for instance, have a function in the DID level 3, which means that it is a safety function to control of accident within the design basis. The pre-operational phases of the system (design, manufacturing, etc.) and the maintenance of the system are DID level 1 activities. Surveillance testing is a DID level 2 activity, and the system function itself in a demand situation is a DID level 3 activity. This example shows that the whole set of means for defence-in-depth form a complex system of interrelated activities, which requires that several points of view is fully captured. In this study, both the event sequence perspective and the life cycle perspective will be used to identify and define conditions that should be considered for the DID levels (see figure 2).

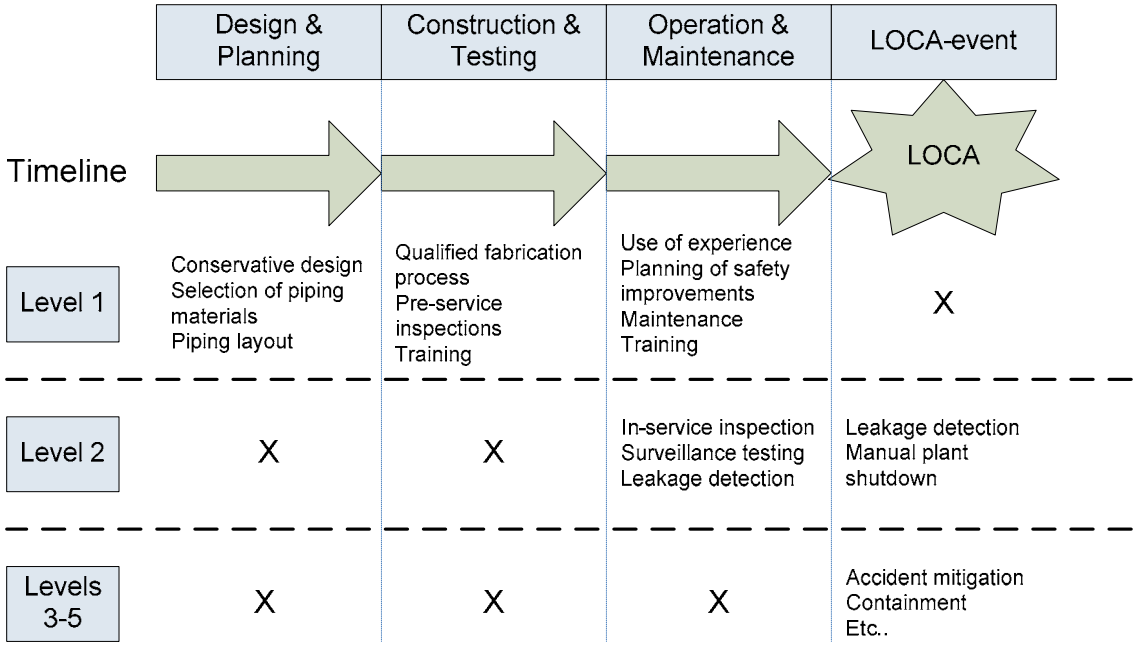

Figure 2. Means for defence-in-depth against LOCA during different phases of the system's lifetime.

2.4 Conditions, measures and PSA–model

Figure 3 explains the idea of risk-informed defence-in-depth assessment. Risk-informed defence-in-depth assessment is based on the living PSA model that is used for the calculation of the average plant risk, but that can be used for various applications. Each application requires generation of application specific data and may require some new modelling work. The quantification and result presentation parts will be handled in the next phase of the study in 2008.

In the risk-informed defence-in-depth assessment, new modelling knowledge is needed to the specification of the event sequences from DID-levels point of view. Effectively, it means taking into account *conditions* affecting DID levels. Example of a condition is the quality of an operability verification method. Poor quality means high probability of failed operability verification, which in turn can mean higher unavailability of a safety system.

In order to quantify the contribution of conditions for the overall risk (core damage frequency, large release frequency) data are needed for the estimation of the probability of existence of a condition and the conditional probability of consequences of that condition. These data are called measures for the DID conditions. In the operability verification example, measures express quantitatively the quality of the operability verification method so that the probability of failed operability verification can be estimated.

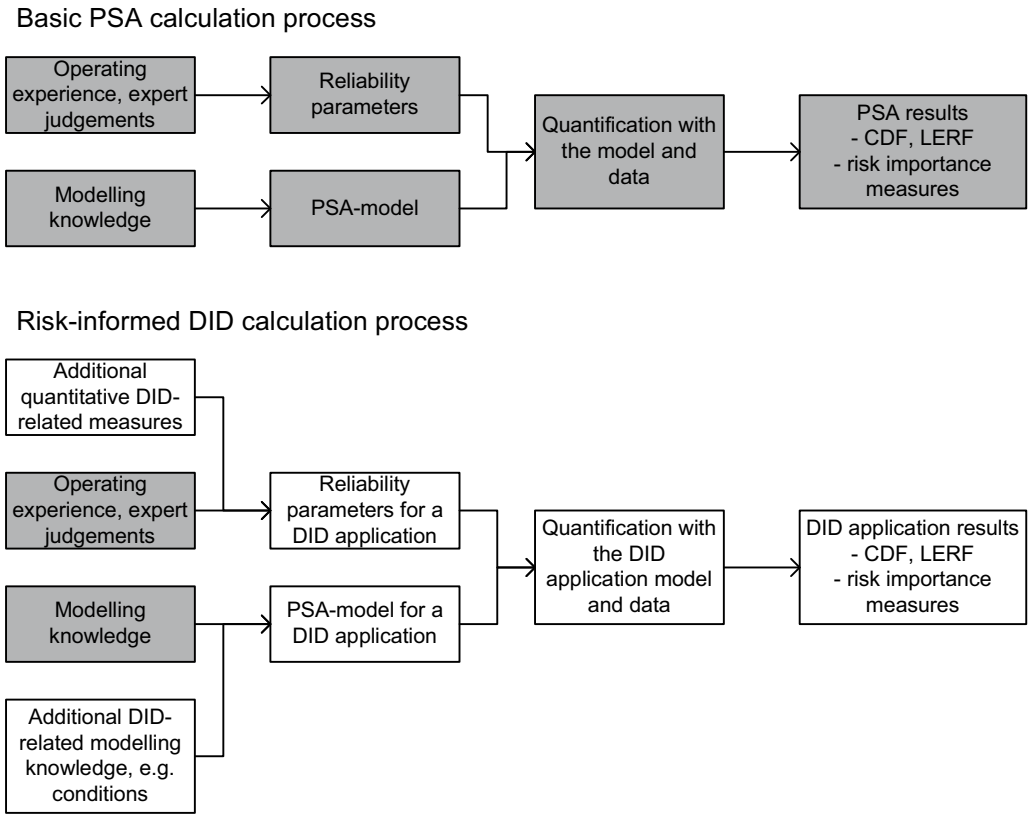

Figure 3. Illustration of differences in an average risk calculation (grey boxes) and a PSA application calculation (white boxes).

Concept	**Definition**
Condition	Something that directly or indirectly causes a failure of a defence-in-depth level
Qualitative measure	Information about the status of the condition.
Measure, quantitative measure	Quantity, a quantitative result from an analysis of DID barrier. Can be used as a parameter in a PSA-model, e.g., failure rate, failure probability
Safety barrier, Barrier function, Barrier system	Safety barrier are physical or non-physical means planned to prevent, control or mitigate undesired events or accidents. A barrier function is a function planned to prevent, control or mitigate undesired events or accidents. Barrier functions describe the purpose of safety barriers or what the safety barriers shall do. A barrier system is a system implementing the barrier function.
Deterministic safety analysis	Method to analyse that the plant design meets the safety and radiological design criteria. Design basis events and their consequences are analysed using calculational methods.
Defence-in-depth	Safety management strategy to have multiple methods, barriers or lines of defence against in the plant's safety features.
Initiating event	An event that requires the starting of the plant safety functions. The initiating event can be an internal or external event e.g. a component failure, a natural phenomenon or a human caused hazard.

Concept	Definition
Safety function	Function intended to prevent the appearance or progression of disturbance and accident situations or to mitigate the consequences of accidents.
LOCA	Loss of coolant accident including primary system breaks resulting in loss of primary coolant. Pipe breaks and ruptures of different sizes, inadvertent opening and failures to re-close valves are being considered in this category.
Risk measure Risk metrics	Risk measure and risk metrics are two concepts used in the presentation and interpretation of results from a risk assessment. The risk measure is an operation for assigning a number to something, and the risk metrics is our interpretation of the assigned number. In the PSA context, the various numeric results obtained from the quantification of the model are risk measures. The interpretations of these numbers as core damage risk, plant risk profile, safety margin, etc., are risk metrics.
Risk importance measure	Risk importance measure is an indication of the contribution of a certain element of the system to the total risk.

2.4.1 Mathematical formulation of risk-importance measures for defence-in-depth

This chapter gives a short introduction to the theoretical framework for the quantification of risk importance measures in the risk-informed DID application. The framework will be further developed in the next phase of the study (2008) when the calculations also will be demonstrated by using examples from a real PSA-study.

In the risk-informed assessment of DID levels the risk model is decomposed into terms representing risk contribution of each DID level. The total risk of a nuclear power plant is composed of risk from a number of event sequences, each starting from a unique initiating event IH_i, $i = 1, \ldots, M$. It should be noted that an "initiating event" in this context can be a much more specific event than a typical "PSA initiating event," that represents a category of initiating events with similar plant response. Here initiating event means a breach of the DID level 1. In PSA context, it is a breach of the DID level 1 or 2.

The conditional probability that a DID level k will be breached given that preceding DID levels have been breached is denoted by

$$q_{ik} = \begin{cases} P(DID_2 \mid IH_i), k = 2, \\ P(DID_k \mid IH_i, DID_2, \ldots, DID_{k-1}), k = 2, \ldots, K. \end{cases}$$

Since the number of the DID levels is five, we have $K = 5$.

The frequency of an event sequence breaching DID level k, given IH_i is

$$f_{ik} = \begin{cases} f(IH_i), k = 1, \\ f(IH_i) \prod_{j=2}^{k} q_{ij}, k = 2, \ldots, K. \end{cases}$$

The total plant risk, with respect to consequence C_k, i.e., breaching DID level k, can be represented as

$$f(C_k) = \sum_{i=1}^{M} f_{ik}, k = 1,\ldots K.$$

This is a kind of minimal cut set representation, even though the "basic events" may be different from those defined in a typical PSA model. In fact, the main effort in a risk-informed analysis of DID is to develop the above DID decomposition of the plant risk, using the plant-specific PSA as a basis.

The probabilistic DID risk importance measures represent the relative importance of an item (system, component, method, …) to the plant risk, in terms of conditional probability of breaching a DID level. The total risk associated with an item A is the frequency of set of event sequences associated with A, i.e.,

$$f_A(C_k) = \sum_{i=1}^{M} f_{ik} 1_{\{IH_j, DID_2, \ldots DID_K \in A\}},$$

where the indicator function $1_{\{\cdot\}}$ expresses that only those event sequences are accounted in the calculation that are associated with A. The meaning of "association" is case specific.

Then we can define the following conditional probabilities

$$q_A(C_k) = \frac{f_A(C_k)}{f_A(C_{k-1})}, k = 2,\ldots,K,$$

so that the A-specific plant risk is

$$f_A(C_k) = f_A(C_1)\prod_{j=2}^{k} q_A(C_j), k = 2,\ldots,K.$$

The calculation of the probabilistic DID risk importance measures is illustrated with the following simple LOCA example. In this example, we consider the following event sequence. The initiation of a crack is the initiating event. The crack can be identified by in-service-inspection (ISI). This method belongs to the DID level 2. If the ISI-method fails, a leak will occur. This is an initiating event in PSA. The leak, which is assumed to be a small LOCA, can propagate to a large LOCA if the leak detection system fails. Both the small and large LOCA can lead to core damage, if safety systems fail. The leak detection system and the safety systems are in this example DID level 3 methods.[1] DID levels 4 and 5 are omitted in this example. See Figure 4 for an event tree.

[1] The leakage detection systems are usually classified as DID level 2 methods. However, they can have a function even in the DID level 3, e.g., the isolation monitoring system.

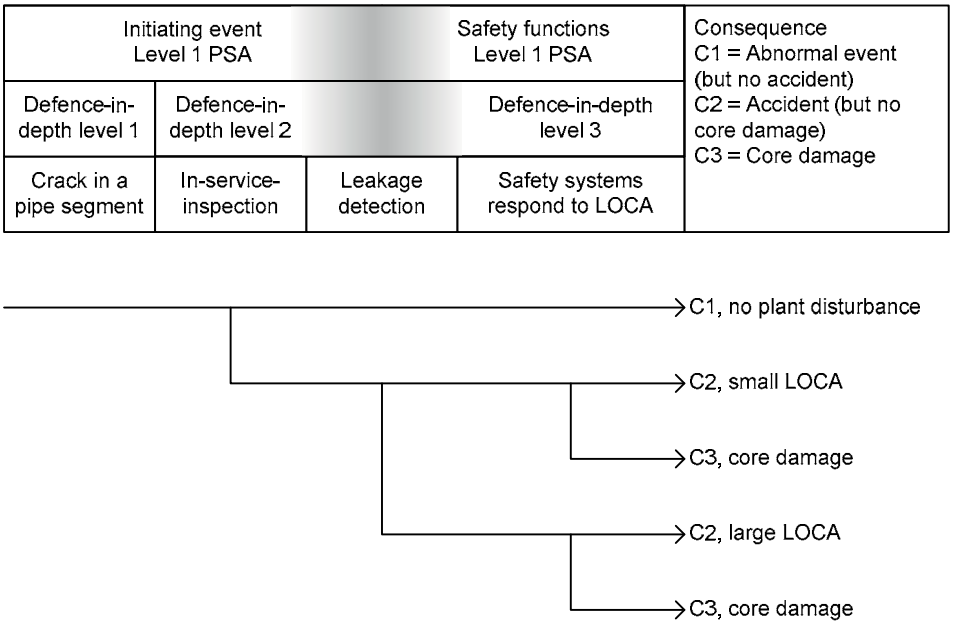

Figure 4 - Simple LOCA example. The border between an initiating event and safety functions is indefinite since a leakage detection system can have a function to both prevent an initiating event and to initiate safety functions. The border between DID level 2 and 3 is also indefinite due to the two roles of the leakage detection system.

The plant risk model consists of three segments (1–3) having different crack frequencies and crack detection (ISI) as well as leak detection probabilities as shown in Table 2.

Table 2 - Initial data in the simple LOCA example. Failure of in-service-inspection implies that crack grows to a leak. Failure of leak detection implies that a leak grows to a large LOCA.

		Failure probabilities		f(LOCA)		
		In-service-inspection	Leak detection			
Segment	f(crack)	P(leak | crack)	P(large LOCA | leak)	Small	Large	Sum
1	2,0E-06	0,01	0,05	1,9E-08	1E-09	2,0E-08
2	2,0E-07	0,3	0,05	5,7E-08	3E-09	6,0E-08
3	2,0E-08	0,01	0,1	1,8E-10	2E-11	2,0E-10
Sum	**2,2E-06**			**7,6E-08**	**4,0E-09**	**8,0E-08**

The core damage frequencies can be derived when the conditional core damage probabilities (CCDP) given small and large LOCA are known, see Table 3.

Table 3. Assessment of conditional core damage probabilities, CCDP, and core damage frequencies, f(CD), in the simple LOCA example.

	CCDP			f(CD)		
Segment	small LOCA	large LOCA	average	small LOCA	large LOCA	sum
1	1,0E-05	1,0E-03	6,0E-05	1,9E-13	1,0E-12	1,2E-12
2			6,0E-05	5,7E-13	3,0E-12	3,6E-12
3			1,1E-04	1,8E-15	2,0E-14	2,2E-14
Sum						**4,8E-12**

The average unreliability of the ISI method is

$$q(ISI) = f(LOCA) / f(crack) = 8,0E-8 / 2,2\ E-6 = 3,6E-2.$$

The average unreliability of the leak detection method is

$$q(LD) = f(Large\ LOCA) / f(LOCA) = 4,0E-9 / 8,0E-8 = 5E-2.$$

The average unreliability of the safety systems is

$$q(SS) = f(CD) / f(LOCA) = 6E-5.$$

The total risk is

$$f(CD) = f(Crack) * q(ISI) * q(SS) = 2,2E-6 * 3,6E-2 * 6E-5.$$

The numbers f(crack), q(ISI) and q(SS) can be used as risk metrics for DID levels 1, 2 and 3 in a comparison with other event sequences.

The results are summarized in Table 4 and graphically in Figure 5. The risk metrics of each DID level is plotted so that frequencies for breaching each DID level 1–3 are in the x-axis, and the conditional failure probabilities of DID levels are in the y-axis. Note that diagonally connected points form an equi-risk line (f * p = constant).

Table 4. DID risk metrics in the simple LOCA case.

Pipe segment	DID risk metrics				
	Frequency of C_i, i= 1, 2, 3 C_i = breaching of DID level i			Conditional probability of C_i given C_1, ..., C_{i-1}	
	$f(C_1)$	$f(C_2)$	$f(C_3)$	$q(C_2)$	$q(C_3)$
Segment 1	2,0E-6	2,0E-08	1,2E-12	1,0E-2	6,0E-5
Segment 2	2,0E-7	6,0E-08	3,6E-12	3,0E-1	6,0E-5
Segment 3	2,0E-8	2,0E-10	2,2E-14	1,0E-2	1,1E-4
Total	2,2E-6	8,0E-08	4,8E-12	3,6E-2	6,0E-5

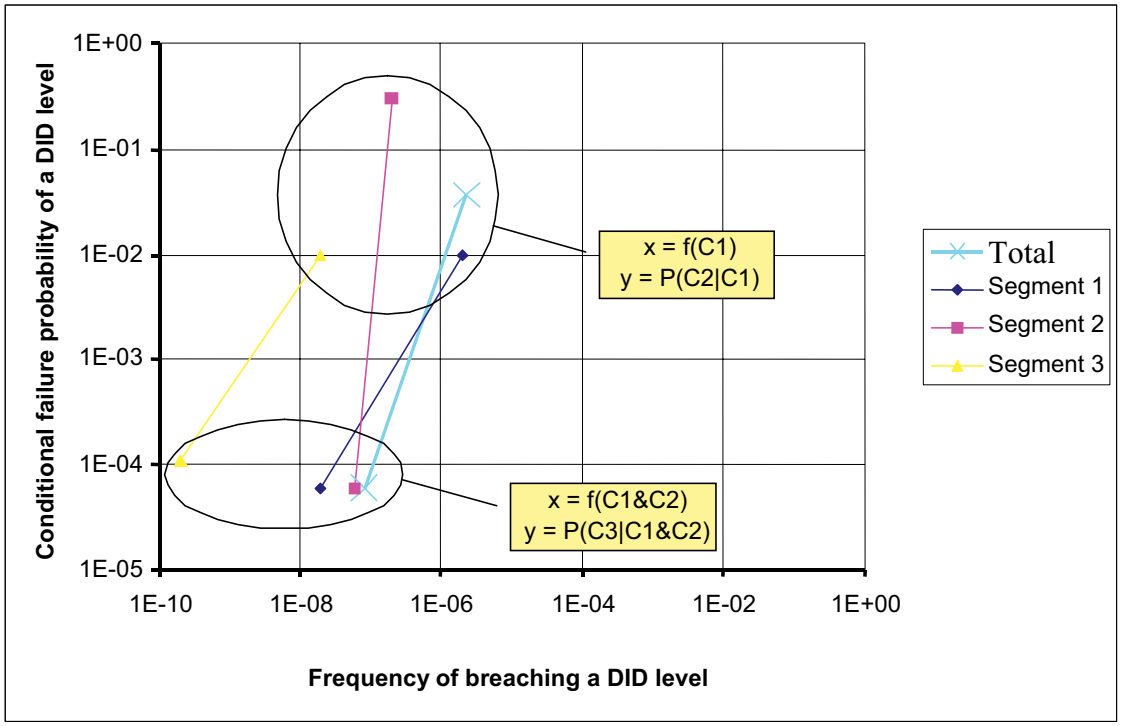

Figure 5. Simple LOCA example. Total and pipe segment specific DID risk metrics for the piping system (DID levels 1–3).

2.5 Working approach of the study

The work has been divided inte the following steps:

1. Identification of activities in DID levels 1 and 2 for the different LOCA categories.
2. Specify examples of conditions that are important for these activities.
3. Specify examples of qualitative measures eg. qualitative information necessary for determining failure data for, and analyzing the defined activites.
4. Defining qualitative measures. It is suggested that failure data is determined through human reliability analysis (HRA), risk-informed in-service-inspection (RI-ISI) methodology and plant specific failure data for the system analyses.

3 LOCA

3.1 LOCA Categories

An initiating event is defined as an incident that requires automatic or operator initiated actions to bring the plant into a safe and steady-state condition. Loss of coolant accident is an initiating event that results in the primary circuit leaking coolant in significant amounts due to broken piping, leaking valve or ruptured reactor tank [4].

Historically the focus on LOCAs has been on the rupture of large diameter piping. A rupture in a pipe with a large diameter leads into a rapid loss of coolant, which in turn creates a need for a high capacity of alternative means of providing coolant to the reactor. Since large LOCAs are used as design basis accidents, this sets the lower limit

for emergency core cooling system capacities. The importance of smaller LOCAs was noticed when Reactor Safety Study first analyzed LOCA initiating events with a PSA in 1975 [5], and that importance was underlined by the Three Mile Island accident in 1979. In the Reactor Safety Study, the LOCA initiating events were categorized into 3 groups based on the size of the pipe break. Conclusion of the Reactor Safety Study was that also the smaller category LOCAs was safety significant. Thus, a balanced defence-in-depth scheme should take into account all LOCA sizes.

For ease of analysis, LOCAs are grouped into a manageable number of categories based on the size of the pipe break and the plant response to different LOCA sizes. LOCA pipe breaks can be defined as a function of the diameter of the piping (or correspondingly cross-sectional area). These LOCA category sizes are different for boiling and pressurized water reactors, and for sections of piping that contains steam vs. water. Usual measure for the plant response is the demand caused for the safety systems. Thus, for different plant designs LOCA categorizations should be different, depending on the capacities, number of redundancies and layout of the emergency cooling safety systems. The Nuclear Regulatory Commission has gathered data [6] for purposes of assessing initiating event frequencies for eight different types of LOCA events. LOCA events are divided into accidents inside containment and outside containment with failed isolation.

LOCAs are generally grouped by their size from 3 to 5 size categories, taken from the following list:

- Very very small LOCA
- Very small LOCA
- Small LOCA
- Medium LOCA
- Large LOCA

There can be differentiations for LOCAs inside and outside containment, reactor tank rupture and steam generator tube rupture (in PWRs).

In categorizing LOCAs the main weight is on the plant response. A LOCA with leak size below a certain level does not affect the plant processes, or is not necessarily even noticed by sensors that activate safety systems, like pressure-, pressure change- or drainage volume monitors. Lower limit for LOCA initiating events is generally in the range of 5–10 kg/s for the amount of water or half of that for steam, depending on the detection limits of the alarm systems. NPPs can also include leak detection systems with much lower detection limits (0,1–0,6 kg/s), and while such leaks are sometimes classified as LOCAs in databases, they are not initiating event LOCAs.

LOCAs during shutdown are categorised principally in similar manner as LOCAs during power operation, i.e., based on size (small–large) and location (bottom/top, inside/outside of containment) as well as phase of shutdown. Cause of LOCA during shutdown is however most likely a human error, e.g., erroneous dismounting of a valve in junction to the primary circuit. The probability of a pipe break is assumed to be insignificant for a pressure less reactor.

3.2 LOCA as event sequences

In order to specify DID methods against LOCA, the sequence of events from an intact primary circuit to a LOCA condition needs to be defined.
Figure 6 presents different event sequences leading to a LOCA. The categorisation is made from the phenomenological point of view and not from the LOCA size point of view used in PSA. LOCA size is a less important attribute when defining the DID methods. The following categories are considered:

- A crack grows to a pipe break.
- Material wastage causes a pipe break.
- A safety relief valve opens or remains open in an uncontrolled way.
- Overpressurisation of a low power system interfacing to RCPB causes a pipe break.
- A valve or other piping system component is erroneously dismounted causing a leakage (during maintenance outage).

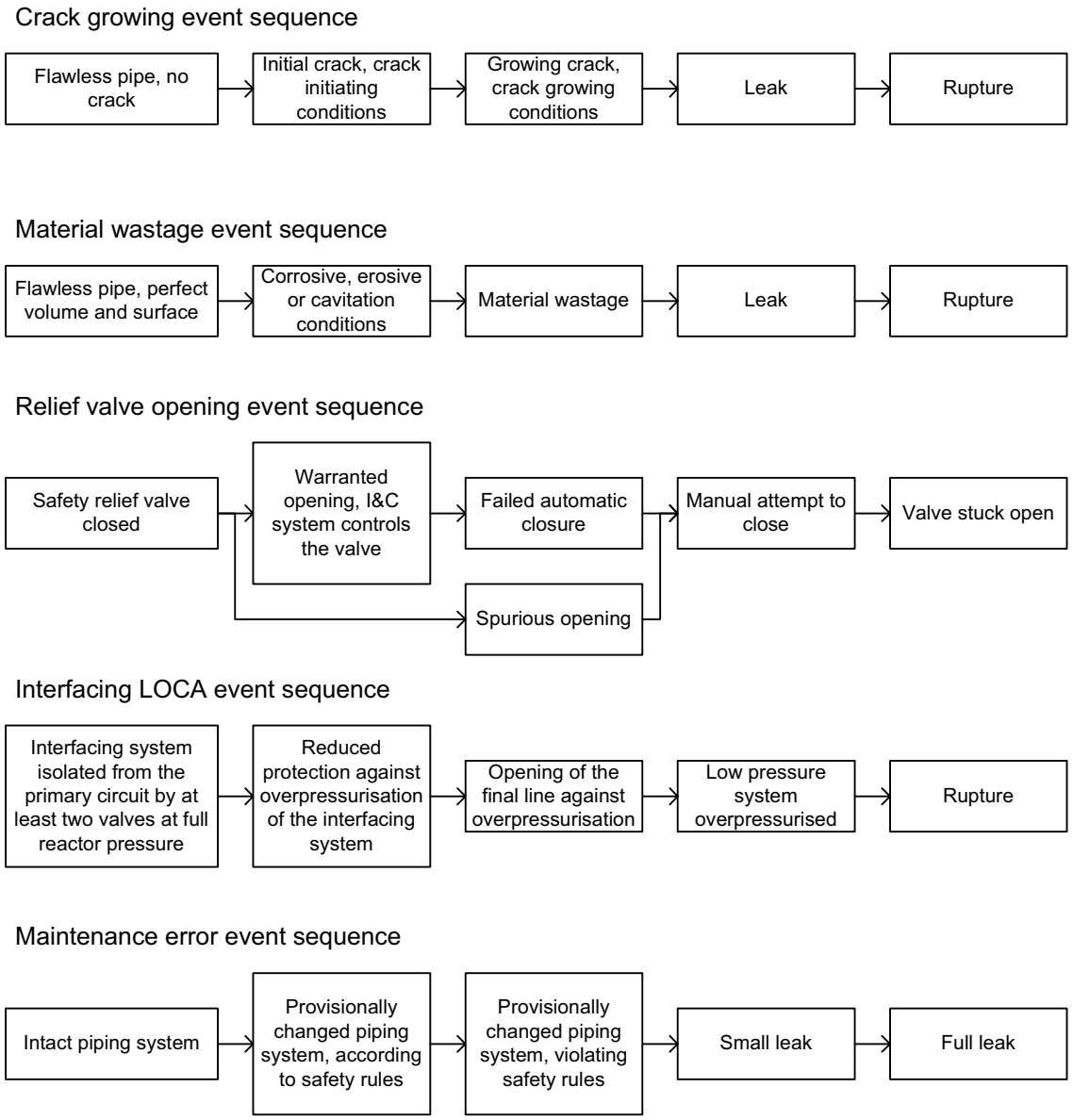

Figure 6. Event sequences leading to a LOCA.

3.3 Prevention and control methods against LOCA-accidents during power operation

3.3.1 Introduction

This study focus on the first two levels of defence in depth against LOCA events. The purpose of these two levels is to preserve the integrity of the piping during normal use and transients, ensuring adequate cooling of the reactor. LOCAs can occur mainly in two ways: valve failure or pipe break. Valve failure can either be the result of a human error (wrong position) or a mechanical failure. Pipe breaks can occur as a result of a degradation mechanism that slowly develops into cracks or other faults over time.

In the DID level 1, the most important measures against LOCAs are design of the piping system, the choice of materials used, use of qualified manufacturing processes and pre-service inspections. Design affects the conditions inside the piping during power operation and may make the pipes subjected to unnecessary degradation mechanisms. The choice of materials and the quality of the manufacturing process are also essential in how a possible degradation mechanism affects the piping.

3.3.2 In-service inspection

In the level 2 of the defence in depth the main activities in pipe break prevention are in-service inspections (ISI) and leak detection. Usually nuclear power plants have extensive ISI programs that degree how and which piping sections that are inspected. The purpose of these inspections is to detect any developing cracks in the piping before they advance into breaks. The basic idea is to more often inspect piping sections that are subjected to aggressive degradation mechanisms or where the consequences of a break is large. A developing crack might go unnoticed in ISI for two reasons: the section where the crack is, is not inspected, or the inspection fails to detect the crack. Inadequate performance at these tasks can be due to design or operation. For example, a certain weld in a piping section might be left uninspected if it by design is in a difficult to reach position and a crack in another weld might be undetected due to human error of the inspection crew.

Table 5 lists the inspection methods for different degradation mechanisms. For any given piping section, the inspected area and the used inspection method depend on the characteristics of the piping. These characteristics include the shape, the material used and conditions inside the piping during operation. In the EPRI RI-ISI method the inspections depend on the degradation mechanism. Degradation mechanisms are evaluated by expert judgements, conditions inside the piping and existing plant data [7].

Table 5. In-service inspection methods for different degradation mechanisms [7].

Degradation mechanism	**Affected regions**	**Examination method**	**NDT method**
Thermal fatigue	Nozzles, branch pipe connections, safe ends, welds, heat affected zones (HAZ), base metal, regions of stress concentration	Volumetric	Ultrasound
Corrosion cracking			
Chloride cracking (OD)	Base metal, welds and HAZ	Surface	Ultrasound
Chloride cracking (ID)	-"-	Volumetric	Ultrasound
Crevice corrosion	-"-	Volumetric	Ultrasound
PWSCC (primary water stress corrosion cracking)	Nozzles, welds, HAZ without stress relief, thermo wells	Visual	
		Volumetric	Ultrasound Eddy currents where inside of the pipe is accessible Radiography

Degradation mechanism	Affected regions	Examination method	NDT method
IGSCC (inter-granular stress corrosion cracking)	Austenic steel welds and HAZ	Volumetric	Ultrasound*
Microbiologically influenced corrosion (MIC)	Fittings, welds, HAZ, and base metal, especially regions containing crevices	Volumetric or visual, VT3	Ultrasound
Erosion-cavitations	Fittings, welds, HAZ, and base metal	Volumetric	Ultrasound, radiography or both
Flow-accelerated corrosion (FAC)		Volumetric	Ultrasound** Radiography***

* = Due to the characteristics of IGSCC the normal shear-wave ultrasound examination will yield too much noise for identification of cracks.
** = FAC is gradual wear over an area, so spot thickness measurements are enough, provided they are done in same spots each time to gather data.

3.3.3 Leakage detection

Another safeguard against pipe breaks at the level 2 of defence in depth is leakage detection. A crack in a piping wall can develop into a small leak before a full-scale break occurs. A small leak in this context means a leak where the amount of water lost from circulation is so small that it does not affect processes in the power plant. Detecting the leak means that the consequences of a break can be reduced if the leak is detected before it grows into a larger break. Leak detection systems monitors different measurements in a room with piping, alerting the operators when leak limits are reached.

A large leak from the RCPB will be detected by an isolation monitoring system that automatically initiates a reactor protection function, i.e., a reactor scram and some form of isolation of the RCPB. In PSA, such leakages are classified as LOCAs if the leak comes from the RCPB. Otherwise it is an spurious actuation of an isolation signal. The isolation monitoring system can monitor several environmental parameters such as water level close to the floor, room temperature and pressure. The monitor type depends on size of rooms and their drainage capacity and the ventilation capacity. As a safety system, there are always redundant monitors in each monitored room. Due to the redundant structure, the isolation monitoring system is typically highly reliable.

A leak below the triggering limit of the isolation monitoring system can be detected by other leak detection systems including water collection in floorwells. The alarm limits of leak detection systems are generally set at a considerable lower level of leakage compared to the LOCA definitions. It may be difficult for the operators to identify of the source for the leakage. Therefore several leakage detection methods must be available as required in [8] and [9]. Table 6 summarises different leak detection methods.

Table 6. Leakage detection methods (partly from [9]).

Leakage detection method (system)	**Purpose**	**Effectiveness against LOCA/DID level**
Isolation monitoring system	To provide protection against the consequences of accidents involving the release of radioactive materials from the fuel and reactor coolant pressure boundary. The system initiates automatic isolation of appropriate pipelines whenever monitored variables exceed pre selected operational limits. The monitored parameter can be e.g. pressure, pressure increase, temperature.	Primary method to initiate automatic safety functions in case of large leak from RCPB. DID level 3
Leakage monitoring systems	To supplement the isolation monitoring system by alarms which are initiated at limiting values below the tripping limits in the isolation monitoring system.	Early warning of small leakages. Redundant leakage detection method. DID level 2
Floor drain system	To collect and dispose of wastewater from rooms. Sump level and sump pump discharge flow can be monitored in main control room.	Early warning of small leakages. Diverse leakage detection method. DID levels 1 and 2
Condensate flow rate from air coolers Humidity monitoring	To collect and monitor the liquid run-off from the drain pans under containment air cooler units	Method for detecting vapour phase leakages. Poor for leak location detection. DID levels 1 and 2
Radiation level monitoring radiogas activity radiopaticulate activity	To monitor radiation levels of various processes and provide signals to the alarm system and to the reactor protection system for automatic actuation of safety actions when tripping limits are exceeded.	Early warning of small leakages. Diverse leakage detection method. Also applicable for intersystem leakage monitoring. DID levels 2 and 3
Reactor coolant inventory (PWR)	To maintain coolant inventory balance. Controlled coolant additions and discharges can be measured, recorded and corrected to maintain balance.	Good for detecting imbalance in coolant inventory. Poor for leak location detection. DID levels 1 and 2.
Visual observation: camera field operator plant tour (daily check)	Visual check of conditions at the plant.	Early warning of abnormal conditions, e.g., water in the floor and unusual noise. Provides information from rooms that are not monitored by other methods. Good for leak location identification. DID levels 1 and 2.

3.3.4 DID means against LOCA

Appendix 1 shows the different means against LOCAs at levels 1 and 2 of the defence-in-depth in different life cycle phases. The columns in the table show the different pipe conditions, starting from a perfectly manufactured pipe on the left, and ending in a broken pipe (LOCA event) at the right. The rows list defence in depth means at each level, and the elements in the table list how those means might fail for the pipe to

advance into a worse condition. A piping section might not go through all the columns in degradation, for example a crack may develop directly into a LOCA without resulting in a leak before break in the process.

The rightmost column, for the LOCA event pipe break, and the last row, for defence in depth levels 3–5, are included for the sake of completeness

3.4 Prevention and control methods against LOCA during refuelling outage

LOCA during refuelling outage is most likely caused by a human error resulting in a leakage from the primary circuit. There are a number of different maintenance activities where human errors can lead to loss of water from the reactor or fuel pools. For example during maintenance of the reactor coolant pumps or because of that valves are opened to interfacing systems that are under maintenance.

DID methods against LOCA during refuelling outage are based on administrative controls (technical specifications, work orders, work permits, work routines) and provisional mechanical barriers installed during maintenance actions, e.g. plugs, flanges, hand valves, I&C interlocks.

A proposal is made in this study that the DID level 1 is comprised of planned maintenance actions where safety rules and procedures are followed. Design, maintenance procedures and administrative controls are important measures. I&C systems provide means to avoid errors by system status indications and alarms and by interlocking functions. The possible human errors that can be done to break the DID level 1 is due to misplanning, conducting maintenance activities in the wrong order or manoeuvre errors.

At the DID level 2 the human error is detected and corrected before it leads to serious consequences. There are numerous of ways in which this can be done depending on the case. The steps in the procedure following the mistake can for example give clear indications of the mistake, for example drainage of water (RC pump house) that never stops or water that pours out when the component/system is about to be opened, and the work is stopped. In these cases the mistake is corrected directly after the mistake is done. Plugging of the pipe, valve closing, installation of a flange etc. after being detected by a detection system or other personnel in the plant can also isolate a leak. In this case you have a loss of water that may be substantial but it does not lead to any major consequences if the leak is isolated in time.

4 Examples of conditions and measures for LOCA

4.1 Identified examples of conditions and measures

In appendix 2, the identified examples of conditions and measures are given. The conditions are potential deficiencies of the DID. The qualitative measure is information about the conditions of the defence in depth that can be used when determining failure data or the quantitative measures. The quantitative measures are the inputs (parameters) to the PSA.

There exist analyses methods in the disciplines of RI-ISI and HRA that can be used for defence in depth analysis of LOCA. Therefore the scope of this work has been limited to only identifying those methods that can be used when determining the parameter input to the PSA rather than listing quantitative measures.

It shall be noted that it is only examples that has been identified in appendix 2 and not a complete list of conditions and measures.

4.1.1 Example from appendix 2 – LOCA during power operation

Pre-service inspection (PSI) has been identified as one DID activity of level 1. The condition that affects the risk of a LOCA is the quality of this activity. There are many different pre-service inspections done. The effectiveness of the different inspections, knowledge of problems from the pre-service inspections are examples of qualitative measures. Unless other DID level 1 activities make up for lacked quality in pre-service inspection it is a significant contributor to the frequency of the DID level 1 failure. Level 1 failure in this case is the existence of flaws that possible can develop into a LOCA if the activities of the DID level 2 fails.

In-service inspection is a DID level 2 activity and its efficiency is one condition to take into account in the calculations. If there are locations (pipe segments) where ISI is not performed or where it is difficult to perform is examples of qualitative measures. Another activity of the DID level 2 is leak detection systems.

Quantitative measures can be calculated with RI-ISI methodology with results shown in Table 7. Numbers in Table 7 are hypothetical.

Table 7. Example results from a hypothetical RI-ISI application. Leak frequencies with and without ISI and leak detection.

Segment and failure mode	Small leak		Large leak			
	no ISI	with ISI	No ISI, No LD	With ISI, No LD	no ISI, with LD	with ISI, with LD
Segm. X Thermal fatigue	1,1E-5	2,2E-7	3,3E-6	4,4E-9	5,6E-8	6,7E-10
Segm. Y Thermal fatigue	7,8E-5	8,9E-7	1,0E-5	1,1E-9	2,2E-8	3,3E-10

ISI = In-service-inspection
LD = Leak detection

4.1.2 Example from appendix 2 - LOCA during the outage period

Safety routines during maintenance is an activity of the DID level 1 during the outage period. Errors made during maintenance is conditions that may cause a LOCA. The probability of these failures is derived from HRA. The DID level 1 is breached if a leak or a LOCA occurs. A LOCA becomes an initiating event to the DID level 3 if a substantial amount of reactor coolant is lost. According to this definition recovery actions is part of DID level 2. One example of condition of DID level 2 is if the

following steps in the procedure give indication of the mistake that caused the leak or LOCA.

Quantitative measures can be calculated with HRA methodology with results shown in Table 8. Numbers in Table 8 are hypothetical.

Table 8. Example results from an HRA of initiating events for a hypothetical shutdown PSA for a BWR.

Maintenance error	Error A (DID level 1)	Error B (DID level 1)	Recovery (DID level 2)
RCP plug is lifted	Technical failure	Plug is lifted to early or wrong plug is lifted	Much more force is needed to lift plug than normal and the lift is interrupted and plug re-installed
Probability	1E-3	1E-2	2E-2

5 Conclusions

The methods that is used today in PSA are also applicable for evaluating DID levels 1 and 2. In the framework of these methodologies there are many different conditions and measures used. These methods are available for the analysts which means that it in this work has been possible to only identify examples rather than trying to be conclusive. Failure data can be determined through: human reliability analysis (HRA), risk-informed in-service-inspection (RI-ISI) methodology, system reliability analysis and directly from plant specific failure data for the components.

Several DID activities and systems identified in this study can play a role in several DID levels, and the determination of the DID level must then be judged by the initiating event. It was also observed that many DID activities against LOCA are not explicitly modelled in typical PSA-studies. It may be of interest to expand the PSA-model and to quantify the risk importance of the DID level 1 and 2 activities.

The risk importance of in-service-inspection is analysed and quantified in RI-ISI applications but so far results from RI-ISI have not been incorporated into PSA. LOCA frequencies used in PSA-studies are based on generic pipe rupture frequencies or pipe failure data where the role of in-service-inspection is only implicitly reflected.

Very few leakage detection systems are modelled in PSA-studies, normally only the isolation monitoring system actuating automatically the containment isolation. Leakage detection systems in DID levels 1-2 are typically omitted.

The next step is to implement the ideas in a real PSA and to demonstrate how DID levels 1 and 2 can be incorporated more explicitly in PSA than in today's PSA. Another task is to develop a method for the presentation of results. After these developments PSA can then become a tool for identifying relative and absolute weaknesses in activities for preventing and controlling abnormal events.

References

[1] Fleming, K.N., Silady, F.A., A risk informed defence-in-depth framework for existing and advanced reactors, Reliability Engineering and System Safety 78 (2002) 205–225.

[2] Sklet, S. Safety Barriers on Oil and Gas Platforms. Means to Prevent Hydrocarbon Releases. Doctoral Theses at NTNU, 2006:3, 2006.

[3] International Nuclear Safety Advisory Group, INSAG-10 Defence in Depth in Nuclear Safety, IAEA, Vienna, 1996, 30 pages

[4] IAEA-TECDOC-719, Defining initiating events for purposes of probabilistic safety assessment, IAEA, Vienna, 1993, 150 pages

[5] Reactor safety study: An assessment of accident risks in U.S. commercial nuclear power plants. U.S. Nuclear Regulatory Commission. WASH-1400, NUREG-75/014, Washington D.C., 1975.

[6] Poloski, J.P., Marksberry, D.G., Atwood, C.L., Galyean, W.J., Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995, NUREG/CR-5750, U.S. Nuclear Regulatory Commission, 1998.

[7] Gosselin, R., Risk-Informed In-service Inspection Evaluation Procedure, EPRI, Palo Alto, 1996.

[8] Regulatory Guide 1.45, Reactor coolant pressure boundary leakage detection systems, U.S. Nuclear Regulatory Commission, 1973. 4 p.

[9] ISA–67.03–1982, Standard for Light Water Reactor Coolant Pressure Boundary Leak Detection, Instrument Society of America, 1982. 43 p.

Appendix 1. Defence in depth means against pipe breaks and causes for failures of the means.

DID level	Defence-in-depth principle or activity in different life cycle phases	Pipe condition — crack growth event sequence from perfect conditions to a break (LOCA)				
		Perfect condition	**Initial crack**	**Crack growth**	**Leak-before-break**	**Break**
Level 1	Design & planning	Unsuitable material	- Design error causes piping susceptible to degradation mechanisms - Unsuitable material causes piping to be susceptible to a degradation mechanism	- Safety margins designed too narrow - Unsuitable material causes piping to fail to a degradation mechanism before end of plant lifetime - Segment is not included in the ISI-programme: - Hard to access - Radiation	Pipes: - Safety margins designed too narrow - Unsuitable material causes piping to fail to a degradation mechanism before end of plant lifetime Leakage detection: - No system installed in room - Wrong alarm margins	Design failure of a DID level 3-5 system
	Manufacturing	Error in manufacturing causes initial cracking			Error in manufacturing leakage detection devices	Manufacturing failure of a DID level 3-5 system
	Installation, commissioning & pre-service inspection	- Initial faults not detected in pre-SI - Not inspected			Error in the installation or commissioning of the leakage detection devices	Installation of commissioning failure of a DID level 3-5 system
	Operation			Unsuitable conditions inside pipe cause piping to fail to a degradation mechanism before end of plant lifetime - Water hammer - Temperature transients - Etc.	Unsuitable conditions inside pipe cause piping to fail to a degradation mechanism before end of plant lifetime	

DID level	Defence-in-depth principle or activity in different life cycle phases	Pipe condition — crack growth event sequence from perfect conditions to a break (LOCA)				
		Perfect condition	**Initial crack**	**Crack growth**	**Leak-before-break**	**Break**
	Maintenance				Maintenance error of leakage detection systems	Maintenance error in DID level 3-5 safety systems
	Utilization of operating experience	Failure to identify degradation mechanism			Failure to identify problems with leakage detection systems	Failure to identify problems with DID level 3-5 safety systems
Level 2	Operation				Leakage detection system unavailable	
	In-service-inspection, surveillance testing			- Not inspected - Failure to identify degradation mechanism - Failure to detect - Human error - Equipment fault - Detected, but no corrective actions taken	Failure to detect in a visual inspection at regular ISI inspections Failed operability verification of leakage detection systems	Failed testing of DID level 3-5 safety systems
Levels 3-5	Operation - Accident prevention - Containment - Off-site emergency procedures - Etc.					Operational failure of safety systems (reactor scram, emergency core cooling, etc.)

Appendix 2. Conditions, qualitative information and methods for determining quantitative measures in the LOCA example

DID principle or activity	Conditions, Examples	Qualitative (measures) information for expert judgements, Examples	Methods for failure data (Quantitative measures)
LOCA DiD level 1.			
Design & Planning	Specification lacked in quality	Are there locations susceptible for flow assisted wall thinning? Are there any locations where water or steam hammer could occur? Are there any areas of potential high vibration? Are there any locations where piping could experience large temperature changes?	RI – ISI
Choice of material	Specification lacked in quality	Are there any known problems caused by the choice of material?	RI – ISI
Qualified manufacturing	Quality problems during manufacturing.	Where there any problems observed during fabrication, pre-service inspection or hot functional testing of the system?	RI – ISI
Pre-service inspection	Pre-service inspection lacked in efficiency to reduce the number of fabrication flaws.		
Operation	Transients, operation at higher power than original design for		RI – ISI
Maintenance	Maintenance problems	Are there any known maintenance problems (e.g. leaks or repairs, problems with valves, bellows, etc.) in this or similar systems?	RI – ISI
Utilization of operating experience	Maintenance organisation fails to identify or handle degradation mechanism.	Are there any known industry problems that should be considered?	RI – ISI

DID principle or activity	**Conditions, Examples**	**Qualitative (measures) information for expert judgements, Examples**	**Methods for failure data (Quantitative measures)**
LOCA DiD level 2.			
In service inspection	In-service inspection lacks in efficiency to detect flaws.	Are there locations where ISI is not performed or where it is difficult to perform?	RI – ISI
Leak detection systems	System unavailable or cannot detect leak. Operators misjudge leak detection system information.	Are there locations where leakage will not be detected? Can it be difficult for the operators to make the right decisions when a leak is detected?	System reliability analysis, component failure data
Interfacing LOCA DiD level 1.			
Maintenance	Operation verification fails to detect that valve has been left open after maintenance during the outage period.	Experience of operation verification.	HRA
Operation	Spurious opening of valve causes Interfacing LOCA	Are there valves that can open spuriously (independent technical faults, fire, internal flooding etc.) and cause an Interfacing LOCA.	System reliability analysis, component failure data
Interfacing LOCA DiD level 2.			
Corrective actions to isolate break.	Insufficient with time to detect and isolate the break.	Are there procedures that support the operator in handling the interfacing LOCA? Are there sufficient with time available for the operator to handle the interfacing LOCA before RT?	HRA
Safety relief valve does not close after being activated, DiD level 1			
Operation	Equipment fault or insufficient maintenance.	Reported unavailability, test intervals.	System reliability analysis, component failure data
Safety relief valve does not close after being activated, DiD level 2			
Disturbed operation	Operator fails to identify problem and close valve.	Are there any deficiencies in the operator procedures? Is the event practiced in simulator?	HRA

DID principle or activity	**Conditions, Examples**	**Qualitative (measures) information for expert judgements, Examples**	**Methods for failure data (Quantitative measures)**
Leakage due to human error during the outage period DiD level 1.			
Planning	Planning error		HRA
Maintenance	Timing error, manoeuvre error	Are there any critical steps in the procedure where timing errors or manoeuvre errors are more likely.	HRA
Utilization of maintenance experience.	Maintenance organisation fails to identify or handle shortcomings in procedures, skills, education, etc.	Are there any known problems that have not been handled?	HRA
Leakage due to human error during the outage period DiD level 2.			
Detection of leakage	System unavailable or cannot detect leak.	Are there any leak detection system and personal available that may detect the leak?	System reliability analysis, component failure data
Stop the work procedure, return back one step and correct the mistake	Following steps in the procedure do not give any indication of the committed mistake that caused the leak.	Are there steps in the procedure where it is likely that the human error made is discovered and corrected?	HRA
Plugging of the hole, valve closing, installation of a flange etc.	Isolation of the leak is not possible or difficult to perform.	Is it physically possible to isolate the leak? Are there enough time to isolate the leak?	HRA

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se