ASAMPSA_E SEVENTH FRAMEWORK PROGRAMME	Advanced Safety Assessment Methodologies: extended PSA	EURATOM

"NUCLEAR FISSION "

Safety of Existing Nuclear Installations

Contract 605001

The Link between the Defence-in-Depth Concept and Extended PSA

- *This version of the report will be submitted to a peer review*
- *The conclusions of the review will be discussed during the ASAMPSA_E workshop with PSA End-Users (12-14th Sept. 2016)*
- *The report will then be improved before the end of the project (31st Dec. 2016)*

Reference ASAMPSA_E

Technical report ASAMPSA_E / WP30 / D30.4 / 2016-26

Reference IRSN PSN/RES/SAG/2016-209

Andreas Wielenberg (GRS), Eric Cazzoli (CCA), Gian-Luigi Fiorini (NIER), Pavlin Groudev (INRNE), Stanislaw Hustak (UJV), Manorma Kumar (LRC), Horst Löffler (GRS), Mirela Nitoi (ICN), Andrej Prošek (JSI), Stefano La Rovere (NIER), Jirina Vitazkova (CCA)

Period covered: from 01/07/2013 to 31/12/2016	Actual submission date: 10-06-2016	
Start date of ASAMPSA_E: 01/07/2013	Duration: 42 months	
WP No: 30	Lead topical coordinator : A. Wielenberg, H. Löffler	His organization name : GRS

Project co-funded by the European Commission Within the Seventh Framework Programme (2013-2016)		
Dissemination Level		
PU	Public	No
RE	Restricted to a group specified by the partners of the ASAMPSA_E project	Yes
CO	Confidential, only for partners of the ASAMPSA_E project	Yes

ASAMPSA_E Quality Assurance page

Partners responsible of the document :	**GRS**
Nature of document	Technical Report
Reference(s)	Technical report ASAMPSA_E/ WP 30 / D30.4 / 2016-26 Rapport IRSN-PSN-RES/ SAG/2016-209
Title	The Link between the Defence-in-Depth Concept and Extended PSA
Author(s)	A. Wielenberg (GRS), E. Cazzoli (CCA), G.L. Fiorini (NIER), P. Groudev (INRNE), S.Hustak (UJV), M. Kumar (LRC), H. Löffler (GRS), M. Nitoi (ICN), A. Prošek (JSI), S.La Rovere (NIER), J. Vitazkova (CCA)
Delivery date	10-06-2016
Topical area	Defence-in-Depth, PSA
For Journal & Conf. papers	No

Summary :

This report is dedicated to the investigation of the link of Probabilistic Safety Assessment (PSA) and assessment with respect to the Defence-in-Depth (DiD) concept for NPP.
The DiD, and all its principles, on which lies its implementation, represent the foundation of the deterministic approach to build a NPP safety architecture. The PSA results provide an overview of the plant's safety performances in terms of probabilities and consequences, with the potential to identify issues which contribute significantly to risk.
The concepts of DiD and PSA have been initially developed independently in the history of NPP safety. The traditional role of DiD is in the design of the plant and its safety provisions, while PSA calculates the probability for failure of the safety provisions and quantifies the risk profile of the NPP. Therefore, PSA is a tool for complementarily evaluating the level of safety achieved by implementing the DiD concept including all other safety related activities.
Keeping in mind these complementary objectives of DiD and PSA, it is recommended that DiD and PSA be developed independently of each other. If a NPP could demonstrate that it follows all applicable DiD rules, and if an independent PSA confirms a low risk of this plant, there would be a well-founded confidence in an adequate level of safety for this plant. If, on the other hand, PSA identifies a high or unbalanced risk profile for the plant, there are doubts as to whether the current application of the DiD concept is sufficient and additional safety provisions are expected. This impact of PSA is now included in the DiD concept, as a complement for the design.
There are a few issues which establish links between DiD and PSA:

- PSA should be structured in such a way that the individual levels of DiD can be identified.
- DiD as well as PSA have their own concepts for including or dismissing events or phenomena from their respective analyses. It is not recommended to harmonize these features in order to keep the benefits of diversity. In contrast, any differences in assumptions should be clearly identified and documented.

Conversely, the conclusions and recommendations address several issues regarding the relationship between PSA and DiD, which could not be investigated in depth in this report and need to be subject of future discussions.

Visa grid

	Main author(s) :	**Verification**	**Approval (Coordinator)**
Name (s)	Andreas Wielenberg and al. (see above)	Horst Löffler	E. Raimond
Date	2016-05-25	2016-05-27	2016-06-10
Signature			

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
Rev. 0		A. Wielenberg	All	Initial version
Rev. 1	28/09/2015	A. Wielenberg, M. Kumar, etc.	All	Introduction, Revision Section 2, Input Section 5.
Rev. 2	15/10/2015	A. Wielenberg, S. Hustak, A. Prosek, P. Groudev,etc.	All	Further revision DiD description, SSC classification, etc.
Rev. 3	18/11/2015	S. La Rovere, M. Nitoi, A. Wielenberg (ed)	All	Integration of NIEW and ICN contributions
Rev. 4	12/02/2016	A. Wielenberg	All	Restructuring the document
Rev 5	08/04/2016	H . Löffler	several	Integration of JSI comments
Rev 6	07/06/2016	H. Löffler, A. Wielenberg, S. La Rovere		Consolidated version. A summary of the NIER report "memorandum on PSA and DiD added".
Rev 7	09/06/2016	E. Raimond		Approval review. Few modifications proposed. The report needs external review and additional views on the topic.

LIST OF DIFFUSION

European Commission (scientific officer)

Name	First name	Organization
Passalacqua	Roberto	EC

ASAMPSA_E Project management group (PMG)

Name	First name	Organization	
Raimond	Emmanuel	IRSN	Project coordinator
Guigueno	Yves	IRSN	WP10 coordinator
Decker	Kurt	UNIVIE	WP21 coordinator
Klug	Joakim	LRC	WP22 coordinator until 2015-10-31
Kumar	Manorma	LRC	WP22 coordinator from 2015-11-01
Wielenberg	Andreas	GRS	WP30 coordinator until 2016-03-31
Löffler	Horst	GRS	WP40 coordinator WP30 coordinator from 2016-04-01

REPRESENTATIVES OF ASAMPSA_E PARTNERS

Name	First name	Organization
Mustoe	Julian	AMEC NNC
Grindon	Liz	AMEC NNC
Pierre	Cecile	AREVA
Godefroy	Florian	AREVA
Dirksen	Gerben	AREVA
Kollasko	Heiko	AREVA
Pellisseti	Manuel	AREVA
Bruneliere	Hervé	AREVA
Hasnaoui	Chiheb	AREXIS
Hurel	François	AREXIS
Schirrer	Raphael	AREXIS
Gryffroy	Dries	Bel V
De Gelder	Pieter	Bel V
Van Rompuy	Thibaut	Bel V
Jacques	Véronique	Bel V
Cazzoli	Errico	CCA
Vitázková	Jirina	CCA
Passalacqua	Roberto	EC
Bonnevialle	Anne-Marie	EDF
Bordes	Dominique	EDF
Vasseur	Dominique	EDF
Panato	Eddy	EDF
Romanet	François	EDF
Lopez	Julien	EDF
Gallois	Marie	EDF
Hibti	Mohamed	EDF
Brac	Pascal	EDF
Jan	Philippe	EDF
Nonclercq	Philippe	EDF
Bernadara	Pietro	EDF
Benzoni	Stéphane	EDF
Parey	Sylvie	EDF
Rychkov	Valentin	EDF
Coulon	Vincent	EDF
Banchieri	Yvonnick	EDF
Burgazzi	Luciano	ENEA
Karlsson	Anders	FKA
Hultqvist	Göran	FKA
Pihl	Joel	FKA
Ljungbjörk	Julia	FKA
KÄHÄRI	Petri	FKA

Name	First name	Organization
Wielenberg	Andreas	GRS
Loeffler	Horst	GRS
Tuerschmann	Michael	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	GRS
Serrano	Cesar	IEC
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Apostol	Minodora	INR
Nitoi	Mirela	INR
Stefanova	Antoaneta	INRNE
Groudev	Pavlin	INRNE
Laurent	Bruno	IRSN
Clement	Christophe	IRSN
Duluc	Claire-Marie	IRSN
Leteinturier	Denis	IRSN
Raimond	Emmanuel	IRSN
Corenwinder	François	IRSN
Pichereau	Frederique	IRSN
Georgescu	Gabriel	IRSN
Bonneville	Hervé	IRSN
Denis	Jean	IRSN
Bonnet	Jean-Michel	IRSN
Lanore	Jeanne-Marie	IRSN
Espargilliere	Julien	IRSN
Mateescu	Julien	IRSN
Guimier	Laurent	IRSN
Bardet	Lise	IRSN
Rahni	Nadia	IRSN
Bertrand	Nathalie	IRSN
Duflot	Nicolas	IRSN
Scotti	Oona	IRSN
Dupuy	Patricia	IRSN
Vinot	Thierry	IRSN
Rebour	Vincent	IRSN
Guigueno	Yves	IRSN
Prošek	Andrej	JSI
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Olsson	Anders	LRC
Häggström	Anna	LRC
Klug	Joakim	LRC
Kumar	Manorma	LRC
Knochenhauer	Michael	LRC

Name	First name	Organization
Kowal	Karol	NCBJ
Borysiewicz	Mieczyslaw	NCBJ
Potempski	Slawomir	NCBJ
Vestrucci	Paolo	NIER
La Rovere	Stephano	NIER
Brinkman	Hans (Johannes L.)	NRG
Zhabin	Oleg	SSTC
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Caracciolo	Eduardo	RSE
Gorpinchenko	Oleg	SSTC
Dybach	Oleksiy	SSTC
Vorontsov	Dmytro	SSTC
Grondal	Corentin	TRACTEBEL
Claus	Etienne	TRACTEBEL
Oury	Laurence	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Yu	Shizhen	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	TUS
Kubicek	Jan	UJV
Holy	Jaroslav	UJV
Kolar	Ladislav	UJV
Jaros	Milan	UJV
Hustak	Stanislav	UJV
Decker	Kurt	UNIVIE
Prochaska	Jan	VUJE
Halada	Peter	VUJE
Stojka	Tibor	VUJE

REPRESENTATIVE OF ASSOCIATED PARTNERS (External Experts Advisory Board (EEAB))

Name	First name	Company
Hirata	Kazuta	JANSI
Hashimoto	Kazunori	JANSI
Inagaki	Masakatsu	JANSI
Yamanana	Yasunori	TEPCO
Coyne	Kevin	US-NRC
González	Michelle M.	US-NRC

EXECUTIVE SUMMARY

This report is dedicated to the investigation of the link of Probabilistic Safety Assessment (PSA) and assessment with respect to the Defence-in-Depth (DiD) concept for NPP.

After the Fukushima accident the question of further improvements of DiD returned to the focus of discussions.

The DiD, and all its principles, on which lies its implementation, represent the foundation of the deterministic approach to build the safety architecture. The PSA, on its side, through the systematic assessment of all the plausible scenarios and the identification of the challenging sequences, can allow quantifying the degree of progressiveness of the safety architecture, and to verify its tolerant and forgiving character. In this context, looking for the link between DiD and PSA with the objective to optimize their complementarity, is an essential step to help improving the nuclear installation's safety."

The main focus in this report is on the discussion of how an "extended PSA" can be used to verify the adequacy of the application of the defense-in-depth concept. In line with other activities of the ASAMPSA_E project, the report treats mainly PSA Level 1 and Level 2 issues.

In section 2, the report reminds the most important aspects of the current understanding of the DiD concept and discusses important links to PSA in general and extended PSA in particular. Based thereon, several specific issues are identified for further investigation. Section 3 treats the link between the initiating event determination for an extended PSA, intermediate PSA results and the classification of potential initiating events (PIE) for DiD assessments. Section 4 is dedicated to classification schemes for systems, structures, and components (SSC), the reliability of engineered safety functions and the links to PSA. Complementary, in section 5, the report looks at requirements on PSA models to facilitate DiD-related assessments and other important DiD-related issues not previously discussed. Finally, in section 6 conclusions and recommendations are provided.

The concepts of DiD and PSA have been initially developed independently in the history of NPP safety. The traditional role of DiD is in the design of the plant and its safety provisions, while PSA calculates the probability for failure of the safety provisions and quantifies the risk profile of the NPP. Therefore, PSA is a tool for complementarily evaluating the level of safety achieved by implementing the DiD concept including all other safety related activities.

Keeping in mind these complementary objectives of DiD and PSA, it is recommended that DiD and PSA be developed independently of each other. If a NPP could demonstrate that it follows all applicable DiD rules, and if an independent PSA confirms a low risk of this plant, there would be a well-founded confidence in an adequate level of safety for this plant. If, on the other hand, PSA identifies a high or unbalanced risk profile for the plant, there are doubts as to whether the current application of the DiD concept is sufficient and additional safety provisions are expected. This impact of PSA is now included in the DiD concept, as a complement for the design..

However, beyond this basic concept of independence there are a few issues which establish links between DiD and PSA:

- PSA should be structured in such a way that the individual levels of DiD can be identified ;this will enable to verify the contribution of each level of DiD to the overall safety, and it can identify potential weaknesses in individual levels of DiD;
- DiD as well as PSA have their own concepts for including or dismissing events or phenomena from their respective analyses ; it is not recommended to harmonize these features in order to keep the benefits of diversity ; in contrast, any differences in assumptions should be clearly identified and documented ;the evaluation of such differences may be more fruitful than striving for a more unified approach;

- the discussion on the evolution of the DiD concept – partly to be found in the present document – is not related to the progress in PSA methods; whatever the DiD concept, PSA will be able to reflect it in principle; this does not mean that the PSA method is perfect ;here are important deficiencies in PSA (e.g. lack of data, incompleteness, insufficient methods for some human actions, large requirement of resources, etc.), but they are not related to DiD issues;
- If PSA shows that a particular level of DiD does not contribute significantly to reducing risk, or if PSA indicates that even without a particular level of DiD risk targets can be met, there are arguments to relieve DiD requirements for this particular plant; on the other hand, if PSA indicates a high risk, it is advisable to improve the design, possibly by strengthening the DiD approach; the consideration of "extended PSA" results as an important safety indicator in that context can be promoted but this, however, requires that the PSA accomplishes the highest quality standards.

Conversely, there are several issues regarding the relationship between PSA and DiD, which could not be investigated in depth in this report and need to be subject of future discussions:

- discussion and recommendations in this report are largely at a conceptual level ; this is partly due to the lack of previous investigations into the subject and partly due to a lack of practical implementations and feedback on good practices in the PSA community ; therefore, specific guidance on how to do practical modelling of PSA with a view to do DiD assessments could be subject to subsequent work;
- PSA models often have been produced without the specific objective of assessing the implementation of DiD by DiD levels; therefore, existing PSA models would have to be modified to comply with the recommendations of this report; however, guidance on how to do this in an effective manner could not be achieved in this project; moreover, changing the structure of an existing PSA model to fall in line with DiD levels is a significant effort; there is still no clear consensus if the added value justifies the work; both aspects require further discussion;
- an important aspect of the feasibility of PSA modelling is the availability of data for initiating events as well as failure probabilities of SSC; a PSA model that systematically includes SSC on DiD level 2 (or even DiD level 1) would require additional data that are not readily available from existing PSA models; whether existing operating experience databases could supply the required information or if data gathering practices would need to be changed should be investigated.

CONTENT

ABBREVATIONS

AOO	Anticipated Operational Occurrence
BDBA	Beyond Design Basis Accident
BWR	Boiling Water Reactor
CDF	Core Damage Frequency
DBA	Design Basis Accident
DEC	Design Extension Condition
DiD	Defence in Depth
DSA	Deterministic Safety Assessment
ERF	Early Release Frequency
FDF	Fuel Damage Frequency
FMEA	Failure Mode and Effect Analysis
IE	Initiating Event
ISLOCA	Interfacing System LOCA
LERF	Large Early Release Frequency
LOCA	Loss of coolant accident
LRF	Large Release Frequency
LWR	Light Water Reactor
NPP	Nuclear Power Plant
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Analysis
PWR	Pressurized Water Reactor
RR	Research Reactor
SFP	Spent Fuel Pool
SNETP	Sustainable nuclear energy technology platform
SSC	Systems, Structures, and Components

1 INTRODUCTION

This report is dedicated to the investigation of the link of Probabilistic Safety Assessment (PSA) and assessment with respect to the Defence-in-Depth (DiD) concept for NPP.

After the Fukushima accident the question of further improvements of DiD returned to the focus of discussions as it happened earlier after the major accidents in TMI2 and Chernobyl. This attitude has been supported by many publications, e.g. by SNETP [61] where it is said that "enhancement of further defence-in-depth capabilities for any type of initiating events, especially for severe natural hazards and any of their combinations is found to be substantial as well as to address more systematically at the design stage the plant features for coping the design extension conditions (beyond design basis accidents) to assure the robustness of the defence-in-depth and to avoid cliff edge effects. The approach should include situations where several units on the same site are affected by a beyond design basis event." In the given reference also it can be found that "development of multiple and more robust lines of defence with respect to design basis events and design extension conditions is necessary to define additional measures to be considered in the design."

As an introduction to the topic, the paper on peculiar roles of DiD and PSA in NPP [59] states the following:

"The safety architecture of a nuclear installation shall allow meeting the safety objectives while complying with the principles defined, for example, within the IAEA SF1.

The optimization of plant's safety performances both in terms of physical performances and in terms of reliability in achieving the requested safety functions is a complementary objective which resumes the compliance with the full set of basic principles which shall support the plant's design and its safety assessment.

Exhaustiveness, progressiveness, as well as the tolerant, forgiving and balanced character of the plant's safety, are characteristics / indicators which can help assessing the degree of optimization.

The DiD, and all its principles, on which lies its implementation, represent the foundation of the deterministic approach to build the safety architecture. If correctly interpreted / implemented, DiD help guaranteeing – as far as feasible – exhaustiveness and progressiveness. The correct design of the provisions which characterize – and materialize – the different DiD's levels help guaranteeing the tolerant and the forgiving character of the plant's safety.

The PSA, on its side, through the systematic assessment of all the plausible scenarios and the identification of the challenging sequences, can allow quantifying the degree of progressiveness of the safety architecture, and to verify its tolerant and forgiving character.

The PSA results provides an overview of the plant's safety performances in terms of degree of "balance" for the prevention, the management and the consequences limitation for the whole set of the considered design basis conditions, as well as for the design extension conditions. This provides essential insights to correct – as needed and as feasible – possible discrepancies.

In this context, looking for the link between DiD and PSA with the objective to optimize their complementarity, is an essential step to help improving the nuclear installation's safety."

The main focus in this report will be on the discussion of how an "extended PSA" can be used to verify the adequacy of the application of the defense-in-depth concept." [17], p. 16. In line with other activities of the ASAMPSA_E project, the report treats mainly PSA Level 1 and Level 2 issues.

In section 2 we recap the most important aspects of the current understanding of the DiD concept and discuss important links to PSA in general and extended PSA in particular. Based thereon, several specific issues are identified for further investigation. Section 3 treats the link between the initiating event determination for an

extended PSA, intermediate PSA results and the classification of potential initiating events (PIE) for DiD assessments. Section 4 is dedicated to classification schemes for systems, structures, and components (SSC), the reliability of engineered safety functions and the links to PSA. Complementary, in section 5 the reports looks at requirements on PSA models to facilitate DiD-related assessments and other important DiD-related issues not previously discussed. Finally, section 6 proposes some conclusions and recommendations on the link between DiD and extended PSA.

2 THE DEFENCE-IN-DEPTH CONCEPT AND THE LINK TO PSA

The concept of Defence-in-Depth (DiD) as basic approach for achieving a high level of safety for nuclear installations was first described in the late 1960s and early 1970s [6]. While the concept was initially limited to multiple barrier systems, the DiD concept has been expanded to apply to all safety functions for nuclear installations (and even beyond) [5], [6], [27], [29]. In this respect, the DiD concept can be seen as one of the most important aspects of the safety philosophy for nuclear facilities and activities. This broad scope of the DiD concept in its current usage is well reflected in the definition given in the IAEA Fundamental Safety Principles SF-1 [1], p. 13f:

The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. […] The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

Defence in depth is provided by an appropriate combination of:

- *an effective management system with a strong management commitment to safety and a strong safety culture.*
- *adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy, mainly by the use of:*
  - *design, technology and materials of high quality and reliability;*
  - *control, limiting and protection systems and surveillance features;*
  - *an appropriate combination of inherent and engineered safety features.*
- *comprehensive operational procedures and practices as well as accident management procedures."*

In this sense, the DiD concept entails a sound design and engineering approaches to implement a safety architecture characterized by highly reliable provisions (inherent and engineered safety features, operational procedures and practices as well as accident management procedures) and structured in independent layers of provisions, so that if a failure were to occur, it would compensated for or corrected by appropriate measures [7]. Beyond the safety architecture (i.e. technical and I&C systems, including the associated hardware and software, etc.), DiD has also been applied to security issues (then phrased e.g. as "protection-in-depth"), to radiation protection, to software security and reliability as well as other areas. It should be noted that the definition of SF-1 encompasses the organizational (management system and safety culture) and human performance issues related to the specific realization of DiD as well. The DiD concept is strongly endorsed by WENRA for existing [26] and new reactors [7]. WENRA positions are based on IAEA SSR-2/1 with some specific changes explained below.

With respect to NPP, IAEA SSR-2/1 provides additional guidance [2]. Specifically, SSR-2/1 re-iterates that the DiD concept shall be "applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown modes". [2], p. 6. Furthermore, SSR-2/1 describes different areas of application for the DiD concept [2], p. 7f, and gives further requirements related to the design of a NPP [2], p. 14f. The resulting areas are relevant to the issue of this report, i.e. the link of DiD and (extended) PSA, and are therefore shortly summarized in the following.

1. SSR-2/1 defines five level of Defence in Depth [2], p. 7f. (cf. also [43]) related to
   1.1. Prevention of deviations from normal operation (DiD Level 1)

1.2. Detecting and controlling deviations from normal operational states (anticipated operational occurrences – DiD Level 2)

1.3. Detecting and controlling postulated initiating events (PIE) as design basis accidents (DiD Level 3)

1.4. Mitigating the consequences of failures of the third DiD level (including postulated core melt) and maintaining containment integrity for design extension conditions (previously Beyond Design Basis Accidents - DiD Level 4)

1.5. Mitigated consequences of significant accidental releases (on- and off-site – DiD Level 5)

A short summary of the most important characteristics of the five levels of DiD, in a recent variant by the WENRA Reactor Harmonization Working Group is given in Fig. 1adapted from [7], with a further subdivision of level 3 in level 3a (single failure events) and level 3b (postulated multiple failure events). Following WENRA, "Even though no new safety level of defense is suggested, a clear distinction between means and conditions for sub-levels 3.a and 3.b is lined out. The postulated multiple failure events are considered as a part of the Design Extension Conditions in IAEA SSR-2/1" [7], i.e. for the prevention of severe fuel damage. The complementary set of Design Extension Conditions corresponds to the postulated severe fuel damage [26].

SSG-2 [3] gives recommendations on the frequency of occurrence for (postulated) initiating events. These can be considered as complementary to that provided by WENRA and allows to correlate the DiD levels to the estimated frequency of certain initiating event scenarios (failures). Further, one can consider that this allows roughly identifying reliability targets for the sets of provisions which materialize the different levels of the DiD.

2. For each of the aforementioned levels of DiD, safety provisions (inherent features, systems, or procedures) should be defined to reach the respective safety goal. Importantly, the layers of provisions for each level of DiD should be independent from each other and should be effective [2] [7]. SSR 2/1 gives further (generic) recommendations for the design of safety related systems, e.g. in requirements 4 to 28 [2], cf. also [43]. These additional requirements are not an integral part of the DiD concept, however, but means for reaching independent and effective provisions for the respective safety functions[1]. It should be noted that safety functions at the DiD levels 1 to 4 relate to the design and operation of the plant itself, while DiD level 5 (off-site releases) relates mainly to off-site emergency planning.

3. A further aspect according to SSR-2/1 consists of the realization of different (physical) barriers for the confinement of radioactive material [2], p. 8. These provisions entail not only the barriers themselves but extend to safety features for maintaining the integrity/effectiveness of the barriers (confinement of radioactive material). Again, the barriers should be independent and reliable.

[1] In more specific (national) regulation, there are sometimes quite detailed technical requirements on NPP systems with reference to the level of DiD they are designed for, e.g. with respect to redundancy, diversity, independence, single-failure-criterion, etc.

Table 1. Subdivision of postulated initiating events according to SSG-2, [3], p. 8

Occurrence (1/reactor year)	Characteristics	Plant state	Terminology	Acceptance criteria
10^{-2}–1 (expected over the lifetime of the plant)	Expected	Anticipated operational occurrences	Anticipated transients, transients, frequent faults, incidents of moderate frequency, upset conditions, abnormal conditions	No additional fuel damage
10^{-4}–10^{-2} (chance greater than 1% over the lifetime of the plant)	Possible	Design basis accidents	Infrequent incidents, infrequent faults, limiting faults, emergency conditions	No radiological impact at all, or no radiological impact outside the exclusion area
10^{-6}–10^{-4} (chance less than 1% over the lifetime of the plant)	Unlikely	Beyond design basis accidents	Faulted conditions	Radiological consequences outside the exclusion area within limits
$<10^{-6}$ (very unlikely to occur)	Remote	Severe accidents	Faulted conditions	Emergency response needed

For existing reactors, WENRA distinguishes two categories of Design Extension Conditions (DEC): DEC A covers scenarios for which severe fuel damage can be prevented and results in respective provisions and DEC B entails scenarios with postulated severe fuel damage and thus calls for respective provisions for the mitigation of postulated severe fuel damage [26], p. 20. Dedicated provision to address DEC A or DEC B are properly allocated to DiD Level 4. A representative set of DEC A scenarios shall be determined based on DSA, PSA, and engineering judgement insights. DEC A should cover events for operational states of the plant, hazard events, and common cause failures, “which cannot be considered with a high degree of confidence to be extremely unlikely to occur” [26], p. 20. For DEC A, the objectives of the analysis shall be a demonstration that the plant can maintain the fundamental safety functions for preventing core degradation, whereas for DEC B the objective is that the plant can maintain the confinement of radioactive material released after core degradation. With respect to DEC A, WENRA reference levels for existing reactors call for more strict acceptance criteria for a safety demonstration than implicated in SSR-2/1. Conversely, SSR-2/1 requires grouping multiple failure events like e.g. common cause failure initiators into the design basis based mainly on their likelihood [2], p. 24, which is not explicitly addressed in [30]. It has to be recognized that the WENRA Reference Levels are formally intended to be applied to existing reactors, while SSR-2/1 conceptually addresses the design of (new) reactors. In that regard, WENRA’s position on existing reactors is fundamentally consistent with SSR-2/1 if applied to existing reactors.

For new reactor designs, the RHWRG under the auspices of WENRA has published a position paper [7]. The application of DiD for new reactors is explicitly discussed. RHWG recommends reinforcing and strengthening the DiD approach (compared to previous realizations). Most prominently, RHWG subdivides DiD Level 3 into sub-level 3a, which entails postulated single failure events, and sub-level 3b, which covers multiple failure events not leading to a postulated severe accident (cf. Fig. 1)

. Thereby, DiD Level 4 addresses postulated severe accident scenarios. With the introduction of DiD Level 3b, RHWG tightens the acceptance criteria for multiple failure events compared to SSR-2/1 (cf. [7], p. 13f), if these multiple failure events were assigned to DEC[2] according to SSR-2/1.

RHWG gives specific guidance for the identification of multiple failure events for sub-level 3b. It entails common cause failure events, not caused by a postulated hazard, which affect similar equipment in provisions for safety functions [7], p. 19. CCF events should be considered, which either affect the fulfilment of a safety function needed to controls an AOO or single PIE or which are needed to fulfil the fundamental safety functions in normal operation. A set of bounding scenarios should be derived considering the frequency of the event, available grace times, margins to cliff-edge effects, and potential radiological consequences. RHWG explicitly mentions that cut off-frequencies should be justified considering overall CDF [7], p. 21. In summary, [7] defines more stringent criteria for the assignment of multiple failure events into DiD level 3 than SSR-2/1, and explicitly requires consideration of CCF events.

The ASAMPSA_E report "Bibliography on Defense in Depth for Nuclear Safety" [27] provides an overview over a lot of references relevant to the DiD concept for nuclear safety and NPP in particular with a focus on regulatory sources. For a more in-depth discussion of DiD, the interested reader is referred to the references cited therein and in this report [5], [6], [7], [40]. In the following, the link between DiD (a concept for achieving safety) and PSA (a safety assessment approach) in general and extended PSA in particular will be established.

[2] As already mentioned above, according to SSR-2/1 multiple failure events can be classified as design basis accidents, i.e. assigned to DiD Level 3, depending mainly on their likelihood of occurrence.

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact	Postulated single initiating events
Level 3 3.b		Additional safety features , accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures	

Fig. 1 Levels of Defence in Depth for new reactors adapted from RHWG 2013 [7], p. 11

The adequate realization of the DiD concept needs to be assessed (cf. e.g. SSR-2/1 [2], p. 34). GSR Part 4 defines that safety assessments are performed "by means of deterministic and also probabilistic methods" [18], p. 11, and explicitly points out that "[p]robabilistic approaches may provide insights into system performance, reliability, interactions and weaknesses in the design, the application of defence in depth, and risks, that it may not be possible to derive from a deterministic analysis." [18], p. 24f.

Thereby, the link between the DiD concept and an (extended) PSA is clearly established. Moreover, there arise multiple potential issues for further discussion.

1. The assignment of postulated initiating events of a certain category and, through the WENRA proposal (cf. Fig. 1), to the level of DiD relies (explicitly or at least partially[3]) on an estimation of the frequency of occurrence of said PIE (cf. e.g. SSG-2 [3], [40], [7]). This can be either done based on a statistical evaluation of operating experience, expert judgements or probabilistic assessments. WENRA specifically mentions that selection of PIE shall be based on deterministic as well as probabilistic methods [26]; this is reiterated in [7] for the selection of events for sub-level 3b. Consequently, using PSA insights for the selection of PIE and their assignment to levels of DiD is relevant to this report (section 3.1).

[3] Especially for design basis accidents and design extension conditions (DiD levels 3 and 4), some regulatory bodies have defined requirements for the inclusion or even exclusion of certain events (cf. e.g. [11]). These requirements often include considerations other than the frequency of occurrence, e.g. deterministic assessments, historical precedent, precautionary principle, etc.

2. The reliability of the different DiD levels, i.e. the reliability with which the safety functions are achieved by the corresponding "layers of provisions" [2], [43], [44], is an important aspect of DiD (cf. e.g. GSR-4 [18]). There are a number of deterministic design requirements and practices, which are intended to ensure a high reliability of the material and immaterial provisions: engineered safety features, inherent characteristics, procedures, operator interventions, etc.

   For safety systems, these principles include: physical separation, independence, fail safe design, redundancy, diversity, safety margins, conservative design, and single failure criterion [2]. The reliability of an engineered safety features can be analysed quantitatively using a probabilistic assessment. For some safety features, e.g. passive safety systems and/or safety related inherent characteristics, requirements such as redundancy or independence, can be relaxed if the designer can guarantee, with the selection of adequate design options, that the key objectives in terms of physical performances (i.e. the capability to correctly achieve the requested mission) and reliability (i.e. to achieve the mission with the due reliability); for the latter the role of PSA is obviously essential. This is related for example to the probabilistic assessment of passive safety system reliability, which is still an issue of on-going research and which covers, e.g., probabilistic fracture mechanics to address possible pipes failures, probabilistic thermal hydraulics to address concerns related to natural convection, etc.

   For immaterial provisions, such as for example the operator interventions, the probabilistic assessment will bring insights providing that the human factor is correctly addressed and taken into account. .

3. The independence of subsequent layers of provisions (including safety systems and other safety features) for controlling an initiating event between different levels of DiD (especially levels 3 and 4) is an important aspect of DiD (cf. e.g SSR-2/1 [2]). The need for provisions of safety functions on different levels of DiD to be independent is implicitly required in the WENRA Safety Reference Levels as well, cf. issue E2 [27], p. 13 and issue G3 [27], p. 24. Independence of all levels of DiD is presented as position 2 by the RHWG for new reactor designs [7] and objective 4 in a November 2010 statement [34], requesting that SSC for safety functions are not adversely affected by the operation or failure of other SSCs on other levels of DiD and that effects of the PIE, including secondary effects, do not compromise the SSC as well [7], p. 15. Further sources of dependent failures affecting multiple, redundant layers of provisions include functional dependencies, dependencies through system interfaces, multiple functions assigned to systems and components, operator error, and common cause failures [44]. This aspect can usually be assessed mainly with deterministic means. In a lot of cases, however, it is rather difficult to demonstrate complete independence especially of active safety features (because of common support systems, connections via operating systems, potential common cause failures, etc.) on different DiD levels, so that a reasonably practicable degree of independence needs to be demonstrated [7]. To this end, RHWG recommends justification by an appropriate combination of DSA, PSA, and engineering judgement [7], p. 16. This entails the use of PSA for the assessment of the degree of independence between DiD layers of provisions. Moreover, the systematic approach of a PSA can be instrumental to discovering interdependencies between safety features, the analysts were previously not aware of, cf. also SSG-3 [4], p 40ff on dependent failures. This is further discussed in section 5.2

4. As part of the design of systems, structures, and components (SSC), they need to be classified for their importance for safety [2], [26]. Based on their classification(s), SSC and, more generally all the provisions which are integral part of the safety architecture, become subject to specific requirements on applicable design rules, qualification requirements, safety margins, testing regimes, limits and conditions, acceptance criteria for safety demonstrations, etc. Classifying the provisions (including SSC) and (based on the sequences which follow postulated initiating events), assigning them to different levels of DiD is an important aspect of the DiD concept. Specifically, the requirement of independence between the different levels of DiD [26], as

discussed above, is dependent on a prior classification of the provisions (including SSC) which are constitutive of the corresponding layers. While the classification of SSC and immaterial provisions shall be based primarily on deterministic methods, probabilistic input may be considered if appropriate [2], [26]. This establishes a clear link to PSA insights (cf. section 4.1).

5. The probabilistic assessment of the progression of an (accident) event scenario through the (five) levels of DiD and the successful operation or failure of the safety features on these different levels of DiD is clearly an issue. For this application, the PSA would have to be structured along the levels of DiD - and have a sufficient scope, e.g. be able to represent and model the whole set of layers of provisions and their detailed content. In that case, it could provide for immediate input for assessment of DiD.
6. It is a well-known fact that some PSA tools for risk monitoring provide information about the "status of DiD" or more precisely the "*status of safety functions, individual safety systems and the set of safety systems required for an initiating event/ plant transient*" [23], p. 4, which are seen to "*give an indication of the level of redundancy, diversity, defense-in-depth for a specific level, safety margins, etc. available for the current plant configuration*". [23] p. 121. In most cases, this information is based on available trains of (safety) systems and related to the requirements on the technical specifications for the availability of these trains. The data about system or component availability and plant operating status are often fed into the risk monitor models directly from an integrated operation management system. To the extent this DiD status information is derived solely from logical rules and presented as qualitative risk information [23], this constitutes a secondary use of the fault tree models of a PSA related to deterministic requirements and rules (cf. SSG-3 [4], p.144) . This can be complemented by quantitative information about the risk status of certain systems. Both cases are relevant to this report, especially in connection to the previous issue.

These issues will be discussed in more detail in the following sections.

3 CONSISTENCY BETWEEN PIE AND PSA IE AND INTERMEDIARY RESULTS

3.1 POSTULATED INITIATING EVENTS

The identification of postulated initiating events (PIE) is the initial step of a safety analysis. Thus, it is also a cornerstone in the application of the DiD concept. In this section, the link between the assignment of PIE to levels of DiD and to the frequency determination of events for PSA will be discussed in more detail.

Combining the guidance in SSR-2/1 [2], SSG-2 [3], and WENRA Reference Levels [26] as well as international good practice, PIE are classified and assigned to the different levels of DiD as described below. Classification, grouping, and assignment of PIE are to be based on deterministic as well as probabilistic insights, operating experience and other considerations[4]. The identification of PIE for all operating states extends to hazard events as well. A common understanding of the term "postulated initiating event" is that is defined by a specific event, e.g. the failure of one non-safety system or one component or a specific hazard impact scenario and their respective consequential effects. However, scenarios typically considered as PIE for DBA or DEC can easily be the results of several (more or less likely) faults. In order to better capture multiple failure events due to CCF - because CCF

[4] Some national regulators have drawn up lists of (generic) PIE already classified and assigned to levels of DiD.

mechanism impact is often not postulated when defining PIE - the RHWG introduced sub-level 3b for new reactor designs [7].

A very important, but not the only input to the classification and assignment of PIE is the (assumed or ascertained) frequency of the event or hazard (scenario) [2], [26]. It should be noted that neither SSR-2/1 [2] nor the WENRA Reference Levels for existing reactors [26] do give specific recommendations on frequency thresholds for the different categories below. Similarly, the RHWG report [7] does not provide numbers for these categories for new reactor designs, although scenarios leading to unacceptable releases are required to be practically eliminated.

Notably, SSG-2 contains references to frequency ranges commonly applied when classifying PIE [3], see also [44]. The numbers given below should be considered as qualitative indicators rather than rigid limits. In particular, there may be events which are traditionally considered as design basis accidents (e.g. large break LOCAs) although they may have lower frequencies than those indicated in the table for design basis accidents. This results in the following categories:

- anticipated operational occurrence (AOO), which should be contained with provision on DiD level 2
  SSG-2 states a frequency threshold of $\gtrsim 10^{-2}$ /yr;
- design basis accident (DBA), which should be contained with provisions associated to DiD level 3 at the most
  SSG-2 states a range for the frequency of occurrence between $\lesssim 10^{-2}$ /yr and $\gtrsim 10^{-4}$ /yr.
  The separation into DiD level 3a (single failure events) and level 3b (postulated multiple failure events by RHWG is not made explicitly in terms of frequency of occurrence, but rather qualitatively by explicitly assuming CCF event impact. CCF events are usually studied in PSA, where typical values for CCF event probability per year can be significantly below 10^{-4} /yr. It is noted by the RHWG that PIE on DiD level 3b can be classified as design extension conditions according to SSR-2/1 [7], p. 19, especially having in mind SSG-2 recommendations.
- Design extension condition (DEC) (previously termed beyond design basis accidents [12]), which should be contained with provisions associated to DiD level 4 at the most
  with a frequency of occurrence between $\lesssim 10^{-4}$ /yr and $\gtrsim 10^{-6}$ /yr according to to SSG-2.
  For DEC scenarios, limited core damage and releases into the containment can be acceptable. According to SSR-2/1 ensuring the containment safety function and thus practically eliminating unacceptable releases is one focus of DEC analysis. For existing nuclear power plants, WENRA further subdivides DEC scenarios into DEC A related to the prevention of severe fuel damage and to DEC B, related to mitigating accidental releases [26]. For new designs, WENRA reference levels state that unacceptable (large) releases need to be practically eliminated [7].
  It should be noted that SSG-4 references a value of $\lesssim 10^{-6}$ / yr for Large Release Frequency (unacceptable release) of current NPP designs [13], some national regulators have set even smaller values up to $\lesssim 10^{-7}$ / yr.
  Based on these remarks, DEC events should be treated in PSA Level 1, if they do not involve a core or fuel damage scenario (i.e. DEC A), or in PSA Level 2, if they do (i.e. DEC B). Notably, certain events considered as DEC might be screened out from further detailed analysis in a PSA (cf. ASAMPSA_E D30.5 [36]) if they meet the respective screening criteria for screening them out. If e.g. the WENRA position on practical elimination of unacceptable releases is applied, this might result in respectively small screening frequency thresholds for initiating events related to DEC A and DEC B scenarios. The report ASAMPSA_E D30.3 [35] discusses screening for an extended PSA in more detail.

Sequences which are known as Severe accidents (SA) entailing an unacceptable release to the environment correspond to measures assigned to DiD level 5, and a frequency of occurrence $\lesssim 10^{-6}$ /yr according to SSG-2. SSR-2/1 and WENRA for new reactors [7] require that scenarios with an unacceptable accidental release are "practically eliminated" [2], p. 6. However, in these cases no quantitative number is given for practical elimination. One can assume that that threshold is somewhere around 10^{-9} - 10^{-6} /yr. Moreover, the limited validity/high uncertainty of probabilistic analyses for such extremely rare scenarios should be taken into account.

It should be noted that the value of $\gtrsim 10^{-4}$ given in several documents as a lower limit for design basis accidents is the same as the CDF target of 10^{-4} /yr for reactors existing in the 1980s as referenced e.g. in SSG-3 [4]. This a notable coincidence as the development of the DiD concept was influenced by the initial risk assessments for NPP (cf. e.g. [45]).

There is obviously some need to harmonize the recommended frequency thresholds for the PIE classification scheme of SSG-2 [3] with recent quantitative probabilistic safety criteria/design objectives, which relate to PSA end states. This is mainly relevant for the deterministic approach and will not be investigated in-depth in this report.

Another important aspect is of course the determination of PIE frequency of occurrence. Neither SSG-2 [3] nor other deterministic guidelines present specific methodology for the determination of PIE frequencies, so approaches commonly used for PSA, such as those recommended in SSG-3 [4], are expected to be applied. SSG-3 recommends using data from operating experience (plant specific and/or generic) or from expert judgement or assessments with initiating event fault trees for PSA Initiating Events [4]. For this discussion, it is assumed that for a lot of (more frequent) PIE the respective frequencies that are used for an assignment to the different categories (respectively the levels of DiD), particularly for anticipated operational occurrences and design basis accidents, can be determined using basically the same data and similar methods and approaches as applied for the corresponding Initiating Events in PSA. A potential difference could be that the PIE frequency can be estimated conservatively for a deterministic analysis, whereas a related IE frequency would be determined as best estimate value under best estimated boundary conditions and with uncertainty distribution for a state-of-the-art PSA. However, especially for rare events, this distinction becomes largely moot due the scarcity of data. Other PIE investigated in DSA can be related to intermediary states in a PSA, e.g. if the specific failure conditions of safety features are assumed, which are arrived at in the PSA event tree modelling of a related scenario. In any case, the frequency values assumed for PIE in deterministic analyses should be consistent to the related IE frequency or event tree sequence results of the PSA, as applicable. For DEC events, the respective probabilistic results can often be found in sequences of PSA Level 1 and/or Level 2.

It should however be noted, that

1. From historical evidence, actual severe accidents happened more often than predictions for the least likely DBAs, e.g. no large break LOCA occurred. If risk analysts were to disregard or wrongly evaluate the risk of initiators and scenarios leading to severe accidents and if such cases are not subject to risk analyses, plant risk may not be balanced ,
2. Actual events are usually not starting exactly as the postulated DBA initiators.
3. From the point of view of risk, there is no need to make distinctions between initiators/scenarios as "design basis", "design extension conditions" and beyond design or even severe accident.
4. Analysts should be aware that the original sets of DBAs were postulated as "limiting accidents" by nuclear engineers more than 50 ago based on the knowledge and consensus at the time. Now however, the knowledge base (physics, experiments, simulations/models) including statistics on DBAs as well as on SAs

is much more developed and established. This needs to be reflected in the determination of DBA and design extension conditions as limiting scenarios for the design of plants as well as for the deterministic safety evaluation.

The ASAMPSA_E project focuses on extended PSAs, i.e. calculating "the risk induced by the main sources of radioactivity […] on the site, taking into account all operating states for each main source and all possible relevant accident initiating events (both internal and external) affecting one NPP or the whole site." [14], p. 147. In this context, one key aspect is the systematic extension of PSA to all relevant hazards and their relevant combinations. Therefore, the identification of hazard events or combinations of events that could challenge the safety of the plant and recommendations for the estimation of a hazard frequency curve (i.e. hazard intensity vs. frequency of exceedance) are investigated in the ASAMPSA_E project. These topics are treated mainly in WP 21 and WP 22, specifically in the deliverables D21.3/4 on external hazards modelling for PSA and D22.2/3 on the implementation of external hazards modelling in extended PSA [17]. Within WP 30, the deliverable ASAMPSA_E D30.3 [35] discusses the selection of initiating events for an extended PSA and specifically screening criteria for hazard scenarios. Therefore, these issues are not discussed further in this report.

Finally, with regard to the link between DiD and (extended) PSA, two rather obvious remarks need to be made. First, the list of initiating events of an extended PSA (i.e. internal events, hazard event groups, combination events) should be checked against the list of PIE for deterministic safety analyses, i.e. AOOs, DBAs and scenarios for design extension conditions (DEC), cf. SSG-2 [3]. In addition, SSR-2/1 consistent to WENRA [7], [26] explicitly requires that the list of PIE shall be determined "on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment" [2], p. 19. The scenarios analysed in an assessment of DiD (with deterministic methods) should include all scenarios analysed as initiating events in an extended PSA with frequency of occurrence commensurate to design basis events and also design extension conditions, as applicable. In this respect, the list of IE of an extended PSA can be used to check the completeness of the design envelope (AOO, DBA, and DEC). In fact, SSG-2 hints at this link between the classification of PIE and PSA in para 2.9 [3], p. 7. Conversely, the list of PIE for deterministic safety analyses (AOO, DBA and DEC) should be treated in an extended PSA. It should be noted that this does not necessarily mean an extension of the scope of detailed analyses for the deterministic or the probabilistic analyses. For the former, a lot of events can be treated with enveloping PIE in terms of a DiD assessment. For the latter, the grouping of initiating events for accident sequence analysis achieves the same reduction in detailed modelling. In addition, some of the PIE defined deterministically as DBA or for DEC are arrived at in the event progression analysis (event tree sequences) of PSA level 1 or PSA level 2 and some AOO events might not lead to an initiating event for the PSA at all.

Secondly, the frequency of initiating events of the PSA, specifically the frequency of hazard scenario groups or other event groups, needs to be checked against the classification of PIE. In addition, if PIE classified as DBA or DEC are (intermediary) results of an extended PSA, the frequencies determined by the PSA should be checked against the assumptions for the deterministic classification. Particularly if the frequency values or distributions, respectively, determined for the PSA are inconsistent with those used in the classification of PIE as AOO, DBA or DEC for operating plants, the authors recommend that these classifications should be revisited. For new plants such checking can by used as a support to define the initial set of PIEs for AOOs, DBAs or DECs. The potential implications for the design envelope of the plant are obvious. This is one example how PSA can complement the deterministic approach in identifying safety-significant weaknesses in the design of the plant (cf. GSR-4 [18], p. 24f, SSG-3 [4], p. 13, SSG-25 [15], p. 30, SSG-4 [16], p. 61 related to DEC).

As explained in section 2 above, the process for the determination of PIE is using to a large extent the same kind of information as the process for identifying IE for a PSA Level 1. Moreover, intermediate results from PSA Level 1 and – to some extent – PSA Level 2 can be mapped to DBA or DEC events postulated in DiD assessments. This section is dedicated to the discussion of these two links.

The definitions of an IE and PIE found in IAEA guides are presented in the Glossary of this report. Although those definitions themselves inevitably introduce some differences between IE and PIE, there are several other implicit differences to consider. An IE in PSA is usually a trigger event (the very first event in the chain of events potentially resulting in core/fuel damage) in event tree sequences while PIE can be both the single trigger event and a sequence of events. So, PIE considered in DSA can match both IE defined in PSA and intermediate PSA results (i.e. specific sequences in the event tree model, usually of PSA Level 1) and even PSA end states (e.g. sequence of events resulting in core/fuel damage). Some theoretical background on PSA model construction can be found in the appendix of D30.5 [36]. The appropriate mapping of the IEs analysed in PSAs to PIEs analysed in DSAs and vice versa is therefore a crucial issue for any mutual cross checking to find incompleteness or inconsistencies in the specific PSA or DSA. Moreover, the mapping will depend strongly on the IE event determination and screening for the PSA (cf. ASAMPSA_E D30.3 [35] for additional discussion) and the scope and level of detail of the PSA model.

3.2 CONSISTENCY OF FREQUENCY DETERMINATION

Deterministic analyses (DSAs) often assume certain boundary conditions for PIEs (apart from the induced effects and failures caused by the PIE itself). Those conditions often include occurrence of LOOP, occurrence of additional single failure in the safety system, failure of non-safety systems, or application of additional conservative plant parameters (if conservative analyses are used), see SSG-2 [4]. All those conditions (if selected for the given PIE) are usually supposed to occur simultaneously at the time of the PIE occurrence. Importantly, these additional boundary conditions are selected without (explicitly) considering their (conditional) likelihood, but rather to achieve a robust deterministic safety case.

On the other hand, those boundary conditions should be treated in PSA probabilistically (i.e. their simultaneous occurrence is assumed with their conditional probabilities), which gives the less conservative estimation. This can result in very low frequencies of PIEs (including all assumed boundary conditions), particularly if the occurrence of those conditions is independent on the PIE. As an example, if the frequency of large LOCA is assumed 10^{-4}/y and the frequency of a random occurrence of LOOP in an NPP region is 10^{-1}/y, then the simultaneous occurrence of large LOCA and LOOP within 24 hours is approx. 5×10^{-8}/y (if the order of events does not matter).

For any comparison of PIE for DSA and IE for PSA it is therefore important to understand the basic scenario for the PIE (e.g. loss of feedwater, small LOCA) and additional boundary conditions attached to the PIE for DSA (e.g. loss of offsite power). In addition, PIEs classified as AOO, DBA, or DEC can be related in that the DBA case is arrived at by an AOO with postulated additional unavailabilities or failures, and similarly the DEC scenarios has additional failures to the DBA case. In such cases, the deterministic classification usually considers only the frequency estimation for the basic scenario (e.g. loss of feedwater), whereas more severe scenarios (e.g. total loss of feedwater without SCRAM) are often not based on explicit consideration of conditional probabilities. These more severe scenarios are usually arrived at in PSA models via failures of the respective safety functions in specific event tree sequences. Conversely, the IE often considered in the PSA Level 1 are often DBA scenarios (e.g. a lot of PSA consider total loss of feedwater as an initiating event, which is usually a DBA scenario), whereas less severe events (disturbance in the feedwater system leading to SCRAM, which justifies an AOO classification) are not

analysed in detail. Moreover, additional boundary conditions assigned to a PIE are usually addressed in PSA in the fault tree/event tree modelling.

It follows that a meaningful comparison of the frequency determination results for PIE and for IE should consider the following aspects:

- the IE of the PSA need to be mapped to the appropriate PIE and vice versa; depending on the level of detail of the PSA Level 1, the IE will usually correspond to either AOO or DBA scenarios,
- additional boundary conditions for PIE from DSA should only be considered in the comparison if they are similarly applied for the PSA IE; as default, only the basic PIE (e.g. small LOCA) should be compared to the respective IE in the PSA; these events are usually arrived at by doing top-down analyses (e.g. with master logic diagrams) using common categories (cf. e.g. SSG-3, p. 26, and SSG-2, p. 6),
- IE for PSA are often defined by grouping several scenarios into one representative bounding event definition (e.g. loss of feedwater); the screening and grouping process of the PSA has to be evaluated in order to identify the types of events subsumed into the IE definition and identify their corresponding PIE from DSA; often, one IE actually analysed in detail in PSA will correspond to and thus gather frequency distributions from several scenarios which can be assigned to separate AOOs or even DBAs from DSA,
- if IE frequencies in the PSA are determined by initiating event fault trees, a similar analysis of the initiator considered in the fault tree needs to be done,
- hazard scenarios in DSA are usually postulated using hazard frequency curves; such curves are usually a major input to hazard PSA as well, using the same parameters (e.g. peak ground acceleration for seismic); in these cases the comparison can be done directly on the hazard frequency curves; if the resilience of certain features is considered for deterministic classifications (e.g. dyke failure probabilities for flooding), the corresponding state in the hazard PSA model has to be identified.

If these aspects have been considered, the IE frequency as determined for the PSA can be compared to the PIE (mostly for internal events AOO or DBA) as assumed for DSA in a meaningful way. The authors recommend checking for the following issues:

- are the data sources (operating experience, engineering judgement, fault tree modelling) used for PSA basically consistent with those referenced for the respective PIE(s)?
- is the IE frequency (distribution) from PSA consistent with the estimated value for the PIE(s)?
  As explained above, due to grouping processes in PSA and DSA, it may be necessary to sum up frequency estimates; usually, several PIE from DSA can be assigned to one IE in the PSA.

If there are inconsistencies in the data base, these should be addressed. For PSA, it is of particular interest if the data sources used to quantify the IE frequency are complete with regard to all events actually grouped into the event definition. To this end, a cross check with the PIE is valuable.

If the data are consistent, the frequency determination should lead to basically consistent results. Here consistency means that the uncertainty bands of the distribution for the IE frequency (e.g. the 95 percentile value) should not deviate by orders of magnitude from PIE assumptions. Should that be the case, assuming the PSA frequency values are reliable, the deterministic classification should be revisited. The following scenarios can be considered:

- the frequency assumed for the PIE is significantly lower than the PSA results for a corresponding IE; if the PSA IE result supports a re-classification of a DBA as AOO or a DEC as a DBA, this should be seriously considered;
- the frequency assumed for the PIE is significantly higher than the PSA for the corresponding IE; if the PSA IE result supports a re-classification of an AOO as DBA or DBA as DEC, this issue needs further consideration; the authors recommend to apply a risk-informed decision making process to any lowering

of the deterministic classification of a PIE; the authors furthermore point out that qualitative safety arguments, regulatory precedent, or preservation of safety margins may be valid reasons for maintaining a PIE classification irrespective of its assumed frequency.

4 CLASSIFICATION OF SSC

4.1 CLASSIFICATION OF SYSTEMS, STRUCURES, AND COMPONENTS

WENRA [26] following IAEA [2] requires the classification of SSCs according to the relevance for safety and sets requirements for the classification process. The safety classification process consistent with the concept of defence in depth set out in SSR-2/1 [2] is recommended in IAEA SSG-30 [37]. As in WENRA [26], it is recommended to apply deterministic methodologies and to complement them where appropriate by probabilistic safety assessment and engineering judgement to achieve an appropriate risk profile. An appropriate risk profile is achieved by a plant design for which events with a high level of severity of consequences have a very low predicted frequency of occurrence. This principle is illustrated in Fig. 2. The safety classification process considers the functions[5] performed at all five levels of defence in depth and classifies the associated SSCs according to their safety significance. Similarly, design provisions[6] are also classified.

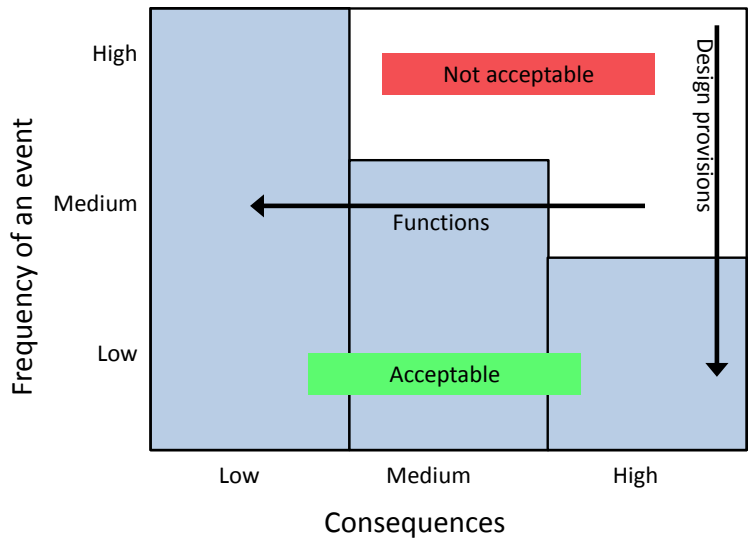


Fig. 2 The basic principle of frequency versus consequences (adapted from Fig. 2 of [37])

As shown in Fig. 2 the design provisions are implemented primarily to decrease the probability of an accident and functions are implemented to make the consequences acceptable with regard to its probability.

The proposed classification as per SSG-30 [37] is a top down process. It begins with a basic understanding of the plant design and safety features, its safety analysis and how the main safety functions will be achieved. In this sense it should consider the whole of the safety architecture. This information is used for identification of functions and design provisions required to fulfil the main safety functions. The identification is done systematically for all plant states. In normal operation all modes are considered. The functions are primarily those that are credited in the safety analysis and should include functions performed at all five levels of defence in depth (i.e. prevention, detection, control and mitigation safety functions).

[5] For the purpose of SSG-30, a 'function' is defined as any action performed by a single SSC or a set of SSCs.
[6] For the purpose of SSG-30 'design provisions' are termed SSCs designed specifically for use in normal operation.

The safety classification process is based on the results of deterministic and probabilistic safety analyses, together with engineering judgments [7]. The classification approach requires assigning categories to each safety function according to its importance to safety, identifying for each safety function the SSC involved in achieving the functions objective and assigning to them a classification based on the importance of the safety functions they perform.

A safety function could be categorized by analyzing multiple factors, as the following: the consequence of its unavailability; its goal (if is necessary to prevent, to protect against or to mitigate the consequences of an event); its potential to initiate a fault or to increase the consequence of an existing fault.

All SSC should be classified in different safety classes, in the context of their contribution (direct or indirect) to safety functions, both in normal and in accident conditions, according to their importance from safety point of view (main line provision of the related safety function or not) [2].

In the classification process the following principles should be considered: [2]

- a given system may contain components having different safety classes and some components may have subparts with different classifications;
- the failure of a SSC that belong to a specific safety class should not lead to the failure of a SSC that belong to a higher safety class;
- the interfacing components which separate interconnecting systems having different safety classes should be assigned to the higher safety class;
- the support systems of a safety system should be classified accordingly in the same safety class as the safety system, if their failure will induce the unavailability of the safety system; the reliability, redundancy, diversity and independence requirements for the support systems should be in accordance with the performance requirements of the safety system.

The U.S. NRC has defined a set of requirements and suitable risk metrics for the assessment classification of SSC with PSA related to DiD, cf. RG 1.201 [57]. Namely, the 10CFR50.69 rule [32] proposes an alternative set of requirements for the classification of the categorization of SSC. The safety significance of SSCs is determined by an integrated decision-making process, incorporating risk and traditional engineering insights. The SSCs of the NPP are classified into four Risk-Informed Safety Classes (RISC) as shown on Fig. 3.

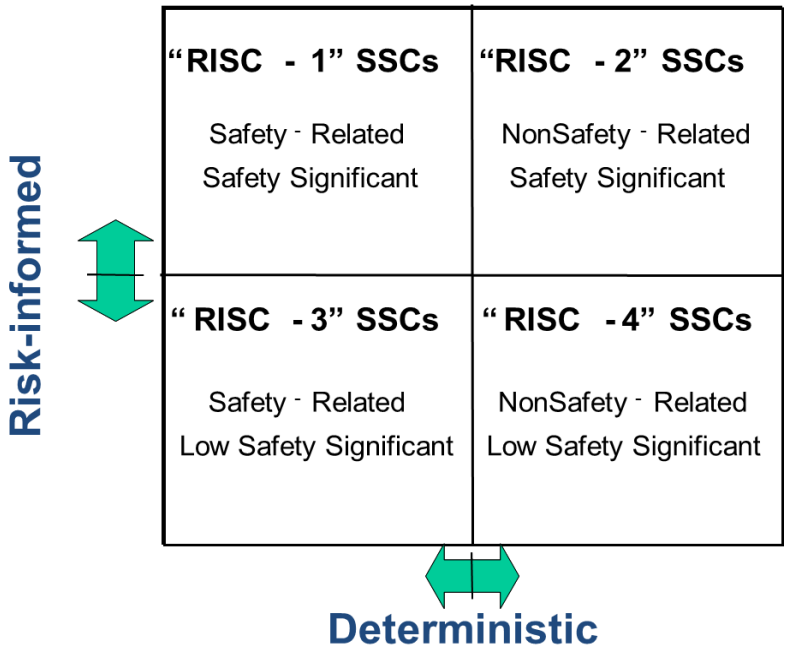


Fig. 3 10 CFR 50.69 RISC Categories

The classification is based on the function performed by the SSC and if its safety related. SSCs are considered to be safety-related if they are relied upon to remain functional during and following design basis events to assure:

- the integrity of the reactor coolant pressure boundary,
- the capability to shut down the reactor and maintain it in a safe shutdown conditions or
- the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guidelines exposures.

The safety significant function is defined as a function whose degradation or loss could result in a significant adverse effect on DiD, safety margin, or risk [32].

The risk measures defined by the NRC for identification of the SSC safety significance are the following importance measures related to Core Damage Frequency and Large Early Release Frequency:

- sum of Fussel Vessely (FV) for all basic events modelling the SSC of interest, including common cause failures to be larger than FV > 0.005,
- maximum of component basic event Risk Achievement Worth RAW > 2,
- maximum of applicable common cause basic events RAW > 20.

If any of these criteria are assessed or exceeded for the analysed SSC then it is considered as a candidate safety significant SSCs.

A PSA with appropriate technical capability is required for the categorization of SSCs relative to the internal events, at-power risks [32], [33], [57]. Importance measures related to CDF and LERF are used to identify the safety-significant functions and all SSCs required for those functions are categorized as safety-significant (RISC-1 or -2).

For safety-related SSCs initially identified as low safety significant LSS (i.e., RISC-3) from the results of the risk significance categorization, an additional DiD assessment is performed.

The DiD assessment is based on a set of deterministic criteria. The deterministic criteria are based on the design basis accident considerations to ensure adequate redundancy and diversity during the design basis events. This assessment evaluates the SSC functions with respect to core damage mitigation, early containment failure/bypass,

and long term containment integrity. If one of these SSC functions is found to be safety-significant with respect to DiD, then it is considered safety-significant and categorized as safety-significant (RISC-1) for further analysis.

In Romania, the use of PSA for revision of SSC classification in safety classes is required by CNCAN, however no specific risk measures or numerical criteria are defined [46]. Similarly, the Finnish guide YVL A.7 does require the application of PSA to classify SSC, but neither YVL A.7 [48] nor YVL B.2 [49] give specific risk measures or thresholds. Also the Slovenian guide JV5 [60] requires that each SSC shall be classified into a safety class according to its importance to safety. SSC categorisation means the classification of SSCs into four safety categories according to their relevance to risks determined with a probabilistic safety assessment. However, no specific risk measures or numerical criteria are defined in JV5 [60]

In Switzerland, ENSI-A06 [22] states specific criteria for the classification of components as significant to safety. The following thresholds on importance measures (cf. D30.5 [36]) with regard to core damage frequency, fuel damage frequency[7] and large early release frequency shall be applied.

- Fussell-Vesely importance ≥ 10^{-3}
- Risk Achievement Worth ≥ 2

It should be noted that the Swiss regulation specifically applies to components and does not address systems and structures.

Overall, the use of PSA for the classification of SSC seems to follow the approach endorsed by the US NRC or basically similar approaches, with differences in the detail. There seems to be agreement on using risk importance measures based on Level 1 (CDF) and Level 2 (LERF) values. With respect to an extended PSA, we can make the following remarks. As discussed in D30.5 [36], the standard risk measure for PSA Level 1 and Level 2 as CDF or LRF can be easily applied to an extended PSA. Consequently, the importance measures derived from these risk measures are applicable as well. The respective thresholds for the classification of SSC can be applied to results from an extended PSA. The authors recommend using PSA information for the classification of SSC as described above. However, with respect to PSA Level 2 results, the classification should consider other risk measures than LERF, either in addition or as a substitution, e.g. a total risk measure (summing up all activity releases multiplied by their respective frequencies) or release category measures as recommended in D30.5 [36].

4.2 RELIABILITY ASSESSMENT OF SAFETY FUNCTIONS

GSR-4 requires for all safety functions an assessment which shows that they “have an adequate level of reliability” [18], p. 15. Furthermore, GSR-4 explicitly mentions that “[p]robabilistic approaches may provide insights into […] reliability, […] the application of defence in depth, […] that it may not be possible to derive from a deterministic analysis.” [18], p. 24f. There is extensive guidance on the probabilistic modelling of safety functions (cf. e.g. SSG-3 [4]). The safety functions (e.g. reactivity control, heat removal and confinement of radioactive materials) can be performed successfully using multiple systems. The reliability with which a safety functions is achieved is usually modelled using a fault tree approach for the safety (system/layers of provisions) function unavailability. Fault

[7] It should be noted that in Switzerland, CDF applies to the fuel in the reactor core during power operation whereas fuel damage frequency applies to fuel in the reactor core or the spent fuel pool during non-full-power operation, cf. ENSI-A05 [47]. This distinction differs from the definition and discussion on the respective risk metrics given in D30.5 [36].

trees should consider as basic events component hardware failures, human errors, maintenance/test unavailabilities or any other relevant failure that can lead to the undesired considered event.

The fault tree model should include all the components of safety function that are required to be operational and all components of support systems. The relevant passive components (whose failures could lead to failure of the system) and component dependencies should be taken into account explicitly. The level of resolution should be adequate for the goal of analysis.

Such fault tree models allow for a direct quantification of safety function reliability or unavailability, respectively, if the appropriate boundary conditions are set. Moreover, safety functions, especially front line safety functions, are often used as headings in the development of the accident sequence modelling in event trees [4]. In these cases, the PSA tools allow for an explicit consideration of the respective initiating event boundary conditions and previous failures of systems or components (or structures), which can affect the reliability (effectiveness) of the safety function under investigation. Consequently, there are well-developed probabilistic assessment methods for the reliability assessment of safety functions available (nevertheless, for some external hazards, the fragility of all equipment related to a safety function can be difficult to assess – e.g. the tightness of containment building and its extension after a beyond design earthquake can be difficult to assess for the containment function).

With respect to an extended PSA, there are no major changes in the methodological approach. It suffices to note that the systematic addition of hazard scenarios and the consideration of all major potential sources of releases enhance the capability of the PSA model for assessing the reliability of safety functions for the different relevant boundary conditions. This underscores the need for developing extended PSAs.

While the assessment methods for the reliability of safety functions are readily available, there is less information about suitable quantitative probabilistic thresholds on the conditional failure probability of these safety functions. In fact, there are only few regulatory publications which contain specific quantitative requirements with respect to the reliability of safety function. Known examples include :

- The Canadian regulatory authority had required that the maximum unavailability for each of two shutdown system in a CANDU type reactor had to be below 10^{-3} (cf. R-8 [19], p. 2, superseded by current regulation). The same maximum value of unavailability is requested (in availability requirements part) also for the containment system, cf. R-7 [50], and for the emergency core cooling system, cf. R-9 [51]. The norms (one for each of the systems mentioned above) contain specific requirements, grouped into the following categories: basic requirements, design requirements (performance, availability, separation and independence requirements; environmental requirements; minimum performance requirements) operating requirements (both for normal and accident conditions), testing requirements ;

  The same requirement is specified in the new regulatory document by the CNSC, REGDOC-2.5.2 [52], which sets out the requirement for the safety systems and their support systems to have the maximum probability of failure on demand from all causes lower than 10^{-3};
- Romanian regulatory norms requires that the maximum unavailability for emergency core cooling system, cf. NSN-11 [54], for special safety systems (i.e. first and second shutdown systems), cf. NSN-13 [55], and for the containment system, cf. NSN-12 [56], to be below 10^{-3};
- The U.S. NRC has effectively defined an objective for the conditional failure probability of the containment in case of a core melt accident (CPCFB) for evolutionary designs to be below 10^{-1} [20], [21].

Despite these examples, there are no generally accepted failure probability thresholds for the design of safety systems or safety functions. Typical PSA results indicate that safety systems/safety functions reach conditional failure probabilities in the range of 10^{-3} to 10^{-1}, depending on the boundary conditions and their design basis.

That probabilistic criteria are missing is probably due to the complexity of setting such values. The following considerations have to be taken into account:

- It's not always possible to define a clear mapping of (technical) system boundaries and provisions for safety functions. Importantly, in some cases certain safety functions are realized with multiple, possibly diverse, systems. Therefore, systems-based reliability requirements are hard to justify.
- The reliability of a system or safety function strongly depends on the PIE and scenario under consideration. Therefore, defining "the" conditional failure probability or "the" reliability is difficult as well.
- SSR-2/1 defines three fundamental safety functions: "(i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases" [2] p. 12. Often, safety systems are contributing to the fulfilment of more than one fundamental safety function. Conversely, each fundamental safety functions can be achieved with multiple systems (working simultaneously or in sequence). Complicating matters further is the fact that safety functions as elements of an event tree model of a PSA are usually not defined in terms of the fundamental safety functions.
- The DiD concepts calls for independent and effective measures at each level of defence in depth (cf. SSR-2/1 [2], p. 7). This includes that at each level of DiD, the fundamental safety functions have to be maintained, if applicable. In light of the previous remark, it's in no way simple to break these requirements down to specific provisions for specific safety functions and/or to specific safety systems. This complicates the setting of reliability thresholds as well.
- Conversely, there are as yet no examples where reliability requirements have been set on levels of defense in depth and thus applying to the set of all provisions assigned to each level.
- Probabilistic safety criteria are usually based on the risk metrics of Core Damage Frequency or Large (Early) Release Frequency [4], [16]. They may be complemented by criteria related to balancedness of the risk, usually referring to importance measures based on the above-mentioned risk metrics (cf. e.g. Swiss regulatory guide ENSI/A06 [22]). A quantitative criterion on e.g. the frequency of core damage implicitly includes requirements on the reliability/conditional failure probability of the provisions for safety functions. Given one initiating event with a frequency of 10^{-3} /yr for example[8], which needs to be contained with safety features assigned to DiD level 3, and an overall target value for CDF[9] of 10^{-6} /yr, the conditional failure probability for the provisions for safety functions on DiD level 3 needs to be (significantly) below 1 10^{-3}, if preventive accident management (i.e. measures traditionally assigned to DiD level 4) are not considered. In this respect, specific reliability requirements on provisions of safety functions per level of DiD could be judged as redundant or even superfluous, since they are implicitly imposed by probabilistic safety targets.

With respect to an extended PSA, it can be pointed out to the following intermediate conclusions. Reliability assessments of systems or safety functions do not require different methods or risk measures if the PSA is extended. Using an extended PSA will basically increase the significance of the risk information. A more systematic use of PSA information in risk-informed decision making on the adequate reliability of systems, safety functions,

[8] This value puts the IE example in the DBA range, which should be contained with DiD level 3 features..
[9] For a lot of designs, entry into core damage means entry into design extension conditions (i.e. DEC B), which should be addressed (deterministically) with DiD level 4 features.

and even structures (i.e. including passive safety features) is recommended. The risk measures of choice should be conditional failure probabilities/availabilities. Reliability targets need to be set on a case-by-case basis. Setting on reliability targets on specific functions or systems can be one important aspect of a risk-informed design process or a robust risk management system, cf. also e.g. [58].

Moreover, current PSA models are often not built in a way that facilitates the reliability assessment of systems or safety functions; as such a use was often not foreseen for these models. Section 5.1 contains further discussion of current experiences and research results related to this issue.

5 DEFENCE-IN-DEPTH AND PSA FOR NPP

Fundamentally, there is no methodological difference between a PSA which analyses a system with explicit consideration of DiD, and a PSA which analyses a system without such an explicit consideration. But with the contribution of PSA, complementary and essential insights can be identified and safety characteristics such as progressiveness and a tolerant, forgiving and balanced character of the safety architecture can be assessed. The PSA will always seek to quantify the vulnerability of the system and to identify weak points and potential improvements of the system.

However, trying to do PSA assessments of DiD poses several specific challenges:

- the levels of DiD and plant conditions that can be associated with these levels (especially level 2, level 3, and level 4) do not easily map to the traditional PSA end states (e.g. CDF and release categories) and the initiating events; indeed, there is considerable debate in the community about which initiating events, boundary conditions, safety functions and other elements of a PSA should be assigned to which level of DiD; this has to be clarified for the plant and it's PSA; based thereon, a specific structure for the PSA needs to be implemented along the lines of DiD if it is desired that PSA checks DiD.
- the best-estimate approach of PSA is not necessarily compatible with the (conservative, safety case oriented) deterministic approach for a DiD assessment; one salient example is the consideration of non-safety systems, which can be considered in a PSA, but usually are neglected in a deterministic assessment; the different approaches can impede the construction of a PSA model suitable for DiD assessment.

5.1 EXISTING EXPERIENCES

5.1.1 LINK BETWEEN DID AND PSA PROJECT ASSOCIATED TO SSCS

One important activity in recent years specifically dedicated to the relationship between DiD and PSA was a multi-year research project funded by the Swedish regulatory body SSM and was run in close coordination with the Nordic PSA group. Main insights and results from the project reports [8], [9], [28] are summarized below.

The objective of the SSM research project was to investigate to what extent measures and parameters of PSA can be used in order to give estimates of the five levels of DiD. This implied to make an inventory and explored the possibilities to perform calculations and present results in such a way that structures, systems, components (SSCs), operator actions and procedures can be linked to DiD levels and be ranked and graded in relation to their risk contribution.

The SSM project was performed in various phases, starting with a survey of qualitative parameters of each level of DiD, including identification and structuring of the SSCs that belong to each DiD level and thus considered for potential PSA evaluation. Moreover, 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 project 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 high level description of some connections between the five levels of the DiD and PSA levels was developed by SSM and is shown in Fig. 4.

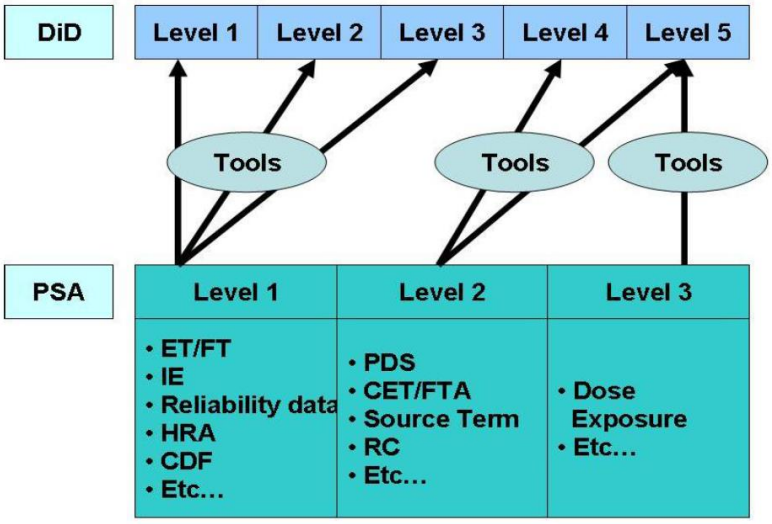


Fig. 4 DiD – PSA Possible Evaluation

DiD and its interpretation

IAEA INSAG -10, INSAG – 12 and IAEA Safety Report Series No. 46 discuss the implementation of a DiD concept centred on several levels of protection, including successive barriers preventing the release of radioactive material to the environment.

Generally, the DiD levels and relations with PSA can also be represented by an event tree as depicted in Fig. 5. Note that severe accident management addresses DEC situations, more specifically DEC B.

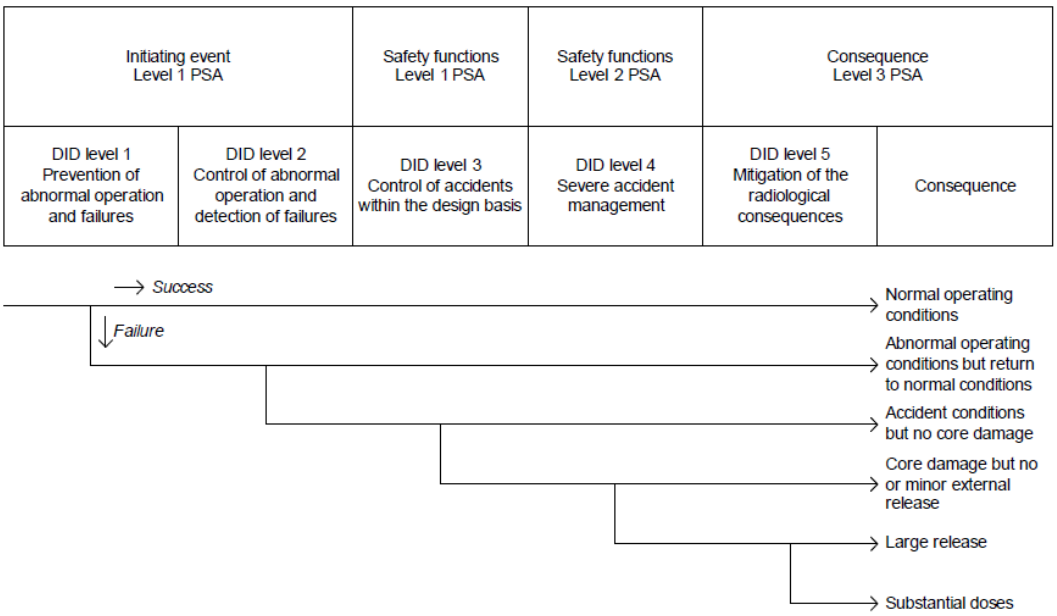


Fig. 5 DiD Event Tree

The above event tree 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 of PSA Level 1 cover DiD levels 1 and 2. Failures of both levels mean that reactor protection limits are reached. It is 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 which can be included in the PSA model. OK sequences without need for reactivity control, where the plant can continue power operation will then be a special type of sequences. Historically, the PSA models are constructed with requirements for reactivity control as the first function needed to avoid core damage, and if that fails then core damage will result, therefore it is argued that the PSA initiating event is a failure of both DiD levels 1 and 2.

In SSM report, it is recognised that the first three levels in DiD are particularly troublesome to relate to the PSA framework. Hence, it becomes important to scrutinize the definitions to fully align DiD to the PSA perspective, which is also interpreted in the referenced SSM report.

The extended DiD levels definitions are provided in the SSM report. Moreover a new DiD framework is discussed as illustrated in Fig. 6 below.

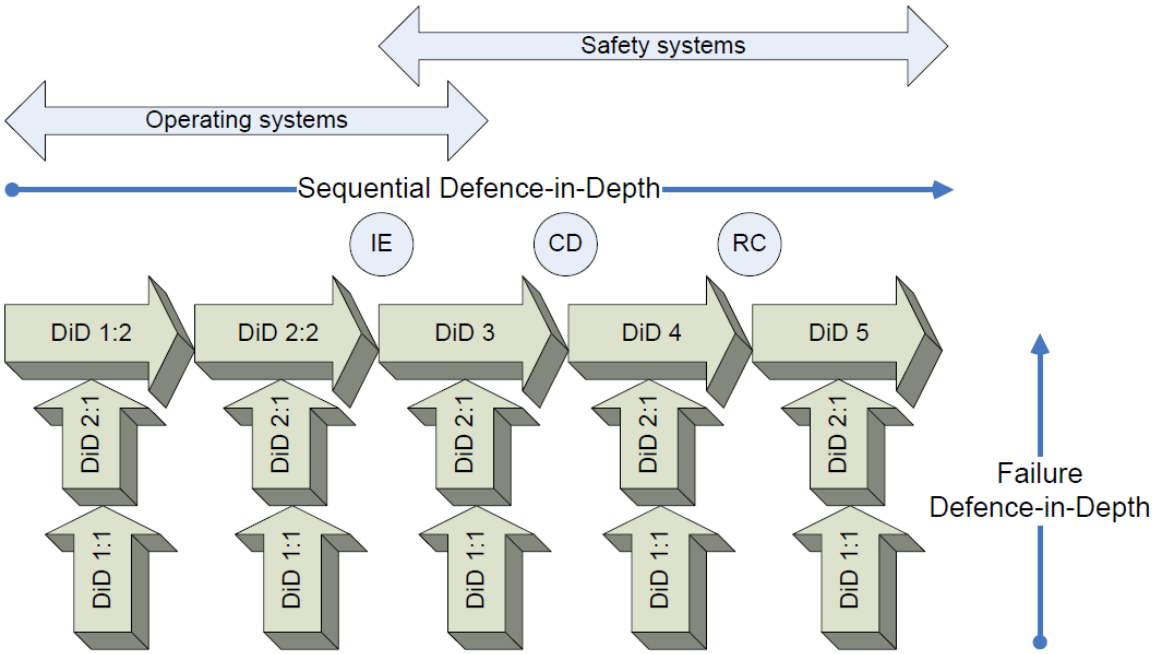


Fig. 6 The failure in DiD and the sequential DiD (The restructured DiD framework)

Fig. 6 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.

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, 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.

Quantitative Evaluation - PSA

This chapter 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 DiD levels, as shown in Table 2 below.

Table 2. 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 events)	1:2-3
	Conditional consequence probability given specific initiating event, all other initiating events set to zero	3
Plant damage state in level 2 PSA	Consequence frequency (all initiating events)	1:2-3
	Consequence frequency (specific initiating events)	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.	

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

The SSM report also proposed the ways to measure the performance of the DiD levels with PSA which are illustrated in Fig. 7 :

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

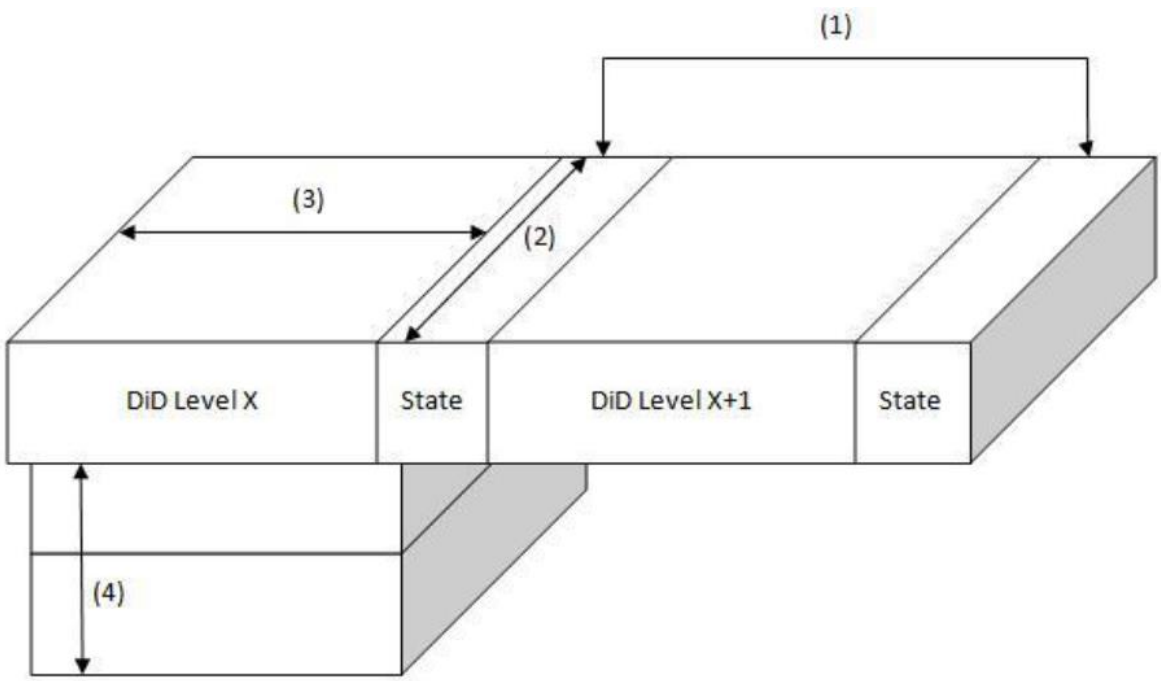


Fig. 7 Measures of DiD levels

A summary of existing and potential PSA measures of DiD levels are presented in Table 3 below.

Table 3. Summary of Probabilistic Risk 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.

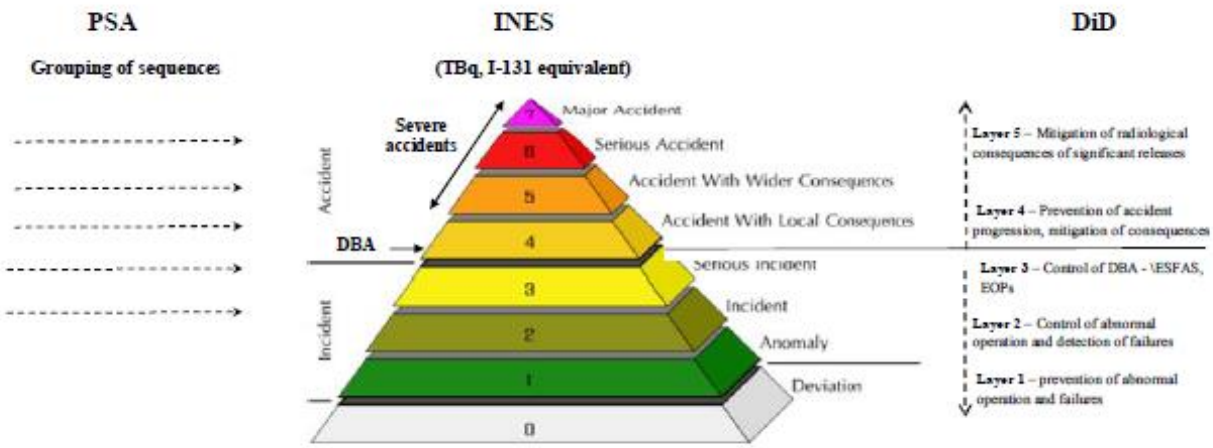
5.1.2 CCA'S DEVELOPMENT OF DID CONCEPT

The starting of the CCA development of the DiD concept is captured in the following observation in the INES Manual, Table 11 [62]:

TABLE 11. RATING OF EVENTS USING THE SAFETY LAYERS APPROACH

Number of remaining safety layers	Maximum potential consequences		
	(1) Levels 5, 6, 7	(2) Levels 3, 4	(3) Levels 2 or 1
A More than 3	0	0	0
B 3	1	0	0
C 2	2	1	0
D 1 or 0	3 [a]	2 [a]	1 [a]

The same relationship can be shown as follows:



It should be noted, that actually the 5th layer of DiD representing "Mitigation of radiological consequences" does not belong *per se* to safety as it is defined by the IAEA [70]:

> "Safety involves the prevention and minimization of danger whereas radiation protection involves the protection of health. Safety is thus primarily concerned with maintaining control over sources, whereas radiation protection is primarily concerned with controlling exposure to radiation, whatever the source, to mitigate its effects."

This means that "risk of releases" (which are analyzed in L2 PSA) can be tied to DiD physical barrier 4 (containment) and INES level 5 (Accident with wider consequences) can be taken an appropriate measure of safety of the plant in terms of Severe Accidents. The 5th DiD layer is related to radiological consequences (which are analysed in L3 PSA) depending on success of organisational countermeasures that are not part of nuclear plant design.

Defence in depth can be understood as the tool of deterministic analyses, performed for DBA purposes as it follows from the IAEA definition published in IAEA SSG-2 [3]: "The deterministic approach is based on the two principles: leak tight barriers and the concept of defence-in-depth."

CCA asserts, that as DiD is defined now, it is not dedicated to severe accidents, i.e. PSA purposes, but for DBAs only with some exceptions like some containment systems e.g. hydrogen ignitors, but these are among the last barriers from the point of view of all DiD layers and barriers.[10] In some cases like venting systems, the provisions in fact violate the function of the last DiD barrier, i.e. the containment, exactly because of their purpose and their nature.

With respect to the necessity for probabilistic assessment see further in the same reference above, e.g. "Thus a deterministic safety analysis alone does not demonstrate the overall safety of the plant, and it should be complemented by a probabilistic safety analysis." [3]

or

"While deterministic analyses may be used to verify that acceptance criteria are met, probabilistic safety analyses may be used to determine the probability of damage for each barrier. Probabilistic safety analysis may thus be a suitable tool for evaluation of the risk that arises from low frequency sequences that lead to barrier damage, whereas a deterministic analysis is adequate for events of higher frequency for which the acceptance criteria are set in terms of the damage allowed." [3]

Within recent research and development, CCA performed analysis of current understanding of DiD with respect to uncertainties in PSA and safety margins. The following summarizes the contents of a publication in 2014 [63]. CCA extrapolated the method for demonstration of safety margins with uncertainties in the deterministic view, published in IAEA SRS No. 52 [64] .

[10] It should be noted that this understanding of the relationship between DiD, PSA and severe accidents is not shared by all authors.

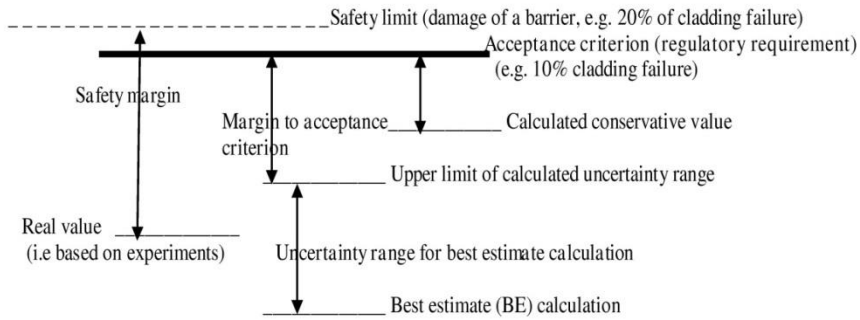


Fig. 8 Safety margins with uncertainties in deterministic view [64]

Extrapolating this approach to PSA, the figure below is obtained when considering real severe accidents. Four core melts with large releases (1xChernobyl, 3x Fukushima) in reported 14,500 reactor years represent the "actual" large release frequency equal to 2.8 E-4/Ry. Considering also the range of LRF/LERF objectives/limits in different countries, CCA arrives at the following figure:

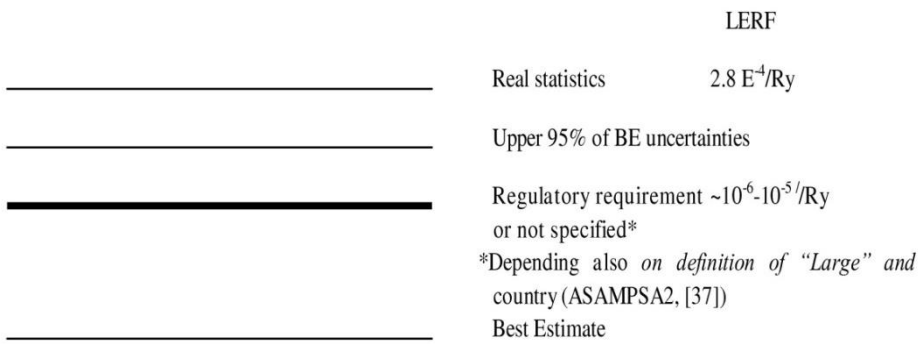


Fig. 9 Safety margins with uncertainties in probabilistic view [63]

The figure demonstrates the veracity of the statement given above that DiD, as it is defined currently, is the tool of deterministic analyses and thus it can assure enough safety margins for events considered in deterministic analyses (DBAs) but do not assure safety margins for events considered in probabilistic analyses (PSAs).

In the given reference [63] an analysis of current DiD was performed based on the major principle:
No safety layer/barrier of defence in depth introduces any risk addition and no safety layer/barrier reducing risk should be omitted

A short summary of CCA arguments and observations can be found below:

DID Safety barriers:

a) Fuel matrix

- CCA does not see that its role in the DiD is clearly defined.
- Indeed it does not include core inventory in the sense of its extent (amount) and quality (mix of radionuclides) which are the basis of the extent of source terms (radionuclide releases)
- Extent of possible releases depends on the core inventory extent

b) Fuel cladding

- Fuel cladding for LWR is mostly manufactured of zirconium alloy
- It is contributor to risk because of hydrogen production in the exothermic oxidation reaction of cladding material at very high temperatures (i.e. severe accident conditions).

c) Primary coolant boundary

- For beyond design basis/severe accidents its role as safety barrier is not guaranteed because of beyond design thermal and mechanical loads

d) Containment

- Should provide limitation of radioactive releases under normal and fault conditions and protect against hazards, however
- Containment vent systems
  - Oriented on the protection of containment structural integrity while releasing radioactivity to the environment
  - This demonstrates that most current containments are not able to bear the loads, which may occur during severe accidents
- Containment leak tightness
  - Containment should keep all accident- resulting radioactivity inside
  - This aspect is omitted in DiD concept (limits are missing).
- Safety barrier against underground leaks and leaks into water
  - Not considered in the current designs and not considered in current DiD either

CCA continues with a discussion of safety layers applicable to DiD.

DID Safety layers:

a) Conservative design

- None of the currently operating plants was designed to withstand severe accident conditions.
- CCA concludes that this is not reliable enough as safety layer of DID

b) Human interactions

- The DiD concept involves organizational, administrative and provisional measures and off-site emergency response all involving human interactions
- All major severe accidents involved human errors
- CCA concludes that operator interventions are not reliable enough as safety layer of DiD

c) Safety standards/criteria/goals

- Basic acceptance criteria are usually defined as limits and conditions set by a regulatory body, and their purpose is to ensure the achievement of an adequate level of safety.
- The most commonly used PSA safety criteria in particular countries are just frequencies. CCA points out that the goal of PSA, as the driver of safe design, should be risk assessment.
- CCA concludes:
  - There is a gap in DiD with respect to safety/risk criteria
  - Quality of risk criteria is insufficient
  - There should be a common understanding of safety itself and risk criteria

d) Probabilistic analyses PSA

- PSA should be one of the safety layers confirming that the design is conservative enough to guarantee the safety – PSA is missing in current DiD
- Here the following aspects must be analyzed:
  - The gap in DiD with respect to PSA
  - Gap in PSA with respect to risk assessment
  - Analysis of results in form of frequencies (focusing only on LERF)

e) Uncertainties

Concept of "sufficient safety margin" stemming from deterministic analyses for design basis accidents is based on several levels, where experiments show much lower values (e.g.1% claddings fail) in comparison to acceptance criteria (e.g. 10%) adopted by an authority which is still lower than supposed "threshold" safety limit (e.g.20%), see Fig. 8.

Based on these considerations, CCA proposes the following changes to DiD [63]:

DiD barriers:

1st barrier – Core inventory: reducing the maximum potential risk either by reducing core size or the composition of the core – new to DiD

2nd barrier - Fuel cladding: Ignore this as safety layer, since cladding represents significant additional risk source

3rd barrier – primary coolant boundary

Extend by consideration of secondary side/balance of plant taking into account post-Fukushima lessons learned on the ultimate heat sink

4th barrier – Containment: Ignore this safety barrier in case venting system installed

Define adequate and acceptably safe leak limits

Specifically consider underground leaks – new to DiD

Leaks into waters/oceans – new to DiD

CCA adds the following DiD layers:

1st layer – Harmonized, commonly internationally accepted safety standards

CCA finds these are missing as part of DiD

2nd layer - PSA

Include PSA as tool for risk evaluation is missing in current DiD <u>guiding for design and operation</u>

Do risk assessment with full assessment of uncertainties

Add analysis of current results with respect to large releases and the context to basic events/initiators

3rd layer – Conservative design

However, ignore this as safety layer for current plants design to outdated practices

5.1.3 PSA ASSESSMENT OF DEFENSE IN DEPTH – ADDITIONAL REPORT BY NIER

An additional report [69] about the peculiar roles of the DiD concept and the PSA approach has been developed during the ASAMPSA_E project in order to support the editing of present D30.4 deliverable (by NIER, not reviewed by all partners).

Preliminarily, general indications have been provided about a global process for the verification, through PSA, that the implemented safety architecture complies with the principles of the DiD [66]. The content of the report [69] goes further making explicit the possible relationship between DiD and PSA.

The process proposed for the assessment of the safety architecture implementing DiD is fully consistent with the indications provided by the IAEA GSR Part 4 [18] and is based on some concepts introduced by the Generation IV Risk and Safety Working Group ([67] and [68]). It is articulated in four main steps devoted to (1) the formulation of the safety objectives, the (2) identification of loads and environmental conditions, the (3) representation of the safety architecture and (4) the evaluation of the physical performance and reliability of the levels of DiD. A final additional step achieves the practical assessment of the safety architecture and the corresponding DiD with the support of the PSA.

The risk space (frequency/probability of occurrence versus consequences) is the framework for the integration between the DiD concept and the PSA approach. Additional qualitative key-notions are introduced in order to address the compliance of the safety architecture with a number of (IAEA) safety requirements.

The Objective Provision Tree methodology and the complementary notion of Line of Protection/Layers of Provisions (developed within the context of the IAEA activities and endorsed, among others, by the Generation IV International Forum / Risk & Safety Working Group) are proposed for an exhaustive - as practicable – representation of the safety architecture implemented by the nuclear installation. It allows the development of a PSA model with a structure that better complies with the DiD principles and that, in turn, allows the evaluation of the physical performance and reliability of the levels of DiD.

Details on the proposed process and tools are provided in the aforementioned report [69].

In summary, the acceptability of a safety architecture shall be based on the degree of meeting the DiD principles while fulfilling the applicable Safety Fundamentals and Requirements. Deterministic and probabilistic considerations shall be integrated into a comprehensive implementation of Defence in Depth. The role of the PSA shall be no longer limited to the verification of the fulfilment of probabilistic targets but can include different contributions to the assessment of the safety architecture implementing DiD:

- PSA can provide additional evidences of the independence among DiD levels and specific insights about plausible dependent failures, also accounting for external (natural or man-made) hazards;
- PSA can support the deterministic design and sizing of provisions, by addressing the effects of their reliability and contributing to the definition of acceptable boundary conditions;
- PSA can support the demonstration of the “practical elimination” of plausible events and sequences which could lead to early or large releases;
- PSA can support the demonstration of the gradual degradation of the safety architecture in case of loss of safety functions, before that harmful effects could be caused to people or to the environment (progressive character of the safety architecture);
- PSA can provide specific insights about the effectiveness of redundancies among implemented provisions, about the modelling of human factor (for immaterial provisions) and about the uncertainties on input data and their propagation through the model (tolerant character of the safety architecture);
- PSA can contribute to the demonstration of the proper priority in the operation of different means required to achieve safe conditions, through inherent characteristics of the plant, passive systems or systems operating

continuously in the necessary state, systems that need to be brought into operation, procedures (forgiving character of the safety architecture);

- PSA can provide specific insights addressing the balanced/unbalanced contributions of the different events / sequences to the whole risk identifying the presence (to be avoided) of excessive or significantly uncertain contributors to risk (balanced character of the safety architecture).

5.1.4 OTHER EXPERIENCES

In reference [40], the authors briefly discuss the link between DiD, PIE assignment to DiD levels, and the link between PSA and DiD. Their summary of the relationship between PSA levels and DiD levels, with an examplary event tree structured along DiD levels is shown in Fig. 10.

Level 1 PSA Initiating events		Level 1 PSA Safety Functions			Level 2 PSA Safety Functions	Level 3 PSA Consequences	
Prevention (EOPs)		Mitigation (SAMG)					
		DiD Level 3					
DiD Level 1	DiD Level 2	DiD Level 3a Class 1	DiD Level 3a Class 2	DiD Level 3b Types A, B, C	DiD Level 4	DiD Level 5	End Sate Consequences
DBC 1	DBC 2	DBC 3	DBC 4	DEC	SA		
Normal operation Prevention of abnormal operation and failures Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	Anticipated Operating Occurrences (AOOs) Control of abnormal operation and failures Control and limiting systems and other surveillance features	Postulated accident by a single event Control of accident to limit radiological releases and prevent escalation to core damage conditions *(2)* Reactor protection system, safety systems, accident procedures	Postulated accident by a single event Control of accident to limit radiological releases and prevent escalation to core damage conditions *(2)* Reactor protection system, safety systems, accident procedures	Postulated multiple failure events Control of accident to limit radiological releases and prevent escalation to core damage conditions *(2)* Additional safety features *(3)*, accident procedures	Postulated core melt accidents (short and long term) Control of accidents with core melt to limit off-site releases Complementary safety features *(3)* to mitigate core melt, Management of accidents with core melt (severe accidents)	- Mitigation of radiological consequences of significant releases of radioactive material Off-site emergency response Intervention levels	
Is Level 1 of DiD successful?	Is Level 2 of DiD successful?	Is Level 3a of DiD successful?	Is Level 3a of DiD successful?	Is Level 3b of DiD successful?	Is Level 4 of DiD successful?	Is Level 5 of DiD successful?	

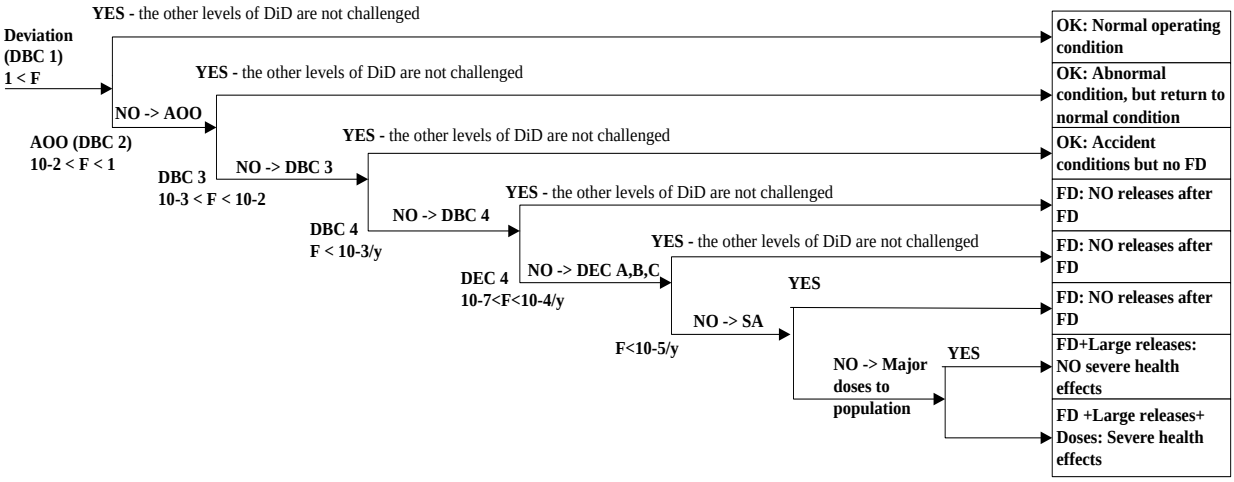


Fig. 10 The relationship between PSA levels and DiD levels [40]

5.2 INDEPENDENCE

As already mentioned above, the independence of provisions achieving a given safety function at one level of DiD to the provisions at others levels of DiD is a very important aspect of DiD (cf. SSR-2/1 [2] and WENRA [7], [26]). It should be noted that the DiD concept does not, by itself, require that systems, trains of systems, etc. at the same level of DiD are also independent of each other. Respective requirements result usually from the need for reliable systems and related good design practices. Consequently, SSR-2/1 requires safety systems (fulfilling safety functions(s) irrespective of the placement in terms of DiD) as well as redundant elements thereof to have "physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate" [2], p. 25. Moreover, safety systems "shall take due account of the potential of common cause failure" [2], p. 26, shall fulfil the single failure criterion [2], p. 26, and "shall be designed for fail-safe behaviour" [2], p. 27. The demonstration of these characteristics, if applicable, for all PIE considered in the design is a central task in the deterministic assessment of the safety of the plant (cf. also GSR-4 [18], p. 15f, 21f). The available deterministic assessment methods, design standards and technical guides as well as good design practices are generally suitable for doing this task.

Lessons learnt from the Fukushima Dai-ichi accident show the importance of proper implementation of the DiD concept which requires the implementation of an increased reliability for safety functions (implicit this means the assessment of the unavailability). All levels of defence-in-depth should have an enhanced independence, in particular through diversity provisions.

As main requirements for reliability of safety functions, the following specific requirements by WENRA for new reactor designs should be considered [7] :

- the NPP shall provide the decay heat removal in any severe conditions and shall ensure the protection of necessary electrical power supplies against the hazards; loss of ultimate heat sink or access to it should be considered in the design.
- the electrical power supply reliability should be increased, with enhanced provisions of long term operation of emergency power supply (fuel, lubricating oil, possibilities to use mobile power supply units, increased capability of batteries, possibility to re-charge them); the fail-safe position of safety related equipment in case of loss of power supply should be considered in the design, and consequently reflected in the fault tree model.

Romania and Canada have similar norms regarding the availability, diversity and redundancy of safety systems. The main requirements are summarized below, cf. [52], [19], [50], [51], [53], [54], [55], [56].

- the partial or total loss of a protection barrier should not affect the availability of other protection barriers,
- the principles of separation, diversity and independence, single-failure criterion and fail-safe design are required to be incorporated into design, especially for safety systems and components. -The protective (shutdown) systems should be physically and operationally independent from control systems, for all normal operating conditions, anticipated transients and accident conditions. The separation and independence principle requires for the shutdown systems to be diverse and physically and operationally independent from each other, from the process systems and from other safety systems. The same principle requires for ECCS and containment system to be physically and operationally independent from other safety systems and from all process systems,
- the safety systems should have sufficient redundancy such that no failure of any single component of the system would induce a critical impairment of system performances. Physical separation is required mainly

between redundant parts of a safety system and of a safety support system, as well as between a safety support system and a process system,

- provisions for online maintenance and online testing of systems important to safety should be included in the design.
- the effectiveness of a specific safety system in performing its related safety function shall not be dependent on the correct functioning of any process system or any other safety system,
- the availability of any safety support equipment necessary for safety system operation shall follow the availability requirements of the safety system. The support safety systems shall be independent one of other, eliminating the possibility of failure due to common causes,
- instrumentation shall not typically be shared between safety systems,
- no part of a specific safety system shall be used as part of another safety system; where justified, there may be sharing between a safety system and a non-safety system, but only if there are no impairments (impairments induced by normal operation or any kind of failure in other systems, and by any cross-links) induced by the proposed sharing on the safety system reliability,
- SSCs important to safety shall not be shared between two or more reactors, and in case when this is happening, the safety systems and turbine generator buildings shall not be shared,
- each special safety systems shall be designed to have the unavailability lower than 10^{-3}.

For Slovenia the WENRA [26] requirement E9.4 for reliability of the systems of existing reactors is covered in the Slovenian rule JV5, article 3 (design principles). The design of a radiation or nuclear facility shall adhere to the following principles: 1. defence-in-depth principle; 2. single-failure principle; 3. independence principle; 4. diversity principle; 5. redundancy principle; 6. fail-safe principle; 7. proven-components principle; 8. graded-approach principle. Each of these principles is further defined in detail.

With regard to the use of PSA specific for the assessment of adequate independence of safety functions, PSA can complement deterministic approaches. GSR-4 explicitly mentions that PSA “may provide insights into system performance, reliability, interactions and weaknesses in the design, [and] the application of defence in depth” [18], p. 24f. The systematic modelling approach for construction fault tree models requires analysing system failures until the basic events (mainly components) are functionally independent from each other (cf. SSG-3 in requiring e.g. that “the functional dependencies and component failure dependencies are taken into account explicitly” [4], p. 38). Moreover, the PSA modelling requires a systematic analysis of potential dependent failures due to functional dependencies, physical dependencies, human interactions, and common cause failures (cf. SSG-3 [4], p. 40ff.). For hazard PSA, one of the main tasks is the identification and modelling of hazard induced dependencies among failure events considered as independent events in an internal events PSA, i.e. the analysis of hazard-induced common cause failures (SSG-3 [4], e.g. p. 65, p. 107). Such hazard induced dependent failures may lead to the occurrence of IE assumed in the internal events PSA under more severe boundary conditions like the total or partial loss of multiple plant systems/safety functions for accident mitigation. This is an important issue within the ASAMPSA_E project [17]and is discussed for example in the six hazard-specific reports of the ASAMPSA_E project.

In order to assess the independence of provisions for achieving safety functions by means of a PSA, the general approach is readily available. The fault tree models for safety functions (or trains thereof), for which sufficient independence is to be shown, have to be analysed for common cut sets (failures) under the boundary conditions of the initiating event of interest. Usually, this can be done by a simple cut-set analysis of a suitable fault tree combining the functions of interest or by analysing the cut sets of suitable event tree sequences. If there are any

significant dependencies, the resulting failure probability will be (orders of magnitude) larger than simply multiplying the failure probabilities of the respective individual safety function probabilities[11]. With respect to extended PSAs it should be noted that hazard-induced dependencies should be quantified as well, since they need to be systematically modelled for an extended PSA. Therefore, extended PSAs can and should be used to complement the respective deterministic assessments. There is, however, no specific need to develop new methods for identifying and quantifying dependencies between safety functions with an extended PSA, which has already been produced to high quality standards.

A further question is of course which (probabilistic) criteria could be used to assess whether any dependencies between safety functions (or trains of provisions which achieve the safety function) are acceptable. Such criteria could be set e.g. in terms of importance values on single events or common cause failures that disable more than one line of defence or in the presence of such cut-sets within the leading cut-sets (e.g. with more than 1% contribution to overall unavailability). However, the authors are not aware that such criteria have actually been set. Moreover, the authors point out this could be due to the fact that such criteria might be superfluous or at least largely redundant. If, e.g., probabilistic risk criteria related to CDF and LRF are applied, then these implicitly impose reliability targets on the conditional failure probability of the provisions for achieving the safety functions for the respective initiating events as explained in section 4.2. Furthermore, it has already been explained how IE for PSA (including hazards) are connected to PIE for deterministic assessments. Thus, the added value of imposing specific criteria on the independence of safety functions on different levels of DiD is limited. Against this background, the authors do not recommend to specifically set criteria as to the independence of safety functions. Conversely, the authors do recommend using PSA results to check for common cause failures and other dependent failures which disable multiple safety functions requested for a specific event or hazard scenario. Such investigations can in general be performed using established (extended) PSA models without a need for restructuring PSA models along the levels of DiD. Judgements on the acceptability of any findings should be made on a case-by-case basis.

5.3 DEFENCE-IN-DEPTH AND RISK MONITORS

The use of risk monitors is a well-known application of a PSA in NPPs. SSG-3 gives some guidance on the use and limitations of risk monitors as well as on the changes in PSA models required for risk monitors [4], p. 141ff. There are several software tools available, which are actually applied in NPP risk monitors. A number of risk monitor software tools allow to present qualitative (risk) information related to the availability of safety systems [23]. This is often labelled as status information related to defence-in-depth [23], [24], [25]. This assessment, whether qualitatively or quantitatively, has as a prerequisite an appropriate structure of the underlying PSA model..

In reference [39] an example of developing a risk monitor system is described. The concept of risk monitor has been expanded to be applicable for various accident situations ranging from prior to core melt to after core melt. The basic configuration of the risk monitor system is a two-layer system: “plant DiD (Defense-in-Depth) risk monitor” and “reliability monitor”. The “plant DiD risk monitor” is meant to evaluate the intactness of the whole safety system based on the results of individual reliability monitors. It will monitor the safety functions

[11] This will routinely be the case in an analysis for the combined failure (e.g. 3 out of 4 or 4 out of 4) of redundant trains of a safety system. Then, common cause failures usually will determine the overall unavailability of the safety function.

incorporated in the plant system, which are maintained by multiple barriers of defense in-depth (DiD). The "reliability monitor" is meant for the daily monitoring of the reliability state of individual subsystems.

To monitor the safety performance of the plant, the risk based safety indicators can be used. PSA can provide indicators for many different levels of safety, as follows (see also [71][72]):

- high level indicators – plant risk can be measured in terms of CDF, frequency of release categories, population risk,
- second level indicators - frequency of initiating events, probability of core damage, probability of radioactive release (PSA level 2 required),
- intermediate level indicators - safety function unavailability,
- lower level indicators - system unavailability, train unavailability, component unavailability.

The PSA used to produce risk based indicators should include all internal and external hazards specific to the plant.

For the relevant hazards, using deterministic and probabilistic techniques, it should be demonstrated that the preventive and mitigating measures against the hazard are adequate.

5.4 FURTHER REMARKS AND CONNECTION TO AN EXTENDED PSA

The IAEA is further developing the approach for the representation and assessment of DiD in nuclear installations emphasizing the need for a holistic consideration of the levels of DiD in conjunction with deterministic and probabilistic goals and success criteria [33]. For measuring and assessing the adequacy of the DiD framework, success criteria (expressed in deterministic and probabilistic terms) need to be defined for each level of defence. The holistic consideration of DiD in conjunction with deterministic and probabilistic success criteria can assist in determining requirements for reliability of normal operation, control, and engineered safety features of an NPP. This is especially important in the process of designing new NPPs.

In the analysis of compliance with DiD, PSA can be an excellent tool to verify the independence of provisions on different levels of DiD. PSA used in the process of assessing compliance with DiD and determining the requirements for reliability of normal operation and safety systems, 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. an extended PSA as understood by the ASAMPSA_E project) is usually required. Level 1 PSA is needed to assess compliance with Level 3 of DiD and specify requirements for reliability parameters. Level 2 PSA is needed to evaluate compliance with Level 4 of DiD.

Simplistically one can consider that the solution is to represent, for a given initiator and for a given safety function, the safety architecture through different levels of defence in depth, and for each DiD level, to consider all the provisions that make up the "layers of provision" expected to achieve the safety function under consideration. The event tree is built with nodes that correspond to different levels of defence in depth. For each level, i.e. for each node, the fault tree applied to the layer of corresponding provisions establishes the probability of success or failure of the DiD level.

Of course the reality is more complex because it is important to consider, with the PSA, the possibilities of partial failures for the layers of provisions and to integrate the mutual dependencies between different safety functions. Indeed, especially for the latter type of dependency, the total or partial realization of a given safety function, determines the conditions of implementation of other safety functions (e.g. the embodiment of the "reactivity control", determines the mission which corresponds to the "evacuation of the power").

6 CONCLUSIONS AND RECOMMENDATIONS FOR THE LINK BETWEEN DEFENCE-IN-DEPTH AND EXTENDED PSA

The concepts of DiD and PSA have been initially developed independently in the history of NPP safety. The traditional role of DiD is in the design of the plant and its safety provisions, while PSA calculates the probability for failure of the safety provisions and it quantifies the risk profile of the NPP. Therefore, PSA is a tool for complementarily evaluating the level of safety achieved by implementing the DiD concept including all other safety related activities.

Keeping in mind these complementary objectives of DiD and PSA, it is recommended that DiD and PSA be developed independently of each other. If a NPP could demonstrate that it follows all applicable DiD rules, and if an independent PSA confirms a low risk of this plant, there would be a well-founded confidence in an adequate level of safety for this plant. If, on the other hand, PSA identifies a high or unbalanced risk profile for the plant, there are doubts as to whether the current application of the DiD concept is sufficient and additional safety provisions are expected. This impact of PSA is now included in the DiD concept, as a complement for the design.

However, beyond this basic concept of independence there are a few issues which establish links between DiD and PSA:

- PSA should be structured in such a way that the individual levels of DiD can be identified ;this will enable to verify the contribution of each level of DiD to the overall safety, and it can identify potential weaknesses in individual levels of DiD;
- DiD as well as PSA have their own concepts for including or dismissing events or phenomena from their respective analyses ; it is not recommended to harmonize these features in order to keep the benefits of diversity ; in contrast, any differences in assumptions should be clearly identified and documented ;the evaluation of such differences may be more fruitful than striving for a more unified approach;
- the discussion on the evolution of the DiD concept – partly to be found in the present document – is not related to the progress in PSA methods; whatever the DiD concept, PSA will be able to reflect it in principle; this does not mean that the PSA method is perfect ;here are important deficiencies in PSA (e.g. lack of data, incompleteness, insufficient methods for some human actions, large requirement of resources, etc.), but they are not related to DiD issues;
- If PSA shows that a particular level of DiD does not contribute significantly to reducing risk, or if PSA indicates that even without a particular level of DiD risk targets can be met, there are arguments to relieve DiD requirements for this particular plant; on the other hand, if PSA indicates a high risk, it is advisable to improve the design, possibly by strengthening the DiD approach; the consideration of “extended PSA” results as an important safety indicator in that context can be promoted but this, however, requires that the PSA accomplishes the highest quality standards.

Conversely, there are several issues regarding the relationship between PSA and DiD, which could not be investigated in depth in this report and need to be subject of future discussions:

- discussion and recommendations in this report are largely at a conceptual level ; this is partly due to the lack of previous investigations into the subject and partly due to a lack of practical implementations and feedback on good practices in the PSA community ; therefore, specific guidance on how to do practical modelling of PSA with a view to do DiD assessments could be subject to subsequent work;
- PSA models often have been produced without the specific objective of assessing the implementation of

DiD by DiD levels; therefore, existing PSA models would have to be modified to comply with the recommendations of this report; however, guidance on how to do this in an effective manner could not be achieved in this project; moreover, changing the structure of an existing PSA model to fall in line with DiD levels is a significant effort; there is still no clear consensus if the added value justifies the work; both aspects require further discussion;

- an important aspect of the feasibility of PSA modelling is the availability of data for initiating events as well as failure probabilities of SSC; a PSA model that systematically includes SSC on DiD level 2 (or even DiD level 1) would require additional data that are not readily available from existing PSA models; whether existing operating experience databases could supply the required information or if data gathering practices would need to be changed should be investigated.

In order to define a way to go beyond the above considerations and overcome the highlighted limits, further investigations have been developed during the project about the peculiar roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations. An additional report [69] describes the proposed process and tools (see §5.1.3). All the proposals are based on consolidated terminology [42] and shared concepts ([4], [65], [7] and [67]), and consistent with the (IAEA) Safety Fundamentals [1], Safety Requirements [2] and process for the Safety assessment [18]. Further activities are required in order to finalize the proposal, mainly about the criteria and metrics to be adopted and the development of practical applications.

7 GLOSSARY

Initiating Event (IE)

An initiating event is an event that could lead directly to fuel damage or that challenges normal operation and which requires successful mitigation using safety or non-safety systems to prevent fuel damage.

Note: This is a modified definition from SSG-3 [4] to address also the risk from spent fuel storage facilities (spent fuel pool, etc.). Note that core damage is a subset of fuel damage (fuel as a source of significant plant releases can be located in the reactor core, spent fuel pool, etc.). The original SSG-3 definition is "An initiating event is an event that could lead directly to core damage (e.g. reactor vessel rupture) or that challenges normal operation and which requires successful mitigation using safety or non-safety systems to prevent core damage." [4], p. 25

Postulated Initiating Event (PIE)

For the purpose of PIE, an initiating event is an event that leads to anticipated operational occurrences or accident conditions. This includes operator errors and equipment failures (both within and external to the facility), human induced or natural events, and internal or external hazards that, directly or indirectly, challenge one or more of the systems required to maintain the safety of the plant, see SSG-2 [3].

The selection of PIEs associated with DSA is usually prescribed by design basis requirements complemented with events recommended by national or international guidelines (that's why the term "postulated" is used). This is one important difference from IEs defined for the purpose of PSA, since the selection of IEs in PSA is a subject to the specific selection and screening process as a standard PSA task (see SSG-3 [4], Initiating Event Analysis Section. The PSA screening process may therefore screen out or group into bounding events scenarios that are treated as PIE in DSA.

Note: PIE requires the definition of anticipated operational occurrence and definition of accident conditions. PIE definitions, coverage and the process of selection can be different from IE definition that "challenges normal operation and which requires successful mitigation using safety or non-safety systems to prevent fuel damage" [4].

Hazard

The term "hazard" is used in IAEA documentation in the general sense[12], it is defined neither in IAEA Safety Glossary [42] nor in SSG-2 [3], SSG-3 [4], SSG-18 [41], IAEA General Safety Requirements GSR Part 4 [18], etc.

If a hazard meets definition of initiating event (IE) then the term "hazard" is used in PSA for events which have an ability to cause IE and simultaneously reduce IE mitigation capability (e.g. also to reduce or defeat more DiD Levels) of a nuclear power plant, usually by affecting multiple components or structures in a plant (see e.g. IAEA Specific Safety Guide SSG-3 [4], para. 6.1).

Note: An IE is a subset of hazard in PSA, i.e. some hazards need not to be IEs (e.g. hazard resulting only in unavailability type of events, such us input to Technical Specification due to loss of standby safety system).

According to SSG-3, hazards can be further categorized as:

(a) **Internal hazards** originating from the sources located on the site of the nuclear power plant, both inside and outside plant buildings. Examples of internal hazards are internal fires, internal floods, turbine missiles, on-site transportation accidents and releases of toxic substances from on-site storage facilities.

(b) **External hazards** originating from the sources located outside the site of the nuclear power plant. Examples of external hazards are seismic hazards, external fires (e.g. fires affecting the site and originating from nearby forest fires), external floods, high winds and wind induced missiles, off-site transportation accidents, releases of toxic substances from off-site storage facilities and other severe weather conditions.

[12]Example: A hazard is a situation that poses a level of threat to life, health, property, or environment.

8 LIST OF REFERENCES

[1] International Atomic Energy Agency (IAEA), "Fundamental Safety Principles", Safety Fundamentals No. SF-1, November 2006

[2] International Atomic Energy Agency (IAEA), "Safety of Nuclear Power Plants: Design", Specific Safety Requirements No. SSR-2/1, January 2012

[3] International Atomic Energy Agency (IAEA), "Deterministic Safety Analysis for Nuclear Power Plants", Specific Safety Guide No. SSG-2, December 2009

[4] International Atomic Energy Agency (IAEA), "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-3, April 2010

[5] INSAG, "Defence in Depth in Nuclear Safety", INSAG-10, June 1996

[6] Sorensen, J. N., "Historical Notes on Defense in Depth", Memorandum to the US NRC Advisory Committee on Reactor Safeguards, October 1997

[7] WENRA, "Safety of New NPP Designs, Study by Reactor Harmonization Working Group RHWG", March 2013

[8] Holmberg, J., J. Nirmark, "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, SKI report 2008:33, February 2008

[9] Hellström, P. M. Knochenhauer, R. Nyman, "SSM Research Project on Defence-in-Depth PSA – Assessing Defence-in-Depth Levels with PSA Methods" in: 10th International Probabilistic Safety Assessment and Management Conference (PSAM10), 2010

[10] Frey, W. at al., "Auswertung und Modellierung von Maßnahmen auf der Sicherheitsebene 1 und 2 anhand einer PSA", GRS-A-3682, September 2012

[11] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, "Sicherheitsanforderungen an Kernkraftwerke" from 20 November 2012, BAnz AT 24.01.2013 B3

[12] Gasparini, M., "The Draft of the Revised 'Safety of Nuclear Power Plants: Design, NS-R-1'", presentation at 5th GIF/INPRO Interface Meeting, March 2011

[13] International Atomic Energy Agency (IAEA), "Development and Application of Level 4 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-4, May 2010

[14] Guignot, Y. et al., "Synthesis of the Initial Survey Related to PSAS End-users Needs", Technical Report ASAMPSA_E/WP10/D10.2/2014-01, 2014

[15] International Atomic Energy Agency (IAEA), "Periodic Safety Review for Nuclear Power Plants", Specific Safety Guide No. SSG-25, March 2013

[16] International Atomic Energy Agency (IAEA), "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants", Specific Safety Guide No. SSG-4, May 2010

[17] Raimond, E. et al., "Annex I – 'Description of work' ASAMPSA_E", April 2013

[18] International Atomic Energy Agency (IAEA), "Safety Assessment for Facilities and Activities", General Safety Requirements Part 4 No GSR Part 4, May 2009

[19] Atomic Energy Control Board, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants", Regulatory Document R-8, February 1991

[20] OECD/NEA, "Use and Development of Probabilistic Safety Assessment, An Overview of the Situation at the End of 2010", NEA/CSNI/R(2012)11, December 2012

[21] U.S. NRC, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission", NUREG/BR-0058, Revision 4, September 2004

[22] ENSI, "Probabilistic Safety Analysis (PSA): Applications", Guidelines for Swiss Nuclear Installations ENSI-A06/e, March 2009

[23] OECD/NEA, "Risk Monitors: The State of the Art in their Development and Use at Nuclear Power Plants", NEA/CSNI/R(2004)20, 2004

[24] Lloyd's Register Consulting, "RiskSpectrum Magazine 2014", June 2014

[25] Kuramoto, T., "Risk Monitoring for Nuclear Power Plant Applications using Probabilistic Risk Assessment", Nuclear Safety and Simulation, Vol. 3, No. 3, p. 226-231, September 2012

[26] Western European Nuclear Regulators Association (WENRA), "WENRA Safety Reference Levels for Existing Reactors", draft update, November 2013

[27] ASAMPSA_E, "Bibliography on defense in depth for nuclear safety", A. Wielenberg (ed.), ASAMPSA_E D30.1, November 2014

[28] P. Hellström, "DiD-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA", SSM 2015:04, January 2015

[29] International Atomic Energy Agency (IAEA), "Assessment of Defence in Depth for Nuclear Power Plants", Safety Reports Series No. 46, February 2005

[30] WENRA, "WENRA Safety Reference Levels for Existing Reactors", September 2014

[31] International Atomic Energy Agency (IAEA), "Safety of Nuclear Power Plants: Design", Specific Safety Requirements No. SSR-2/1, 2012.

[32] NRC. 10 CFR 50.69 Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors. Washington2004.

[33] NEI. 10 CFR 50.69 SSC Categorization Guideline. NEI 00-04 (Rev 0)2005.

[34] Western European Nuclear Regulators Association (WENRA), "WENRA Statement on Safety Objectives for New Nuclear Power Plants, Novenber 2010

[35] ASAMPSA_E, "Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA", ASAMPSA_E D30.3, draft, unpublished

[36] ASAMPSA_E, "Risk Metrics and Measures for an Extended PSA", ASAMPSA_E D30.5, draft, unpublished

[37] International Atomic Energy Agency (IAEA), "Safety Classification of Structures, Systems and Components in Nuclear Power Plants", Specific Safety Guide No. SSG-30, May 2014.

[38] OECD/NEA, "Use and Development of Probabilistic Safety Assessment, An Overview of the situation at the end of 2010", Report. No. NEA/CSNI/R(2012)11, 2013.

[39] Matsuoka, T., "Installation of GO-FLOW into the risk monitor being developed at Harbin Engineering University", Nuclear Safety and Simulation, Vol. 3, Number 4, December 2012

[40] Groudev, P., P. Petrova, E. Kitchev, K. Mancheva, "PSA Contribution in Development and Application of Severe Accident Guidelines", Proceedings of ESREL2015, p. 399ff, September 2015

[41] International Atomic Energy Agency (IAEA), "Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations", Specific Safety Guide No. SSG-18, November 2011

[42] International Atomic Energy Agency (IAEA), "Terminology Used in Nuclear Safety and Radiation Protection", IAEA Safety Glossary, 2007 Edition, June 2007

[43] International Atomic Energy Agency (IAEA), "Safety of Nuclear Power Plants: Design", Specific Safety Requirements No. SSR-2/1, (Rev 1), 2016

[44] International Atomic Energy Agency (IAEA), "Considerations on the Application of the IAEA Safety Requirements for Design of Nuclear Power Plants", draft IAEA TECDOC, May 2015, under publication

[45] Sorensen, J.N., "Historical Notes on Defense in Depth", Memorandum to the US NRC Advisory Committee on Reactor Safeguards, October 1997

[46] CNCAN, Normă privind evaluările probabilistice de securitate nucleară pentru centralele nuclearoelectrice, CNCAN NSN-08, 07 November 2006

[47] ENSI, "Probabilistic Safety Analysis (PSA): Quality and Scope", Guidelines for Swiss Nuclear Installations ENSI-A05/e, March 2009

[48] STUK, Probabilistic risk assessment and risk management of a nuclear power plant, YVL A.7, 15 November 2013

[49] STUK, Classification of systems, structures and components of a nuclear facility, YVL B.2, 15 November 2013

[50] Atomic Energy Control Board, "Requirements for Containment Systems for CANDU Nuclear Power Plants", Document R-7, February 1991

[51] Atomic Energy Control Board, "Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", Document R-9, February 1991

[52] CNSC, "Design of Reactor Facilities: Nuclear Power Plants", REGDOC-2.5.2, May 2014

[53] CNCAN, "Norme de securitate nucleara privind proiectarea si constructia centralelor nuclearoelectrice", NSN-02, 23 November 2010

[54] CNCAN, "Norme privind sistemul de răcire la avarie a zonei active pentru centralele nuclearoelectrice de tip CANDU", NSN-11, 11 May 2006

[55] CNCAN, "Norme privind sistemele de oprire rapidă pentru centralele nuclearo-electrice de tip CANDU", NSN-13, 23 November 2005

[56] CNCAN, Norme privind sistemul anvelopei pentru centralele nuclearoelectrice de tip CANDU, NSN-12, 23 November 2005

[57] US NRC, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance", RG 1.201 Rev. 1, May 2006

[58] NASA, NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1, November 2011

[59] G.L. Fiorini, S. La Rovere, P. Vestrucci, "Peculiar Roles of the Defense in Depth and the Probabilistic Safety Assessment in NPP Safety Performances Optimization", ICAPP2015, May 3-6, 2015

[60] SNSA, "Pravilnik o dejavnikih sevalne in jedrske varnosti (JV5)", Ur. l. RS 92/2009. (translated "Rules on radiation and nuclear safety factors (JV5)", Off. Gaz. of RS 92/2009)

[61] SNETP (Sustainable Nuclear Energy Technology Platform): Identification of Research Areas in Response to the Fukushima Accident, January 2013, in Report of the SNETP Fukushima Task Group, Chairman Jozef Misak: Challenges from the lessons learned from Fukushima, http://www.snetp.eu/report-of-the-snetp-fukushima-task-group/

[62] IAEA: INES: The International Nuclear and Radilogical Event Scale User's Manual, 2008 Edition, Non-Serial publications, IAEA-INES-2009, 206 pp., Vienna 2009

[63] J.Vitazkova, E.Cazzoli: The principle of DiD in the perspective of probabilistic safety analyses in the wake of Fukushima, Risk Analysis IX, 2014

[64] IAEA Safety Report Series No.52, "Best estimate Safety Analysis for Nuclear Power Plants: Uncertainty evaluation", Vienna, 2008, http://www.pub.iaea.org/MTCD/Publications/PDF/Pub1306_web.pdf

[65] NUREG 2150 - A Proposed Risk Management Regulatory Framework, April 2012

[66] G.L. Fiorini, S. La Rovere, P. Vestrucci – Peculiar Role of the Defence in Depth and the Probabilistic Safety Assessment in NPP safety performances optimization. ICAPP 2015 - 03- Nice, 07 May 2015

[67] GIF/RSWG/2010/002/Rev.1 – An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems; June 2011

[68] GIF/RSWG - Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems - Revision 1; November 24, 2008

[69] ASAMPSA_E, "The PSA assessment of Defense in Depth - Memorandum and proposals", Gian-Luigi Fiorini, Stefano La Rovere (NIER), unpublished

[70] IAEA, Concepts and terms of IAEA Safety Standards – Introductory website - http://www-ns.iaea.org/standards/concepts-terms.asp?s=11&l=90 ti

[71] IAEA-TECDOC 1200, Applications of probabilistic safety assessment to nuclear power plants, February 2001

[72] IAEA-TECDOC 1141, Operational safety performance indicators for nuclear power plants, May 2000

9 LIST OF TABLES

10 LIST OF FIGURES