Advanced Safety Assessment Methodologies: extended PSA

"NUCLEAR FISSION "

Safety of Existing Nuclear Installations

Contract 605001

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

Reference ASAMPSA_E

Technical report ASAMPSA_E / WP30 / D30.7/2017-31 volume 4

Reference IRSN PSN-RES/SAG/2017-00019

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: 31-12-2016	
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	Yes
RE	Restricted to a group specified by the partners of the ASAMPSA_E project	No
CO	Confidential, only for partners of the ASAMPSA_E project	No

ASAMPSA_E Quality Assurance page

Partners responsible of the document :	**GRS**
Nature of document	Technical Report
Reference(s)	Technical report ASAMPSA_E/ D30.7/2017-31 volume 4 Rapport IRSN-PSN-RES/ SAG/2017-00019
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	31-12-2016
Topical area	Defence-in-Depth, PSA
For Journal & Conf. papers	No

Summary :

This report is dedicated to the investigation of the link between the Probabilistic Safety Assessment (PSA) and the Defence-in-Depth (DiD) concept for Nuclear Power Plant (NPP). The discussion is mainly focused on the capability of an “extended PSA” to support the assessment of DiD.

The concepts of DiD and PSA have been developed independently in the history of NPP safety. If appropriately developed, the PSA can provide essential contributions for determining whether the safety objectives are met, the DiD requirements are correctly taken into account, the risk related to the installation is As Low As Reasonably Achievable, and a graded approach to safety is adopted. Moreover, the PSA has the potential to provide insights and results for the assessment of DiD, e.g.: on the independence among DiD levels, on the reliability to be required to provisions, on the modelling of immaterial provisions (e.g. human factor), on the propagation of uncertainty, on the “practical elimination” of events which could lead to early or large releases.

The ability of the PSA to reflect the DiD concept (always true in theory) and its potential to provide information complementing the deterministic assessment of DiD are recognized and unquestionable. On the other hand, the use of PSA and its results for the assessments of DiD introduces specific challenges only partially investigated during the ASAMPSA_E project. Among them, the existing PSA models have been often produced without the specific objective to assess the implementation of DiD. If the PSA is used with this particular objective, its results should be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified. This change of structure of the PSA model could require a significant effort and there is still no clear consensus if the added value justifies it. Furthermore, in spite of the said complementarity, the independent implementation of the DiD concept and development of PSA, together with their native diversity, has been recognized as a benefit to maintain.

As general recommendation, both DiD and PSA should be developed and their contributions optimized. In order to enhance their complementarity, the optimization to be searched should maintain a degree of independence in their execution and meantime integrate their “needs” (of data and models) and results, for an exhaustive assessment of the safety architecture based on both deterministic and probabilistic insights.

This report provides elements to feed the thoughts about the optimization between the contributions of DiD and PSA to guarantee the safety of the nuclear installation, but further discussion and practical experiences (e.g. benchmarking) are needed to achieve consensus on objectives, scope and approaches for the use of PSA in the assessment of DiD concept and to develop a practical guideline.

Visa grid			
	Main author(s) :	**Verification**	**Approval (Coordinator)**
Name (s)	S. La Rovere; G.L. Fiorini	Horst Löffler	E. Raimond
Date	2016-12-18	2016-12-19	2017-02-01

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 NIER 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.
Rev 8	15/12/2016	G.L.Fiorini, S La Rovere	All	General review of the documents, following the Vienna Meeting on 13-14 September 2016.
Rev 8	01/02/2017	E. Raimond	Few	Approval review, minor modifications.

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
Wielenberg	Andreas	GRS
Loeffler	Horst	GRS
Hage	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	Stefano	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 between the Probabilistic Safety Assessment (PSA) and the Defence-in-Depth (DiD) concept for Nuclear Power Plant (NPP).
The discussion is mainly focused on the capability of an “extended PSA” to support the assessment of DiD.
In line with other activities of the ASAMPSA_E project, the report treats mainly PSA Level 1 and Level 2 issues.

The concepts of DiD and PSA have been developed independently in the history of NPP safety. The traditional role of DiD is within the design of the plant with the identification, the sizing and the implementation of the safety provisions, while PSA calculates the probability/frequency of failure of safety provisions and quantifies the risk profile of the NPP. The implementation of the DiD is explicitly required at the European level by the Council Directive 2014/87/EURATOM of 8 July 2014 [1]. As an essential part of the safety demonstration, requirements are explicitly formulated for its assessment, among others and in a wider context, by the IAEA ([2], [4], [5]). After the Fukushima accident the question of further improvements of DiD returned to the focus of discussions.

The PSA provides a comprehensive, structured approach for the assessment of the plausible scenarios, for the identification of the challenging sequences of events, for the evaluation of the corresponding damages to the facility and for the estimation of the risk for workers, public and environment.
If appropriately developed, the PSA can provide a methodological support and essential contributions for determining whether the safety objectives are met, the DiD requirements are correctly taken into account, the risk related to the installation is As Low As Reasonably Achievable, and a graded approach to safety – as requested by the regulators - is correctly implemented.
Moreover, the PSA has the potential to provide insights and results for the assessment of DiD, including e.g.: the independence between DiD levels and specifically the effects of dependent failures and the effectiveness of implemented redundancies, the reliability to be required in the design and sizing of provisions, the modelling of immaterial provisions (e.g. human factor), the propagation of uncertainty on input data through the model, the “practical elimination” of plausible events and sequences of events which could lead to early or large releases.
If a NPP safety analyses could demonstrate that the applicable DiD safety requirements are respected, and if PSA confirms an acceptable risk of this plant, there would be a well-founded confidence in an adequate level of safety; on the other hand, if PSA identifies a high or unbalanced risk profile for the plant, there are doubts on the adequacy of the current application of the DiD concept and additional safety provisions are expected. A third case could occur: the PSA results indicate that the risk is acceptable but the principles of DiD are not properly implemented; additional requirements may be expected to address this discrepancy.

Iterations between the two approaches are necessary during the whole design. As mentioned by IAEA in the SSR-2/1 (Rev.1) [4]: “The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses”.

Further, qualitative safety objectives should be considered in the assessment of DiD, as foundation of the deterministic approach to build the "safety architecture"[1] of the NPP. In this wider context, the PSA could support the verification of further requirements stated in the SSR-2/1[4], about the degree of "progressiveness" of the response of the safety architecture and the verification of its "tolerant", "forgiving" and "balanced" characters (see §2.4 and §5.3).

The ability of the PSA to reflect the DiD concept (always true in theory) and its potential to provide information useful for the assessment of DiD are unquestionable. On the other hand, the use of PSA and its results for the assessments of DiD introduces specific challenges only partially investigated during the ASAMPSA_E project.

The existing PSA models have been often produced without the specific objective for assessing the implementation of DiD. This is partly due to the lack of previous investigations into the subject and partly due to the lack of practical implementations and feedbacks about good practices in the PSA community. If the PSA is used with this particular objective, it should be properly structured in order to provide results that can be correlated with the performances (capability, reliability and robustness) required to the individual DiD levels (i.e. relevant layer of provisions) while having a sufficient scope.

A different structure of the PSA models (i.e. the re-structuring the existing PSA) has been proposed by different works (see § 5.1, §5.3, §5.6, §5.7), but this does not seem an unquestionable need. Guidance on how to re-structure the PSA to fall in line with the DiD levels is neither precisely available nor developed during the ASAMPSA_E project (out of scope), only generic thoughts have been formulated. Moreover, this activity could require a significant effort and there is still no clear consensus if the added value justifies it.

Additionally:

- the levels of DiD and the associated plant conditions do not easily map to the traditional PSA end states and initiating events; at this regard, the debate is open about which initiating events, boundary conditions, safety functions and other elements of a PSA should be assigned to which level of DiD;
- the best-estimate approach typically used in PSA is not immediately compatible with the (conservative, safety case oriented) deterministic approach for a DiD assessment;
- non-safety systems should be considered in the PSA, but they are usually neglected in the Deterministic Safety Assessment (DSA);
- the comparison between the IE in PSA (with related frequency of occurrence) and the classification of PIE could be difficult mainly because of the (potential) different grouping of events and the different assumptions on boundary conditions and concurrent failures in PSA and DSA;
- a PSA model for the assessment of DiD could require additional data if they are not already included in the existing non-full scope PSA models (e.g. about initiating events and SSCs failure at the DiD level 2);
- deterministic assessments (DSAs) often assume certain boundary conditions to occur simultaneously at the time of the PIE occurrence, without considering their likelihood; differently, they are usually addressed in the PSA with their conditional probabilities, giving less conservative estimations.

[1] According to GIF/RSWG [36], in the context of DiD, the "Safety Architecture" is "*the full set of provisions - inherent characteristics, technical options and organizational measures - selected for the design, the construction, the operation including the shut down and the dismantling, which are taken to prevent the accidents or limit their effects.*"

Furthermore, in spite of the said complementarity, the independent implementation of the DiD concept and development of PSA, together with their native diversity, has been recognized as an advantage to be maintained. Specifically:

- DiD and PSA have their own concepts for including or dismissing events or phenomena from their respective analyses; to keep the benefits of diversity, the harmonization of these features should not be an objective per se; at the same time, any differences in assumptions should be clearly identified and addressed in order to contribute to an exhaustive consideration of all the events and phenomena challenging the installation;
- the discussion on the evolution of the DiD concept (partly provided in the present document) is not directly related to the need for progresses in PSA methods; the deficiencies recognized in the actual PSA (e.g. lack of data, incompleteness, insufficient methods for some human actions, large requirement of resources, etc.), which motivate a specific work for their improvement, are not related to DiD issues.

Nevertheless, taking into account their complementary objectives, both DiD and PSA should be developed and their contributions optimized in order to:

- maintain a degree of independence in their execution which, combined with their native diversity, could provide the required confidence on the results of the safety assessment;
- integrate their needs (about data and models) and results, for an exhaustive assessment of the safety architecture, based on both deterministic and probabilistic insights.

As key condition to achieve this optimization, the PSA used with the particular objective to verify the implementation of the DiD concept, should be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified.

By summarizing, the present report provides elements to feed the thoughts about the optimization between the contributions of DiD and PSA to guarantee the robustness of the safety assessment of the installation, but further discussion and practical experiences (e.g. benchmarking) are needed to achieve consensus on objectives, scope and approaches for the use of PSA in the assessment of DiD concept and to develop a practical guideline.

CONTENT

ABBREVATIONS

AOO	Anticipated Operational Occurrence
ATWS	Anticipated Transients Without Scram
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
FV	Fussel Vessely
GIF	Generation IV International Forum
GSR	General Safety Requirements
IE	Initiating Event
ISLOCA	Interfacing System LOCA
INES	International Nuclear And Radiological Event Scale
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 Assessment
PWR	Pressurized Water Reactor
RAW	Risk Achievement Worth
RR	Research Reactor
RSWG	Risk & Safety Working Group
SF	Safety Fundamentals
SFP	Spent Fuel Pool
SNETP	Sustainable Nuclear Energy Technology Platform
SSC	Systems, Structures, And Components
SSR	Specific Safety Requirements

1 INTRODUCTION

After the Fukushima accident the question of further improvements of the Defense-In-Depth (DiD) concept returned to the focus of discussions, as it happened earlier after the major accidents in Three Mile Island and Chernobyl. This attitude has been supported by many publications, e.g. "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."* Moreover, "*the 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.*" [68].

Several definitions of the concept of DiD, perfectly consistent among them, are available within a number of reference documents such as the European Council Directive [1], the IAEA fundamentals and requirements ([2], [4], [5]), and the WENRA's recommendations for existing and new reactors ([23], [24]).
In spite of the evidence that no existing NPPs strictly fulfil the requirements related to the DiD concept (as currently defined), the latter remains "t*he primary means of preventing and mitigating the consequences of accidents*" [3] and then the reference for any safety assessment and reasonably practicable safety improvements.

The need for the assessment of DiD is explicitly recognized by the GSR Part 4 (Rev1) [5], which defines the context for the safety assessment of a nuclear installation, encompassing DiD concept and PSA, and details the objective to be pursued: "*It shall be determined in the assessment of Defence-in-Depth whether adequate provisions have been made at each of the levels of Defence-in-Depth.*" Safety assessments are performed "*by means of deterministic and also probabilistic methods*"; "*probabilistic 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.*" ([5], Requirement 13).
Requirements are specified for the assessment of DiD, among others and in a wider context, by the INSAG reports [19], by the IAEA standards and guidelines ([3], [4], [5], [14]) and by recommendations from the Western European Nuclear Regulators Association ([23], [24], [25]).

The DiD concepts and the PSA approach have been developed independently in the history of NPP safety.
The traditional role of DiD is within the design of the plant with the identification, the sizing and the implementation of the safety provisions, i.e. through the Deterministic Safety Assessment (DSA); on its side, the Probabilistic Safety Assessment (PSA) estimates the probability/frequency of failure of these provisions and quantifies the risk profile of the nuclear installation.

The PSA provides a comprehensive, structured approach for the assessment of the plausible scenarios, for the identification of the challenging sequences of events, for the evaluation of the corresponding damages to the facility and for the estimation of the risk for workers, public and environment. If appropriately developed, the PSA can provide a methodological support and essential contributions for determining whether the safety objectives are met, the DiD requirements are correctly taken into account, the risk related to the installation is As Low As Reasonably Achievable, and a graded approach to safety – as requested by the regulators - is implemented.

Moreover, the PSA has the potential to provide insights and results for the assessment of DiD, including e.g.: the independence between DiD levels and specifically the effects of dependent failures and the effectiveness of redundancies; the reliability to be required in the design and sizing of provisions; the modelling of immaterial provisions (e.g. human factor); the propagation of uncertainty on input data through the model; the "practical elimination" of plausible events and sequences of events which could lead to early or large releases.

Despite the potential of the PSA and the recognition of its complementarity with the (deterministic) DiD concept, no specific requirements are formulated about the use of PSA for the assessment of DiD, or only conceptual framework are proposed (i.e. without practical guidance and examples of application) (e.g. [63], [71], [74]).

This report is dedicated to the investigation of the link between the Probabilistic Safety Assessment (PSA) and the DiD concept for NPP. The discussion is mainly focused on the capability of an "extended PSA" to support the DiD assessment, i.e. the verification that the DiD concept - and all its principles - is adequately implemented. In line with other activities of the ASAMPSA_E project, the report treats mainly PSA Level 1 and Level 2 issues.

In order to contribute to the state-of-art on the above topics, and being conscious that a single position or a shared synthesis of the different approaches proposed cannot be the objectives of the activities done during the ASAMPSA_E project, this report aims at:

- reminding the most important aspects of the current understanding of the DiD concept, their implications and the needs (and the objectives) of the assessment of DiD;
- discussing the link between DiD and PSA, with specific focus on the potential use of an "extended PSA" to verify the adequacy of the application of the DiD concept, providing recommendations on the general objectives and insights for further investigations;
- providing contributions (coming from the ASAMPSA_E partners) for future discussion and experiences about the optimized use of the DiD concept and PSA approach to guarantee the safety of nuclear installation.

The ASAMPSA_E report "Bibliography on Defense in Depth for Nuclear Safety" [41] provides an overview over a number of references relevant to the DiD concept for nuclear safety (and NPP in particular), with a focus on regulatory sources. A summary of the discussions and definitions that have been used in the literature and overall historical observations on the concept of DiD are provided in the NUREG/KM-0009 [29].

This section provides a brief introduction on the content and structure of this report.

Section 2 introduces the main issues related to the DiD concept, including the reference structure of the levels of DiD, the essential requirement about their independence, the need(s) for the safety and DiD assessments of NPP and some insights on DiD and risk monitoring.

Section 3 is focused on the notions of Postulated Initiating Event (PIE) and Initiating Event (IE), their usage in the Deterministic Safety Assessment (DSA) and Probabilistic Safety Assessment (PSA), and their consistency.

Section 4 is focused on the schemes to be used for the classification of Systems, Structures and Components (i.e. for the provisions implemented in the safety architecture), on the reliability of the engineered safety functions and on the relevant relationships with DiD and PSA.

Section 5 presents some practical experiences, national and/or made by the partners before or during the ASAMPSA_E project. Contributions are reported without any need of coherence and any objective of synthesis. They should be not retained or rejected, but considered as elements for future discussions.

Section 6 provides some general conclusions and recommendations.

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

This section introduces the main issues related to the Defence-in-Depth (DiD) concept, including the reference structure of the Levels of DiD, the essential requirement about their independence, the need(s) for the safety and DiD assessment of NPP and some insights on DiD and risk monitoring.

2.1. DEFENCE-IN-DEPTH

The concept of DiD was first described in the late 1960s / early 1970s [26] as basic approach for achieving a high level of safety for nuclear installations. The DiD concept was initially limited to multiple barrier systems (i.e. focused on the confinement safety function) and then expanded to apply to all safety functions for nuclear installations ([8], [12], [19], [26]).

Today, the implementation of the Defence-in-Depth (DiD) is explicitly required at the European level by the Council Directive 2014/87/EURATOM of 8 July 2014 [1].

The actual broad scope of the DiD concept is reflected in the IAEA Fundamental Safety Principles SF-1 ([3], 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 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."*

The IAEA SSR-2/1 (Rev.1) provides additional guidance about NPP: 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 states*" ([4], p. 6). Furthermore, the SSR-2/1 (Rev.1) describes different areas of application of the DiD concept ([4], p. 7) and at this regard gives requirements about the design of NPPs ([4], p. 13, 14).

According to the SSR-2/1 (Rev.1), the implementation of DiD consists of the realization of different physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations ([4], p. 8). The number of barriers will depend upon the initial source term, the effectiveness of barriers, the possible internal and external hazards, and the potential consequences of failures. Barriers should be properly independent and reliable.

According to the SSR-2/1 (Rev.1), the concept of DiD is applied in order "*to ensure that all safety related activities are subject to independent layers of provisions*[2] *so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures*". ([4], p. 6).

2.2. LEVELS OF DID AND PLANT STATES

The reference structure of the levels of DiD and their associations to the plant states are defined by the IAEA requirements [4] and by recommendations from the Western European Nuclear Regulators Association (WENRA)[3].

The IAEA SSR-2/1 (Rev.1) ([4], p. 7) defines five levels of Defence in Depth aimed at:

1.1. Preventing 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 the Design Extension Conditions (previously Beyond Design Basis Accidents - DiD Level 4);
1.5. Mitigating the radiological consequences of radioactive releases that could potentially result from accidents (on- and off-site – DiD Level 5).

The safety functions achieved through the DiD levels 1 to 4 relate to the design and operation of the NPP itself, while the DiD level 5 relates mainly to the off-site emergency planning. For each levels of DiD, safety provisions (including Systems, Structures and Components, inherent features, or procedures) should be identified, sized and implemented in order to provide the required capability to achieve the requested mission, with the due reliability and robustness against internal and external hazard[4], and then to meet the respective safety objectives.

The levels of DiD can be associated to different states of plant (see Fig. 1).

About NPP states, some definitions in the SSR-2/1 (Rev. 1) [4] differ from ones in the Safety Glossary [2] and define the “updated” references. A Design Basis Accident is a “*postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits*” ([2], [4]). The term Design Extension Condition supersedes the term Beyond Design Basis Accident as a "*postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting*”. ([4], p. 66).

[2] The notion of “provision” used in this requirement encompasses the physical Structure, Systems and Components (SSC), the passive systems, as well as the immaterial means (e.g. procedures, inherent characteristics), covering all the safety features which contributes to the safety of the installation.

[3] The SSR-2/1 (Rev.1) [4] is taken as reference for the definition of the Levels of DiD, even if some differences exists with the ones (previously) defined in the INSAG-10 [19] (e.g. about the DiD Level 2 definition), which is still the reference for some operators.

[4] According to the SSG-30[11]:
- Capability is the ability of an SSC to perform its designated function as required;
- Reliability is the ability of an SSC to perform its required function with a sufficiently low failure rate consistent with the safety analysis;
- Robustness is the ability of an SSC to ensure that no operational loads or loads caused by Postulated Initiating Events (PIEs) will adversely affect the ability of the SSC to perform its function).

A refined structure of the levels of DiD, applicable to new reactor design, is discussed by the WENRA Reactor Harmonization Working Group (RHWG) [23]. RHWG recommends to reinforce and strength DiD approach (compared to previous realizations), provides a summary of the most important characteristics of the DiD concept, and specifies the five levels of DiD in Fig. 1 in terms of objectives, essential means and radiological consequences.

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 (1)	3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions (2)	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact (4)	Postulated single initiating events
	3.b		Additional safety features (3), accident procedures		Postulated multiple failure events
Level 4		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)	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 (5)	-

Fig. 1 The refined structure of the levels of DiD proposed by WENRA/RHWG (footnotes in [23])

Most prominently, according to Fig. 1, each level of DiD is related to a different plant conditions category. Moreover, DiD Level 3 is subdivided into:

- a sub-level 3a, which covers the Postulated single failure events;
- and a sub-level 3b, which covers the Postulated multiple failure events (addressed to prevent the escalation to a severe accident).

WENRA RHWG gives specific guidance for the identification of multiple failure events related to the sub-level 3b. It entails postulated common cause failures or inefficiency of all redundant trains of a safety system implemented to control an Anticipated Operational Occurrence (AOO) or a single PIE, or which is needed to fulfil the fundamental safety functions in normal operation. ([23], p. 20).

Moreover, "I*n choosing the multiple failure events to be addressed in the design, the following factors should be considered together: the frequency of the event; the grace time for necessary human actions; the margins to cliff edge effects; and the radiological or environmental consequences of the event (care should be taken to scenarios with containment bypass*)". ([23], p. 21).

The introduction of the sub-level 3b allows “capturing” explicitly the multiple failure events due to Common Cause Failures (CCF), which are often not postulated within PIE [23].

Level 3.b events are part of the Design Extension Conditions in the SSR-2/1 (Rev. 1) ([23], p. 19). The essential difference between the events considered under the levels 3a and 3b is the approach adopted for deterministic analysis: while a conservative approach is requested for the Level 3a (i.e. for single failure events), a best estimate approach is tolerated for the level 3b (i.e. for multiple failures events). The safety objective is defined by the SSR-2/1 (Rev. 1) [4]: “*the design shall be such that for Design Extension Conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures*”. ([4], p.25). The Council Directive 2014/87/EURATOM of 8 July 2014 [1] formally endorses this objective.

The SSR-2/1 (Rev.1) conceptually addresses the design of (new) reactors. About existing reactors, it states that: “*It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction.*” In addition, “*it might not be feasible to modify designs that have already been approved by regulatory bodies.*” On the other hand, “*For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements.*” ([4], p.1)

For existing reactors, WENRA distinguishes two categories of Design Extension Conditions (DEC):

- DEC A covers scenarios for which severe fuel damage can be prevented, in particular through the implementation of ad-hoc provisions;
- DEC B covers scenarios with postulated severe fuel damage and thus requiring specific provisions for the mitigation of the postulated consequences ([24], p. 20).

Provisions addressing DEC A or DEC B are allocated respectively into the DiD Level 3b and Level 4.

A representative set of DEC A scenarios shall be determined based on DSA, PSA, and engineering judgements. DEC A should cover events and combination of events resulting from internal or external hazards and from CCF, “*which cannot be considered with a high degree of confidence to be extremely unlikely to occur*” ([24], p. 20). It shall be demonstrated that the plant can maintain the fundamental safety functions preventing core degradation.

DEC B events shall be postulated and justified in order to cover situations where the capability of the plant to prevent severe fuel damage is exceeded or the implemented measures are not effective ([24], p. 21). It shall be demonstrated that the plant can maintain the confinement of radioactive material released with the core degradation.

2.3. INDEPENDENCY BETWEEN LEVELS OF DID

The request of independence between "layers of provisions" achieving a given safety function at the different levels of DiD (for a given initiator or sequence of events) is embedded in the DiD concept (e.g. [4], [23], [24]).

At this regard, the SSR-2/1 (Rev.1) [4] gives further recommendations for the design of safety related systems, which are not an integral part of the DiD concept but they are means for implementing independent and effective provisions for the respective safety functions.

The independence among the DiD levels is presented (as Position 2) by the WENRA RHWG for new reactors [23] and (as Objective 4) in a dedicated Statement on Safety Objectives [25], requesting that SSCs[5] achieving safety functions are not adversely affected by the operation or failure of other SSCs on other levels of DiD ([23], p. 15).

For WENRA, the basic safety expectation is that "*There shall be independence to the extent reasonably practicable between different levels of DiD so that failure of one level of DiD does not impair the defence in depth ensured by the other levels involved in the protection against or mitigation of the event.*" ([23], p. 16).

The means to achieve independence between SSCs (i.e. provisions) are adequate applications of diversity, physical separation (structural or by distance), and functional isolation.

WENRA RHWG recommends to justify "*The adequacy of the achieved independence by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgement*". It is clearly stated that "*for each postulated initiating event (starting with DiD level 2), the necessary SSCs should be identified and it shall be shown in the safety analysis that the SSCs credited in one level of DiD are adequately independent of SSCs credited in the other levels of DiD*". ([23], p. 16).

The independence between provisions is mainly assessed through deterministic means. In a number of cases, however, it is difficult to demonstrate the complete independence (e.g. active safety features, because of common support systems, connections via operating systems, potential common cause failures, etc.); in this case, a reasonably practicable degree of independence shall be demonstrated.

The GSR-4 (Rev. 1) explicitly mentions that PSA "*may provide insights into system performance, reliability, interactions and weaknesses in the design, [and] the application of defence in depth*" ([5], p. 24). The SSG-3 [7] requires that "*the functional dependencies and component failure dependencies are taken into account explicitly*" ([7], p. 38).

The general approach to assess, through PSA, the independence between provisions achieving safety function(s) at the different levels of DiD, for each plausible sequences of events, is readily available.

The systematic approach for the construction of the PSA fault trees (modelling the failure of the relevant layer of provisions) allows the analysis of the dependencies among the different safety functions embedded into the model for a given level of the DiD (e.g. management of accident conditions and dependency between the reactivity control, the heat removal and the confinement).

With reference to a safety function achieved at two different levels of DiD through the relevant layers of provisions, two fault tree models can represent the failure of the relevant layers of provisions; these fault trees have to be analysed for common cut sets under the boundary conditions of their initiating event. This can be done through a simple cut-set analysis on a fictitious fault tree combining (by an AND gate) the single fault trees developed or directly on the fault tree-event tree linked model (the event tree introduce itself the logical combination between the single fault trees for the cut-set analysis).

[5] The concept should be applied to the more general term "provision" used by the SSR-2/1.

If there is a significant dependency, the resulting failure probability will be (orders of magnitude) larger than simply multiplying the failure probabilities of the respective individual safety function probabilities[6].
Moreover, according to the IAEA SSG-3 [7] , the PSA modelling requires a systematic analysis of the dependent failures due to functional dependencies, physical dependencies, human interactions, and common cause failures ([7], p. 40). For PSA covering the internal or external hazards (i.e. for an extended PSA), one of the main tasks is the identification and modelling of the dependencies among failures due to external hazard event [7]. Such hazard-induced concurrent failures may lead to the occurrence of an IE already included in the internal events PSA but under more severe boundary conditions (e.g. the total or partial loss of multiple plant systems/safety functions for accident mitigation). This issue is discussed in the six hazard-specific reports of the ASAMPSA_E project [39].

As main result, there is no specific need to develop new methods for identifying and quantifying dependencies between safety functions by an extended PSA, if the latter has already been produced with high quality standards.
However, no information is available on the setting of criteria to assess whether any dependency between safety functions at different levels of the DiD is acceptable. The reason could be due that such criteria are be superfluous or largely redundant. For instance, if probabilistic risk criteria related to CDF and LRF are applied, these implicitly impose reliability targets on the conditional failure probability of the provisions implementing safety functions for the respective initiating events.[7] For example, such criteria could be set in terms of "importance" of single events or common cause failures in the disabling of more than one line of defence, or in their presence/absence within the leading cut-sets (e.g. with more than 1% contribution to the risk measure).

Conversely, the use of PSA results is recommended to check for common cause failures and other dependent failures, which have the potential to disable multiple safety functions requested for a given initiator. Such investigations can in general be performed using established (extended) PSA models. PSA should have a sufficient scope (e.g. include all the operational modes and events and represent the whole set of layers of provisions). A priori, it does not require the development of new PSA or the restructuring of the existing PSA models. Judgements on the acceptability of any findings should be made on a case-by-case basis.

Anyway, even if the information about dependent failures can be embedded in the PSA models and extracted in order to verify the independence required to different DiD levels, their completeness cannot be guaranteed by the PSA itself. This task is mainly related to deterministic considerations. The adoption of a systematic approach for the identification of the layers of provisions implementing the DiD levels should be considered a prerequisite for the assessment of their independence.
For instance, the Objective Provision Tree methodology is proposed by the Generation IV International Forum / Risk & Safety Working Group (GIF/RSWG) for an exhaustive (as practicable) representation of the safety architecture implemented by the nuclear installation. OPTs (and the way they are constructed) allow the identification of the provisions required against the mechanisms challenging the safety function(s) implemented at

[6] This is usually the case in the analysis of combined failure of redundant trains of a safety system (e.g. 3 out of 4 or 4 out of 4). In these cases, CCFs usually determine the overall unavailability of the safety function.

[7] It is necessary to be aware that the verification of a given risk measure (CDF or LRF) does not mean that the principles of DiD are correctly implemented. In this context, it seems important to recall that the safety analysis (and among other the results of the PSA) is only part of the Safety assessment [5]. The compliance with the full set of requirements remains essential.

the different DiD levels, supporting the assessment of failures with potential impact on the required independence.

2.4. SAFETY AND DID ASSESSMENT

The objective of an assessment of the implementation of the DiD comes explicitly from the GSR Part 4 (Rev.1): "*It shall be determined in the assessment of Defence in Depth whether adequate provisions have been made at each of the levels of Defence in Depth" (*[5], *Requirement 13).* This requirement explicitly refers to the content of each level of DiD, coherently with the by "layers of provisions" mentioned by the SSR-2/1 (Rev.1) [4].

A comprehensive Safety assessment[8] of the design of the NPP is required to demonstrate the achievement of the fundamental safety objectives. According to the SSR-2/1 (Rev.1), "*Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements … are met throughout all stages of the lifetime of the plant….*" ([4], p. 17). According to the GSR Part 4 (Rev. 1) [5], safety assessments are to be undertaken as a means of evaluating compliance with safety requirements, and includes (but is not limited to) safety analysis"[9].

Discussing the combination of events and failures, the SSR-2/1 (Rev.1) [4] indicates that "where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence" ([4], p. 26).

The graded approach to safety requires that the SSCs having higher safety importance should assure the required capability with higher reliability and robustness against internal and external hazard.

The reliability and robustness of the "layers of provisions" implementing the different levels of DiD are essential goals for the fulfilment of the safety objectives.

There are a number of deterministic design requirements and practices aimed at ensuring a high reliability of the provisions; for safety systems, they include: physical separation, independence, fail safe design, redundancy, diversity, safety margins, conservative design, and single failure criterion [4].

The role of PSA in the demonstration of the graded approach to safety and of the overall reliability and robustness achieved is obviously essential. It is related, for instance, 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 pipes failures, probabilistic thermal hydraulics to address concerns related to natural convection, etc.[10].

Qualitative safety objectives should be considered in the assessment of the safety architecture implementing DiD, in order to verify the fulfilment of safety requirements stated in the SSR-2/1 (Rev.1). In this context, the Probabilistic safety Assessment, through the systematic assessment of all the plausible scenarios and challenging

[8] Safety assessment is the assessment of all aspects of a practice that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility (IAEA Safety glossary [2]).

[9] Safety analysis is the evaluation of the potential hazards associated with the conduct of an activity. (IAEA Safety glossary [2]).

[10] The reliability assessment of passive safety functions defined as the probability to fail the requested mission to achieve a generic safety function, depends, more than for active systems, on environment (physical, nuclear or chemical phenomena) that can interfere with the expected performance (e.g. stratification for the natural convection; surface modifications – presence of dust - for the radiation phenomena; friction or blockages for the gravity driven phenomena, etc.).

sequences of events, can allow the quantification of the degree of progressiveness[11] of the plant's safety architecture and the verification of its tolerant[12], forgiving[13] and balanced[14] characters (see §5.3).
The probabilistic assessment of the progression of an accident scenario through the (four[15]) levels of DiD and the successful operation (or failure) of the related safety features is clearly an issue.
In the assessment of DiD, PSA can support the verification of the proper implementation and independence of the layers provisions at the different levels of DiD (as previously discussed), and the specification of requirements for their reliability during normal operation and any postulated accidental condition.
If a NPP safety analyses could demonstrate that the applicable DiD safety requirements are respected, and if an PSA confirms an acceptable risk of this plant, there would be a well-founded confidence in an adequate level of safety; on the other hand, if PSA identifies a high or unbalanced risk profile for the plant, there are doubts on the adequacy of the current application of the DiD concept and additional safety provisions are expected. As a matter of example, if for a given initiating event and the corresponding sequence(s) of plausible failures PSA shows that features belonging to a particular level of DiD does not contribute significantly to risk reduction, or if PSA indicates that even without a particular level of DiD the risk targets can be met, there are arguments to relieve DiD requirements (for this particular sequence); on the other hand, if PSA indicates a high risk, it is advisable to improve the plant design or the operation, possibly by strengthening DiD. A third case could occur: the PSA results indicate that the risk is acceptable but the principles of DiD result not properly implemented; additional requirements may be expected to address this discrepancy.

Iterations between the two approaches, deterministic and probabilistic, are necessary during the whole design. As mentioned by IAEA in the SSR-2/1 (Rev.1) [4]: “The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses”.

Fundamentally, there should be no methodological difference between a PSA which analyses a system or without with explicit consideration of DiD. The PSA will always seek to quantify the vulnerability of the system and to identify weak points and potential improvements of the system.

[11] The Progressiveness character of the safety architecture represents the capacity “to degrade gradually” in case of hazardous event and loss of safety functions, the objective is to avoid that the failure of a given provision (or layer of provisions) entails a major increase of consequences, without any possibility of restoring safe conditions at an intermediate stage.

[12] The Tolerant character of the safety architecture represents the capacity to manage intrinsically variations in the operating conditions of the plant, i.e. avoiding those small deviations of the physical parameters outside the expected ranges lead to significant consequences.

[13] The Forgiving character of the safety architecture guarantees the availability of a sufficient grace period and the possibility of repair during accidental situations; it represents the capacity to achieve safe conditions through – in priority order - inherent characteristics of the plant, passive systems or systems operating continuously in the necessary state, systems that need to be brought into operation, procedures.

[14] The Balanced character of the safety architecture represents the evenness of contributions of different events / sequences to the whole risk, i.e.: no sequence participates in an excessive and unbalanced manner to the global frequency of radioactive releases.

[15] The first four levels of defense in depth are directly related to the design of the facility. The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires the provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.

Taking into account the ability of the PSA to reflect the DiD concept (always true in theory) and the potential to provide information useful for the assessment of DiD implementation (the unquestionable topic), and their complementary objectives, both (DiD and PSA) should developed and their contributions optimized.

If the PSA is used with the particular objective to verify the implementation of the DiD concept, its results should be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified. Specifically, the PSA should be properly structured, in order to:

- provide results that can be correlated with the performances (capability, reliability and robustness) required to the individual levels of DiD (i.e. relevant layer of provisions implementing safety function(s));
- have a sufficient scope (e.g. it should include all the operational modes and events and represent the whole set of layers of provisions and their content); with reference to the actual structure of the PSA models, quite simplistically, Level 1 / Level 2 PSA is needed to evaluate the compliance with Level 3 / Level 4 of DiD respectively.

On the other hand, beyond the aforementioned concept of complementarity, the independent implementation of the DiD concept and development of PSA is recognized a benefit to maintain. Specifically:

- DiD and PSA have their own concepts for including or dismissing events or phenomena from their respective analyses; to keep the benefits of diversity, the harmonization of these features should not be an objective per se; in contrast, any differences in assumptions should be clearly identified and addressed in order to contribute to exhaustiveness of all events and phenomena challenging the installation;
- the discussion on the evolution of the DiD concept is not directly related to need for progresses in PSA methods; even if important deficiencies are recognized in the actual PSA (e.g. lack of data, incompleteness, insufficient methods for some human actions, large requirement of resources, etc.), motivating a specific work for their improvement, they are not related to DiD issues

Moreover, the use of the PSA model and its result for the assessments of DiD provides several specific challenges:

- the levels of DiD and the associated plant conditions do not easily map to the traditional PSA end states (e.g. CDF and release categories) and initiating events; at this regard, there is a considerable debate 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;
- the best-estimate approach typically used in PSA is not immediately compatible with the (conservative, safety case oriented) deterministic approach for a DiD assessment;
- non-safety systems should be considered in the PSA, but they are usually neglected in the DSA[16].

Finally, and more fundamentally, the assessment preconized by the GSR Part 4 (Rev.1) [5] could be inscribed in the Integrated Risk Informed Decision Making Process (see INSAG 25 [21]) where the PSA can play an essential role.

2.5. DID AND RISK MONITORING

As well as the quantitative risk measures (CDF and LERF), most Risk Monitors provide qualitative measures that indicate the level of availability of safety systems to carry out safety functions and to respond to plant transients

[16] The notion of “layers of provisions”, which characterize, the content of each level of the DiD for a given initiating event, is not in contradiction with a PSA including non-safety systems.

([33], p. 121). This information can be correlated to 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*” ([33], 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*” ([33], 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 [33], this constitutes a secondary use of the fault tree models of a PSA related to deterministic requirements and rules ([7], p.144). This can be complemented by quantitative information about the risk status of certain systems.

3 INITIATING EVENTS IN PSA AND DSA

This section is focused on the notions of Postulated Initiating Event (PIE) and Initiating Event (IE), their usages in the Deterministic Safety Assessment (DSA) and Probabilistic Safety Assessment (PSA), and their consistency.

The ASAMPSA_E project focuses on "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." ([40], p. 147). The identification of hazard events or combinations of events that could challenge the safety of the plant and recommendations for the estimation of the relevant hazard frequency curves are investigated in the ASAMPSA_E project. These topics are treated mainly in WP21 and WP22, focused on the external hazards modelling and on their implementation into an extended PSA respectively [39]. Within WP30, the deliverable ASAMPSA_E D30.3 [43] discusses the screening criteria for the selection of the initiating events for an extended PSA. These issues are not discussed further in this report.

3.1. IDENTIFICATION OF PIE

An Initiating Event (IE) is "an identified event that leads to anticipated operational occurrences or accident conditions" [2]. An IE 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" [7][17].

A Postulated Initiating Event (PIE) is "an event identified during design as capable of leading to anticipated operational occurrences or accident conditions" [2]. Postulated Initiating Events typically refer to equipment failures and human errors, also due to internal and external hazards[18] that challenge, directly or indirectly, one or more safety systems [6]. As common understanding, a PIE is one specific event (e.g. due to SSCs of or to a hazard impact scenario) and their respective consequential effects. However, scenarios typically considered as PIE for DBA or DEC can be the results of several (more or less likely) faults.

The identification of PIE is the initial step of a safety analysis and then a cornerstone in the application of the DiD concept. According to the SSR-2/1 (Rev.1), "*the design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of PIEs such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and*

[17] This is a modified definition from SSG-3 [7] 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." ([7], p. 25)

[18] The term "hazard" is used in IAEA documentation in the general sense (e.g. as situation that poses a level of threat to life, health, property, or environment) and it is not defined neither in IAEA Safety Glossary [2] nor in GSR Part 4 (Rev.1) [5], SSG-2 [6], SSG-3 [7], SSG-18 [9], etc.
In PSA, the term "hazard" is used 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 SSG-3 ([7], para. 6.1).
According to SSG-3 [7], hazards can be further categorized as:

- Internal hazards originating from the sources located on the site of the nuclear power plant, both inside and outside plant buildings (e.g. internal fires, internal floods, turbine missiles, on-site transportation accidents and releases of toxic substances from on-site storage facilities);
- External hazards originating from the sources located outside the site of the nuclear power plant (e.g. seismic hazards, external 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).

are considered in the design”. To such an aim, “*the postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment*". ([4], p. 19).

Practically, PIEs are selected in the context of the Deterministic Safety Analysis, usually prescribed by design basis requirements and complemented with events recommended by national or international guidelines[19]. Differently, IEs in PSA are selected through specific screening process and criteria. This may screen out PIE in DSA or group them into bounding scenarios. The ASAMPSA_E report D30.7 vol 2 [43] discusses screening criteria for extended PSA.

The following further remarks concern the definition of PIE.

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. *All the Operational states (NO and AOOs) and Accident conditions (DBAs and DECs) provide input to the design basis (i.e. the identification and sizing) of safety related provisions and safety features for the control and the mitigation of consequences of DBAs and DECs.”*

The safety features for DECs include design features for multiple system failures (for core melt prevention) and mitigatory design features (for core melt scenarios) [15].

Analysts should be aware that, from historical evidence, actual severe accidents (i.e. design extension conditions with core degradation) 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 subjected to risk analyses, the plant risk profile may be not correct.

Analysts should be aware that the original sets of DBAs were postulated as “enveloping accidents” by nuclear engineers more than 50 years 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 should be reflected in the determination of DBA and DEC as enveloping or bounding scenarios for the design of plants and for the deterministic safety evaluation.

3.2. CLASSIFICATION OF PIE

According to the SSR-2/1 (Rev.1) “*The postulated initiating events used for developing the performance requirements for the items important to safety in the overall safety assessment and the detailed analysis of the plant shall be grouped into a specified number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety*". ([4], p.20)

Classification, grouping, and assignment of PIEs should be based on deterministic as well as probabilistic insights, operating experience and other considerations[20]. A very important, but not the only input to the classification of PIE, is the (assumed or ascertained) frequency of the event ([4], [24]).

The insights and results coming from PSA have the potential to support the selection of PIE and their assignment to a level of DiD. Indeed, the assignment of a PIE to a certain plant conditions category and, through the WENRA proposal (Fig. 1) to the level of DiD, relies (explicitly or at least partially[21]) on an estimation of the frequency of occurrence of the PIE (e.g. SSG-2 [6]).

[19] Therefore the use of the term “postulated”.

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

[21] Especially for DBA and DEC (DiD levels 3 and 4), some regulatory bodies define requirements for the inclusion or

According to WENRA RHWG for new reactors, "*the identification procedure shall be performed for any operational state and should include failures of spent fuel pool cooling. Based on this, a selection of a reasonable number of limiting (bounding) cases, which present the greatest challenge to the acceptance criteria and which define the performance parameters for safety related equipment, should be made using experience feedback, engineering judgment and probabilistic assessment*." ([23], p. 20) About quantitative references, "any *general cut-off frequency should be justified, considering in particular the overall core damage frequency*". ([23], p. 21)

Neither the SSR-2/1 (Rev. 1) [4] nor the WENRA Reference Levels for new and existing reactors ([23], [24]) give quantitative references or specific recommendations for frequency thresholds between different plant condition categories. Also the classification of events into the DiD sub-level 3a (single failure events) and 3b (postulated multiple failure events) introduced by WENRA RHWG [23] is qualitative. Approaches commonly used for PSA, as those recommended in the SSG-3 [7], are expected to be applied.

The SSG-3 [7] 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 [7].

The SSG-2 [6] provides quantitative references for the frequency of occurrence of events, commonly applied in the classification of PIEs [15]. These threshold values, provided in Table 1, should be considered as indicators rather than fixed limits. Some harmonization are still needed between these frequency thresholds and some historical assumptions (for instance, some events - e.g. large break LOCAs - are traditionally considered DBA although they may have a frequency lower than the related threshold) and recent probabilistic safety criteria/design objectives (for instance, about the need of practical elimination of some scenario).

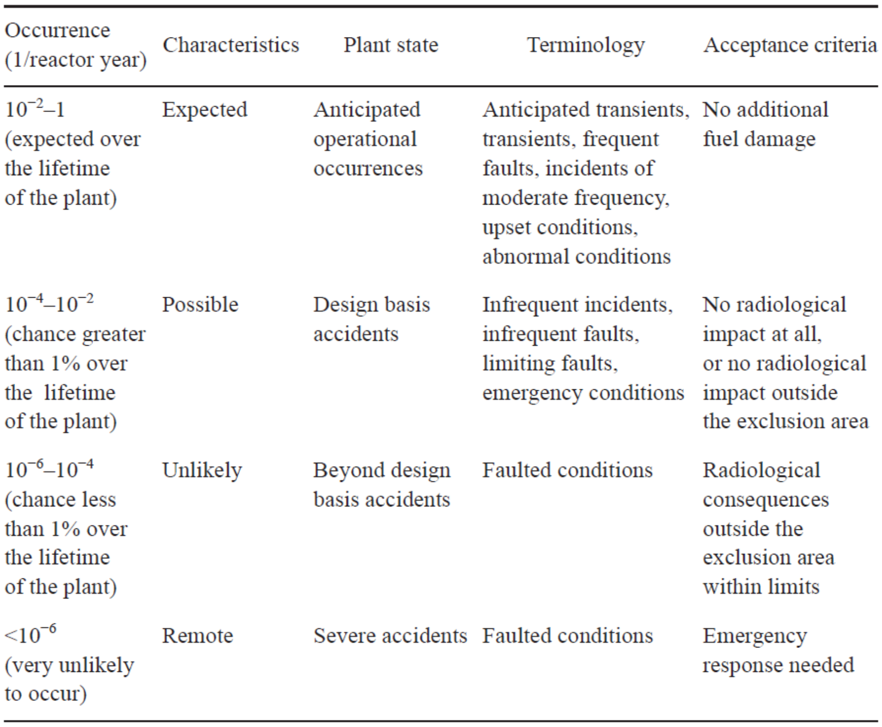
These quantitative references complement the indications provided by WENRA and allows to correlate the DiD levels to the different plant states characterized by estimated frequency.

Further, they allows identifying reliability targets for the layers of provisions which materialize the levels of DiD.

Discussing the management of Severe Accidents, the SSR-2/1 (Rev. 1) [4] and WENRA for new reactors [23] require that *situation that could lead to early or large releases of radioactive materials* are "practically eliminated" ([4], p. 6). According to these references, the practical elimination of an accident sequence cannot be claimed solely based on compliance with a cut-off probabilistic value. It shall be demonstrated on a case by case basis exploiting both deterministic and probabilistic insights. Concerning the probabilistic threshold, according to Table 1 [6], severe accidents (SA), which entail an unacceptable release to the environment and correspond to a frequency of occurrence $\lesssim 10^{-6}$ /yr. Some national regulators have set even smaller values up to $\lesssim 10^{-7}$ / yr. In practice, the frequency of occurrence of an event or sequence of events to be practically eliminated should be "significantly" below the 10^{-6}/yr (at least one order of magnitude). Uncertainty on data should be taken into account carefully managing such extremely rare scenarios.

even exclusion of certain events (e.g. [45]). These requirements often include considerations other than the frequency of occurrence, e.g. deterministic assessments, historical precedent, precautionary principle, etc.

Table 1. Subdivision of postulated initiating events according to the SSG-2 ([6], 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

Two further remarks concern the link between the DiD concept (within the DSA) and the PSA.

First, the list of initiating events considered for an extended PSA (i.e. internal events, hazard event groups, combination events) should be checked against the list of PIE for deterministic safety analyses. The scenarios analysed in an assessment of DiD (with deterministic methods) should include all the 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).

Conversely, the list of PIE for deterministic safety analyses should be treated in an extended PSA. It does not necessarily mean an extension of the scope of the deterministic or 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 as DEC appear as intermediate or end states in PSA, and some AOO events might not lead to an IE at all[22].

Secondly, the frequency of initiating events of the PSA needs to be checked against the classification of PIE. In addition, if PIE classified as DBA or DEC are (intermediate or final) results of an extended PSA, the frequencies estimated should be checked against the assumptions for the deterministic classification. If the frequency values (or distributions) estimated by PSA are inconsistent with those used in the classification of PIE, they should be revisited. For new plants, this check can support the definition of the initial set of PIEs (for AOOs, DBAs or DECs). This is one example of how PSA can complement the deterministic approach in identifying safety-significant weaknesses in the design of the plant ([5], [7], [8], [10]).

[22] This is obviously the case for all the AOO whose potential consequences are inherently below the acceptable consequences for the corresponding category (see the Frequency – Consequence curve).

3.3. CONSISTENCY BETWEEN PIE AND IE

Although the definitions of IE and PIE (provided in §3.1) introduce some differences, there are several other implicit differences to be considered about their usage in Probabilistic Safety Assessment (PSA) and Deterministic Safety Assessment (DSA) respectively.

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 the event tree sequences; a PIE in DSA can be either the single trigger event or a sequence of events.

Therefore, PIE in DSA can match with IE, with intermediate results (i.e. specific sequences in the event tree model[23]) and with end states (e.g. sequence of events resulting in core/fuel damage) in PSA.[24] For DEC events, the respective probabilistic results can often be found in sequences of PSA Level 1 and Level 2.

The appropriate mapping of the IE analysed in PSAs to the PIE analysed in DSAs and vice versa is a crucial issue for any mutual cross checking to find incompleteness or inconsistencies. This mapping generally depends on the screening criteria for the selection of IE (see the ASAMPSA_E deliverable D30.7 vol 2 [43] for additional discussion) and on the scope and level of detail of the PSA model.

In any case, the frequency values assumed for PIE classification should be consistent with the frequency estimated for initiators or (intermediate or final) results of the PSA, as applicable.

Inconsistencies in the data sources (operating experience, engineering judgement, fault tree modelling) used for PSA with those referenced for the respective PIE(s) should be addressed. At this regard, the frequency of occurrence of (a lot of) the PIE in DSA, used for their assignment to the different plant conditions categories (and then to the levels of DiD) can be determined using the same data and similar methods and approaches as applied for the corresponding IE in PSA. The completeness of data in PSA should be also verified with respect to all the events grouped into the PIE.

If the data are consistent and complete, the frequency determination should lead to basically consistent results.

A potential difference could be that PIE frequency (for classification) is estimated conservatively, whereas the related IE frequency in PSA is determined as best estimate value, under best estimated boundary conditions and with uncertainty distribution (if any). However, especially for rare events, this distinction becomes largely moot due the scarcity of data.

In this context, “consistency” between data means that the uncertainty on the IE frequency (e.g. the 95 percentile value) should not deviate by orders of magnitude from the PIE assumptions (i.e. should not lead to a different classification, according to the associated plant condition categories and their frequency thresholds). Should that be the case, assuming the PSA frequency values are reliable, the deterministic classification of PIE should be revisited:

- if the frequency assumed for the PIE is significantly lower than the PSA results for a corresponding IE, the re-classification of a DBA as AOO or a DEC (DEC A) as a DBA should be seriously considered;
- if the frequency assumed for the PIE is significantly higher than the PSA results for the corresponding IE, the re-classification of the event needs further consideration; a risk-informed decision making process should be applied to any lowering of the deterministic classification of a PIE; qualitative safety arguments, regulatory precedent, or preservation of safety margins may be valid reasons for maintaining a PIE classification irrespective of its estimated frequency.

[23] E.g. A PIE defined deterministically as DBA or DEC appears in the event progression analysis (event tree sequences) of PSA level 1 (usually) or PSA level 2.

[24] Some theoretical background on PSA model construction can be found in the appendix of D30.5 [44].

Different difficulties are in the comparison between the IE identified in PSA with the related frequency of occurrence, and PIE defined and classified in DSA (according to the related frequency of occurrence).
Because different grouping processes can be adopted in PSA and DSA, it may be necessary to sum up the frequency estimates. It can happen that one IE in PSA corresponds (and thus gathers the frequency of occurrence) to several PIE in DSA, which can be assigned to different AOOs or DBAs, or vice-versa.

DSA often assumes certain boundary conditions for PIE (apart from the induced effects and failures caused by the PIE itself). Those conditions often include the occurrence of Loss of Offsite Power (LOOP), of additional (single) failure of safety or non-safety systems, or the application of conservative values for the key parameters of the plant (SSG-2 [7]). All the selected conditions are usually supposed to occur simultaneously at the time of the PIE occurrence, without (explicitly) considering their (conditional) likelihood, in order to achieve a robust deterministic safety case. Differently, in PSA the additional boundary conditions assigned to a PIE are usually addressed in the fault tree/event tree models, with their conditional probabilities, leading to less conservative estimations. This can result in very low frequencies of PIE including all the boundary conditions, particularly if they occur independently from the PIE[25].
In addition, PIE classified as DBA can be related to an AOO (similarly DEC can be related to a DBA) event with postulated additional unavailability or failure of SSCs. In such cases, PIE are classified usually according to the frequency of the basic scenarios (e.g. loss of feedwater), without considering the conditional probability of the aggravating. Differently, in PSA models these scenarios are fully described because of the loss or degradation of the respective safety functions, with their conditional probability, in specific event tree sequences.

Moreover, the IE considered in the existing 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.

Therefore, <u>any comparison with the IE in PSA requires to understand the basic scenario associated to the PIE, including all the related boundary conditions and concurrent failures.</u>
Specifically, the frequency estimated for IE in PSA can be compared effectively with the classification (and relevant frequency) of PIE (mostly for internal AOO or DBA events) if the following aspects are considered:

- the IE in PSA need to be mapped to the appropriate PIE in DSA and vice versa; depending on the level of detail of the PSA Level 1, IE will usually correspond to either AOO or DBA scenarios,
- additional boundary conditions for PIE in DSA should be considered in the comparison only if they are similarly applied in PSA; as default, only the basic PIE (e.g. small LOCA) should be compared to the respective IE;
- IE for PSA are often defined by grouping several scenarios into one representative bounding event definition; the screening and grouping process in the PSA has to be evaluated in order to identify the events subsumed into the IE definition and to identify their corresponding PIE from DSA;
- hazard scenarios in DSA are usually postulated using hazard frequency curves, which are usually a major input for PSA as well as for DSA; if the same parameters are used in PSA and DSA for the elicitation of the frequency

[25] E.g. If the frequency of large Loss of Coolant Accident (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 approximatively 3 x 10^{-8}/y (10^{-4}/y x 1/365 x 10^{-1}/y ≅ 3 x 10^{-8}/y).

value(s) (e.g. peak ground acceleration for seismic), the comparison can be done directly on the hazard frequency curves;

- if the resilience of certain design features is considered for the classifications of a PIE in DSA (e.g. dam failure probabilities for flooding), the corresponding state in the (hazard) PSA model has to be identified.

4 CLASSIFICATION OF SSC

This section is focused on the classification schemes for Systems, Structures and Components (i.e. for the provisions implemented in the safety architecture), on the reliability of the engineered safety functions and on the relevant links with DiD and PSA.

As part of the Nuclear Power Plant (NPP) design, the Systems, Structures, And Components (SSCs) need to be classified for their importance for safety ([4], [24]). Based on their classification(s), SSCs are subjected to specific requirements on applicable design rules, qualification, safety margins, testing regimes, limits and conditions, acceptance criteria for safety demonstrations, etc.

The classification of SSCs and their assignment to different levels of DiD is an essential aspect of the DiD concept. Specifically, the independence between the different levels of DiD [24] is related to a prior classification of the provisions materializing the corresponding layers.

Although the classification of SSCs (and immaterial provisions) shall be based primarily on deterministic methods, probabilistic input may be considered if appropriate ([4], [24]).

4.1. CLASSIFICATION OF SSC (FROM IAEA SSG-30)

According to the IAEA SSG-30 [11], the classification[26] of the Structures, Systems and Components (SSCs) of a (fission) nuclear installation shall be derived from the categorization of the safety functions, according to their “safety significance” (i.e. risk-reduction required).

The SSG-30 [11] provides recommendations and guidance on how to meet the requirements established in the SSR-2/1 (Rev. 1) [4] and GSR Part 4 (Rev. 1) [5] for the identification of SSC important to safety and for their classification on the basis of their function and safety significance.

The classification process recommended by the SSG-30 is “*consistent with the concept of defence in depth set out in the SSR-2/1*”. The functions to be addressed are “*primarily those that are credited in the safety analysis and should include functions performed at all five levels of DiD*”. [11]

The classification proposed by the SSG-30 [11] follows 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. This information is used for identification of safety functions[27] and design provisions[28] required to fulfil the main safety functions.

[26] The term “categorization” is reserved for functions, the term ”classification” for SSCs [11].

[27] For the purpose of SSG-30 [11], a “function” is defined as any action performed by a single SSC or a set of SSCs.

[28] For the purpose of SSG-30 [11], “design provisions” are SSCs designed specifically for use in normal operation:

- Design features designed to such a quality that their failure could be practically eliminated.
- Features that are designed to reduce the frequency of an accident.
- Passive design features that are designed to protect workers and the public from harmful effects of radiation in normal operation.
- Passive design features that are designed to protect components important to safety from being damaged by internal or external hazards.
- Features that are designed to prevent a postulated initiating event from developing into a more serious sequence without the occurrence of another independent failure.

Within the context of this document the term provisions is basically used, coherently with the terminology of the SSR 2/1 (Rev. 1), to indicate all the material and immaterial components of the “layers of provisions” for the different levels of the DiD, i.e. all the SSCs important to safety as well as the inherent features that contribute to the fulfillment (or can affect) the fundamental safety functions, for all plant states.

According to Fig. 2, in the view of the SSG-30 [11], "*design provisions (with their reliability) are implemented primarily to decrease the probability of an accident; functions are implemented to make the consequences acceptable with regard to the event probability*".

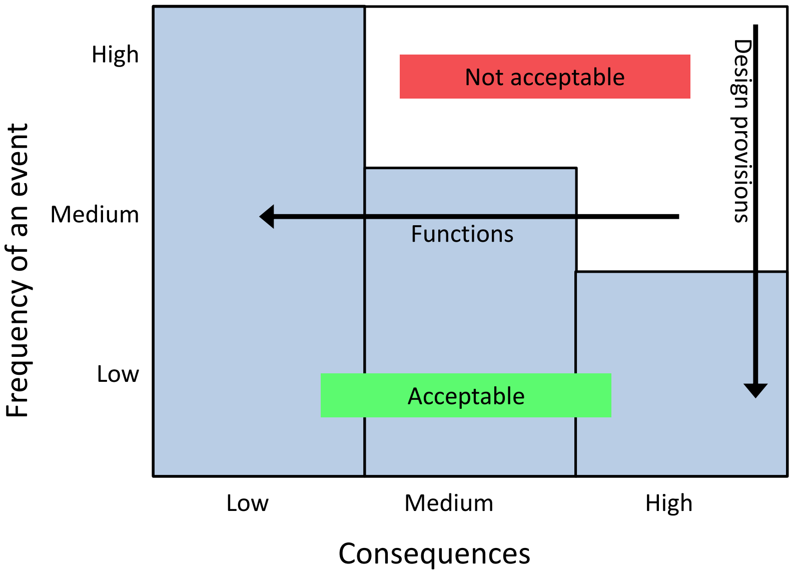


Fig. 2 The basic principle of frequency versus consequences (adapted from [11])

The safety classification considers the functions performed at all five levels of Defence in Depth, both in normal and in accident conditions, and classifies the associated SSCs according to their safety significance. Design provisions are classified similarly.

According to the SSG-30 [11], the classification of safety functions and relevant SSCs shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken for: (i) the safety function(s) to be performed by the item; (ii) the consequences of failure to perform a safety function; (iii) the frequency with which the item will be called upon to perform a safety function; (iv) the time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

Table 1 provides the definition of the (three) Severity levels proposed by SSG-30 [11]. Their assignment is made on the basis of the worst consequences that could arise if the function under investigation is not performed.

Table 1. Severity levels and criteria for assignment defined by the SSG-30 [11]

Severity levels	Criteria for assignment
High	If failure of the function could, at worst: ▪ Lead to a release of radioactive material that exceeds the limits accepted by the regulatory body for design basis accidents; or ▪ Cause the values of key physical parameters to exceed acceptance criteria for design basis accidents.
Medium	If failure of the function could, at worst: ▪ Lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or ▪ Cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences.
Low	If failure of the function could, at worst: ▪ Lead to doses to workers above authorized limits.

The following principles should be considered in the classification process [11]:

- 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 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.

4.2. CLASSIFICATION OF SSC, EXAMPLES OF NATIONAL APPROACHES

In the **United State**, the NRC has defined a set of requirements and suitable risk metrics for the assessment classification of SSC with PSA related to DiD (RG 1.201, [31]). Namely, the 10CFR50.69 rule [32] proposes an alternative set of requirements for the classification of SSCs. Their safety significance is determined by an integrated decision-making process, incorporating risk and traditional engineering insights.

SSCs are classified into four Risk-Informed Safety Classes (RISC), as shown on Fig. 3.

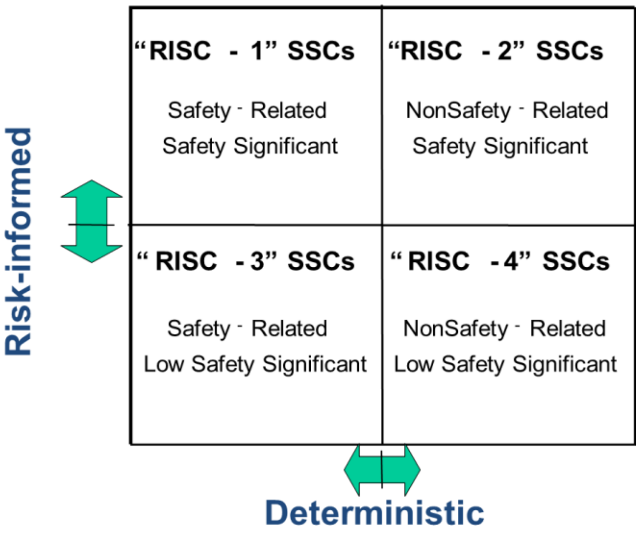


Fig. 3 10 CFR 50.69 RISC Categories

The classification is based on the function performed by the SSCs, which are considered 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 degradation or loss of a "safety significant" function could result in a significant adverse effect on DiD, safety margin, or risk [31].

Some Importance measures related to the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) are proposed by the NRC for the identification of the safety significant functions and related SSCs (RISC-1 or -2).

The analysed SSC is a safety significant SSCs candidate if any of these criteria are exceeded:

- 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.

An appropriate PSA is required for the categorization of SSCs relative to the internal events ([31], [31], [35]).

For safety-related SSCs initially identified as low safety significant (RISC-3), an additional assessment is performed through a set of deterministic criteria. The adequate selection of these criteria can provide insights about the nature and quality of the DiD implementation (e.g. redundancy and diversity against design basis events, in order to appreciate the degree of independence among the DiD levels).

The functions carried out by the SSCs are assessed 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 the above criteria, it is categorized as safety-significant (RISC-1) for further analysis.

In **Romania**, the use of PSA for the classification of SSCs is required by CNCAN, however no specific risk measures or numerical criteria are defined [59].

Similarly, the **Finnish** guide YVL A.7 [48] requires the application of PSA to classify SSCs, but neither YVL A.7 [48] nor YVL B.2 [49] give specific risk measures or thresholds.

Also the **Slovenian** guide JV5 [50] requires that each SSC shall be classified into a safety class according to its importance to safety. The SSCs classification adopts four safety categories, assigned according to their relevance to risks determined with a probabilistic safety assessment. However, no specific risk measures or numerical criteria are defined.

In **Switzerland**, ENSI-A06 [47] states specific criteria for the classification of components as significant to safety[29]. The following thresholds on importance measures with regard to core damage frequency, fuel damage frequency[30] and large early release frequency shall be applied: Fussell-Vesely importance ≥ 10^{-3}, Risk Achievement Worth ≥ 2.

In a number of national applications, the use of PSA for the classification of SSC follows (with some specificities) the approach endorsed by the US NRC. There is an agreement on the usage of importance measures (mainly Fussell-Vesely and Risk Achievement Worth), based on PSA Level 1 and Level 2 risk measures. Moreover, according to ASAMPSA_E Deliverable D30.5 [44], the standard risk measures for PSA Level 1 (CDF) and PSA Level 2 (LERF) can be easily applied to an extended PSA. Thus, the use of PSA information for the classification of SSC and specifically the approach endorsed by the US NRC (or basically similar approaches) is recommended. 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 D30.7 vol 3 [44].

[29] Swiss regulation specifically applies to components and does not address systems and structures.

[30] 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 [46]. This distinction differs from the definition and discussion on the respective risk metrics given in the ASAMPSA_E deliverable D30. 7 vol 3 [44].

4.3. RELIABILITY OF SAFETY FUNCTIONS

A general recommendation regards the application of deterministic methodologies and to complement them, where appropriate, probabilistic safety assessment and engineering judgement to achieve an appropriate (NPP) risk profile [24]. 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.

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 need to assure the physical performances (capability) of specific provisions (including SSCs) with the due reliability (against random failures) and robustness (against hazards), in order to achieve a reliable behaviour of the layers of provisions as a whole. Consequently, the SSR-2/1 (Rev. 1) requires safety systems (fulfilling safety functions(s) irrespective of the placement in terms of DiD level), as well as redundant elements thereof, to have "*physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate*" ([4], p. 26). Moreover, safety systems "*shall take due account of the potential of common cause failure*" ([4], p. 27), shall fulfil the "*single failure criterion*" ([4], p. 27), and "*shall be designed for fail-safe behaviour*" ([4], p. 28).

At this regard, the GSR Part 4 (Rev.1) requires for all safety functions an assessment showing " *whether the structures, systems and components and the barriers that are provided to perform the* (main) *safety functions*[31] *have an adequate level of reliability, redundancy, diversity, separation, segregation, independence and equipment qualification, as appropriate, and whether potential vulnerabilities have been identified and eliminated*." ([5], p. 15).

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. The available deterministic assessment methods, design standards and technical guides as well as good design practices are generally suitable for doing this task.

Meantime, there is extensive guidance on the probabilistic modelling of the main safety functions (e.g. SSG-3 [7]).

The combination of events (e.g. failure or unavailability of SSCs) that lead to the loss or degradation of a given safety function can be represented by a Fault tree. All the plausible failures of all the required provisions should be consider as basic events, e.g. component failures, human errors, unavailability due to maintenance/test, failures of support systems and auxiliaries, or any other circumstance that can lead to the undesired (top) event. Passive components (whose failures could lead to the system failure) should be included. Dependencies among components should be considered explicitly. These fault trees allow a direct quantification of the reliability of the layer of provisions implementing the given safety function, under given boundary conditions.

Moreover, safety functions are often used (as headings) in the modelling through event trees of the development of accident scenario, in terms of sequence of events [7]. In these cases, the boundary conditions related to the initiating event can be explicitly considered, as well as previous failures of SSCs affecting the reliability of the safety function under investigation.

In the view of the above considerations, well-developed probabilistic assessment methods seem to exist for the reliability assessment of safety functions. However, in spite of this potential, no direct link is formally established between the fault tree structure and the levels of the DiD.

[31] According to the IAEA Safety Glossary [2], the functions formerly named "fundamental safety functions" are now named "main safety functions".

On the other hand, one main weakness recognized for PSA, with specific implication in the development of extended PSA, concerns the fragility of equipment implementing safety functions, which are difficult to be assessed for some external hazards (e.g. the tightness of containment building and its extension after a beyond design earthquake can be difficult to assess for the containment function).
Moreover, 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 functions. Some known examples are provided in the following.

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} (R-8, [52], p. 2, superseded by current regulation). The same maximum value of unavailability is requested (in availability requirements part) also for the containment system (R-7, [51]), and for the emergency core cooling system (R-9, [53]). 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 [54], 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 require the maximum unavailability for emergency core cooling system (NSN-11 [56]), for special safety systems (i.e. first and second shutdown systems) (NSN-13 [57]) and for the containment system (NSN-12 [58]) to be below 10^{-3}.
In the **United States**, the NRC has defined an objective for the conditional failure probability of the containment in case of a core melt accident for evolutionary designs to be below 10^{-1} ([27], [28]).

Despite these examples, there are no generally accepted failure probability thresholds for the design of safety systems or safety functions. The following considerations have to be taken into account.
Typical PSA results indicate that safety systems/safety functions reach conditional failure probabilities in the large range of 10^{-3} to 10^{-1}, depending on the boundary conditions and their design basis.
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 by multiple, possibly diverse, systems.
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.
Often, safety systems contribute to the fulfilment of more than one fundamental safety function; conversely, each fundamental safety functions can be achieved by multiple systems (working simultaneously or in sequence). Complicating matters further, the elementary safety functions in the PSA event tree model are usually not defined in terms of the fundamental safety functions as defined by the SSR-2/1 (Rev. 1)[32]

[32] The SSR-2/1 (Rev. 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"* ([4] p. 12).

The independence among the layers of provisions implementing DiD for a given initiator requires the achievement of fundamental safety functions at each level of DiD, if applicable. The propagation of these requirements down to the specific provisions implementing safety functions is a complex task. Conversely, there is no example where reliability requirements have been set on the layer of provisions implementing DiD levels. Nevertheless, indications could be deduced by the frequency of occurrence provided in Table 1 for the different plant condition categories and by the correspondence between these categories and the DiD levels shown in Fig. 1.

Probabilistic safety criteria are usually based on two risk metrics: Core Damage Frequency and Large (Early) Release Frequency ([7], [8]). They may be complemented by criteria related to the balanced character of the safety architecture of the risk, usually through importance measures based on the above-mentioned risk metrics.
For instance, according to the **Swiss regulatory** guide ENSI/A06 [47], 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[33], and an overall target value for CDF[34] of 10^{-6}/yr, the conditional failure probability for the provisions implementing safety functions at DiD level 3 needs to be (significantly) below 1 10^{-3} [35]. In this respect, specific reliability requirements for singular provisions should be consistent with the global reliability requested for the "layer of provisions", representative of the level of the DiD, considered as a whole.

With respect to an extended PSA, there are no major changes in the methodological approach: the internal or external hazards are considered as specific and complementary environmental boundary conditions. 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. Therefore, the assessment of the reliability of the provisions (including SSCs) implementing the safety functions does not require different methods or risk measures for an extended PSA. However, a more systematic use of PSA information coming recommended in risk-informed decision making on the reliability of safety functions and SSCs (i.e. including passive features). The measure should be their conditional failure probability/availability. Targets to be achieved by specific functions or systems need to be set on a case-by-case basis. Their setting is an important aspect of a risk-informed design process or risk management system (e.g. [66]). Moreover, current PSA models are often not built in a way that facilitates the assessment of systems and safety functions reliability.

Qualitative requirements are specified about the reliability of safety functions. According to WENRA [23]:

- NPP shall provide the decay heat removal in any severe conditions and ensure the protection of necessary electrical power supplies against hazards; loss of ultimate heat sink or access to it should be considered;
- 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 reflected in the PSA model.

[33] This value puts the IE in the DBA range, which should be controlled and managed by DiD level 3 provisions.

[34] 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.

[35] Of course, the values must be used with caution because, on the one hand, the probability of the initiating event is representative of a singular event (or of the family of events represented) and, on the other, the allowed core damage frequency (CDF) is integral of the contribution of all internal events. The wording "(significantly) below" should be understood as (at least) one decade below.

Romania and Canada have similar norms regarding the availability, diversity and redundancy of safety systems[36]. The main requirements are summarized below ([51], [52], [53], [54], [55], [56], [57], [58]):

- 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 and other safety systems; the same principle requires for the emergency core cooling (ECCS) and containment systems 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 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.

For **Slovenia,** the WENRA requirement (E9.4) about the reliability of the systems of existing reactors [24] is covered by the article 3 (design principles) of the Slovenian rule JV5 [50]. The design of a radiation or nuclear facility shall adhere to the following principles: defence-in-depth principle; single-failure principle; independence principle; diversity principle; redundancy principle; fail-safe principle; proven-components principle; 8. graded-approach principle. Each of these principles is further defined in detail.

[36] In fact these Romanian and Canadian norms, applicable for example for the shutdown and the ECCS, can be generalized in saying that the objective is to guarantee the possibility for the independent fulfilment of the requested mission by each level of the DiD (functional redundancy), the separation and independence principle requires for the corresponding provisions to be diverse and physically and operationally independent from each other, from the process systems and from other safety systems.
It should be noted that "functional redundancy" does not mean that the performances in terms of objectives to be achieved are exactly the same for the different levels of the DiD for it is allowed to have, for less frequent plant conditions, higher allowable consequences.

5 DEFENCE-IN-DEPTH AND PSA FOR NPP

This sections presents some practical experiences (national and/or made by the partners before or during the ASAMPSA_E project), without any need of coherence and any synthesis, as elements for future discussions.
The texts have been provided by the related authors and left practically unchanged. Some comments or complementary questions are raised through foot notes.

5.1. 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-years research project funded by the Swedish regulatory body (SSM).
Main insights and results from the project reports are summarized below ([62], [63], [64]).

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, 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.

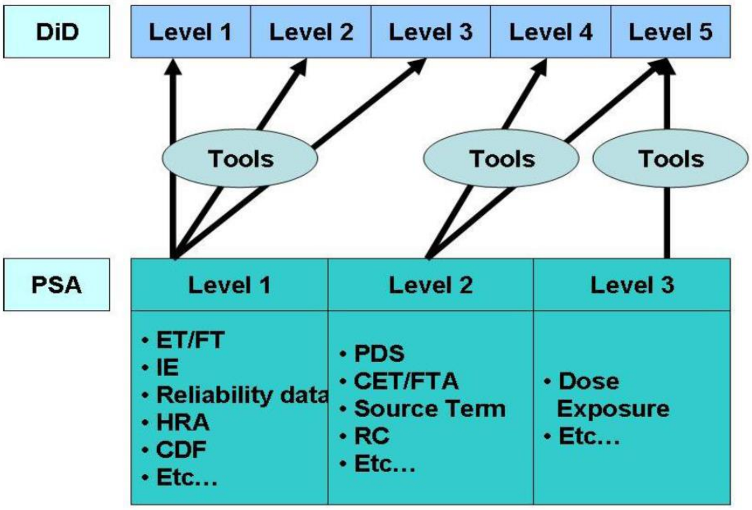
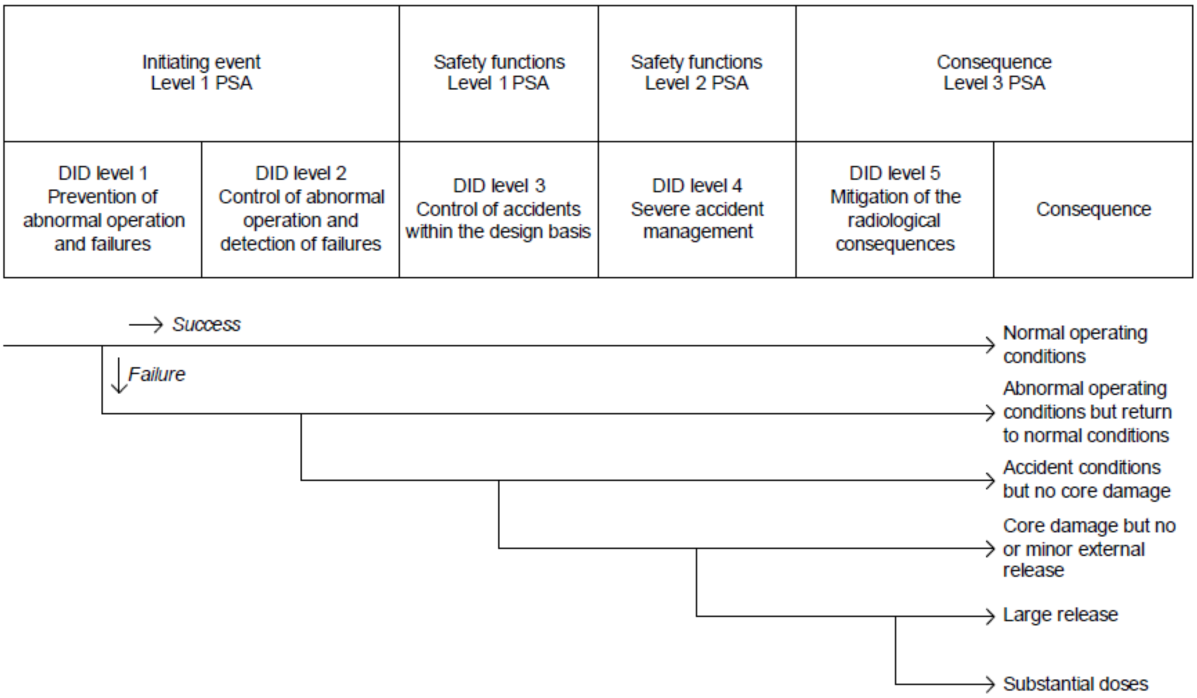


Fig. 4 DiD – PSA Possible evaluation

DiD and its interpretation

IAEA INSAG-10 [19], INSAG–12 [20] and IAEA Safety Report Series No. 46 [12] 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.



Initiating event Level 1 PSA		Safety functions Level 1 PSA	Safety functions Level 2 PSA	Consequence Level 3 PSA	
DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management	DID level 5 Mitigation of the radiological consequences	Consequence

Success
Failure
Normal operating conditions
Abnormal operating conditions but return to normal conditions
Accident conditions but no core damage
Core damage but no or minor external release
Large release
Substantial doses

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.

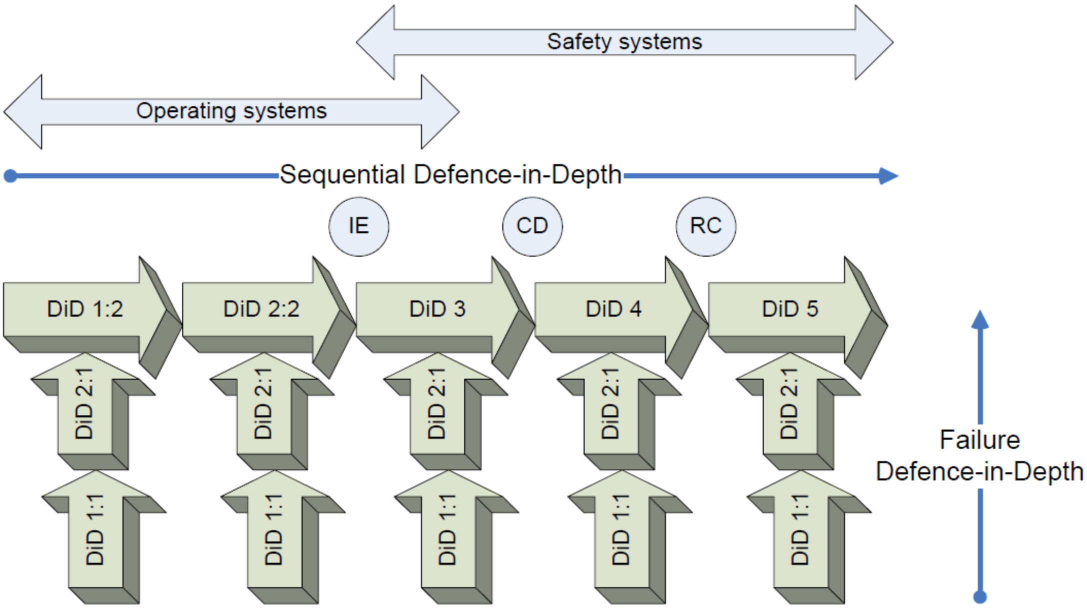


Fig. 6 The failure in DiD and the sequential DiD (The restructured DiD framework)

Fig. 6 shows that PSA results actually measure the strength of first two DiD levels 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 (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

Table 2 shows an example of quantitative PSA parameters, managed by PSA software, for measuring DiD levels

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.	

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; according to 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

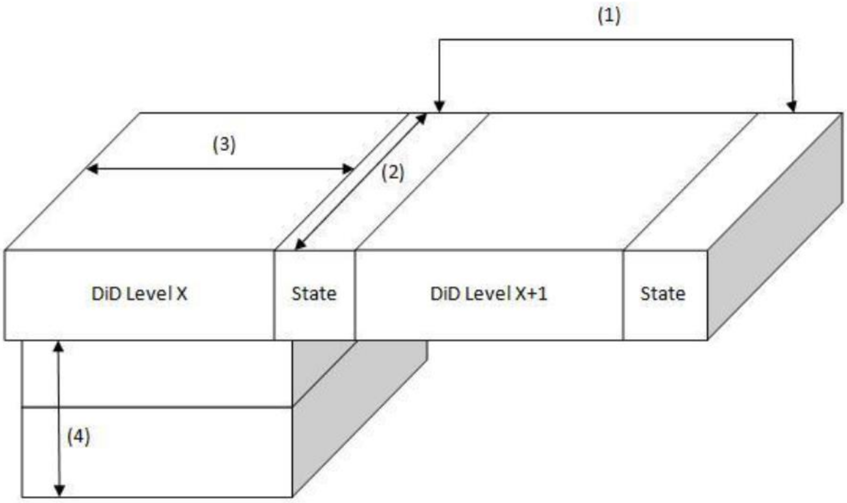


Fig. 7 Measures of DiD levels

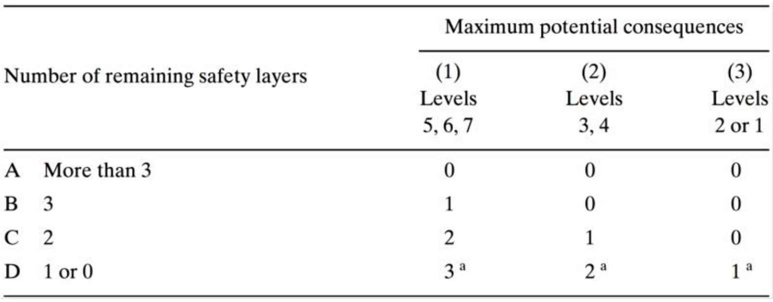
A summary of existing and potential PSA measures of DiD levels are presented in Table 3 below.

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 DiD level 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.

5.2. CCA'S DEVELOPMENT OF DID CONCEPT (CAA)

The starting point of the CCA development of the DiD concept is captured in Fig. 8, taken from the INES Manual (Table 11, [22]).



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]

Fig. 8 Rating of events using the safety layer approach

The same relationship can be shown as in Fig. 9.

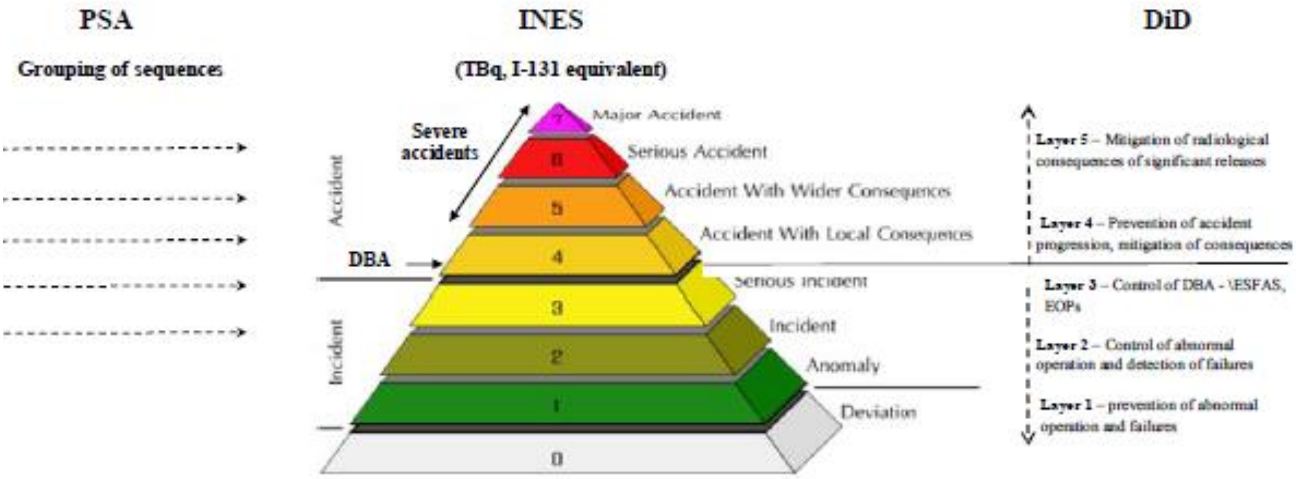

PSA
Grouping of sequences
INES
(TBq, I-131 equivalent)
DiD
Severe accidents
Accident
DBA
Incident
7
6
5
4
3
2
1
0
Major Accident
Serious Accident
Accident With Wider Consequences
Accident With Local Consequences
Serious Incident
Incident
Anomaly
Deviation
Layer 5 – Mitigation of radiological consequences of significant releases
Layer 4 – Prevention of accident progression, mitigation of consequences
Layer 3 – Control of DBA - \ESFAS, EOPs
Layer 2 – Control of abnormal operation and detection of failures
Layer 1 – prevention of abnormal operation and failures

Fig. 9 Relations between PSA, INES levels and DiD

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 (http://www-ns.iaea.org/standards/concepts-terms.asp?l=90) "*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 analysed in L2 PSA) can be tied to DiD physical barrier 4 (containment) and INES level 5 (Accident with wider consequences) can be taken as an appropriate measure of safety of the plant in terms of Severe Accidents. The 5th DiD layer is related to radiological consequences (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 [6]: "The deterministic approach is based on the two principles: leak tight barriers and the concept of defence-in-depth."

CCA asserts that DiD is not dedicated to severe accidents (i.e. PSA purposes), as it is defined now, but to DBAs with only some exceptions like some containment systems (e.g. hydrogen ignitors) which are among the last barriers from the point of view of DiD. 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.*" 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.*" [5]

Within recent research and development, CCA performed analysis of current understanding of DiD with respect to uncertainties in PSA and safety margins.

Fig. 10 summarizes the contents of a recent CAA publication [69]. CCA extrapolated the method for demonstration of safety margins with uncertainties in the deterministic view, published in IAEA Safety Report Series No. 52 [13].

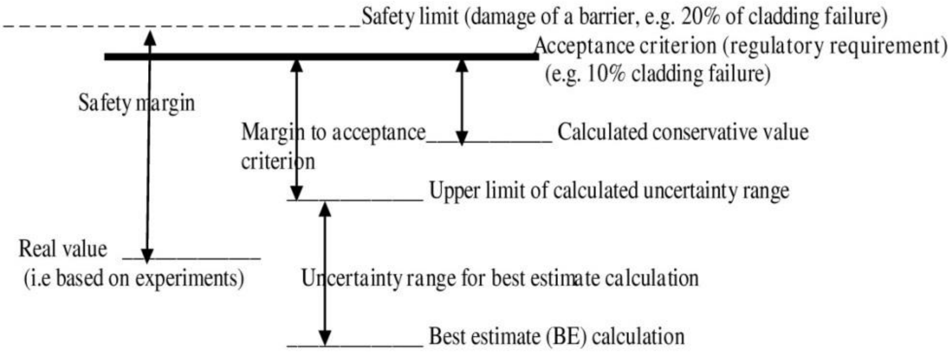

Safety limit (damage of a barrier, e.g. 20% of cladding failure)
Acceptance criterion (regulatory requirement)
(e.g. 10% cladding failure)
Safety margin
Margin to acceptance criterion
Calculated conservative value
Upper limit of calculated uncertainty range
Real value
(i.e based on experiments)
Uncertainty range for best estimate calculation
Best estimate (BE) calculation

Fig. 10 Safety margins with uncertainties in deterministic view [13]

Fig. 11 is obtained extrapolating this approach to PSA, 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. The range of LRF/LERF objectives/limits in different countries is also considered.

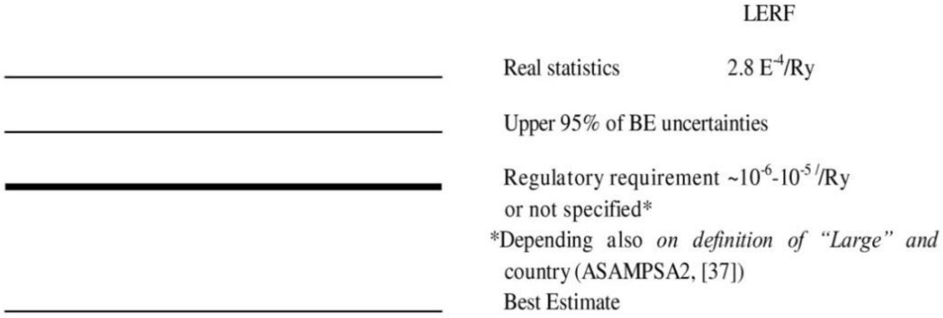

LERF
Real statistics
2.8 E-4/Ry
Upper 95% of BE uncertainties
Regulatory requirement ~10-6-10-5/Ry
or not specified*
*Depending also on definition of "Large" and
country (ASAMPSA2, [37])
Best Estimate

Fig. 11 Safety margins with uncertainties in probabilistic view [69]

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).

An analysis of current DiD was performed [69] 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 analysed:
  - 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. 10.

Based on these considerations, CCA proposes the following changes to DiD [69].

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 guiding for design and operation

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

5.3. ADDITIONAL REPORT: PSA ASSESSMENT OF DID (NIER)

An additional report [42] about the possible role of the PSA in the assessment of the DiD has been developed during the ASAMPSA_E project (by NIER, not reviewed by all partners). This paragraph provides a summary.

The DiD should be the foundation for the definition and the implementation of the plant “safety architecture”. Following the Generation IV International Forum / Risk & Safety Working Group (GIF/RSWG) [36], the “Safety Architecture” is “*the full set of provisions - inherent characteristics, technical options and organizational measures - selected for the design, the construction, the operation including the shut down and the dismantling, which are taken to prevent the accidents or limit their effects.*” The notion of “safety architecture”, to be considered within the framework of the implementation of the DiD, is consistent with the definition of successive “*layers of provisions, functionally redundant so that in the event that a failure were to occur, it would be detected, compensated or corrected by appropriate measures*” *[4].* The objective of the safety architecture representation is to identify, for each plausible plant condition, i.e. for each initiating event and for each sequence generated by any plausible failures, the provisions that embody the different levels of defence in depth. The safety architecture is therefore a multi-dimensional representation of the mode of operation of the installation and its response to abnormal situations. Besides the factual identification of all the available provisions, what is sought is their belonging, vis-à-vis the initiating event and the safety function for which they are requested to the given level of Defence in Depth.

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 (Rev.1) [5] and is based on some concepts introduced by the GIF/RSWG ([37] and [38]). It is articulated in four main steps devoted to (1) the formulation of the safety objectives, (2) the identification of loads and environmental conditions, (3) the 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 implementing DiD with the support of the PSA.

The development of some IAEA Safety Fundamentals [2] and Requirements [4] leads to the definition of additional qualitative objectives. Their introduction allows complementing the probabilistic targets and widening the application field of the PSA approaches, including the contribution to the verification of:

- the achievement of basic design goals (e.g. protective measures limited in times and areas, exhaustiveness of the safety assessment);
- the adequacy of the implementation of DiD principles (e.g. independence of DiD levels, practical elimination of events and sequences, demonstration of design against cliff edge effects);
- the additional characteristics required for the safety architecture (e.g. in terms of progressiveness in the system’s response to abnormal events, forgiving and tolerant characters of system safety response, and balanced contributions of the different events / sequences to the whole risk).

Coherently with the indications provided by the NUREG 2150 [30], the risk space (frequency/probability of occurrence vs consequences) is the framework for the integration between the DiD concept and the PSA approach.

The Objective Provision Tree (OPT) 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 GIF/RSWG) are proposed for an exhaustive (as practicable) representation of the safety architecture implemented.

Some references ([70], [71], [72], and [73][37]) show the results of recent activities on the OPT and its possible use.

OPT could support the development of PSA models 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.

The PSA (fault tree – event tree) model should be consistent with the plant's safety architecture and consider all the subsequent layers of provisions implementing DiD. For a given initiator and safety function, the event tree should reflect the crossing of the different DiD levels; each node represents the success / failure of the safety function at that level. Fault Trees should assess the reliability of the different layers of provisions and establishes the success / failure probability of the DiD levels.[38]

The structure proposed for the PSA (event tree) model integrates some qualitative notions about the practical elimination of both "short" sequences including (i) non-allowed failure of the first levels of DiD (for instance the rupture of the PWR vessel during normal operation or transients without core melt control) and (ii) sequences which lead to unacceptable consequences (i.e. early or large releases in case of failure of the 4th level of DiD). A partial practical example on OPT is provided in the additional report [42], taken from the IAEA TECDOC 1366 [18].

This PSA re-structuring is suggested, but this shall not be considered as an unquestionable need (i.e. the whole process for DiD assessment is not invalidated a priori). Theoretically, different PSA models can embed the same information through different event tree-fault tree structures, and provide all the information required for the DiD assessment (being possible to recognize for each given initiator the subsequent layers of provisions that can fail, leading to the loss or degradation of safety function(s)). What is essential is that the PSA results be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified.

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 should be integrated into a comprehensive implementation of the concept of DiD.

The role of the PSA shall be no longer limited to the verification of the fulfilment of probabilistic targets but can include essential contributions to the safety assessment of the installation in general and to the assessment of DiD in particular:

- PSA can support the deterministic design and sizing of provisions, by addressing the required reliability and contributing to the definition of acceptable boundary conditions;
- 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 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);

[37] OPT implemented by the Japan Nuclear Safety Institute (JANSI) to survey and evaluate the severe accident measures after the Fukushima accident.

[38] 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 main 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 "heat removal").

- 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 support the demonstration of the gradual degradation of the safety architecture in case of loss of safety functions, before that harmful effects are caused to people or environment (progressive 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 excessive or significantly uncertain contributors to risk (balanced character of the safety architecture).
- PSA can support the demonstration of the "practical elimination" of plausible events and sequences which could lead to early or large releases.

Further activities are requested to finalize the proposed approach; they mainly concern the detailed definition of the assessment criteria and metrics, coherently with the indications provided in the document [42].

5.4. WGRISK REPORT: PSA RELATED TO LOSS OF ELECTRICAL SOURCES

A practical example of the link between PSA results and DiD is provided in the recent Task of the CSNI/WGRISK relating to "Probabilistic Safety Assessment insights relating to the loss of electrical sources" [34].
The main insights are briefly summarised below.

a) Probabilistic Safety Assessment Insights Relating to the Loss of Electrical Sources [34]

The OECD/NEA Working Group on Risk Assessment (WGRISK) considered that the loss of electrical power sources is generally an important contributor to the risk related to nuclear power plants. In particular, the importance of external hazards leading to a loss of electrical power sources (external and/or internal to the nuclear plant) has been further underscored by the Fukushima Dai-ichi accident. So the WGRISK determined that a review of current Probabilistic Safety Assessment (PSA) studies would be a useful method to identify safety insights associated with losses of electrical power sources.
Answers to the survey were received from 19 countries (with answers often including the results from several PSA). In total, the survey covered 38 PSA studies. More precisely two types of risk and safety insights were obtained:

- Insights for plant safety related to results and applications of risk calculations - this includes insights related to the overall risk of losses of power sources relative to other contributions, potentially safety weaknesses, the balance between core damage prevention and mitigation, comparison between internal initiating events and hazards, key sources of uncertainty, and safety benefits brought by modifications already implemented or planned (including possible post-Fukushima modifications);
- Insights on PSA methodology - this includes insights related to the identification of good practices, potential methodology gaps, and differences in the methodologies used or developed by member countries.

The report "WGRISK Task 2013(1) Probabilistic Safety Assessment Insights Relating to the Loss of Electrical Sources" [34] was approved by the CSNI in June 2016 and will be published in the near term.

b) Presentation of the results (section 4.3 of the report)

Among the numerous insights presented in this report, a section is particularly devoted to the presentation of the results. In particular topics that are discussed in this section include the Defence in Depth (DiD) concept within the context of identifying PSA insights, LOOP events and their contribution to core damage frequency (CDF), conditional core damage probability (CCDP) given a LOOP event and importance measures.

The intent of this section is to provide a framework for reporting PSA results and identifying risk-insights obtained from the responses to the survey. The concept of defence-in-depth (DiD) provides a useful and practical framework for organizing and assessing these results. However, one of the challenges in addressing DiD is that there is no common definition of what constitutes DiD.

As presented in the IAEA INSAG-10 [19], and also in a recent report by the Swedish Radiation Safety Authority, DiD can be envisioned as multiple levels. If the first level fails, the second one will come into play and so forth.

The levels of DiD described in the report are:

- Prevention of abnormal operation and failures;
- Control of abnormal operation and failures;
- Control of accidents within the design basis;
- Control of severe plant conditions, including prevention of accident progression and consequence mitigation;
- Mitigation of consequences of significant releases of radioactive substances.

While there is no single way to view defence-in-depth, the above concepts help to identify key PSA results and insights that are most relevant to the functional diversity and redundancy of electrical distribution systems.

For the purpose of this task, the following aspects for DiD were considered in order to identify an appropriate structure for highlighting PSA results:

- the LOOP initiating event frequency is equivalent to an initial level of DiD by indicating the likelihood of challenges to plant mitigation systems;
- the relative importance of components can indicate the amount of diversity and redundancy of key safety functions; for example, a component with a high risk achievement worth (RAW) value can imply a reduced redundancy or diversity for the component; conversely, lower RAW values may reflect alternate means to accomplish the safety functions provided by the component; for components with relative higher RAW values, maintaining high reliability (through, for example, design and quality factors) may be important; the relative importance of components to core damage risk provides a measure of the ability of the component to mitigate or control initiating events;
- the conditional core damage probability (CCDP) provides a measure of integrated plant capability to mitigate a hazard. High CCDPs could indicate a reduced ability to mitigate a specific hazard and highlight areas that would benefit from greater diversity or redundancy;
- finally, the relative balance of the contribution of each LOOP hazard category to the plant CDF may provide insights into specific plant vulnerabilities.

General insights related to DiD that were obtained from the survey responses include the use of:

- diverse means to provide alternate sources AC power; some of the alternate AC measures reported include auxiliary transformers, turbine generators, combustion turbines, and emergency Diesel generators;
- some countries rely on additional independent grid connections; for example, a Slovenian plant uses a diverse connection to a gas/steam power plant as an AC power backup;
- batteries also play an important role in DiD for most of the plants.

The following main conclusions can be drawn concerning PSA results:

- the initiating events considered are site specific and grouped differently; however, a global LOOP frequency is in the range of some 10-1/year to 10-3/year for all the responding countries;
- the core damage frequency (CDF) resulting from LOOP events, when provided in the survey, have a wide variability (10-4/year – 10-6/year), with no particular tendency related to the design;

Two general observations can be made:

- BWR plants included in this survey generally have a lower CDF contribution from LOOP than the PWR plants;
- the relative CDF contribution from LOOP for the PWR plants included in this survey tends to have a wider variability than the BWR plants.

This survey shows that challenges related to the plant response to LOOP (i.e. plant recovery from LOOP or from the consequent blackout) can be key contributors in PSA so particular attention needs to be paid to them.

The insights related to the plant response are more generic and consequently more interesting for exchange of knowledge and good practices than initiating events frequencies, which are very site specific. Using the IAEA terminology, it could be said that PSA insights for LOOP are more interesting at DiD level 3 or 4 than level 1 or 2.

c) Comments concerning the use of DiD framework for the presentation of PSA results

This practical example illustrates the interest of PSA for assessing different and progressive levels of safety. Although it appears that the PSA results cannot be used to fit with a too precise definition of the DiD levels, some equivalent structure could be used:

- the PSA initiating events frequency correspond roughly to the DiD level 2;
- DiD level 1 is generally not explicitly assessed since it is included in more global events for which some data can be obtained directly from operating experience (it is the case for LOOP frequency);[39]
- in principle CDF corresponds to the failure of the DiD level 3 (according for example to WENRA definitions although it is not always clear in other documents).

It is important to note that the general objectives of PSA (identification of relative safety weak points and ranking of the problems) do not need to provide results corresponding exactly to DiD definitions.

Even with a PSA which does not fit exactly with DiD levels, PSA can provide insights about a sufficient (or not) implementation of DiD. Besides, another important insight is that this WGRISK survey highlighted the importance of timing in plant response as regards to risk results, and this notion of timing is not addressed by DiD.

5.5. DEFENCE-IN-DEPTH AND RISK MONITORS

The use of risk monitors is a well-known application of PSA for NPPs. The SSG-3 [7] gives some guidance on the use and limitations of risk monitors as well as on the changes in PSA models required for risk monitors ([7], p. 141).

There are several software tools available and applied in NPP risk monitors. A number of them allow to present qualitative (risk) information related to the availability of safety systems [33]. This is often labelled as status information related to DiD ([33], [60], [61]).

This assessment, whether qualitatively or quantitatively, has as a prerequisite an appropriate structure of the underlying PSA model. An example of developing a risk monitor system is described in reference [65].

[39] Nevertheless one can consider that the failure of the DiD level 1 is implicitly considered taking into account the frequency of the initiating event;

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 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 [16], [17]):

- high level indicators –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 it should be demonstrated through deterministic and probabilistic techniques that the preventive and mitigating measures against the hazard are adequate.

5.6. IAEA RECENT ACTIVITIES

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 [74].

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. This is especially important in the design of new NPPs.

Particularly, an investigation is being conducted by the IAEA to explore the use of probabilistic techniques for the assessment of compliance with DiD for new NPP designs.

In order to provide a concise sequential representation of the consideration of compliance with DiD, the event tree technique is used, referring each node to each level of DiD (similarly to the approaches proposed in §5.1, §5.3 and §5.7).

5.7. OTHER EXPERIENCES

In reference [67], the authors briefly discuss the link between DiD, PIE assignment to DiD levels. Their summary of the relationship between PSA levels and DiD levels, with an exemplary event tree structured along DiD levels, is shown in Fig. 12.

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?	

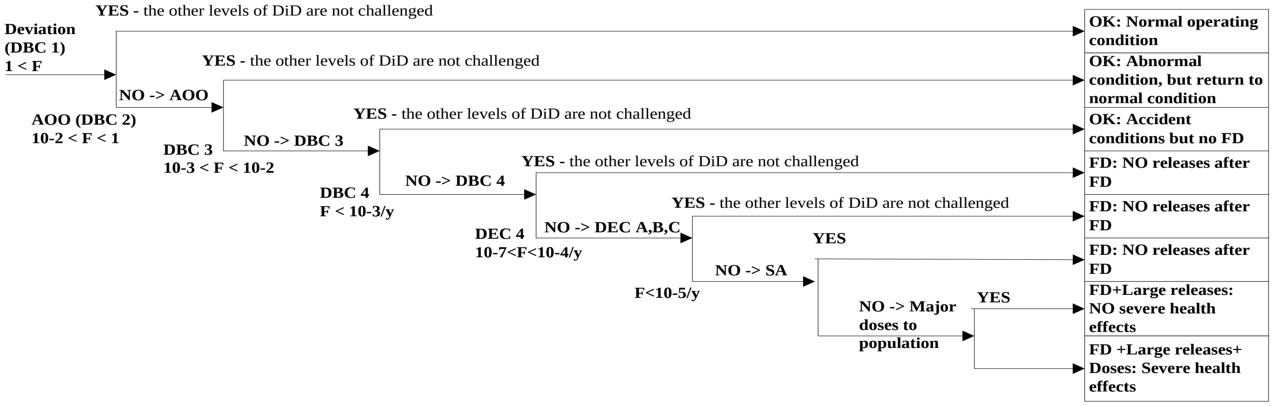

YES - the other levels of DiD are not challenged
Deviation
(DBC 1)
1 < F
NO -> AOO
YES - the other levels of DiD are not challenged
AOO (DBC 2)
10-2 < F < 1
NO -> DBC 3
YES - the other levels of DiD are not challenged
DBC 3
10-3 < F < 10-2
NO -> DBC 4
YES - the other levels of DiD are not challenged
DBC 4
F < 10-3/y
NO -> DEC A,B,C
YES - the other levels of DiD are not challenged
DEC 4
10-7<F<10-4/y
YES
NO -> SA
F<10-5/y
YES
NO -> Major doses to population
OK: Normal operating condition
OK: Abnormal condition, but return to normal condition
OK: Accident conditions but no FD
FD: NO releases after FD
FD: NO releases after FD
FD: NO releases after FD
FD+Large releases: NO severe health effects
FD +Large releases+ Doses: Severe health effects

Fig. 12 The relationship between PSA levels and DiD levels [67]

6 CONCLUSIONS AND RECOMMENDATIONS

This section provides some general conclusions and recommendations coming from the previous discussion about the link between the Probabilistic Safety Assessment (PSA) and the Defence-in-Depth (DiD) concept for NPP, with specific focus on the capability of an “extended PSA” to support the assessment of DiD.

The identification of the Postulated Initiating Events (PIEs) is the initial step of a safety analysis. Thus, it is also a cornerstone in the application of the DiD concept. Some main recommendations were specified discussing (in Section 3) the link between PIE in Deterministic Safety Assessment (DSA) and Initiating Event (IE) in PSA:

- 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;
- the analysts should be aware that, from historical evidence, actual severe accidents (i.e. design extension conditions with core degradation) happened more often than predictions;
- the analysts should be aware that the original sets of DBAs were postulated as “enveloping accidents” by nuclear engineers more than 50 years ago based on the knowledge and consensus at the time;
- the quantitative references for the frequency of occurrence stated in the SSG-2 [6] should be considered as indicators rather than fixed limits; some harmonization are still needed between these thresholds and some historical assumptions and recent safety criteria/design objectives (e.g. practical elimination);
- the list of IE of an extended PSA, including internal events, hazard event groups, combination events, should be checked against the list of PIE for deterministic safety analyses;
- before any comparison with the IE in PSA, the basic scenario for the PIE (e.g. loss of feedwater, small LOCA), the related boundary conditions (e.g. loss of offsite power) and concurrent failures assumed in the DSA should be clearly understood;
- the frequency values assumed for PIE in DSA should be consistent with the related IE frequency or intermediate or final results of the PSA model, as applicable;
- the consistency between the data sources used for the estimation of the IE frequency (value or distribution) in PSA and the classification of PIE should be checked.

The classification of Systems, Structures, And Components (SSCs) and their assignment to different levels of DiD is an essential aspect of the implementation of the DiD concept. Some recommendations were specified discussing (in Section 4) the process and criteria for the classification of SSCs and the reliability of provisions implementing safety functions:

- for the classification of SSCs it is recommended to apply deterministic methodologies and to complement them by probabilistic safety assessment;
- PSA information should be used through the approach endorsed by the US NRC ([31], [32]) or similar approaches based on the importance measures estimated for the SSCs with reference to the PSA Level 1 (CDF) and PSA Level 2 risk measures;
- the assessment of the reliability of the provisions (including SSCs) achieving the safety functions does not require different methods or risk measures for an extended PSA to be used for the assessment of DiD;
- a more systematic use of the information coming from PSA is recommended in risk-informed decision making on the adequate reliability of systems, and structures (i.e. including passive safety features) and, more generally, the safety related provisions; the measure should be their conditional failure probability / availability.

The main issues related to the DiD concept, including the structure of the levels of DiD, and the essential requirement about their independence, and the need(s) for the safety and DiD assessments, have been introduced in Section 2.

The need for the assessment of DiD is explicitly recognized by the GSR Part 4 (Rev1) [5], which defines the context for the safety assessment of a nuclear installation, encompassing DiD concept and the PSA approach, enhancing their complementarity and detailing the objective to be pursued.

Fundamentally, there should be no methodological difference between a PSA which analyses a system with or without explicit consideration of DiD. Taking into account the ability of the PSA to reflect the DiD concept (always true in theory), its potential to provide information useful for the assessment of DiD and their complementary objectives, both (DiD and PSA) should be developed and their contributions optimized.

In order to enhance the complementarity between the implementation of DiD and the development of the PSA, the optimization to be searched should:

- maintain a degree of independence in their execution, which combined with their native diversity could provide the required confidence on the results of the safety assessment;
- integrate their needs (about data and models) and results, for an exhaustive assessment of the safety architecture, based on both deterministic and probabilistic insights.

If appropriately developed, the PSA can provide a methodical support and an essent*i*al contribution for determining whether the safety objectives are met, the DiD requirements are correctly taken into account and the risk (of radioactive releases) related to the installation are kept below the acceptable (dose) limits and As Low As Reasonably Achievable. Moreover, PSA can support the verification of the proper implementation and independence of the layers provisions at the different levels of DiD, the specification of requirements for their reliability during normal operation and any (postulated) accidental condition, the modelling of immaterial provisions (e.g. human factor), the propagation of the uncertainty on input data through the model, the “practical elimination” of plausible events and sequences of events which could lead to early or large releases, the demonstration of the graded approach to safety.

Specifically about the independency among the DiD levels, the adoption of a systematic approach for the identification of the subsequent layers of provisions should be considered a prerequisite for the assessment of independence. There is no specific need to develop new methods for identifying and quantifying dependencies between safety functions by an extended PSA, and no specific criteria are recommended. Conversely, the use of PSA results is recommended to check for common cause failures and other dependent failures, A priori, it does not require the restructuring of the PSA models along the levels of DiD. Judgements on the acceptability of any findings should be made on a case-by-case basis.

In spite of the aforementioned complementarity, the independent implementation of the DiD concept and development of PSA, together with their native diversity, has been recognized a benefit to maintain. Specifically:

- DiD and PSA have their own concepts for including or dismissing events or phenomena from their respective analyses; to keep the benefits of diversity, the harmonization of these features should not be an objective per se; at the same time, any differences in assumptions should be clearly identified and addressed in order to contribute to exhaustiveness of all events and phenomena challenging the installation;
- the discussion on the evolution of the DiD concept is not directly related to the need for progresses in PSA methods; deficiencies recognized in the actual PSA models (e.g. lack of data, incompleteness, insufficient methods for some human actions, large requirement of resources, etc.), motivating a specific work for their improvement, are not related to DiD issues.

At this regard, the DiD assessment as preconized by the GSR Part 4 (Rev.1) [5] could be inscribed in the Integrated Risk Informed Decision Making Process, where the PSA can play an essential role, without the need to define specific assessment process and criteria.

Furthermore, the use of the PSA model and its results for the assessments of DiD introduces specific challenges that have been not further investigated and are subjects for future discussion and subsequent work.

First of all, the existing PSA models have been often produced without the specific objective to assess the implementation of DiD. This is partly due to the lack of previous investigations into the subject and partly due to the lack of practical implementations and feedbacks about good practices in the PSA community.
If the PSA is used with this particular objective, its results should be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified. Specifically, the PSA should be properly structured in order to provide results that can be correlated with the performances (capability, reliability and robustness) required to the levels of DiD and have a sufficient scope.
A different structure of the PSA models (i.e. the re-structuring the existing PSA) has been proposed by different works, but it seems not an unquestionable need. Guidance on how to re-structure the PSA to fall in line with the DiD levels is neither available nor developed during the ASAMPSA_E project (out of scope), only generic thoughts have been formulated. Moreover, this activity could require a significant effort and there is still no clear consensus if the added value justifies it.

Indeed, theoretically, different PSA models can embed the same information through different event tree-fault tree structures, and provide the information required for the assessment of DiD, allowing the identification of the subsequent layers of provisions that can fail (for each given initiator) and lead to the loss or degradation of safety function(s). Practically, there is no evidence about the exhaustiveness of the existing PSA (with respect to the information required for the DiD assessment) and about the need to develop PSA models with a different structure.

Additionally:

- the different progressive levels of DiD and the associated plant conditions do not easily map to the traditional PSA end states (e.g. CDF and release categories) and, on their side, initiating events could be assimilated to the failure of a given level of the DiD; at this regard, there is a 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;
- the best-estimate approach typically used in PSA is not immediately compatible with the (conservative, safety case oriented) deterministic approach for a DiD assessment; on the other hand, taking into account uncertainties and assessing their contribution is now essential to any safety assessment.
- non-safety systems should be considered in the PSA, but they are usually neglected in the DSA[16];
- the comparison between the IE in PSA (with related frequency of occurrence) and the classification of PIE could be difficult mainly because of the (potential) different grouping of events and the different assumptions on boundary conditions and concurrent failures in PSA and DSA;
- a PSA model for the assessment of DiD could require additional data if they are not already included in the existing non-full scope PSA models (e.g. about initiating events and SSCs failure at the DiD level 2);
- deterministic analyses (DSAs) often assume certain boundary conditions to occur simultaneously at the time of the PIE occurrence, without considering their likelihood; differently, they are usually addressed in the PSA with their conditional probabilities, giving less conservative estimation.

At the end, despite the potential of the PSA to support the assessment of DiD and the recognition of its complementarity with the deterministic approach, no specific conclusions are formulated and the only recommendation that can be expressed is the need to deepen the concern looking for a possible consensus about objectives, practical methodologies and scope for assessing the DiD with the support of PSA.

In order to define a way to go beyond the above considerations and to overcome the highlighted limits, some practical experiences (national and/or made by the partners before or during the ASAMPSA_E project) about the link between DiD and PSA have been provided in Section 5, without any need of coherence and any synthesis, as elements for future discussions.

The work done by SSM ([62], [63], [64]) could be the starting point for future work (see §5.1).

An additional report [42] has been developed during the ASAMPSA_E project about the peculiar roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations. It describes the process and tools proposed for the DiD assessment through PSA (see §5.3). All the proposals are based on consolidated terminology [2] and shared concepts ([3], [4], [23], [24], [30], [36], [37]), and are consistent with process for the Safety assessment defined by the IAEA [5] and with the approach proposed by SSM. Further activities, including practical applications, are required in order to finalize the proposals.

By summarizing, the present report provides elements to feed the thoughts about the optimization between the contributions of DiD and PSA to guarantee the safety assessment of the installation, but further discussion and practical experiences (e.g. benchmarking[40]) are needed to achieve consensus on objectives, scope and approaches for the use of PSA in the assessment of DiD concept and to develop a practical guideline.

[40] For instance, it would be necessary to extract from a complete existing PSA a self-supporting portion (e.g., the full set of plausible sequences from a given initiator event) and then to check if and how the (intermediate and final) results available provide the answers required for the assessment of DiD. In parallel, the safety architecture (i.e. the portion involved in the selected sequences of events) should be represented according to the principles of DiD, e.g. through the Objective Provisions Tree methodology, and the PSA (fault tree - event tree) model developed coherently with this representation. The solution of the model and the comparison of results (and embedded information for the DiD assessment) with the ones coming from the existing PSA could provide answers to the open questions (mainly, about the need of a different structure of the probabilistic model).

LIST OF REFERENCES

[1] Council Directive 2014/87/EURATOM of 8 July 2014 amending the Directive 2009/71/ EURATOM establishing a Community framework for the nuclear safety of nuclear installations.

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

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

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

[5] International Atomic Energy Agency (IAEA), "Safety Assessment for Facilities and Activities", General Safety Requirements Part 4 No GSR Part 4 (Rev. 1), Vienna 2016

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

[7] 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.

[8] 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.

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

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

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

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

[13] IAEA Safety Report Series No.52, "Best estimate Safety Analysis for Nuclear Power Plants: Uncertainty evaluation", Vienna, 2008.

[14] International Atomic Energy Agency (IAEA), "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs", IAEA-TECDOC-1570, September 2007.

[15] International Atomic Energy Agency (IAEA), "Considerations on the Application of the IAEA Safety Requirements for Design of Nuclear Power Plants", IAEA-TECDOC-1791, May 2016.

[16] International Atomic Energy Agency (IAEA), "Applications of probabilistic safety assessment to nuclear power plants", IAEA-TECDOC 1200, February 2001.

[17] International Atomic Energy Agency (IAEA), "Operational safety performance indicators for nuclear power plants", IAEA-TECDOC 1141, May 2000.

[18] International Atomic Energy Agency (IAEA), "Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors", IAEA TECDOC 1366, 2003.

[19] International Atomic Energy Agency (IAEA), INSAG, "Defence in Depth in Nuclear Safety", INSAG-10, June 1996.

[20] International Atomic Energy Agency (IAEA), INSAG, "Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1", INSAG-12, October 1999.

[21] International Atomic Energy Agency (IAEA), INSAG, ”A Framework for an Integrated Risk Informed Decision Making Process", INSAG-25, 2011

[22] International Atomic Energy Agency (IAEA), “INES: The International Nuclear and Radiological Event Scale User's Manual”, 2008.

[23] Western European Nuclear Regulators Association (WENRA),, “Safety of New NPP Designs, Study by Reactor Harmonization Working Group RHWG”, March 2013

[24] Western European Nuclear Regulators Association (WENRA), “WENRA Safety Reference Levels for Existing Reactors”, draft update, November 2013.

[25] Western European Nuclear Regulators Association (WENRA), “WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.

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

[27] 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.

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

[29] U.S. NRC, “Historical Review and Observations of Defense-in-Depth », NUREG/KM-0009, April 2016.

[30] U.S. NRC, “A Proposed Risk Management Regulatory Framework”, NUREG 2150, April 2012.

[31] 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.

[32] U.S. NRC, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors”, 10 CFR 50.69, 2004.

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

[34] NEA/CSNI/R(2016)XX WGRISK Task 2013(1) Probabilistic Safety Assessment Insights Relating to the Loss of Electrical Sources – *To be published*.

[35] Nuclear Energy Institute, “SSC Categorization Guideline, NEI 00-04, 2005.

[36] GIF/RSWG/2007/002/Rev.1 - Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems; November 2008.

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

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

[39] Raimond, E. et al., “Annex I – ‘Description of work’ ASAMPSA_E”, April 2013, Grant agreement n°605001,

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

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

[42] ASAMPSA_E, “The PSA assessment of Defense in Depth - Memorandum and proposals”, Gian-Luigi Fiorini, Stefano La Rovere (NIER), ASAMPSA_E/WP30/D30.7/2017-31 volume 5, IRSN/ PSN-RES/SAG/2017-00016,

[43] ASAMPSA_E, “Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA”, ASAMPSA_E D30.7/2017-31 volume 2, IRSN/ PSN-RES/SAG/2017-00017,

[44] ASAMPSA_E, “Risk Metrics and Measures for an Extended PSA”, ASAMPSA_E/WP30/D30.7/2017-31 volume 3, IRSN/ PSN-RES/SAG/2017-00018.

[45] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, “Sicherheitsanforderungen an Kernkraftwerke” from 20 November 2012, BAnz AT 24.01.2013 B3.

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

[47] ENSI, “Probabilistic Safety Analysis (PSA): Applications”, Guidelines for Swiss Nuclear Installations ENSI-A06/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] 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).

[51] Atomic Energy Control Board, “Requirements for Containment Systems for CANDU Nuclear Power Plants”, Document R-7, February 1991.

[52] Atomic Energy Control Board, “Requirements for Shutdown Systems for CANDU Nuclear Power Plants”, Regulatory Document R-8, February 1991.

[53] Atomic Energy Control Board, “Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants”, Document R-9, February 1991.

[54] CNSC, “Design of Reactor Facilities: Nuclear Power Plants”, REGDOC-2.5.2, May 2014.

[55] CNCAN, “Norme de securitate nucleara privind proiectarea si constructia centralelor nuclearoelectrice”, NSN-02, 23 November 2010.

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

[57] CNCAN, “Norme privind sistemele de oprire rapidă pentru centralele nuclearo-electrice de tip CANDU”, NSN-13, 23 November 2005.

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

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

[60] Lloyd’s Register Consulting, “RiskSpectrum Magazine 2014”, June 2014.

[61] 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

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

[63] 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.

[64] 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.

[65] 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.

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

[67] 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.

[68] 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/.

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

[70] G.L. Fiorini; L. Ammirabile, V. Ranguelova, "The ISAM tool Objective Provisions Tree (OPT), for the identification of the Design Basis and the construction of the Safety Architecture. International Conference on Topical Issues in Nuclear Installation Safety: Defence-in-Depth", Advances and Challenges for Nuclear Installation Safety, Vienna, October 2013.

[71] 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, May 2015.

[72] Application of Objective Provisions Tree to Development of Standard Review Plan for Sodium-cooled Fast Reactor Nuclear Design, Moo-Hoon Bae & al (Korea Institute of Nuclear Safety (KINS)), ICAPP 2015.

[73] Masakatsu INAGAKI Japan Nuclear Safety Institute (JANSI): Some considerations for severe accident measures planned by Japan's Nuclear Power Plants; ASAMPSA_E 2nd Technical Meeting, Vienna 11th September 2014.

[74] Kuzmina, I., El-Shanawany, M., Modro, M., Lyubarskiy, A., "An approach for holistic consideration of Defence in Depth for nuclear installation using probabilistic techniques", International Topical Meeting on Probabilistic Safety Assessment and Analysis 2011, PSA 2011, 3, pp. 1812-1824, 2011.

LIST OF TABLES

LIST OF FIGURES