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

"NUCLEAR FISSION "

Safety of Existing Nuclear Installations

Contract 605001

The PSA assessment of Defense in Depth
Memorandum and proposals

Warning : this report has been proposed by NIER to support the development of the deliverable D30.4 (PSA and DiD) of the ASAMPSA_E project. It has not been reviewed by the ASAMPSA_E partners and some issues may need to be discussed further. The report includes some description of practices and reasoning applied for LWRs and Gen IV reactors (SFR for instance) and will be useful for the ASAMPSA_E project.

Comments can be provided during the ASAMPSA_E external review organized from 10th May 2016 to Sept 2016.

Reference ASAMPSA_E

Technical report ASAMPSA_E / WP30 / D30.4 (support material) / 2016-15

Gian-Luigi Fiorini, Stefano La Rovere (NIER)

Period covered: from 01/07/2013 to 31/12/2016	Actual submission date: 11-0562016	
Start date of ASAMPSA_E: 01/07/2013	Duration: 42 months	
WP No: 30	Lead topical coordinator : H. Löffler	His organization name : GRS

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

ASAMPSA_E Quality Assurance page

Partners responsible of the document : NIER Ingegneria	
Nature of document	Technical report
Reference(s)	ASAMPSA_E / WP30 / D30.4 (support material) / 2016-15
Title	The PSA assessment of Defense in Depth (Memorandum and proposals)
Author(s)	G.L. Fiorini, S. La Rovere
Delivery date	11/05/2016
Topical area	Defence-in-Depth, PSA
For Journal & Conf. papers	No

Summary :

This report concerns the peculiar roles of the Defence in Depth (DiD) concept and the Probabilistic Safety Assessment (PSA) approach for the optimization of the safety performances of the nuclear installation. It proposes a process for the assessment of the safety architecture implementing DiD, which is articulated in four main steps devoted to (1) the formulation of the safety objectives, the (2) identification of loads and environmental conditions, the (3) representation of the safety architecture and (4) the evaluation of the physical performance and reliability of the levels of DiD. A final additional step achieves the practical assessment of the safety architecture and the corresponding DiD with the support of the PSA. The risk space (frequency/probability of occurrence, versus consequences) is the framework for the integration between the DiD concept and the PSA approach. Additional qualitative key-notions are introduced in order to address the compliance of the safety architecture with a number of (IAEA) safety requirements. In this context, the role of the PSA is no longer limited to the verification of the fulfilment of probabilistic targets but includes different contributions to the assessment of the DiD identified in this report.

Visa grid			
	Main author(s) :	**Verification**	**Approval (Coordinator)**
Name (s)	G.L.Fiorini; S. LaRovere	A.Wielenberg, H. Loeffler	Emmanuel Raimond
Date	2016-05-11	2016-05-11	2016-05-11
Signature			

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
Rev. 1	04/04/2016	G.L.Fiorini; S. LaRovere	All	First emission
Rev. 2	11/05/2016	G.L.Fiorini; S. LaRovere, H. Löffler, E. Raimond	All	Few modifications after review.

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	Vienna University	WP21 coordinator
Kumar	Manorma	LRC	WP22 coordinator
Wielenberg	Andreas	GRS	WP30 coordinator until 2016-03-31
Löffler	Horst	GRS	WP40 coordinator WP30 coordinator after 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
Michaud	Laurent	AREVA
Pellisseti	Manuel	AREVA
Cordoliani	Vincent	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

Name	First name	Organization
Burgazzi	Luciano	ENEA
Karlsson	Anders	FKA
Hultqvist	Göran	FKA
Pihl	Joel	FKA
Ljungbjörk	Julia	FKA
KÄHÄRI	Petri	FKA
Tuerschmann	Michael	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	GRS
Serrano	Cesar	IEC
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Apostol	Minodora	INR
Nitoi	Mirela	INR
Stefanova	Antoaneta	INRNE
Groudev	Pavlin	INRNE
Laurent	Bruno	IRSN
Clement	Christophe	IRSN
Duluc	Claire-Marie	IRSN
Leteinturier	Denis	IRSN
Armingaud	François	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

Name	First name	Organization
Dupuy	Patricia	IRSN
Vinot	Thierry	IRSN
Rebour	Vincent	IRSN
Guigueno	Yves	IRSN
Prošek	Andrej	JSI
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Rimkevicius	Sigitas	LEI
Matuzas	Vaidas	LEI
Olsson	Anders	LRC
Häggström	Anna	LRC
Klug	Joakim	LRC
Kumar	Manorma	LRC
Knochenhauer	Michael	LRC
Kowal	Karol	NCBJ
Borysiewicz	Mieczyslaw	NCBJ
Potempski	Slawomir	NCBJ
Vestrucci	Paolo	NIER
La Rovere	Stefano	NIER
Brinkman	Hans (Johannes L.)	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI

Name	First name	Organization
Siklossy	Tamas	NUBIKI
Caracciolo	Eduardo	RSE
Morandi	Sonia	RSE
Gorpinchenko	Oleg	SSTC
Dybach	Oleksiy	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
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

N:ER INGEGNERIA

Memorandum
The PSA assessment of Defense in Depth

Revision	Date	*Author(s)*
1	10/05/2016	Gian Luigi Fiorini, Stefano La Rovere

EXECUTIVE SUMMARY

The safety architecture of a nuclear installation shall meet the applicable safety objectives while guaranteeing the compliance with the (IAEA) Safety Fundamentals [2] and IAEA Safety Requirements [3]. Deterministic and probabilistic approaches are complementary tools to check the meeting of these objectives in the wider context of the safety assessment, as defined by the IAEA GSR Part 4 [4].

Consistently with the IAEA Safety Fundamentals [2], the Defence in Depth (DiD) concept, and all principles for its implementation, represents the foundation of the deterministic approach to build the safety architecture; in this context, there is the fundamental need to address the compliance with its principles i.e.: the appropriateness of the approach for the construction of the safety architecture, the adequacy of the implemented "layers of overlapped provisions" (INSAG 10, [11]), and the availability of adequate margins to correctly address the uncertainties. Unquestionably, the Probabilistic Safety Assessment (PSA) could support the demonstration of this compliance, even if – up to now - no formal and one-at-one links are established between DiD concept and PSA approach and no specific requirements are formulated for the assessment of DiD using PSA.

In order to contribute to fill-in of this gap, the peculiar role of the Defence in Depth concept and the Probabilistic Safety Assessment approach for the optimization of the safety performances of the nuclear installation have been preliminarily investigated [30]: general indications have been provided about a global process for the assessment of the DiD, i.e. for the verification, through PSA, that the implemented safety architecture complies with the principles of the DiD.

The content of this report goes further making explicit the possible relationship between DiD and PSA. The proposed process is fully consistent with the indications provided by the IAEA GSR Part 4 [4] and is based on some concepts introduced by the Generation IV Risk and Safety Working Group ([15] and [16]). 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 step achieves the practical assessment of the safety architecture and the corresponding DiD with the support of the PSA.

Concerning the safety objectives (cf. Section 2), the reference to the risk space (frequency/probability of occurrence, versus consequences) is considered essential to assess the whole safety architecture with respect to the achievement of probabilistic targets, the performance allocated to the safety functions to reduce the consequences of plausible events and, finally, the reliability which has to be allotted to the provisions which achieve these functions. Additional qualitative key-notions are introduced, providing general indications about the criteria and metrics which should have to be defined in details and adopted. They refer to basic design goals (e.g. need for protective measures limited in times and areas in case of severe accidents) and to DiD principles (e.g. independence of DiD levels, practical elimination of events and sequences leading to early or large releases, demonstration of the availability of "adequate margins" against possible cliff edge effects).

The development of some Safety Fundamentals and Requirements leads to the definition of additional qualitative objectives; they address the search for exhaustiveness for the design basis events and the design extension conditions considered for the safety design and assessment, the need for progressiveness in the system's response to abnormal events, the need for a forgiving and tolerant character of system safety response, and the suitable balanced contributions of the different events / sequences to the whole risk.

The identification and recognition of all plausible normal and off-normal loads and environmental conditions (cf. Section 3), that can affect the behavior of the installation, is the result of a detailed analysis of the system complemented, as needed, by the consideration of the experience feedback. Since the year 2000 the basis for the design evolved and, today, all the plausible conditions generated by internal and external hazards (Anticipated Operational Occurrences, Design Basis Events and Design Extension Conditions), have to be considered within the Design Basis and, more generically, for the definition of the Safety Case.

Moreover, an explicit one-at-one correspondence is suggested, for example, by WENRA [13] & NUREG 2150 [10] between, on one side, these conditions, the levels of DiD and, on the other side, their positioning within the risk space. This correspondence is essential for the designer who can so superpose the levels of DiD within the area of allowable risk and, simultaneously, gives explicit targets (success criteria, both in terms of performances and reliability) for these levels. It is worth nothing that these targets are essential to classify the System, Structures and Components, complementing the process defined by the SSG-30 Safety Guide [6], and to size the provisions associated with each level of the DiD.

The Objective Provision Tree (OPT) methodology and the complementary notion of Line of Protection/Layers of Provisions (LOP), developed within the context of the IAEA activities and endorsed, among others by the Generation IV International Forum / Risk & Safety Working Group (GIF/RSWG), are proposed for the representation of the safety architecture implemented by the nuclear installation (cf. Section 4); they are fully consistent with the safety assessment process as presented by the IAEA GSR Part 4 [4]. If correctly implemented, these tools can support the identification of possible lacks or the weaknesses of DiD level(s), e.g. lack of independence between the DiD levels, inadequacy of the layers of provisions allocated to a given DiD level, etc. The OPT and LOP also provide the essential information for the subsequent development of probabilistic studies, by representing the whole safety architecture that is successively analytically described by the PSA, with all its internal interactions.

The availability of an exhaustive - as practicable – representation of the safety architecture allows the development of a PSA model with a structure that better complies with the DiD principles and that, in turn, allows the evaluation of the physical performance and reliability of the levels of DiD (cf. Section 5). This structure is based on Event Trees built to reflect the crossing of different levels of DiD and on Fault Trees which, at each crossing, allow assessing the reliability of the implemented layers of provisions.

The structure proposed for the PSA/Event Tree integrates some qualitative notions about the practical elimination of “short” sequences (e.g. in case of 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 controlled by the safety systems) and of sequences which both lead to unacceptable consequences, i.e. early or large releases (in case of failure of the 4th level of DiD). A partial practical example developed starting from the OPT of the IAEA TECDOC 1366 [8] is also presented.

In summary, the acceptability of a safety architecture shall be based on the degree of meeting the DiD principles while fulfilling the applicable Safety Fundamentals and Requirements. Deterministic and probabilistic considerations shall be integrated into a comprehensive implementation of Defence in Depth. The risk space (frequency/probability of occurrence, versus consequences) looks as being the appropriate framework for this integration. In this context, the role of the PSA is no longer limited to the verification of the fulfilment of probabilistic targets but includes different contributions to the assessment of the DiD:

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

ASAMPSA_E PARTNERS

The following table provides the list of the ASAMPSA_E partners involved in the development of this document.

1	NIER Ingegneria	NIER	Italy

Content

ABBREVATIONS

AOO	Anticipated Operational Occurrence
BDBEE	Beyond Design Basis External Event
CCDP	Conditional Core Damage Probability
CERP	Conditional Early Release Probability.
CFDP	Conditional Fuel Damage Probability
CLRP	Conditional Large Release Probability
CDF	Core Damage Frequency
DBA	Design Basis Accident
DBC	Design Basis Conditions
DEC	Design Extension Condition
DiD	Defence in Depth
DPA	Deterministic and Phenomenological Analyses
DSA	Deterministic Safety Assessment
ERF	Early Release Frequency
ET	Event Tree
FDF	Fuel Damage Frequency
FT	Fault Tree
GIF/RSWG	Generation IV Risk and Safety Working Group
IE	Initiating Event
ISAM	Integrated Safety Assessment Methodology
LOCA	LOss of Coolant Accident
LOD	Line Of Defense
LOP	Line Of Protection
LWR	Light Water Reactor
MCCI	Molten Core Concrete Interaction
NPP	Nuclear Power Plant
OPT	Objection-Provision Tree
PIE	Postulated Initiating Event
PIRT	Phenomena Identification and Ranking Table
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Analysis
PWR	Pressurized Water Reactor
QSR	Qualitative Safety features Review
SA	Safety Architecture
SSC	Systems, Structures, and Components

1. INTRODUCTION

1.1. Preamble

The safety architecture[1] of a nuclear installation shall meet the safety objectives while complying with the principles defined within the IAEA Safety Fundamentals (SF1, [2]) and the IAEA Safety Requirements [3]. Specifically, the optimization of plant's safety performances, both in terms of physical performances and reliability, in achieving the requested safety functions is a specific objective which resumes the compliance with the applicable safety principles (5 to 10 of [2])[2]; this search for optimization shall support the plant's design and its safety assessment.

To support the effort for optimization, the quantitative safety objectives which are defined are complemented by qualitative notions (see Section 2) related to design goals including, for example, the implementation of principles of Defence in Depth, and the selection of characteristics which will enable to meet safety requirements. Still within the logic of optimization, the assessment of the safety architecture, with reference to both quantitative and qualitative objectives, shall take full advantage of the possible complementarity between the deterministic and probabilistic approaches.

The Defence in Depth (DiD) concept, and all principles for its implementation, represent the foundation of the deterministic approach to build the safety architecture. If correctly interpreted / implemented, DiD helps guaranteeing – as far as practically feasible – "exhaustiveness" in terms of coverage of plausible abnormal conditions and "progressiveness" in terms of plant response to these conditions. The correct design of the "layers of provisions" which characterize – and materialize – the different DiD levels help guaranteeing the "tolerant" and the "forgiving" character of the plant's safety, i.e. its response versus the abnormal conditions.

On its side, the Probabilistic Safety Assessment (PSA) provides a comprehensive, structured approach to identifying failure scenarios and the corresponding damages to the facility and, as a last step, allows deriving numerical estimates of the risk to the workers, the public and the environment. If appropriately developed, the PSA can provide a methodical support and an essential contribution for determining whether the safety objectives are met, the DiD requirements are correctly taken into account and the risks related to the operation of the installation are As Low As Reasonably Achievable (ALARA).

The potential role of PSA in the assessment of DiD can be summarized in saying that it contributes to achieving the overall assessment of the implemented safety architecture; it allows quantifying the probability of detrimental or unacceptable events from a design point of view (e.g. severe fuel damage conditions – PSA

[1] The safety architecture is the set of provisions that are set up by the designer to:
- ensure the achievement of tasks allocated to the process in satisfactory conditions of safety, i.e. maintaining significant parameters (e.g. the fuel temperature) within allowable operational limits;
- prevent the degradation of the facility, i.e. the exceed of operational limits;
- restore and keep the facility in a safe shutdown condition for the short and long term, in case of failure.

[2] *Principle 5: Optimization of protection; Principle 6: Limitation of risks to individuals; Principle 7: Protection of present and future generations; Principle 8: Prevention of accidents; Principle 9: Emergency preparedness and response; Principle 10: Protective actions to reduce existing or unregulated radiation risks.*

Level 1) through the systematic evaluation of all relevant and plausible incidental and accidental scenarios. If appropriately developed PSA can provide additional insights on the achievement of qualitative objectives and specifically about the degree of "balance" for the prevention, management, and limitation of detrimental or unacceptable consequences for the whole set of the considered design basis and design extension conditions.

Having said that, it is worth noting that, despite the potential of the PSA approach and that of the deterministic DiD approach, and despite the recognition of their complementarity, no specific requirements are formulated about the use of PSA for the assessment of DiD. For instance, it is recognized that PSA results shall be taken into consideration in the design of provisions associated to the last levels of DiD, but the criteria to be used to obtain an optimized design is an open question. In this context, the purpose of this report is the definition of a process to explore the relationship between DiD and PSA, with the objective to optimize their complementarity and to help improving the quality of the overall safety assessment for the nuclear installations.

1.2. SAFETY ASSESSMENT: DID CONCEPT AND LINK TO PSA

1.2.1. Safety assessment process

In order to define the link between the DiD concept and the PSA approach it is important to identify the specific role of the two components within the context of the safety approach for the design and the assessment of a nuclear installation. The organization of the safety assessment, as defined by the IAEA GSR Part 4 [4], can allow achieving this task.

According to the IAEA GSR Part 4: *1.2. Safety assessments*[3] *are to be undertaken as a means of evaluating compliance with safety requirements (and thereby the application of the fundamental safety principles)…. Safety assessment includes, but is not limited to, the formal safety analysis*[4].

Scope, responsibility, and purpose of the safety assessment are detailed in the GSR Part 4 (Requirements 2, 3, 4). Figure 1-1 shows the main elements of the process.

[3] From IAEA glossary [1]: 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.
[4] From IAEA glossary [1]: Safety analysis is the evaluation of the potential hazards associated with the conduct of an activity. Safety analysis is often used interchangeably with safety assessment. However, when the distinction is important, safety analysis should be used for the study of safety, and safety assessment for the evaluation of safety — for example, evaluation of the magnitude of hazards, evaluation of the performance of safety measures and judgement of their adequacy is safety analysis, or quantification of the overall radiological impact or safety of a facility or activity is safety assessment.

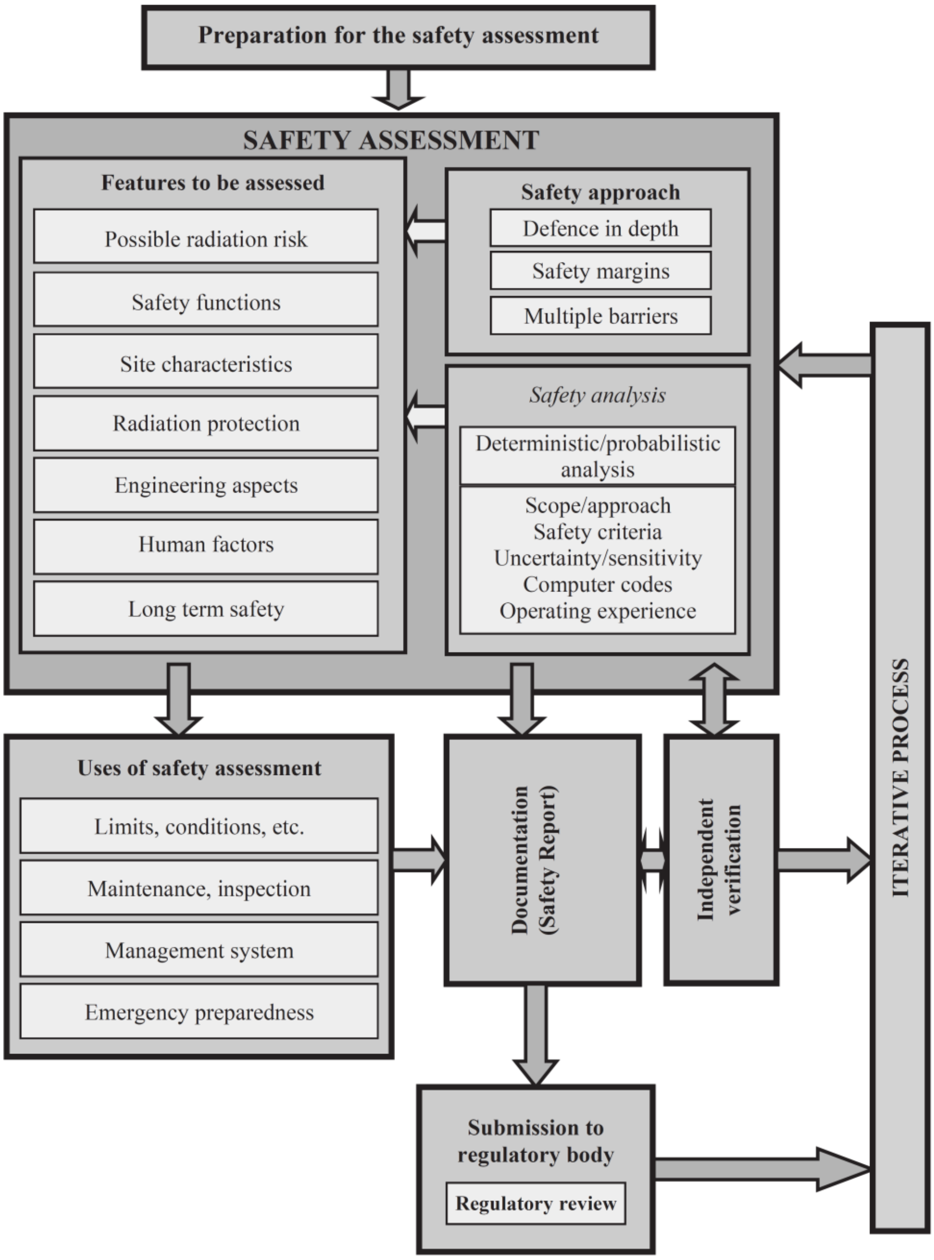


Figure 1-1 *Overview of the safety assessment process* **[4], p. 13**

Defence in depth, Safety margins and Multiple Barriers are the basic elements of the safety approach[5]. Deterministic and probabilistic analyses are the key components of the safety analysis.

The need for assessing the Defence in Depth is explicitly recognized by the GSR Part 4 (Requirement 13) which 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.*"

[5] The authors believe that multiple barriers and safety margin should be considered as integral parts of DiD.

The achievement of this objective is supported by further requirements (4.45-4.58) which can be merged and articulated into four complementary objectives defined as follows:

1) Adequacy of the implemented provisions

"4.45. It has to be determined in the assessment of Defence in Depth whether adequate provisions have been made at each of the levels of Defence in Depth to ensure that the legal person responsible for the facility can:

a) Address deviations from normal operation or, in the case of a repository, from its expected evolution in the long term;

b) Detect and terminate safety related deviations from normal operation or from its expected evolution in the long term, should deviations occur;

c) Control accidents within the limits established for the design;

d) Specify measures to mitigate the consequences of accidents that exceed design limits;

e) Mitigate radiation risks associated with possible releases of radioactive material."

2) Adequacy of the approach for the construction of the safety architecture

"4.46. The necessary layers of protection, including physical barriers to confine radioactive material at specific locations, and the necessary supporting administrative controls for achieving Defence in Depth have to be identified in the safety assessment. This includes identification of:

a. Safety functions that must be fulfilled;

b. Potential challenges to these safety functions;

c. Mechanisms that give rise to these challenges, and the necessary responses to them;

d. Provisions made to prevent these mechanisms from occurring;

e. Provisions made to identify or monitor deterioration caused by these mechanisms, if practicable;

f. Provisions for mitigating the consequences if the safety functions fail."

3) Compliance with the principles of the Defence in depth

"4.47. To determine whether Defence in Depth has been adequately implemented, it has to be determined in the safety assessment whether:

a. Priority has been given to: reducing the number of challenges to the integrity of layers of protection and physical barriers; preventing the failure or bypass of a barrier when challenged; preventing the failure of one barrier leading to the failure of another barrier; and preventing significant releases of radioactive material if failure of a barrier does occur;

b. The layers of protection and physical barriers are independent of each other as far as practicable;

c. Special attention has been paid to internal and external events that have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of safety systems;

d. Specific measures have been implemented to ensure reliability and effectiveness of the required levels of defence."

4) Availability of adequate margins to correctly address the uncertainties

"4.48. It has to be determined in the safety assessment whether there are adequate safety margins in the design and operation of the facility, or in the conduct of the activity in normal operation and in anticipated operational occurrences or accident conditions, such that there is a wide margin to failure of any structures, systems and components for any of the anticipated operational occurrences or any possible accident conditions. Safety margins are typically specified in codes and standards as well as by the regulatory body. It has to be determined in the safety assessment whether acceptance criteria for each aspect of the safety analysis are such that an adequate safety margin is ensured." Moreover, *"where practicable, the safety assessment shall confirm that there are adequate margins to avoid cliff edge effects that would have unacceptable consequences."*

1.2.2. Deterministic and probabilistic approaches for the assessment

Deterministic and Probabilistic analysis are recognized as the two complementary elements for the safety analysis. This complementarity is formulated by the GSR Part 4 [4]: "15. *Both deterministic and probabilistic approaches shall be included in the safety analysis*." The reference recognizes that "*deterministic and probabilistic approaches have been shown to complement one another and can be used together to provide input into an integrated decision making process."* Complementary insights, specific for their contributions are provided by the GSR Part 4:

- *"4.54. The aim of the deterministic approach is to specify and apply a set of conservative deterministic rules and requirements for the design and operation of facilities or for the planning and conduct of activities."*
- *"4.55. The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity, and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined."*

Coherently with the above indications, once principles, requirements, guidelines, objectives and safety options have been defined/selected, the full process (iterative as needed) for the design and the assessment of the installation (i.e. its retained[6] safety architecture), including the safety analysis[7], can be summarized as in Table 1-1. The table resumes - roughly - the crosscutting relationships between, on one side, the steps of the process for the design and assessment of the safety architecture and, on the other side, the expected contribution of deterministic and probabilistic approaches. Its content demonstrates the complementary role of the two approaches. Appendix 1 details the analysis with the support of the Gen IV- RSWG ISAM methodology [15].

[6] Typically, the designer selects among several options the design solution considered as "more pertinent" (e.g. "active" versus "passive" solution, "known" versus "innovative"). The selection is based on several criteria (not all related to safety, as result of an iterative process that ends on a "retained" architecture.
[7] As already indicated, according to GSR Part 4, "Safety analysis" is only a part of the "Safety assessment".

Table 1-1 *Relationships between the steps for the design and assessment of the SA and the role of the deterministic and probabilistic approaches*

Steps for the design and the assessment of the retained safety architecture ⮷	Deterministic	Probabilistic
Regulatory Framework (Goals, objectives, principles, requirements, guidelines)	✓	✓
Selection of Safety Options and provisional Provisions	✓	✓
1. *Compliance / consistency of the design options with the principles, requirements and guidelines*	✓	
2. *Identification, prioritization and correction (if feasible) of discrepancies between design options with the principles, requirements and guidelines,*	✓	
3. *Identification of challenges to the safety functions,*	✓	
4. *Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,*	✓	✓
5. *Selection and categorization of representative design extension conditions (without and with core melting; DEC A & DEC B with the WENRA terminology) to be considered for the design basis*[8]	✓	(✓)[9]
6. *Selection of external events that exceed the design basis and for which safety systems are designed to remain functional both during and after the external event*	✓	(✓)[9]
7. *Identification of plant event events or sequences that could result in high radiation doses or radioactive releases that must be practically eliminated*	✓	✓
8. *Identification and selection of needed provisions, implementation within the corresponding "layers of provisions" for the different levels of the DiD*	✓	
9. *Design and sizing of the provisions,*	✓	✓
10. *Response to DBE and DEC events (safety analysis),*	✓	✓
11. *Final assessment for a safety architecture that* shall meet the safety objectives and should be as far as reasonably possible[10]:		
○ *Exhaustive,*	✓	
○ *Progressive,*	✓	✓
○ *Tolerant,*	✓	✓
○ *Forgiving,*	✓	✓
○ *Balanced.*		✓

[8] The integration of Design Extension Conditions (DEC) within the design basis is consistent with the current requirements expressed by the IAEA SSR 2/1 [2] – Requirement 20.
[9] The contribution to this step is essentially deterministic even if it is recognized that probabilistic assessment can help, for example, for the identification of complex events / sequences which probability of occurrence justify their consideration for the design and / or for the categorization of the selected initiating events.
[10] See Section 2.3 for details concerning these objectives and their rationale / links with the IAEA Safety Standards.

Table 1-1 demonstrates the complementary role of the deterministic and probabilistic approaches, needed for:

- the identification of mechanisms (initiating events) and selection of significant (enveloping) plants conditions to be considered for the design basis[9];
- the selection and categorization of representative design extension conditions (without and with severe fuel damage conditions; DEC A & DEC B) to be considered for the design basis;
- the selection of external events that exceed the design basis and for which safety systems are designed to remain functional both during and after these events;
- the identification of plant events or sequences that could result in high radiation doses or large or early radioactive releases that must be practically eliminated;
- the design and sizing of the provisions;
- the analysis of the response to DBE and DEC events (safety analysis);
- the verification of the progressive, tolerant and forgiving, character of the safety architecture.

The specific key role of the deterministic approach includes the verification of the compliance / consistency of the design options with the principles, requirements and guidelines for the identification, prioritization and correction (if feasible) of discrepancies (if any), the identification of challenges to the safety functions, the identification and selection of needed provisions and their implementation within the corresponding levels of the DiD, and the support to the exhaustiveness in the coverage of "unexpected" plant conditions.

The assessment of the balanced character of the safety architecture is specific to the probabilistic assessment, which allows identifying the presence (to be avoided) of excessive or significant uncertain contributors to risk. Additional contributions that the PSA – if appropriately developed – can provide to the assessment of the implemented safety architecture, are introduced in the following sections.

1.3. THE ASSESSMENT OF DEFENSE IN DEPTH WITH THE PSA

Section 1.2 underlines that deterministic and probabilistic approaches, as they are implemented today, are complementary within the whole context of the design and the assessment of the safety architecture.

The same section points out that for the DiD assessment there is the fundamental need to determine "*whether adequate provisions have been made at each of the levels of Defence in Depth*". The achievement of this objective is articulated into four complementary objectives relevant to (i) the Adequacy of the implemented provisions, (ii) the Adequacy of the approach for the construction of the safety architecture, (iii) the Compliance with the principles of the Defence in depth and (iv) the Availability of adequate margins to correctly address the uncertainties.

The need for checking the "adequacy", the "compliance", and the "existence of adequate margins" generates the necessity for intermediate steps which should create the conditions for the analysis.

Coherently with this objective, the Figure 1-2 presents the whole process for the assessment of the DiD (i.e. for the assessment of the Safety architecture implementing DiD) which is articulated in four main steps relevant to:

- the definition of safety objectives, both quantitative and qualitative;
- the identification and recognition of all loads and environmental conditions that may affect the operation of the installation;
- the representation, as comprehensive as practicable, of the safety architecture in a manner that shall be consistent with the principles of Defense in Depth[11] and useful (and complemented) by PSA[12];
- the evaluation of the effectiveness of DiD levels, i.e. their physical efficiency and reliability.

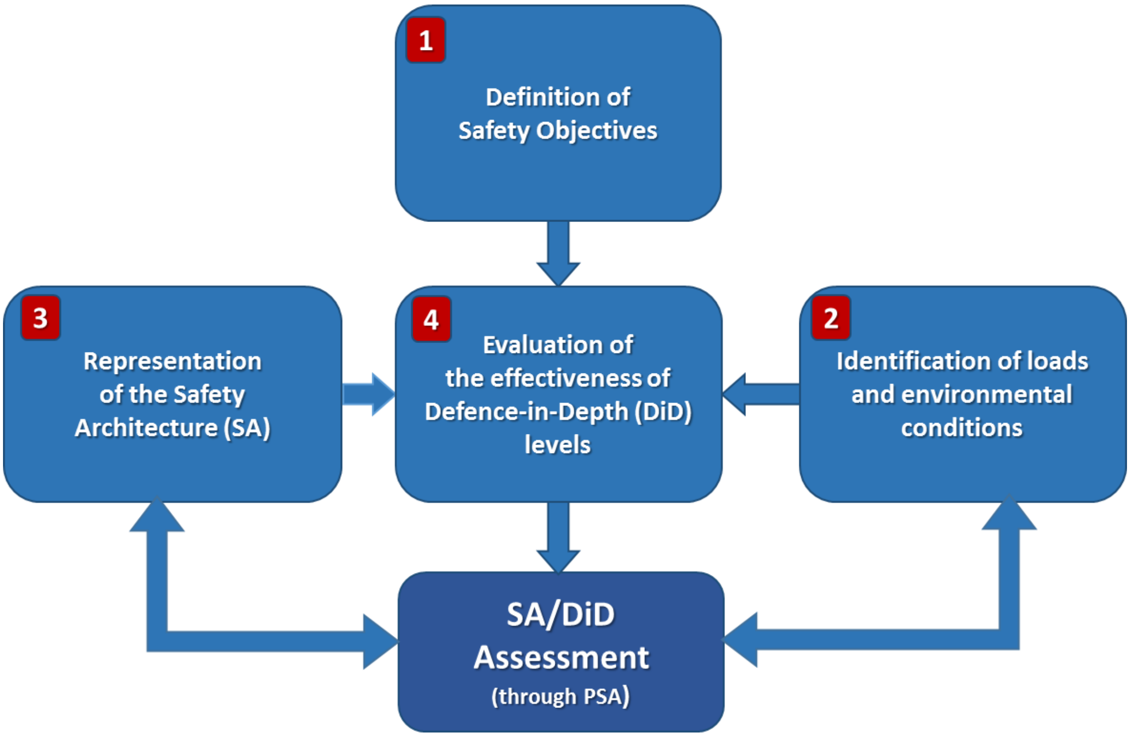


Figure 1-2 *Process for the PSA assessment of Defense in Depth*

The following sections – from 2 to 5 – provide details on each of the four steps of the process. Section 6 presents and discusses the final step with the practical assessment of the safety architecture, and the corresponding, DiD with the support of the PSA.

Some specific remarks on existing reactors and PSA are provided in the Section 7.

Conclusions are summarized in the Section 8.

[11] Different independent levels, functionally redundant and with a clear identification of relevant provisions.
[12] The basic idea is to achieve a representation of the safety architecture that allows answering the questions: what is doing what during the management of an abnormal / accidental condition? Are Did levels (i.e. the layers of provisions for each initiating event) correctly identified, designed/sized and implemented? Are DiD principles, e.g. the independence between the layers of provisions, adequately guaranteed?

2. DEFINITION OF SAFETY OBJECTIVES

2.1. DETERMINISTIC APPROACH AND RELEVANT OBJECTIVES

For nuclear installations in general and for reactors in particular, to fit with the principle of the DiD, the implemented “layers of overlapped provisions” (INSAG 10, [11]), should ensure, both for normal operation of the system, as well as for postulated incidents and accidents, the achievement of the three basic 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 (NSSR 2/1 [3]).

The nuclear safety analysis aims at showing that the implemented provisions are sufficient to ensure compliance with Safety Objectives proposed by the designer and endorsed by the safety authority. This analysis, conventionally "deterministic", is based on a set of initiating events (plant conditions) that are categorized considering their estimated frequency of occurrence (e.g. cat. I to IV) and taken as references for the design basis, for the different possible states of the system (normal operation, shutdown, maintenance, etc.).

In addition to these “design basis” studies, the compliance with the DiD principles requires on one hand to take into account the possible lack of completeness in the deterministic analysis and, on the other hand, to demonstrate the potential for the prevention, control and mitigation of degraded conditions of the installation. To do this, the plant conditions of the facility, as defined above, are conventionally complemented with the consideration of 1) accident situations generated by multiple failures or total loss of redundant provisions without significant fuel degradation, 2) situations of severe accidents with significant fuel degradation (all these being considered as Design Extension Conditions – DEC) or initiating events induced by natural or human-made external hazards exceeding the design basis. Their analysis may lead to the design and the implementation of specific additional provisions and / or the adaptation of existing provisions to ensure that the corresponding safety objectives are met.

Finally, initiators, situations or sequences involving very energetic phenomena, whose consequences could not be mitigated by reasonable technical means and that could lead to large or early releases into the environment, should be identified and “practically eliminated” (see Section 2.4).

The deterministic approach, as described above, is consistent with the recommendations of WENRA for the design of new reactors[13] and, in particular, with the revised structure of the levels of Defense in Depth as shown within the Table 2-1 [13].

For each plant condition category (Associated Plant Conditions), WENRA defines the allowable “radiological consequences” and suggests an unambiguous correspondence between these categories (last column) and the levels of DiD (first column).

[13] If an updating work has to be engaged for the existing NPPs (in operation or in construction), it is reasonable to consider these indications to be followed as better as possible (at least as guidelines).

Table 2-1 WENRA RHWG Proposed revision of the level of DiD[14,15]

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)	-

[14] It may be noted that, within Table 2-1, the level 3a (DiD level 3a - Postulated Single Initiating Events) covers the categories III and IV of the "design basis" (i.e.: the conventional design).
[15] See [13] for detailed comments on the table.

2.2. QUANTITATIVE SAFETY OBJECTIVES

This section introduces some basic concepts through which the assessment of the safety architecture can be engaged with quantitative safety objectives.

2.2.1. The Risk Space

The allowable radiological consequences as defined within the Table 2-1 are – generally speaking - represented by an acceptable domain within the "risk space". Figure 2-1 provides the "Generic F-C Curve, with ALARA region" as reported in the NUREG 2150 [10][16]. The boundaries of this domain are defined by pairs "frequency of occurrence - consequences" (Farmer curve) which allow defining the risk profile[17]. The ALARA concept is added as a systematic and essential complement (cf. Figure 2-1).

NB: *The box "Situations practically eliminated" has been added by the authors to the Figure of* [10][18].

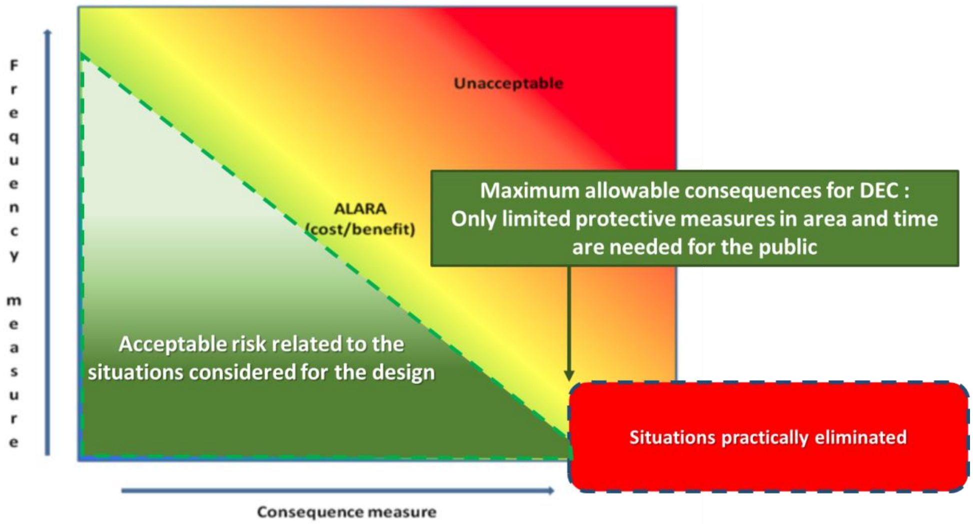


Figure 2-1 ***Risk space, NUREG 2150*** [10]

[16] *"The development and use of the F-C curve similar is perceived by some as a dramatic departure from past practices, but many programs already incorporate aspects of the approach by differentiating between high frequency-low consequence activities and the potential for low frequency-high consequence accidents. In the analyses to support licensing of nuclear power reactors, events have traditionally been defined within the categories of (1) normal operation, (2) anticipated operational occurrences, (3) design-basis accidents, and (4) beyond-design-basis accidents. The primary criteria for placing scenarios within the above categories are related to event frequencies. The allowable consequences (defined in terms of degree of fuel damage) are defined for the categories, and generally more damage is acceptable for scenarios with lower frequencies." [10].*

[17] The figure has a purely conceptual interest; e.g. for the decision maker (designer – regulator) the curve may not necessarily be iso-risk.

[18] The term "Residual risk" is intentionally avoided because no unequivocal definition exists. The term is not defined within the IAEA glossary [1]. Following the IRSN [27] two qualitative "Residual risks" should be considered: *Environmental residual risk: Risk remaining after the reduction in exposure provided by the collective protection equipment; Individual residual risk: Risk remaining after the reduction in exposure provided by the individual protection provisions.* Consistently, following the European Nuclear Society [27], the Residual risk is defined as the "*Remaining risk which cannot be defined in more detail after elimination or inclusion of all conceivable quantified risks in a risk consideration*"; according to this definition, the practical elimination coincides with the rejection into the residual risk. From a quite different perspective, IAEA [29] defines the Residual risk as *the risk which remains despite provisions made to prevent accidents and, if an accident occurs, to minimize the consequences*; according to this definition, roughly speaking, the Residual risk is conceptually the same as the risk accepted for the facility.

Conventionally, several metrics are associated with the risk space typically in terms of frequency related to a defined scenario, e.g.: Frequency of occurrence for the postulated initiating event (PIE); Core damage and fuel damage frequency; Large release and/or early release frequency(ies) (and other release frequency measures). For each initiating event and corresponding sequence, whose consequences are potentially unallowable and are positioned on the risk space, some "conditional metrics" can be defined: Conditional Core Damage Probability (CCDP); Conditional Fuel Damage Probability (CFDP), Conditional Large Release Probability (CLRP), and conditional Early Release Probability (CERP)[19].

Some probabilistic targets are introduced in Section 2.2.2, in order to provide quantitative orders of magnitudes which are needed for the assessment. Following the authors, these targets have to be complemented (without modifying the principle for an acceptable region) with criteria and metrics that translate the requirements and recommendations stated by IAEA and WENRA:

- "*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. .... The independent effectiveness of the different levels of defence is a necessary element of Defence in Depth*." [2];
- in case of severe accidents the consequences shall be consistent with the objective that "*only protective measures that are limited in terms of times and areas of application would be necessary and that off-site contamination would be avoided or minimized*"[20];
- sequences that could result in unacceptable radioactive consequences releases shall be practically eliminated;
- a complementary key notion, which is also critical vis-à-vis the safety objectives and must be taken into account, is that of "*cliff edge effects*"[21] with the "*sufficient margin*" (or *adequate margins*) which must be guaranteed for the sequences which have the potential to trigger these unacceptable effects.

Complementary qualitative safety objectives, related to the notion of robustness, exhaustiveness, progressiveness, as well as tolerant, forgiving and balanced characters, are introduced in §2.3.

Indications on how to manage all the above criteria are provided in §2.4.

---

[19] The availability of these data can, for example, provide insights to the designer to decide if it is better to work on the "upstream" frequency of occurrence of the initiating event or, if it is more interesting to strength the reliability of the architectures (i.e. the different layers of provisions" which are implemented to manage the sequence).

[20] WENRA Objective O3 [13]: ...."*for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures*".

[21] "*A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behavior caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.*" [3]

2.2.2. Probabilistic targets

The prevention of severe accidents

To compensate for the possible lack of completeness in identifying situations considered for the design, in line with the principles of DiD, the designer is requested to conventionally consider plant degradations which mobilize, inside the containment, source terms for which a release outside of the facility would be unacceptable. These situations (generally termed “severe accident”) correspond to that identified with the term "postulated core melt accident" in the Table 2-1.

From a probabilistic point of view, discussing about orders of magnitude, as indicated in the INSAG-12 [11], the objective is a frequency of severe damage to the plant (e.g. core melting) lower than ~ 10^{-5}/reactor year (CDF, equivalent PSA level 1) all initiators considered and combined[22]. This objective shall be correlated with a further reduction of a factor 10 – (10^{-5} > 10^{-6} reactor year)[23] usually endorsed by regulators -, for the unacceptable offsite consequences[24], all events considered and combined (equivalent PSA level 2). On a conceptual level, the containment, acting as a final barrier, provides the necessary order of magnitude to ensure compliance with 10^{-6}/reactor year for unacceptable consequences (10^{-5}/reactor year + containment failure or bypass ⇨ 10^{-6} / reactor year). These global objectives, even if simplified, are not directly usable for the design and need to be translated into practical intermediate goals that can guide the designer for the selection of adequate provisions and their implementation within the architecture of the entire plant and, at the same time, for the definition of the performance of these provisions, as required for the achievement of the safety functions. These intermediate objectives must also provide margins to cover the uncertainties correlated with the probabilistic approach.

The first of these objectives addresses the internal events, which in practice are the basis for the design of all the provisions of the safety architecture. It is therefore proposed to translate the need for improved margins retaining, for the prevention of severe accidents due to the internal initiating events (excluding hazards), an objective of about 10^{-6} per reactor per year. Assuming about ten to twelve independent families of initiating events, considered separately, this figure is reduced to about “10^{-7} per reactor per year per family of initiators”, all safety functions combined. This is the reliability which is requested for the whole set of actions implemented to manage a given initiating event, i.e. by the levels 1 to 3 of the DiD, to prevent severe accidents conditions.

[22] Cf. IAEA No. SSG-3 - Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants: *The objectives for core damage frequency suggested by INSAG12 are (a) 1 × 10^{-4} per reactor-year for existing plants and (b) 1 × 10^{-5} per reactor-year for future plants. It was not explicitly specified in INSAG for which scope of PSA the numerical values are applicable. It is assumed that a full scope PSA is meant.*

[23] Cf. INSAG 12: *Severe accident management and mitigation measures could reduce by a factor of at least ten the probability of large off-site releases requiring short term off-site response.*

[24] Note that, while the figure “10^{-6}/reactor year” does not change, it is the content of the notion of “*unacceptable consequences offsite*” that has been significantly reduced over the years. With the current recommendations the notion of unacceptable consequences offsite does correspond to the objective for having nothing more than (cf. WENRA) “*… limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures*”.

These actions for the control of safety functions, whose failure will lead to the severe accident configuration, are closely interconnected. In these conditions it is not feasible to deduce a specific probabilistic target for a specific safety function. However, the orders of magnitude are the same and the objective for the prevention of this failure can be considered as “fraction of “10^{-7} per reactor year, per family of initiators and per function”.

The management of Severe Accident with core degradation

In accordance with the indications set out in Table 2-1 (i.e. *Control of accidents with core melt to limit off-site releases*) and to guarantee the *Practical elimination of situation that could lead to early or large releases of radioactive materials*, it is necessary to consider the establishment of specific “layers of provisions” for the management of Severe Accident (more generically "conditions with plant degradation"). These layers materialize, for a given sequence, the 4th level of the DiD. The probabilistic targets for the whole sequence are those that are associated with unacceptable consequences, i.e. an order of magnitude over the prevention level: 10^{-6}/reactor year. This additional decade could be tentatively allocated to the reliability of the 4th level of the defense but in practice, given the indications post Fukushima, especially with the requirement for the practical elimination of sequences leading to large or early release, it is a higher reliability that should be guaranteed.

Natural hazards exceeding design basis conditions

The consideration of "*natural hazards exceeding those to be considered for design*" complements what is already done for severe accidents and, in these conditions, there is no reason to modify the probabilistic targets that are associated with unacceptable consequences. Similarly to what is done for Severe Accidents, and in accordance with the indications coming from the post Fukushima “Stress tests”, the designer must identify and implement specific provisions for the management of these situations ("Hardened Safety Core", [18])[25]. These provisions complement those provided for managing situations with core degradation / fuel damaged; they are implemented to ensure proper operation in the extremely degraded conditions and the designer must guarantee the level of their of physical efficiency and reliability (i.e. the capability to achieve the mission as requested).

Events, conditions or sequences practically eliminated

Finally, initiators, situations or sequences that lead to intolerable large or early releases in the environment, involving phenomena (e.g. very energetic) whose consequences could not be mitigated by of reasonable technical means, should be identified and "practically eliminated". To achieve this objective, the loss of provisions performing safety functions whose failure can cause these intolerable effects, should be significantly lower than 10^{-7}/reactor year[26], even if this "cut off value" cannot be used alone to justify the practical elimination (see Section 2.4).

[25] HSC indicates a limited number of material / organisational / human systems providing essential safety functions even in extreme circumstances, i.e. circumstances exceeding those adopted for the general design of the facility. This terms has been used according to the indications provided by the European Nuclear Safety Regulators Group, among the measures imposed after the accident at Fukushima Daiichi to reinforce the safety requirements for the prevention of natural risks, the management of loss of electrical power and cooling systems situations and for management of severe accidents.
[26] It is the overall probability of the sequence which, after the appearance of the initiator continues with the loss – in cascade – of provisions (i.e.: the different LOP implemented at different levels of DiD for the different

2.3. QUALITATIVE SAFETY OBJECTIVES

This section introduces additional objectives, defined qualitatively, to be considered in the assessment of the safety architecture in order to verify that it meets number of safety requirements stated in the SSR 2/1 [3].

Robustness

Among the qualitative objectives, the notion of "robustness" is systematically evoked both for the design and for the assessment of the safety architecture[27]. This notion cannot be reduced, but envelops, the request for "simplicity" of the safety architecture[28] and to the meeting of values / figures consistent with the quantitative safety objectives, even if these figures are extremely low. Obviously, the adequate consideration of uncertainty (either aleatory or epistemic) is essential to improve robustness but the way to achieve safety, which is strongly connected with the implemented Defense in Depth, is also a key contributor. This "way to achieve safety" can be defined qualitatively through corollary notions concerning the essential characteristics required to the safety architecture, namely: Exhaustiveness, Progressiveness, Tolerance, Forgiving and Balanced character. These notions are detailed in the following starting from the proposals formulated by the GIF/RSWG [16] and integrating them with indications aimed at reducing potential ambiguities. The reference to the relevant requirement specified in the SSR 2/1 [3] is provided for each one of them.

Exhaustiveness

<u>The exhaustiveness character of the safety architecture is representative of the capacity to manage a comprehensive set of postulated initiating events, being considered in the design and even those unexpected or unidentified.</u>

This qualitative objective is consistent with the SSR 2/1 [3] Requirement 16: *"The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design."*

---

safety functions) implemented to prevent, to control and manage and, to minimize the consequences of the initiating event.

[27] Within WENRA [13], the notion of robustness is evoked to meet several qualitative objectives:

- "For the DiD approach which is intended *to provide robust means to ensure the fulfilment of each of the fundamental safety functions*.
- To satisfy the basic safety expectations on *the independence between different levels of DiD for which a more robust demonstration of the independence between levels of DiD is requested*.
- For the analysis methodology, for which *adequate methods have to be utilized in order to show the robustness and reliability of the approach*.
- The *robustness of a plant's safety case* which is requested to support the practical elimination.
- A *robust design based on DiD with sizeable safety margins and diverse means for delivering fundamental safety functions as well as comprehensive operator response plans is required* to fully integrate the lessons Learnt from the Fukushima Dai-ichi accident.
- Finally *robust complementary safety features (DiD level 4) shall be specifically designed for fulfilling safety functions required in postulated core melt accidents."*

[28] Considering, for example, a given probabilistic objective for a given sequence, conventionally represented through an event tree - e.g. 10^{-9}/ry -, one can easily understand that the same figure can be obtained in different manners, i.e. nine independent steps/failures each characterized by an unreliability of 10^{-1}/demand or three independent steps/failures each with a reliability of 10^{-3}/demand. One can reasonably suppose that the demonstration will be more easy and robust for the second – more simple - safety case.

The identification of risks, based on challenges to the fundamental safety functions, should look for exhaustiveness. In parallel, the identification of the corresponding scenarios (i.e. the mechanisms and the corresponding provision's failures that materialize the challenges) to be retained to design and size the safety architecture provisions, must be as exhaustive as possible[29].

Among the strong motivations of the DiD, there is the objective to cover the potential lack of comprehensiveness in the identification of events. DiD, with all its principles, aims at supporting a robust demonstration about the acceptability of all "known" risk contributors (including "known" uncertainty), and at providing confidence that the adopted conservatisms allow enveloping the "unknown" ones.

Progressiveness character

<u>The Progressiveness character of the safety architecture is representative of 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.</u>

This qualitative objective is consistent with the IAEA Safety Fundamentals [2]: *"3.31 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."*

A progressive degradation of the safety architecture requires, firstly and consistently with the principles of DiD, the implementation of subsequent levels of protection, each with appropriate performances and reliability, which have to fail before that harmful effects could be caused to people or to the environment and, secondly, to have consequences that evolve, as much as possible, in a linear manner crossing these levels without risk for cliff edge effects (cf. Fig. 2.1).

Tolerant character

<u>The Tolerant character of the safety architecture is representative of the capacity to manage intrinsically variations in the operating conditions of the plant, i.e. avoiding that small deviations of the physical parameters outside the expected ranges lead to significant consequences.</u>

This qualitative objective is consistent with the requirement 5.8 *in the* IAEA SSR 2/1 [3]: *"The expected behavior of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority: (1) A postulated initiating event would produce no safety significant effects …"*.

A Tolerant response of the system is allowed by appropriate design requirements aimed at ensuring the required efficiency, reliability and margins (i.e. conservative design) of material and immaterial provisions which achieve

[29] The requirement for exhaustiveness is not formulated in the same way for proven technology of reactors or for new concepts: for the first, it is essentially the feedback experience that ensures completeness; for the latter it is the requirement of making a Phenomena Identification and Ranking Table (PIRT study, see Appendix 1 – The ISAM methodology [15]) that will confirm the list of events and phenomena to be considered.

the safety functions (e.g. engineered safety features, inherent characteristics). The request for a *tolerant defense* includes the rejection of any risk for "cliff edge effects". The corresponding criteria are established in terms of allowable ranges around the normal operating conditions.

Forgiving character

The Forgiving character of the safety architecture guarantee the availability of a sufficient grace period and the possibility of repair during accidental situations; it is representative of 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.

This qualitative objective is consistent with the requirement 5.8 (1) stated *in the* IAEA SSR 2/1 [3]: "*The expected behavior of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority: (1) A postulated initiating event would produce …. only a change towards safe plant conditions by means of inherent characteristics of the plant; (2) Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems that are operating continuously in the state necessary to control the postulated initiating event; (3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event; (4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures.*"

Corresponding adequate grace delays have to be fixed by the designer and endorsed by the regulator.

Balanced character

The Balanced character of the safety architecture is representative of 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.

The requirement and the corresponding criteria shall be consistent with the requirement *5.76* stated *in the* IAEA *SSR 2/1*[3]: "*The design shall take due account of the probabilistic safety analysis …..(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of Defence in Depth are independent; …*".

Remark: if excessive unbalance is detected following a PSA study it could be a sign of unsuitable safety provisions; for instance Loss Of Offsite Power (LOOP) is often an important contribution to risk and can be a cause of unbalanced results; in that case, additional provisions are needed to reduce core melt frequency of that family event to the same level as other accident families. However, following the authors the notion of "balanced design" should not be considered as excessively mandatory and should be associated with that of "reasonably feasible".[30]

[30] E.g., if one considers the objective of 10^{-6}/yr for the prevention of Severe Accident as a result of all the families of internal initiators, and if the majority of these families are already largely beyond this value (e.g. 10^{-}

2.4. CRITERIA & METRICS

All the key-notions mentioned above should be reformulated by criteria and metrics that contribute to the assessment of the safety architecture through the evaluation of the results coming from the safety analyses. Some indications are provided in the following in order to support the definition of these criteria and metrics (which is an on-going activity, not fully addressed by this document), and to clarify the role of PSA in their assessment.

Off-site measures limited in times and areas

The "*limited protective measures in area and time …needed for the public and* (the) *sufficient time … available to implement … measures*" will be deterministically defined fixing acceptable amounts for the released source term and corresponding kinetics of release. WENRA [13] provides quantitative data about this goal (cf. §3.4 – *Position 4 - Provisions to mitigate core melt and radiological consequences*).

The table in Figure 2-2 provides the interpretation by WENRA (Position 4, [13]) of "limited protective measures". The tables define the acceptable conditions for Permanent relocation, Evacuation, Sheltering and Iodine prophylaxis applicable, as goals, in the design phase of new reactors.

Measure	**Evacuation zone**	**Sheltering zone**	**Beyond sheltering zone**
Permanent relocation	No	No	No
Evacuation	May be needed	No	No
Sheltering	May be needed	May be needed	No
Iodine Prophylaxis	May be needed	May be needed	No

Figure 2-2 Design goals for areas where limited protective measures may be needed [13]

The corresponding safety objectives, in terms of allowable amount and kinetic for the releases, shall be defined as a function of the site. PSA Level 1 and Level 2 play an essential role for the assessment.

Independence of DiD levels

The independence between the DiD levels is one of the key verification to be performed. This requires a comprehensive and appropriate representation of the safety architecture, in terms of provisions implemented for each initiating event and for each level of DiD. The objective is to ensure that the failure of a DiD level does not affect the efficiency and the performance of the next one(s).

7/yr), for those who remain in the range of the target, is not necessary to seek the same type of performance unless it is "reasonably practicable" i.e. without unreasonable efforts.

The Objection-Provision Tree (OPT) methodology and the complementary notion of Line of Protection (LOP), discussed in the Section 4, identify for each initiating event and each level of the defence the provisions implemented and allow identifying possible lack of independence between the DiD levels (e.g. overlapping of provisions on different levels) [31]. In this context, if correctly structured, the PSA can provide additional evidences of this independence by representing the concatenation between the failures of the different layers of provisions, and providing specific insights about plausible dependent failures, also accounting for external (natural or manmade) hazards.

Practical elimination of events and sequences

Following the IAEA NSSR 2/1 [3] and WENRA [13]: *The possibility of certain conditions arising*, whose consequences would be large or early release, *may be considered to have been "practically eliminated" if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise*[32]. For these conditions the safety demonstration is focused on the prevention.

The demonstration is quite easy for those physically impossible.

For those which need a demonstration *with a high level of confidence*, the strategy can be based on the analysis of the safety architecture. Some conditions can correspond to the failure of the 1st level of the defence (e.g. PWR vessel rupture; SFR core support collapse) and the demonstration will be essentially based on Quality Assurance for the design, the fabrication, the implementation and the operation (including the maintenance). Other conditions are the results of uncontrolled sequences, with the successive failure of the DiD levels and eventually that of the 4th level (e.g. PWR pressurized core melting; long term loss of the decay heat removal).

For these conditions, the corresponding layers of provisions implemented in order to prevent, manage and mitigate the sequence's consequences (including those of the Hardened Safety Core) shall be sized and implemented in order to provide the demonstration, *with a high level of confidence*, that their number and quality will be sufficient to avoid the loss of the whole set of DiD levels and, in particular, that of the 4th level of DiD[33].

---

[31] One can raise the question of the acceptability of an architecture in which a given provision would be used for different initiating events and / or at different levels of the DiD, i.e. the provision is part of LOPs allocated to different levels of the DiD, depending on the requesting initiating event. This should be possible and allowed if the events which require the provision under consideration are completely independent.

[32] Following WENRA [13], the "*high degree of confidence*" is translated into the following indications: *"The degree of substantiation provided for a practical elimination demonstration should take account of the assessed frequency of the situation to be eliminated and of the degree of confidence in the assessed. Appropriate sensitivity studies should be included to confirm that sufficient margin to cliff edge effects exist. …"*. The role of probabilistic criteria is established by a specific recommendation: *"Practical elimination of an accident sequence cannot be claimed solely based on compliance with a general cut-off probabilistic value. …"*. Conversely, the limitation of the role of probabilistic analysis is clearly stressed by this recommendation: *"The most stringent requirements regarding the demonstration of practical elimination should apply in the case of an event/phenomenon which has the potential to lead directly to a severe accident. …"*. Contributions of both deterministic (physical efficiency over the time) and probabilistic (reliability performances over the time) studies will support the fulfillment of this recommendation: *"It must be ensured that the practical elimination provisions remain in place and valid throughout the plant lifetime."*

[33] "(4) *The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of Defence in Depth. This is achieved by preventing the progression of such accident*

With the same logic, specific provisions are supposed to ensure adequate safety against extreme natural events, i.e. whose magnitude exceed those considered for design, including adequate margins against cliff edge effects. They are conventionally associated with the DiD level 3b for those that address multiple failures and contribute to the prevention of severe accident situations, and to the DiD level 4 for those devoted to the management of severe accident conditions (cf. Table 2.1).

Deterministic criteria and metrics have to be defined specifically for:

- events that could lead to prompt reactor core / fuel damage and consequent early containment failure, mainly translating Quality Assurance (QA) objectives, to guarantee the highly hypothetical character of the event; probabilistic studies will be implemented to check this QA implementation and to bring the proof of this very low frequency of occurrence;
- the triggering of unallowable phenomena, mainly through the knowledge and the mastering of uncertainty (e.g. with a PIRT analysis, see Appendix 1);
- the elimination of by-pass sequences, by the systematic review of all the containment penetrations and the definition of criteria/constraints on design, operation, maintenance and accident intervention procedures.

ALARA shall be systematic and upstream the practical elimination.

Coherently with the logic described above, the probability to lose the provisions which perform safety functions, and whose failure can cause to intolerable large or early releases in the environment, should be significantly lower than 10^{-7}/reactor year[34]. So far, this "cut off value" cannot be used alone to justify the practical elimination.

Demonstration of design against cliff edge effects

Again, following WENRA [13], *"The degree of substantiation provided for a practical elimination demonstration should take account of the assessed frequency of the situation to be eliminated and of the degree of confidence in the assessed. Appropriate sensitivity studies should be included to confirm that sufficient margin to cliff edge effects exist. …". This recommendation* introduces another key notion which must be taken into account: "*cliff edge effects*" with the "*sufficient margin*" (*adequate margins* with the IAEA SSR 2/1 [3] terminology)[35].

---

and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of times and areas of application would be necessary and that offsite contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be practically eliminated." [3]
In compliance with IAEA SSR-2/1 [3], the acceptance criteria associated to the success of the 4th level shall be defined to comply with the objective of generating the need for *limited protective measures in area and time*.

[34] It is the overall probability of the sequence which, after the appearance of the initiator, continues with the loss – in cascade – of provisions (i.e. materializing the different LOPs at different levels of DiD, for the different safety functions) implemented to prevent, to control and manage and, to minimize the consequences of the initiating event.

[35] As stressed by the IAEA TECDOC [4], adopting margins in the design of a NPP is a common practice to improve the robustness of the design and providing an effective mean to deal with uncertainties even if, on one side, the extension of the design basis with the introduction of DECs has introduced new elements that need to be addressed and, on the other side, the Fukushima Daiichi accident has reinforced the importance of the effects of external events. Generic insights on *Safety margins for design basis accidents* and *Safety margins for design extension conditions* are provided by the IAEA TECDOC [4]. The reference concludes in particular that there could be a substantial difference between the safety margins for design extension conditions without significant fuel degradation and those for design extension condition with core melt, essentially due to the larger uncertainties which are associated with these conditions.

The design against cliff edge effects and the need of adequate margins generate deterministic and probabilistic criteria.

For DEC conditions, deterministic criteria about the performance of provisions should allow facing, without abrupt transition, possible small variations of the plant parameters. Probabilistic criteria are defined, in terms of reliability targets, for the physical performances required for the provisions which are an integral component of the 4th level of the DiD, performances which allow guaranteeing "adequate margins".

Specifically about *natural hazards*, the requirement 5.21a in the SSR 2/1 [3] states that "*The design of the plant shall provide for an adequate margin to protect items ultimately necessary to prevent large or early radioactive releases in the event of levels of natural hazards exceeding those to be considered for design taking into account the site hazard evaluation*" [36]. This requirement affects the design and the margins that have to be guaranteed by the features implemented to mitigate severe accidents. It has the purpose to ensure that, if a severe accident occurs due to an external hazard, there are appropriate assurances that sufficient mitigation means remain available. The design of the corresponding provisions, which realize the 4th level of the DiD[37], is expected to be particularly robust and to include margins to withstand loads and conditions generated by the events exceeding those derived from the site evaluation and considered in the design. This implies that cliff edge effects should not occur not only for small variations in a plant parameter but also for significant variations of the loads and environmental conditions.

Characteristics required to the Safety architecture

Qualitative safety objectives have been introduced, discussed and motivated within the section 2.3. It is appropriate to provide indications about criteria that can be associated to these objectives and to clarify the role of PSA in the assessment of what is advocated in terms of exhaustiveness, progressiveness of the plant response, tolerance to possible alterations of plant conditions, forgiving reaction to abnormal conditions, and balanced contribution versus the whole risk. Insights are provided hereafter, complementing the information provided in Table 1-1 and within the section 2.3.

[36] Following WENRA [13]: "*Rare and severe external hazards are additional to the general design basis, and represent more challenging or less frequent events. This is a similar situation to that between Design Basis Conditions (DBC) and Design Extension Conditions (DEC); they need to be considered in the design but the analysis could be realistic rather than conservative.*"

[37] A specificity of external hazards is the possibility that subsequent level of Defence in Depth (e.g. 4th level) may be impaired before the previous one (e.g. 3rd level); this motivates the requirement and allows covering the possibility that external hazards may challenge levels of DiD without regard to their order.

Exhaustiveness character

The Exhaustiveness character of the safety architecture is addressed deterministically. PSA, if appropriately developed, takes care that the comprehensive set of postulated initiating events is introduced into the model as risk contributors.

Progressiveness character

Among the strong motivations of the DiD concept there is the objective to have a progressive degradation of the safety architecture before that harmful effects could be caused to people or to the environment. Progressiveness of the safety architecture for a specific initiating event is first addressed deterministically by checking the presence of all the needed DiD layers of provisions. PSA can complement the demonstration of the progressive character of the safety architecture, identifying the potential for "short" sequences and guaranteeing their practical elimination. Moreover, PSA - if appropriately developed – contributes to provide evidence of the implemented progressive defence, with the probabilistic assessment of the different intermediate states of the plants which correspond to the failures of the subsequent DiD levels (see Section 6).

Tolerant character

The criteria to assess the Tolerant character of the safety architecture could be established mainly in terms of allowable ranges of operation around the normal operating conditions. Probabilistic studies can contribute to the verification of the Tolerant character of the safety architecture mainly by questioning the margins allowable for the correct behaviour of material (e.g. engineered systems) and immaterial (e.g. inherent characteristics) provisions, and by addressing uncertainty on input data and its propagation through the model.

Forgiving character

PSA, if appropriately developed, can contribute to the demonstration of the Forgiving character of the safety architecture through the probabilistic representation of the chronology and the kinetic of the plausible degradations of the safety architecture. Specific chronology criteria refer to the priority in the operation of different means required to achieve safe conditions (inherent characteristics of the plant, passive systems or systems operating continuously in the necessary state, systems that need to be brought into operation, procedures). Kinetics allows assessing the availability of sufficient grace period for their implementation.

Balanced character

PSA is essential for the assessment of the balanced character of the safety architecture since it allows evaluating the contribution to the whole risk of each specific events and sequences.

One of the principal activities within a risk-informed regulatory process is the ranking of structures, systems and components (SSCs) with respect to their contributions to the (primary) risk measure. This can be done by secondary risk measures, computed through Importance and Sensitivity analysis[38].

Importance measures allow identifying the more important risk contributors, while Sensitivity indices allow identifying the more significant uncertainties which affect the risk. Different importance measures are traditionally used to rank SSCs[39]. They can be classified in risk-significance (if related to the role that the SSC plays in the measures of risk) and safety-significance (if related to the role that the SSC plays in the prevention of the occurrence of an undesired end state) importance measures[40].

[38] Importance and Sensitivity analyses aim at quantifying the contribution of the input variables to the model output (Importance analysis) and to the related uncertainty (Sensitivity analysis).

[39] The aforementioned “traditional” importance measures are “local” ones. (i.e. they deal with a point value of the model output and input variables (basic events or parameters) and cannot be used for finite changes of the input variables or, in this case, they do not include the contributions of non-linear terms. Moreover, they are not “additive”. Further approaches are recently proposed for “Global” Importance and sensitivity analysis (i.e. focused on uncertainty on the model output with reference to the entire range of values of the input variables). See for details the Deliverable D30.5 “Risk Metrics and Measures for an Extended PSA” [25].

[40] They include, for instance, the (safety-significant) “Risk Achievement Worth” (RAW) and the (risk- significant) “Fussell-Vesely” measure (FV). RAW measures the “worth” of the component in achieving the risk level, by considering the maximum increase achievable when the component is always failed. FV is the probability (at a given time) that at least one “minimal cut set” that contains the component is failed (i.e. all components in the minimal cut set are failed), given that the system is failed (at that time).

3. THE IDENTIFICATION OF PLAUSIBLE LOADS AND ENVIRONMENTAL CONDITIONS

The identification and recognition of all plausible[41] normal and off-normal loads and environmental conditions that can affect the behavior of the installation is correlated with the identification of all plausible events which can happen; this identification is the result of a detailed analysis of the system complemented, as needed, by the consideration of the experience feedback.

Once the identification is complete, a step of grouping in a limited number of families, characterized by similar causes and responses, is performed. For each family, event(s) which may reasonably be considered – in terms of consequences – as envelope of all others, are retained as Postulated Initiating Event (PIE) and are used to select and design the facility's provisions, i.e. the safety architecture.

The process is obviously iterative since the implementation of provisions for preventing, managing and / or mitigating abnormal situations can, itself, generate potential accident situations and / or introduce additional hazards whose consequences are not necessarily mitigated by measures already considered[42].

The list of PIE shall be complemented by the consideration of internal and external hazards. The methodology for selecting initiating events and hazards for consideration in an Extended PSA, and specifically the screening approach used to select the External Hazards to be analyzed is addressed in a dedicated ASMAPSA_E deliverable (D30.3, [25]).

Figure 3-1 and Figure 3-2 [17] resumes the evolution of the key elements for the design basis since the requirements of the year 2000 until those, updated, as introduced by IAEA [3] or WENRA [13]. Both references clearly place the conditions generated by internal and external hazards among the design basis[43].

---

[41] "Plausible" is all what it is not "physically impossible".

[42] For example, in standard PWRs the presence of boron in the primary circuit is a provision to help the "Control of chain reactions". It must appear from the provisions listed in the OPT PWR, for example within the first level of DiD. But the implementation of this provision introduces the risk of boron dilution and an initiator raise: the "plug of clear water" directly generated by the provision. Additional provisions are expected to address this specific risk (at the second and third level DiD).

[43] E.g. this is consistent with the WENRA indication: "*For new reactors external hazards should be considered as an integral part of the design and the level of detail and analysis provided should be proportionate to the contribution to the overall risk.*"

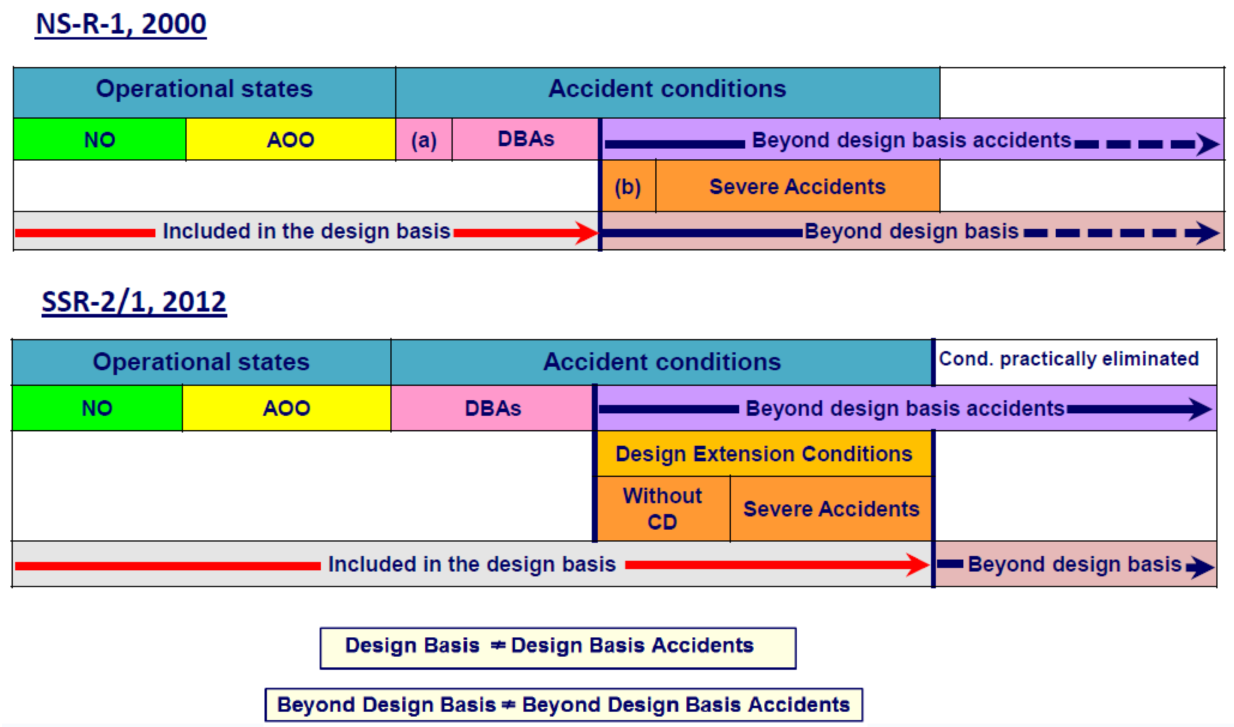


Figure 3-1 Plants states categorization following the IAEA requirements in 2000 and 2012

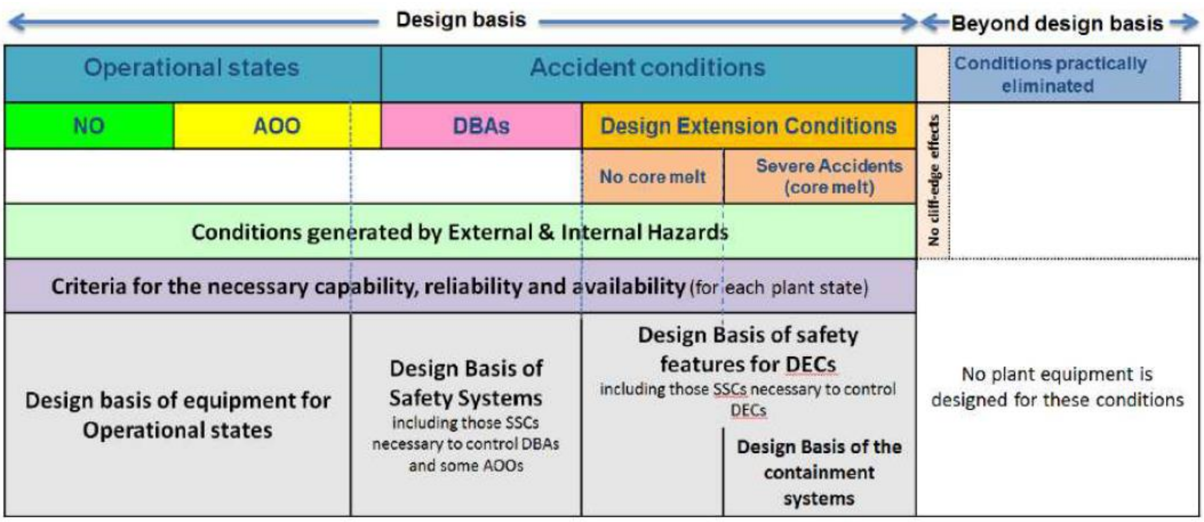


Figure 3-2 Plants states categorization following the updated IAEA requirements in 2016

The initiating events, once identified, are categorized following their estimated frequency of occurrence. For each category, quantitative safety objectives are usually suggested by the designer and endorsed by the regulators; this allows defining the space of acceptable risk (see Section 2.2.1).

This categorization allows assigning the PIE, in a conventional manner, to the various categories: Anticipated Operational Occurrences, Design Basis Events and Design Extension Conditions. According to Figure 3-3, which is composed by contributions from WENRA [13] & NUREG 2150 [10], this categorization can be related with correspondent levels of DiD and their positioning within the risk space (see Section 2.2.1).

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)	-

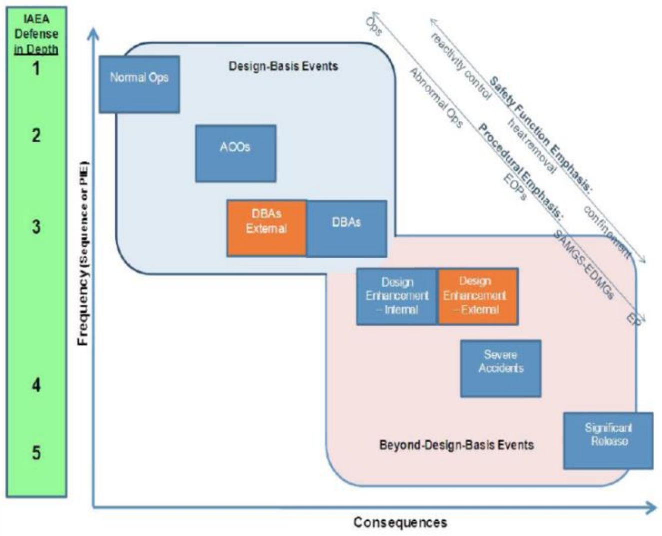


Figure 3-3 Categorization of the PIE and correspondence with the level of the DiD

All PIE are characterized by thermal, hydraulic & mechanical loads and specific environmental conditions. These loads and the environmental conditions shall be taken into account to select and size the provisions to be implemented within the safety architecture.

It is worth noting that the considerations developed in the present document for the assessment of the whole "safety architecture", i.e. the assessment of successive layers of provisions with their physical efficiency and reliability, should be considered to complement the process described by the SSG-30 Safety Guide [6] for the classification of System, Structures and Components[44].

[44] The objective of the SSG-30 [6] is "to provide recommendations and guidance on how to meet the requirements established in the SSR 2/1 [3] and IAEA GSR Part 4 [4] 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 IAEA SSR-2/1. "*All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance*." 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".
According to the SSG-30, the method for classifying the safety significance of items important to safety 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. The reliability required to the SSCs in order to meet the applicable safety objectives by the implemented safety architecture is a further key issue to be considered.

4. SAFETY ARCHITECTURE REPRESENTATION

Around the “reactor process”, whose design and performances are defined to fulfil the basic requirements (power level, ranges of operating temperatures, efficiency, potential for fissile creation, potential for waste management, etc.), a safety related architecture is build up to insure the operability, the availability, and the safety of the system. As already indicated, the safety architecture is a complex set of material (active and / or passive systems and components) and immaterial provisions (intrinsic characteristics, procedures).

The system's response to each abnormal event is specific in the sense that it is achieved by organizing, manually or automatically, a subset of provisions to manage the corresponding mechanisms which challenge the safety function(s) and, finally, to meet the safety objectives. For a given abnormal event, in the logic of Defense in Depth, this subset corresponds to the notion of "layer of provisions" (LOP); if the implementation of the defense is correctly done, the safety architecture should address any possible deficiencies/failures, partial or total, of an LOP through the intervention of another "layer of provisions", functionally redundant, allowing to ensure the achievement of the required mission.

Defense in Depth is so organized into successive levels whose role is defined conventionally (see Figure 3-3): Prevention of any abnormal plant condition (level 1), Detection of all abnormal situations and Control of Anticipated Operational Occurrences (AOO) (level 2), Protection against accidental situations, limitation of their consequences and, more generally, prevention of severe accidents situations (level 3a and 3b), Management of severe accident situations and mitigation of their consequences (level 4).

For each plausible condition, among those that may affect the operation of the installation, the representation of the safety architecture shall allow identifying the contents of each of these levels; their assessment shall be specific to the condition under examination. The overall evaluation of the system is the integral of these singular evaluations; this approach allows identifying any weaknesses among the range of the safety architecture responses.

The Objection-Provision Tree (OPT) methodology and the concept of Line Of Protection (LOP), both described hereafter (Sections 4.1 & 4.2) implement this logic for the representation of the safety architecture while remaining fully consistent with the safety assessment process presented by the IAEA GSR Part 4 [4].

4.1. THE OBJECTIVE PROVISION TREE

The Objection-Provision Tree (OPT) methodology is suggested by the Generation IV Risk and Safety Working Group (GIF/RSWG), as part of the Integrated Safety Assessment Methodology (see Appendix 1 – The ISAM methodology [15]), to complement the traditional deterministic and probabilistic safety assessments.

OPT - see IAEA TECDOC 1366 [8] and IAEA Safety report 46 [9] - allow a standardized representation of the safety architecture by identifying the different levels of Defense in Depth and the corresponding “layers of provision”. The references [22], [23], and [24][45] show the results of recent activities on the OPT methodology and its possible use.

The logic of the OPT lies on the systematic identification, for a given level of DiD and for given “safety functions” (SF), of the plausible “challenges” to this SF; for each of these challenges, the methodology identifies the corresponding relevant “mechanisms and phenomena” to be prevented or controlled by a set of “provisions” which are designed and implemented to meet specific acceptance criteria[46] and to maintain or to bring the plant to controlled or safe states, meeting the safety objectives.

Conventionally, for a given DiD level, the objectives corresponding to a given SF are translated into physical parameters or “decoupling criteria”[47] that reflect the allowable consequences associated with the level under consideration.

---

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

[46] The approach adopted by OPT is fully consistent with the IAEA GSR Part 4: *“4.46. The necessary layers of protection, including physical barriers to confine radioactive material at specific locations, and the necessary supporting administrative controls for achieving Defence in Depth have to be identified in the safety assessment. This includes identification of: (a) Safety functions that must be fulfilled; (b) Potential challenges to these safety functions; (c) Mechanisms that give rise to these challenges, and the necessary responses to them; (d) Provisions made to prevent these mechanisms from occurring; (e) Provisions made to identify or monitor deterioration caused by these mechanisms, if practicable; (f) Provisions for mitigating the consequences if the safety functions fail.”* [4]

[47] *Decoupling Criteria*

The decoupling criteria are deterministic and are used to assess the physical performances of the architecture. Decoupling criteria are physical parameters (e.g. number of clad failures) which make the link between the safety objectives, which are formulated in quite generic manner (e.g. health consequences ⇨ corresponding releases), and quantitative and measurable objectives or acceptance criteria (e.g. maximum clad temperature) which are usable by the designer to check the acceptability of the design. Moreover, through the assessment process, they allow defining measurable safety margins.

As a matter of example, the following decoupling criteria are conventionally used in the safety analysis of LWR: The Departure of Nucleate Boiling ratio (DNBR; >1) to guarantee the avoidance of the fuel clad failure; the fraction of fuel rods experiencing DNB during accident conditions (e.g. < 10%); Specific decoupling criteria are defined for the LOCA conditions, they address : the peak cladding temperature (e.g. 1204°C), the maximum percentage of oxidized cladding thickness (e.g. <17%); the maximum hydrogen generation amount (e.g. <1%); the core geometry that shall remain coolable; the fact that long term core cooling shall be ensured, etc.

Analogous definitions can be found within the IAEA terminology. The terms decoupling criteria is consistent with the notion of “acceptance criteria” defined, as follow, within the IAEA glossary [1]: “*Specified bounds on the value of a “functional indicator” or “condition indicator” used to assess the ability of a structure, system or component to perform its design function.”* The term is nevertheless more generic, including also the notion of “*performance indicator*”, where according to the IAEA glossary [1]:

So, for each safety function, representative parameters can be identified with associated values/figures that reflect compliance with safety objectives.

For the SF under consideration, the partial or total failure of an LOP means the failure of the DiD level. This failure leads to complementary conditions, in terms for example of specific boundary conditions (e.g. temperature, pressure, humidity) that have, in turn, to be considered for the design of the successive LOPS.

Figure 4-1 ([15] and [16]) shows the iterative process for the implementation of the safety architecture by the identification of the contents of all levels of DiD (left side of the figure) and the standard structure of the OPT (right side of the figure).

The OPT can be used to check that:

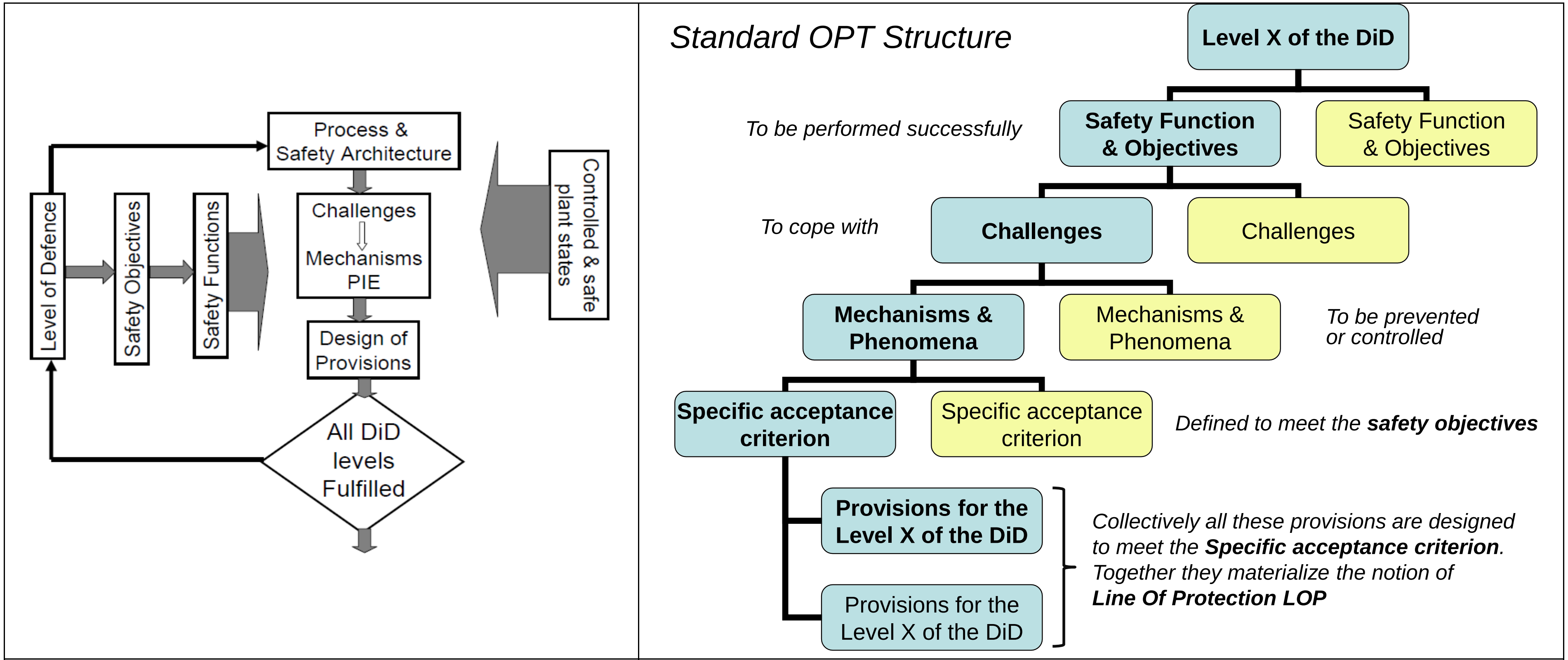
- all the initiators are adequately addressed;
- all levels of DiD are properly structured and organized (i.e. the necessary provisions are in place and are sufficient) to achieve the required missions;
- the mutual independence of the levels of DiD is guaranteed.

According to this last point, coherently with the principles of the DiD, the provisions associated with each level must be independent and, if possible, diversified from those allocated to the other levels of DiD[48].

The benefits from the implementation of OPT are even stronger when it is considered within the whole context of interaction with the other ISAM tools and, specifically, with the PSA for which the OPT represents an essential input in terms of presentation of the whole safety architecture which, once available, is analytically described and assessed by the PSA.

- *"a Condition indicator is a characteristic of a structure, system or component that can be observed, measured or trended to infer or directly indicate the current and future ability of the structure, system or component to function within acceptance criteria."*
- *"a Functional indicator is a condition indicator that is a direct indication of the current ability of a structure, system or component to function within acceptance criteria."*;
- *"a Performance indicator is a characteristic of a process that can be observed, measured or trended to infer or directly indicate the current and future performance of the process, with particular emphasis on satisfactory performance for safety."*

[48] As already indicated, one can raise the question of the acceptability of an architecture in which a given provision would be used for different initiating events and / or at different levels of the DiD, i.e. the provision is part of LOPs allocated to different levels of the DiD, depending on the requesting initiating event. This should be possible and allowed if the events which require the provision under consideration are completely independent.



a - Iterative process for the construction of the safety architecture

b - Standard OPT Structure

Figure 4-1 Process for the implementation of the whole safety architecture and Standard OPT structure

4.2. THE LINE OF PROTECTION METHODOLOGY

Once the probabilistic targets are defined, before the formal assessment through the PSA, it is possible to roughly sketch the safety architecture's characteristics with the Line of Defence (LOD) or Line of Protection (LOP) methodology.

The methodology, which was originally proposed as LOD ([19] and [20]) with, in particular, the notions of strong (noted « a ») and medium (noted « b ») lines of defense[49], evolved within the context of IAEA activities and GIF/ RSWG ([15] and [16]), to better consider the nature of the safety related provisions implemented within the innovative concepts (e.g. the passive systems, inherent characteristics, procedures, etc.). While the LOD method focused on engineered safety systems and without specific relationship with the defence in depth, the concept of LOP embraces the notion of "layers of provisions" as defined by the IAEA Safety Fundamentals, integrating all the possible contributions to achieve safety, i.e. material and immaterial provisions, with a direct correspondence with the DiD level, allowing a more comprehensive representation of the safety architecture[50].

The notion of LOP is an integral component of the Objective provision tree (see Figure 4-1 right side).

The LOP methodology can be used as a guide for the rough verification of compliance with the quantitative probabilistic objectives. The goal is to verify the implementation, for each plausible situation and for all possible pathways toward the severe accident, of a succession of LOPs with adequate reliability. The counting of these lines ensures that the probabilistic targets are met, and ensures that the overall risk associated with the sequence "initial plant condition + possible failure of LOP" is acceptable.

The LOP methodology is based on the adoption of the following rule: … Given a plant condition resulting from an initiating event applied to a given initial state of the installation. … Given a safety function, whose control is requested by the initiating event under examination, the failure[51] of which will lead to potential consequences larger than that allowed in the category of the plant condition… In this situation there is a potential for a release higher than that allowable and therefore for a risk not tolerable. For each plant condition taken into account for the design, and for each safety function that meets the above criteria, the designer shall identify the number and quality of LOP to be implemented in order to meet the objectives of the function, i.e. to ensures that the overall risk associated with the sequence "initial plant condition + possible failure of LOP" remain acceptable.

---

[49] The strong line of defence (a) corresponds to a LOD designed to meet high reliability performances (e.g. safety classified system, designed considering the single failure criterion). Its probability of failure can vary within a range of 10^{-3} to 10^{-4} per year or per demand.
The medium line of defence (b), does not meet the same design or implementation requirements (e.g.: less safety margins than the LOD "a") and it shows a lower reliability (e.g.: operator actions, etc.). Its probability of failure can vary within a range of 10^{-1} to 10^{-2} per year or per demand.
[50] A recent application of LOD/LOP notion is done for the ASTRID project [21].
[51] Failure at the solicitation or at short or long term

Figure 4-2 shows schematically the logic of the methodology, as defined in the '90ies, including the line requested for the management of the severe accident conditions and the rejection of the failure of the 4th level of the DiD into the Residual Risk. The figure also provides the representation of the different area covered by the different levels of DiD.

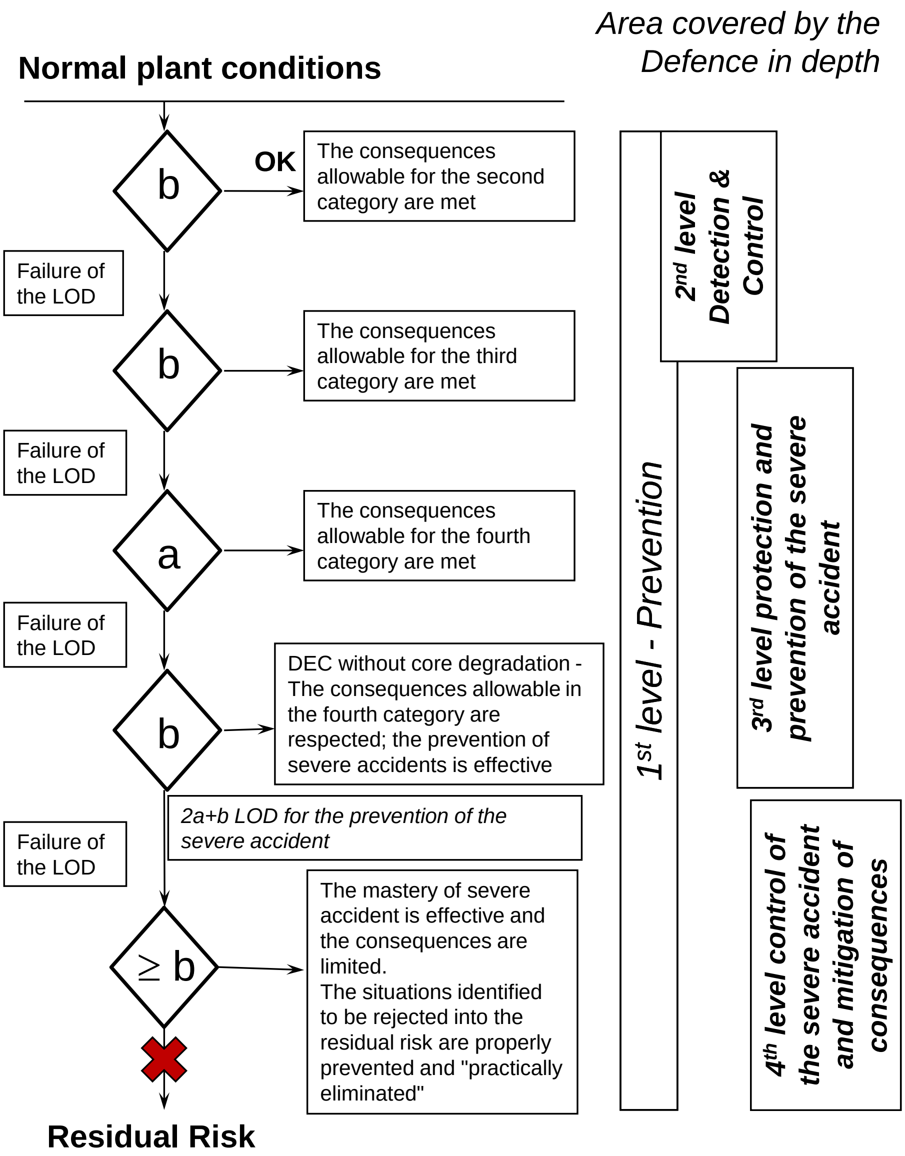


Figure 4-2 Principles for the Lines of Defense methodology

Figure 4-3 shows the same logic for the concatenation of the different levels of the DiD, as suggested recently by WENRA [14] including the very last indications for the integration of the external hazards (i.e. the integration of the post Fukushima studies). The WENRA scheme is completed with indication of the different areas covered by the different levels of DiD, according to Figure 3-3 (right side).

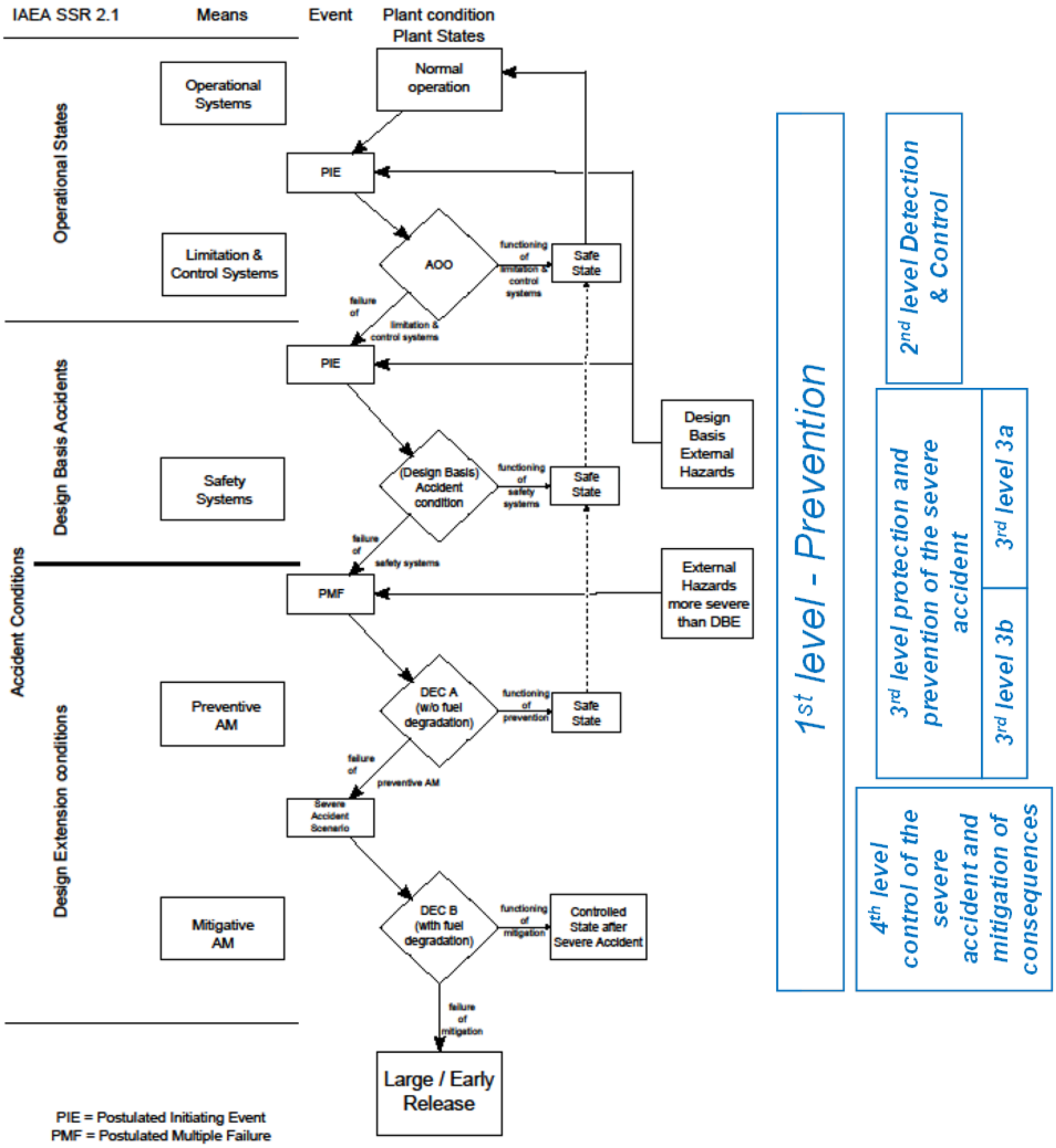


Figure 4-3 WENRA: Scheme of means, events and plant conditions[52]

The content of each LOP, i.e. the provisions which compose the LOP, must be able to ensure the achievement of the requested mission in terms of needed physical efficiency and reliability.

As for the LODs, LOPs are classified in “Strong” $\left(\frac{(10^{-3}\div 10^{-4})}{year} \text{ or } \frac{(10^{-3}\div 10^{-4})}{demand}\right)$ and “Medium” $\left(\frac{(10^{-1}\div 10^{-2})}{year}\ or\ \frac{(10^{-1}\div 10^{-2})}{demand}\right)$, with reference to different reliability targets.

[52] The depiction proposed by the WENRA scheme complies with the principles mentioned but the simplified representation of the chronology between the levels 3a and 3b (in series) seems not sufficient in so far it should be considered the possibility of having the two lines 3a and 3b in parallel, being designed to operate against different (single and multiple) postulated events.

With regard to probabilistic targets, the value "fraction of 10^{-7} / reactor year per family of initiators and per function" for the prevention of severe accidents (cf. Section 2.2.2) corresponds to the implementation, for each sequences starting with a PIE classified as AOO and which, potentially, can lead to a severe accident configuration, to the equivalent of two strong lines plus a medium line (i.e. 2a+b LOPs with, if necessary, b+b=a).

In case of failure of the prevention (level 1) and of the control of incidental / accidental conditions (levels 2 & 3), the severe accident management and the protection against intolerable releases to the environment, require the implementation of ad-hoc provisions for the management of the degraded situations and the mitigation of corresponding consequences (i.e. the layer of provisions which materialize the 4th level of the DiD). Before the Fukushima accident, the reliability allocated to this complementary line was in the range of 10^{-1} – 10^{-2} per demand (equivalent to a medium line, i.e. the order of magnitude reasonably allocated to the containment, cf. Section 2.2.2). After Fukushima, consistently with the new requirements, there is the need to practically eliminate large or early releases and, in this context, to implement specific provisions to achieve the requested missions both for the prevention and for the management of severe accident conditions even in case of *natural hazards exceeding those to be considered for design*. One can reasonably consider that the requirements in terms of reliability for the 4th level of the DiD is more stringent and ambitious than before and that the needed reliability of this additional line (Hardened Safety Core), while not being not defined precisely, should be rather in between “b” and “a” (b/a) or even equivalent to that of a strong line (i.e. “b” ⇨ “a”).

In these conditions the practical elimination of a given sequence whose potential consequences are the large or early releases should corresponds to the failure of more than « 3 times a » LOPs.

Example of qualitative characteristics to distinguish Medium and Strong lines is provided in Table 4-1.

Table 4-1 Qualitative characteristics of Medium and Strong LOPs

Qualitative characteristics	Medium lines	Strong lines
Simplicity	desirable	desirable/recommended
Diversity	desirable	recommended/required
Independence	required	required
Redundancy	desirable/required	required
Fail-safe/Fail-tolerant	required	required
Single Failure Criterion	recommended	required
Testability	recommended	required
Om-service-inspectability	recommended/required	required
Human corrective actions	permitted	not permitted

Table 4-2 provides a proposal for the positioning of Lines Protection (LOP) as indicated by the modified WENRA/RHWG table ([15], [16]). It presents the architecture of LOPs to be interposed between the plant condition whose potential consequences are greater than those allowed for its category, and these consequences, depending on their level of gravity.

Table 4-2 Proposal for the positioning of LOPs, modified WENRA/RHWG table [15], [16]

Level of DiD		Associated plant condition categories		
Level 1		Normal operation		
Level 2		Anticipated operational occurrences	b	
Level 3	3a	DiD Level 3.a Postulated single initiating events 3rd Category	b	
	3a	DiD Level 3.a Postulated single initiating events 4th Category	a	
	3b	DiD Level 3.b Selected multiples failures events including possible failure or inefficiency of safety systems involved in DiD level 3.a Consideration of "*natural hazards exceeding those to be considered for design*"	b	b/a
Total LODs to be implemented for the prevention of severe accidents			*≥ 2a+b*	
Level 4	4	DiD Level 4. Postulated core melt accidents (short and long term) Consideration of "*natural hazards exceeding those to be considered for design*"	b/a	b/a
Minimum number of LODs to be implemented to reject into the residual risk or to practically eliminate			*> 3a*	

In a similar way Table 4-3 provides an example of the complete representation of the safety architecture for the initiating events of 3rd and 4th categories and for events with multiple failures, in terms of positioning of LOPs between the plant condition under investigation and the resulting situation whose limits shall be met.

Table 4-3 Proposal for the positioning of LOPs, complete safety architecture

Category of the initial plant condition ⇨ « **Level of the DiD** » -*Category of the resulting plant condition*	2		3		4		Selection of multiple failures events	*Hazards exceeding those of design*
« **2** » - *Cat II*	b							
« **3a** » - *cat III*	b		b					
« **3a** » - *cat IV*	a		a		a			
« **3b** » - Multiple failure events	b		b		b		b	
« **3b** » - *Hazards exceeding those to be considered for design*		b/a		b/a		b/a		b/a
Total number of LOD to be implemented for the prevention of severe accidents	*≥ 2a+b*		*≥ 2a*		*≥ a+b*		*b*	*≥ b*
Level 4 *- Provisions for the management of degraded situations and mitigation of consequences: Severe Accidents*	b/a		b/a		b/a		b/a	
- Provisions for the management of natural hazards exceeding those to be considered for design		b/a		b/a		b/a		b/a
Total LOD effort to practically eliminate situations whose consequences are unacceptable	*>3a*		*>2a+b*		*>a+2b*		*>2b*	*>2b*

5. THE EVALUATION OF PERFORMANCE OF DID LEVELS

As already indicated, the acceptability of a safety architecture remains based on the degree of meeting the DiD principles. The deterministic and probabilistic considerations, including success criteria, shall therefore be integrated into a comprehensive implementation of Defence in Depth. Such success criteria are essential to design adequately the provisions implementing the levels of the DiD and refer to the required physical efficiency and reliability. The final goal of this process is the optimization of the whole safety related architecture in terms of performances and reliability.

Therefore, the objective pursued with the evaluation of the effectiveness of each level of Defense in Depth is twofold: firstly checking, for a given initiating event, that physical efficiency of the material and immaterial provisions, that are located on that level, allows achieving the task as required and, secondly, that this can be done with a reliability that is consistent with the expectations/needs.

The deterministic assessment is done with conventional rules that are specific to each category of PIE. So for Anticipated Operational Occurrences (AOO) and Design Basis Accidents (DBAs) analysis of physical performance is done with a conservative approach while for Design Extension Conditions (DEC) it is a “best estimate” approach that is adopted.

The equipment reliability is a key issue which integrates insights from probabilistic studies within the deterministic approach for safety assessment. The latter remains the basis for the construction and analysis of the safety architecture, in particular with the background of the Defense in Depth (DiD), but the contribution of probabilistic assessment to accompany the construction or to endorse the final structure is essential.

There are a number of deterministic design requirements and practices aimed at ensuring the required reliability of material and immaterial provisions, including physical separation, independence, fail safe design, redundancy, diversity, safety margins, conservative design, and single failure criterion (SSR 2/1 [3]). Probabilistic studies contribute to the verification of the fulfilment of some of the above requirements, e.g. by questioning the effectiveness of redundancy or diversity among material provisions or by modelling human factor for immaterial provisions. Even more, PSA - if appropriately developed - contributes by modelling probabilistically the plausible degradations of the implemented safety architecture, due to the failure of one or more safety functions; PSA supports the selection of adequate design options, or the verification of the adequateness of implemented solutions, against two key objectives: efficiency (i.e. the capability to correctly achieve the requested mission) and reliability (i.e. to achieve the mission with the due reliability[53]). The final

[53] The reliability of inherent or passive systems / provisions is a matter of extensive work for its assessment. The distinction between active and passive could be no longer justified. What seems essential to select and implement a given technical option, are the physical efficiency (i.e. the capability to achieve the requested mission) and the reliability that can be guaranteed to correctly achieve this mission. It is perfectly true that passive systems could have a higher reliability but it is also true that for several of them large uncertainties

goal of this process is the optimization of the whole safety related architecture in terms of performances, reliability and costs. Figure 5-1 summarizes the logic [16].

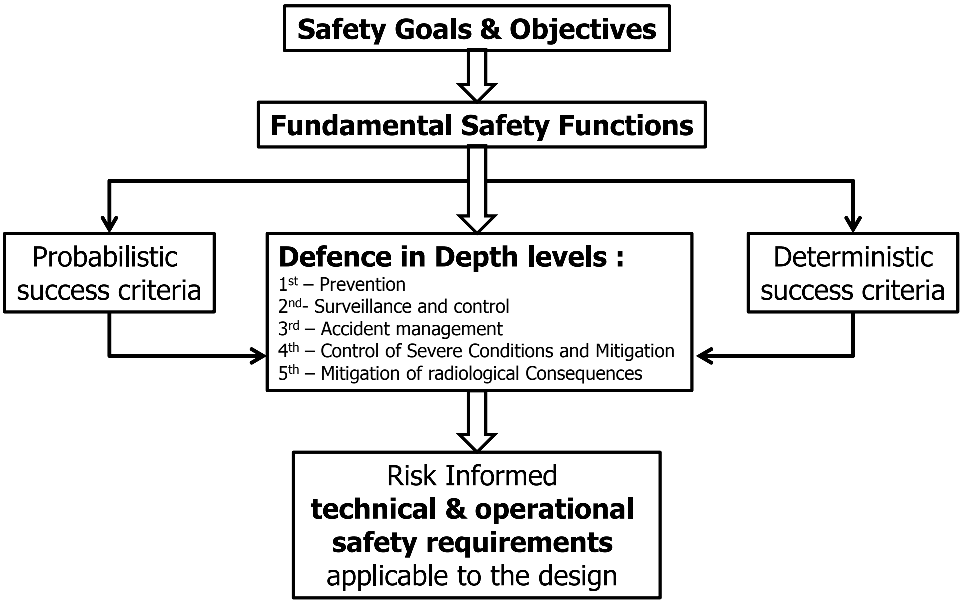


Figure 5-1 ***Defence in depth and Risk-Informed Safety Philosophy [7]***

The concept of risk space introduced in the Section 2 can be used to examine or define the deterministic or probabilistic success criteria, in terms of required performances and reliability of safety functions. The overall intent is illustrated schematically in Figure 5-2. It shows that, for a given initiating event whose consequences are potentially unacceptable, design provisions are implemented[54]:

- to keep or make the consequences acceptable with regard to the likelihood of the initiating event they are requested to control; this allows defining the success criteria in terms of requested physical efficiency that allow maintaining or bringing back the installation into the acceptable area (Control – Mitigation: deterministic success criteria) and /or
- to decrease the likelihood of the accidental sequence; this allows defining the success criteria in term of reliability of the layer of provisions required to ensure that, in case of failure, the sequence "PIE + layers of provisions' failure", is within the acceptable area (Prevention: probabilistic success criteria).

N.B. The figure presents only two extreme configurations: layer of provisions' success / failure. Obviously intermediate cases - partial success / failure - have to be considered in an analogous manner.

characterize their physical efficiency. Finally what seems essential, to motivate the selection of a given option, is the capability to provide an adequate demonstration of both the physical efficiency and the reliability.

[54] For initiating events whose consequences are very low there is no need for mitigation measures; the implementation of provisions to limit the consequences is not necessary.

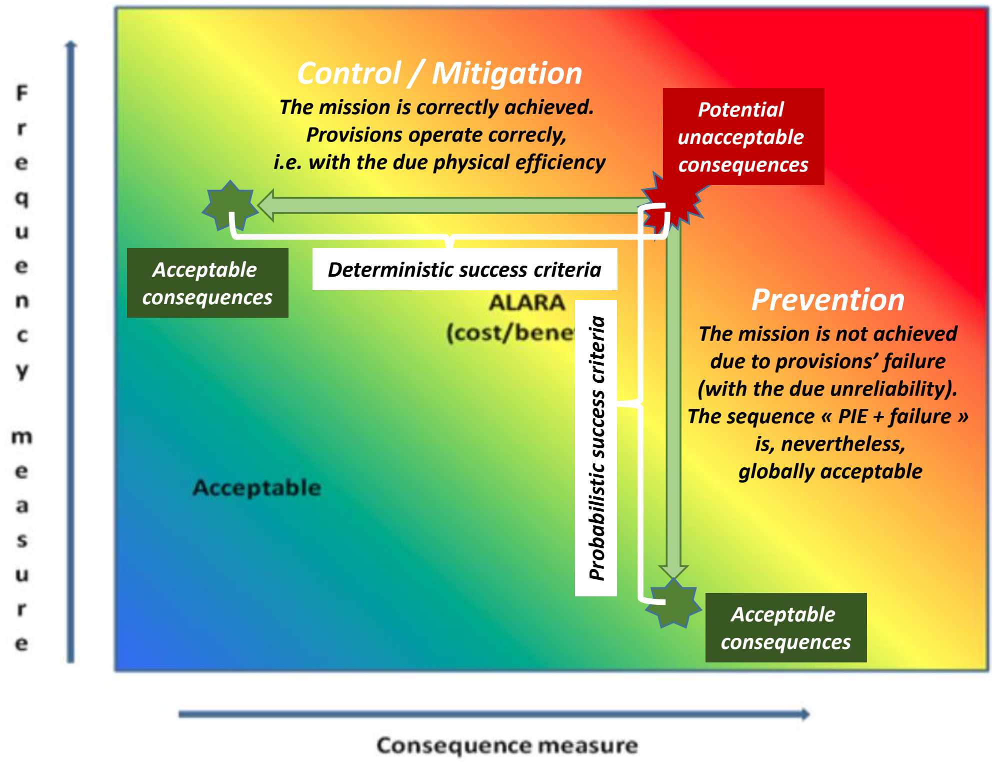


Figure 5-2 Risk space and deterministic / probabilistic success criteria

As a matter of example, guidelines 5.47 – 5.52 stated in the IAEA SSG-3 [5] allow defining the physical performances – in terms of success criteria to be defined deterministically within the risk space - for the singular provisions; they are fully applicable to the suggested approach:

"5.47. The success criterion for each safety system should be defined as the minimum level of performance required to achieve the safety function, taking into account the specific features of each sequence …;

5.48. The safety systems that would fail as a result of the initiating event should be identified and taken into account in specifying the success criteria;

5.49. The success criteria should specify the mission times for the safety systems, that is, the time that the safety systems will need to operate so that the reactor reaches a safe, stable shutdown state and that will allow for long term measures to be put in place to maintain this state;

5.50. The success criteria should also specify requirements for support systems, based on the success criteria for the front line systems, which are performing safety functions directly;

5.51. The success criteria should define the operator actions required to bring the plant to a safe, stable shutdown state as defined by the plant procedures …;

5.52. The Level 1 PSA documentation should include a list of the safety functions, safety systems, support systems and operator actions that are required for each initiating event to bring the reactor to a safe, stable shutdown state."

6. THE PROBABILISTIC ASSESSMENT OF THE SAFETY ARCHITECTURE AND DID

The Level 1 PSA relies on event trees drawn to determine how, following a given initiating event, the accident sequences progress until the severe accident condition (i.e. a fuel damage state, cf. ASAMPSA_E D30.5 [25]). In order to enable a comprehensive evaluation of the safety architecture, the PSA has to consider all the initiating events, all the safety functions, and all the levels of the DiD.

The availability of an exhaustive - as practicable – representation of the safety architecture (see Section 4) allows the development of a PSA model with a structure that better complies with the DiD principles, based on Event Trees (ET) built to reflect the crossing of different levels of DiD and, for each level of DiD, on Fault Trees (FT) built to assess the reliability of the implemented layers of provisions[55].

The PSA's event trees can be built / re-structured directly starting from a representation of the safety architecture through the Objective Provision Trees. Each OPT is specific of a given level of the DiD, of a given safety function and of a given initiating event. For a given PIE, the PSA's event tree allows modelling the failure of LOPs addressing their concatenation, interactions (e.g. the amplitude and the kinetics of the reactivity control will affect the amount of heat to be removed) and plausible dependent failures (including common cause failures and propagating failures) [56].

Figure 6-1 provides the standard structure of the Event Tree for a given PIE which demands for (all) DiD levels intervention. The sequence "hazard + failure of the DiD level 1" materializes the initiating event.

[55] Each node of the ET represents the failure/success of the whole set of provisions (i.e. the layers of provisions, i.e. the Line of protection) which materialize the corresponding DiD level, with the respective conditional failure probability. The latter is assessed by a FT which includes all the provisions required to be operational in order to achieve successfully the requested mission: engineered safety systems and all support system components, passive systems and components (e.g. undetected filter blockages, pipe leaks, etc.) as well as procedures and operator interventions.

[56] On its side, the specificity of the OPT approach is to identify, for a given initiating event and a given safety function, and for each level of DiD, the corresponding LOP with all its provisions. Obviously for different initiating events, but for the same safety function and / or the same DiD level, LOPs are built specifically and not necessarily with exactly the same provisions. Moreover, the provisions which appear at a given level of DiD for an initiating event and a safety function may intervene at another DiD level for another initiating event. Under these conditions, concerning the degree of detail for the PSA input data, it is not interesting to introduce directly the failure of single provisions within the ET (this would certainly be very tedious due to the enormous quantity of possible combinations) but to model the failure of the whole LOP within the ET and the failures of its provisions through a dedicated FT.

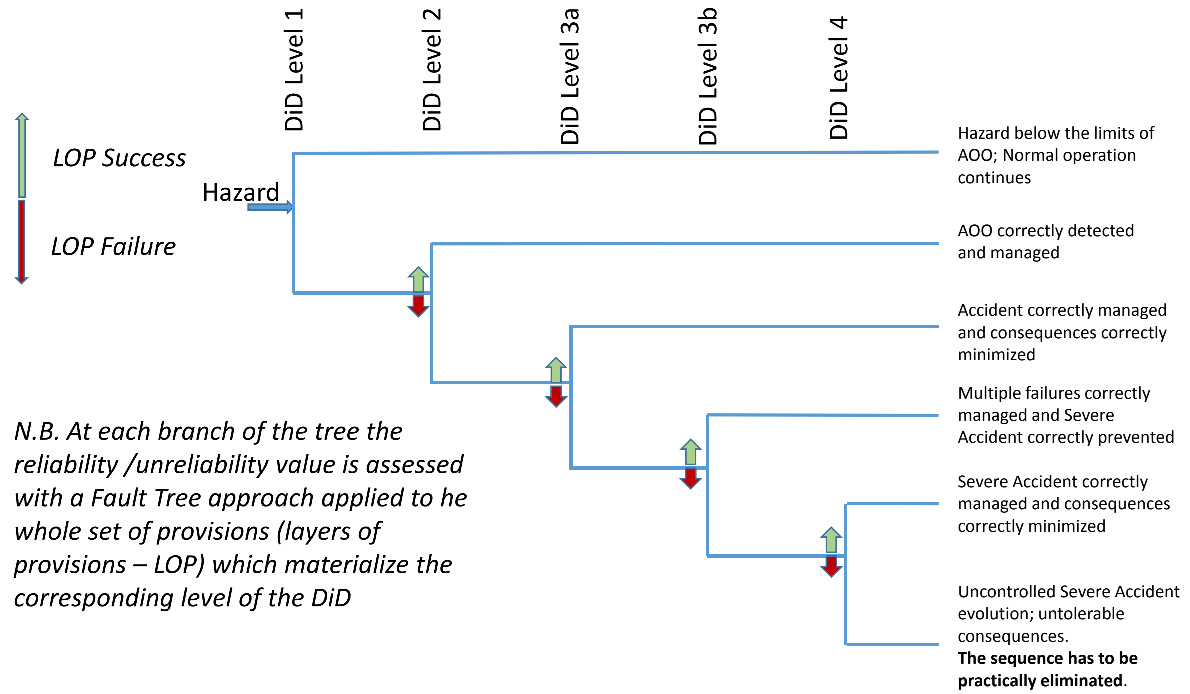


Figure 6-1 Example of Event Tree organized following the structure of the DiD

Figure 6-2 integrates into the standard Event Tree structure the indications about the practical elimination of ("short") sequences by-passing the intermediate levels (2nd and/or 3rd) or leading to unacceptable consequences (in case of failure of the 4th level of DiD). It also shows the possible by-pass of the 3a level of DiD (following the WENRA definition) in case of multiple failures events.

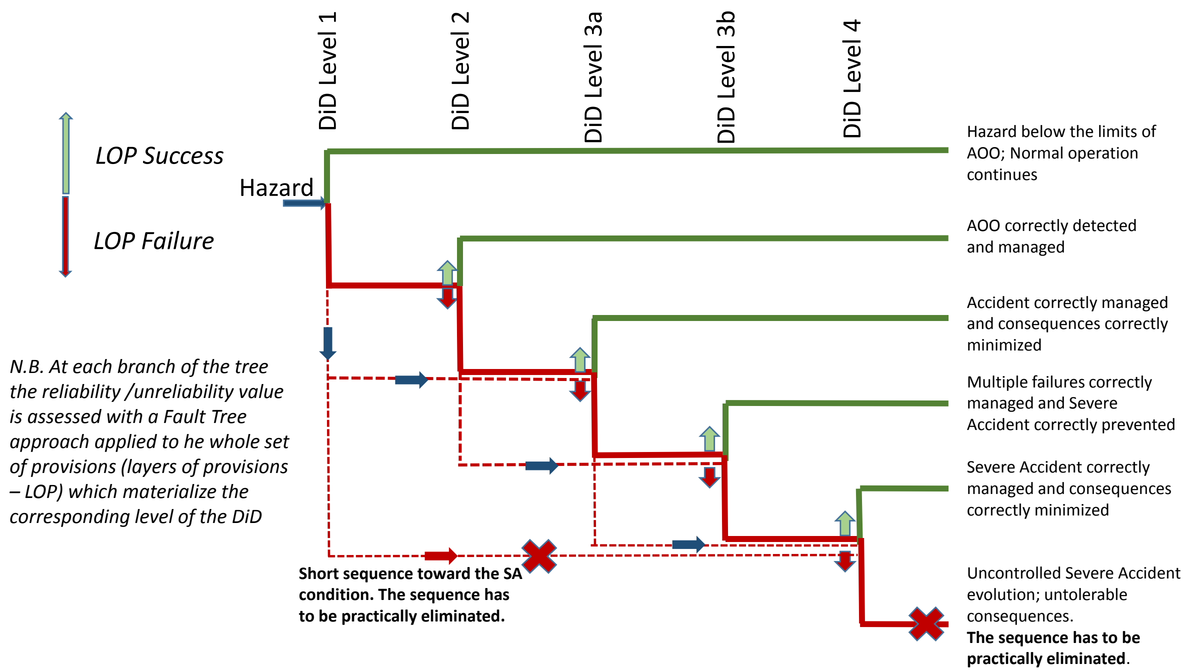


Figure 6-2 Updated example of Event Tree organized following the structure of the DiD

The guidelines specified in the SSG-3 [5] remains applicable to the provisions when aggregated within the LOP: "*5.83. Functional descriptions should be produced for each of the safety systems modelled in the Level 1 PSA to ensure that there is a valid and auditable basis for the logic model being developed. Functional descriptions typically include the following: a) The function of the system; b) The system failure modes; c)The system boundaries; d) The interfaces with other systems; e) The mode of operation being modelled (for systems with more than one mode); f) The components that need to operate or change their state and their normal; g) configuration; h) Whether the component operations are manual or automatic; i) The conditions that must exist for automatic signals to be received by the components.*"

A partial practical example developed starting from the OPT of the IAEA TECDOC 1366 [8] is presented within the "Appendix 2 – Succinct analysis of the OPT IN IAEA TECDOC 1366 [8] – Event trees for the PSA".

N.B. The trees as presented within the TECDOC 1366 are quite old (2001-2002) and should be updated, in particular to take into account the new requirements for the assessment. This step has not been done for the current exercise.

Because previous extensive applications of the proposed approach are not available, it is recommend a specific application exercise. From the perspective of the authors, this aims opening lines of thought to motivate further development.

Figure 6-3 summarizes the whole process for the assessment of the DiD with the support of the PSA, providing details with respect to Figure 1-2 about the significant issues for each one of the four main steps.

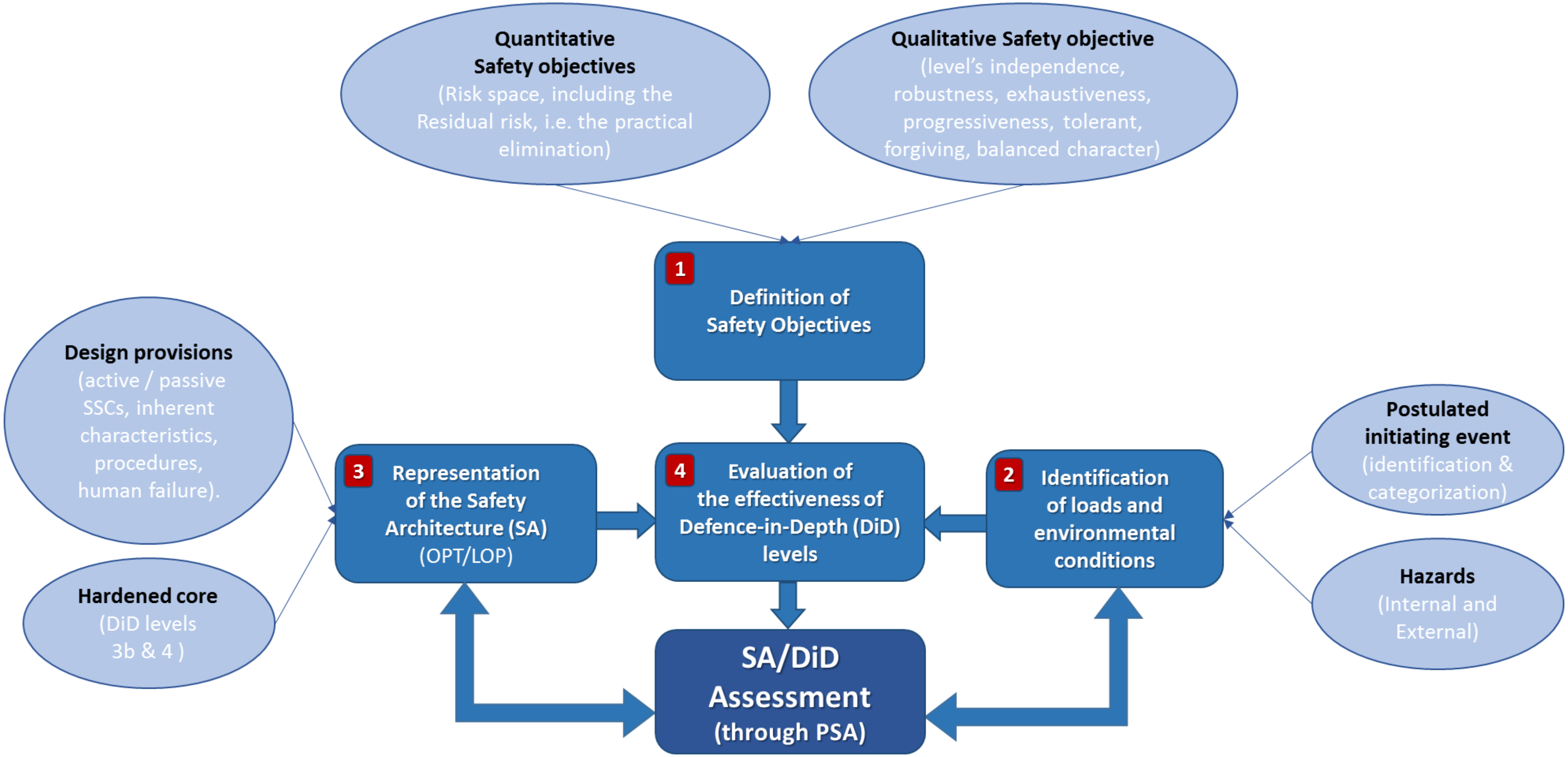


Figure 6-3 *Steps for the PSA assessment of DiD and details*

7. CONSIDERATIONS ABOUT EXISTING REACTORS AND PSA

For existing plants, the improvement of the safety architecture is a “design activity” and, as such, the indications of the SSR 2/1 [3] shall be implemented as far as reasonably practicable.

Specifically, SSR 2/1 (1.3) states that: “*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*”. This obviously applies also to the improvement of a methodology which should integrate all new knowledge and experience which are available. The evolution of the PSA approach, as described within the previous sections, should consider this objective while exploiting the available achievements.

The implementation of an updated methodology on an “old safety architecture“ can obviously identify inconsistencies and determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements. The objective of the designer / analyst should be to try to correct - as far as feasible - these inconsistencies and implement the improvements[57].

One key question can be raised to address the possible role and the needs of extension of the existing PSAs: what can be learnt from an appropriate / innovative representation of the safety architecture (e.g. through the OPT) about the adequacy of an existing PSA (not structured as described in section 6).

Two main answers concern the implemented safety architecture: (i) Identification of missed DiD level(s) for particular initiators (short sequences), even if probabilistically non-significant (e.g. Fukushima); (ii) general insights for the improvement of the safety architecture.

The current PSA approach provides integral results, e.g. versus a given detrimental event (e.g. severe core damage – PSA level 1) and, as such, even if these results comply with the probabilistic success criteria (e.g. the CDF), the first of the above results cannot be achieved; in other terms: the achievement of a given figure for the CDF does not necessarily mean that all the DiD levels are correctly designed and implemented. One can imagine that the levels effectively implemented, even if insufficient in number, are sufficiently strong to guarantee the CDF objective. Another plausible explanation could be the unjustified allocation of a very low frequency of occurrence to the initiating event (cf. Fukushima).

[57] This sort of exercise has been done by JANSI with the support of the OPT to identify and correct weaknesses within the safety architecture of current Japanese plants. Only the synthesis of this exercise is available [24] and no details were found within the open literature.

In these conditions, the appropriate representation of the safety architecture (i.e. consistent with the DiD principles) allows identifying the possible inconsistency between, on one side, the quantitative figures/results (e.g. the CDF) which can be acceptable and, on the other side, the way followed to implement safety; the latter can be questionable from the viewpoint of the DiD principles (e.g. lack of DiD levels, insufficient independence between the DiD levels, etc.) which would not be, or not sufficiently, fulfilled.

The Objective Provision Tree (OPT) and the related concept of Line Protection (LOP), already considered as well suited tool to support the design and assessment of future Gen IV systems, seems appropriate also for the re- assessment and extension of PSA of existing NPP.

Specifically, OPT could support the identification of the initiators to be considered for PSA extension and the systematic representation of the implemented safety architecture, typically not easy to be understood from the PSA, even if conceptually modelled.

The OPT and LOP allow identifying possible deficiencies in the DiD implementation, i.e. the lack of specific “layers of provisions” clearly allocated/correlated to specific DiD levels, and/or inconsistencies for these levels, e.g. lack of independence between the DiD levels. Deficiencies or inconsistencies identified by OPT/LOP, despite the acceptable results of PSA, raise the questions “how the safety is implemented?” and more generally “is the safety demonstration robust enough?”, and prove the weakness of the PSA approach applied alone.

It is important to keep in mind that one of the key objectives of the DiD logic is the coverage of “unexpected” plant conditions, i.e. the possible lack of exhaustiveness in the identification of events or sequences, and the PSA alone is not sufficient to address this eventuality, because it can only address sequences which are “expected” (although they may be extremely unlikely). This is why, even if the PSA results are acceptable from “success criteria” point of view, it is also essential to comply with the DiD principles.

Two more answers to the above question, concern the PSA itself and specifically: (i) the identification of missed events in the PSA (failure of provisions considered in the safety architecture) and (ii) general insights on the improvement of the probabilistic model(s).

Concerning the identification of the initiating events, the contribution of the PIRT/OPT/LOP (see Appendix 1 – The ISAM methodology [15]) can likely help to guarantee the exhaustiveness but nothing proves that this approach is more effective that the conventional methods as suggested, for example by the IAEA SSG-3[58].

[58] According to IAEA SSG-3 [5]: “*5.13. A systematic process should be used to identify the set of initiating events to be addressed in the Level 1 PSA. This should involve a number of different approaches including:*

- *Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for all safety systems to determine whether their failures, either partial or complete, could lead to an initiating event;*

Concerning the improvement of the probabilistic models, the insights produced by the proposed process for the assessment of the safety architecture can support:

- the systematic verification of the completeness and correctness of the representation made by the PSA model of the degraded states of the safety architecture, due to the failure of the layers of provisions which materialize the levels of DiD; this can be done by checking that the information enclosed in/provided by the OPTs (PIE and failure conditions, with respect to the mechanisms challenging the safety function - at the different DiD levels - and to the implemented line of protection) are integrated within the existing PSA;
- the re-structuring of the PSA model based on the indications provided in the Section 6, by Event Trees (ET) built to reflect the crossing of different levels of DiD and on Fault Trees (FT) built to assess the reliability of the implemented layers of provisions.

- *Deductive analyses such as master logic diagrams to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an initiating event;*
- *Comparison with the lists of initiating events developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines;*
- *Identification of initiating events on the basis of the analysis of operating experience from the plant under investigation and from similar plants;*
- *Review of the deterministic design basis accident analysis and beyond Design basis accident analysis and the safety analysis report"*

8. CONCLUSIONS

The definition and implementation of the safety architecture of a nuclear installation must be coherent with the principles of the Defense in Depth (DiD). Moreover for the updating of reactors in operation as well as for the design of innovative plants, it is essential to remain compliant with the applicable Safety Fundamental [2] and Safety Requirements [3] and to fully integrate the recent recommendations related to the lessons learnt by the Fukushima Daiichi event.

Deterministic and probabilistic approaches are recognized to be complementary elements for the safety assessment of nuclear installations, including both the verification of the compliance with the applicable Safety Fundamentals and Requirements as well as the safety analysis, i.e. the meeting of safety objectives. Unquestionably, the assessment of the DiD, i.e. the verification of the compliance of the implemented safety architecture with the DiD principles can be supported by PSA. For this objective, a certain number of practices should evolve. This document presents and motivates the ways to be followed in order to achieve these evolutions.

Concerning the definition of the objectives to be considered for the safety assessment, the reference to the risk space is essential to integrate the insights coming from the deterministic and probabilistic studies and to evaluate the effectiveness of the levels of DiD in terms of 1) physical efficiency to keep the consequences of the event under examination allowable, and 2) reliability of the layers of provisions which perform the requested mission.

Moreover, the introduction of qualitative objectives allows complementing the probabilistic targets and expanding the application field of the PSA approaches, including the support to the verification of 1) the achievement of basic design goals (protective measures limited in times and areas, exhaustiveness of the safety assessment), 2) the DiD principles (independence of DiD levels, practical elimination of events and sequences, demonstration of design against cliff edge effects), and 3) of additional characteristics required for the safety architecture (progressiveness, tolerant, forgiving and balanced characters).

The classification of the Postulated Initiating Event according to their frequency of occurrence, with reference to the plant operational states and their relationships with the DiD levels and with the allowable risk space, are essential for the identification of loads and environmental conditions to be considered in the design and sizing of provisions.

The prerequisite for optimizing the synergies between the deterministic and probabilistic approaches is the representation of the safety architecture that should, as far as possible, reflect the principles of implementations of DiD concept while being assessable by the PSA approach. Specifically, it is the reliability of the layers of provisions (or Lines of protection) that should be assessed by probabilistic studies.

The Objective Provision Tree (OPT) and the Line Of Protection (LOP) are tools proposed to support the identification of possible deficiencies in terms of DiD level and to provide the essential information for the subsequent development of the PSA.

The definition of safety objectives, both quantitative and qualitative, the identification and recognition of all loads and environmental conditions that may affect the operation of the installation and the representation, as comprehensive as practicable, of the safety architecture, allow the evaluation of the performance of each level of Defense in Depth, which is a twofold task: firstly it is verified that, for a given initiating event, the physical efficiency of the material and immaterial provisions are capable to realize the mission required and, secondly, that, if needed, this is done with a reliability that is consistent with expectations.

The availability of an exhaustive - as practicable – representation of the safety architecture allows the development of a PSA model with a structure that better complies with the DiD principles. The standard structure of the PSA Event trees, whose nodes shall represent the failure/success of the DiD levels and the corresponding Lines of Protection, and a partial practical example of application are presented.

All the proposals of this document are based on consolidated terminology [1] and shared concepts ([5], [10], [13] and [15]), and consistent with the (IAEA) Safety Fundamentals [2], Safety Requirements [3] and process for the Safety assessment [4]. They contribute to clarify the possible peculiar role of the PSA approach for the assessment of DiD and to support the on-going evolution of the PSA approach through indications on the general process for DiD assessment and on criteria and metrics to be adopted. Further activities are requested to finalize the proposed approach; they concern the detailed definition of the above criteria and metrics, coherently with the indications provided within the document.

Remark

The last exchange of questions and remarks between the approver (IRSN) and the authors about the approach proposed for the PSA assessment of Defense in depth is provided in the following.

IRSN - A PSA study assesses the risk (core melting, fission product release, dose in the plant vicinity…); the "new tool" proposed in the report wants to assess DiD level efficiency.

> *Authors* - The "new tool", as the previous, will allow assessing the risk while verifying, simultaneously, the compliance of the implemented safety architecture with the DiD principles and, more generally with the whole set of safety requirements. From this point of view, one can consider that the new tool is really an "Extended PSA".

IRSN - Initiating events are chosen independently of the DiD levels in PSAs (several hundred initiating events); in the new tool, the initiating events are, (we suppose), those of the design accidental scenarios;

> *Authors* - The initiating events are at least those selected for the design of the installation (DBE and DEC). Additional initiating events can be accounted in the PSA according to the effective DiD levels.

IRSN - For an initiating event, the accidental scenario in usual PSA is built taking into account the available means needed (human and systems) to perform fundamental safety function (reactivity control, core cooling and fission product containment); in the new tool, the available means are limited to the layer of provisions of a DiD level

> *Authors* - The reference "*to the layer of provisions of a DiD level*" is inclusive rather than restrictive. In fact, the notion of LOP integrates all the safety related features which contribute – as requested - to the achievement of the safety function. By addressing step-by-step all the levels of the DiD allows the whole set of provisions *implemented* for the prevention, control, management and consequences mitigation is considered for each initiating event.

IRSN - So, these differences could be emphasized and the report could explain that the new tool is a mean to verify the quality of the deterministic analysis.

> *Authors* - The key objective of the tool is, as indicated above, assessing the risk while verifying, simultaneously, the compliance of the implemented safety architecture with the DiD principles.

IRSN - Is it useful?

> As recommended, for example *by* IAEA GSR Part 4, the tool can allow making the whole "safety assessment", i.e. the compliance with the safety requirements as well the safety analysis.

IRSN - Is there limitation in the NPP SSCs to be taken into account (then the method may be easier to implement) or shall all NPP SCCs (like in PSA) be taken into account?

> *Authors* - The objective is to achieve the whole representation of the safety architecture. The selection of the appropriate "granulometry" is left *to* the designer / analyst. The notion of provisions includes material and immaterial (e.g. passive systems, inherent characteristics, procedures, …) means.

IRSN - It seems important to us to keep a complete independence between deterministic analysis (useful for design) and PSA study (useful to assess the risk).

> *Authors* - The above comment is exactly the vision, often supported by both the practitioners of DiD deterministic assessment and PSA, that the authors propose to overcome. This allows extending the use of the Probabilistic safety analysis toward the ultimate goal of the Safety assessment of the nuclear installation. Indeed, to assess *the* risk without assessing the compliance with the requirements is a partial approach that does not fully answer the need for the "safety assessment" as defined by the IAEA GSR Part 4 ("Safety assessments are to be undertaken as a means of evaluating compliance with safety requirements and thereby the application of the fundamental safety principles …. Safety assessment includes, but is not limited to, the formal safety analysis" [4]).

9. REFERENCES

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

[2] IAEA Safety Standards Series No. SF 1: Fundamental Safety principles, 2006

[3] IAEA Safety Standards Series No. SSR-2/1, Rev. 1: Safety of Nuclear Power Plants: Design; 2016

[4] IAEA Safety Standards Series No. GSR Part 4, Rev. 1: Safety Assessment for Facilities and Activities, 2016

[5] IAEA Safety Standards Series No. SSG-3: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants; 2010

[6] IAEA Safety Standards Series No. SSG-30: Safety Classification of Structures, Systems and Components in Nuclear Power Plants, 2014

[7] IAEA-TECDOC-1570 - Proposal for a Technology-Neutral Safety Approach for New Reactor Designs; 2007

[8] IAEA TECDOC 1366: Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors – 2003

[9] IAEA-Safety Report 46 Assessment of Defence in Depth for Nuclear Power Plants, 2005

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

[11] INSAG, Defence in Depth in Nuclear Safety, INSAG-10, 1996

[12] INSAG, Basic Safety Principles for Nuclear Power Plants; 75-INSAG-3 Rev. 1 - INSAG-12; 1999

[13] WENRA Report: Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG; March 2013

[14] WENRA: Guidance Document Issue F: Design Extension of Existing Reactors, 2014

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

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

[17] J. Yllera IAEA, Division of Nuclear Installation Safety: Considerations for the Application of the new Safety Requirements for NPP Design, SSR 2/1; RSWG-20, 7-8 October 2014; KINS, Daejeon, Korea

[18] Stress tests performed on European Nuclear Power Plants as a follow-up to the Fukushima accident. Overview and conclusions presented to ENSREG by the peer review Board; April 2012

[19] Justin, Petit, Tanguy: Safety Assessment of Severe Accident in Fast breeder Reactors; Nuclear safety, Vol. 27, 1986

[20] G.L.Fiorini & al. The current CEA/DRN Safety approach for the design and the assessment of Future Nuclear Installations; ICONE 7208, April 1999

[21] P.LoPinto & al. Safety orientations during ASTRID conceptual design phase - International Conference on Fast Reactors & Related Fuel Cycle March 4-7, 2013, Paris, France; IAEA-CN-199 – 267

[22] G.L. Fiorini; L. Ammirabile, V. Ranguelova: The ISAM tool "Objective Provision 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; 21-24 October 2013

[23] Application of Objective Provision 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

[24] 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

[25] ASAMPSA_E: Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA, ASAMPSA_E report D30.3, draft report, 2016

[26] ASAMPSA_E: Risk Metrics and Measures for an Extended PSA, ASAMPSA_E report D30.5, draft report, 2016

[27] Surveillance Radiologique Des Expositions Des Travailleurs Livre Blanc; Une Démarche Collective Multidisciplinaire Pour Une Vision Partagée Sous Le Pilotage De Pierre Barbey (Université De Caen Normandie) Et Du Dr Christine Gauron (Inrs – Retraitée); Sur Saisine De La Dgt Avec La Collaboration De L'ASN ET DE L'IRSN - Direction Générale du Travail Autorité de Sureté Nucléaire Institut de Radioprotection et de Sûreté Nucléaire

[28] https://www.euronuclear.org/info/encyclopedia/r/residual-risk.htm

[29] https://www.iaea.org/ns/tutorials/regcontrol/assess/assess3212.htm

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

APPENDIX 1 – THE ISAM METHODOLOGY [15]

The process for the design and evaluation of a safety architecture

The process for the design and evaluation of a safety architecture follows a logic which begins with the identification of fundamental principles and requirements that are mandatory and imposed by the regulator. Among these principles the compliance with the logic of the Defense in Depth is certainly one of the most important. The strategy of DiD (i.e. the adoption of adequate safety architectures) ensures that the fundamental safety functions are reliably achieved, with sufficient margins, to compensate for equipment failure, human errors and hazards.

In parallel safety goals are established to ensure that public and environmental protection is properly secured. Principles and requirements are accompanied, if appropriate, by guidelines which, while not mandatory, can help selecting the options that will satisfy the principles, the requirements and objectives. Once principles, requirements, guidelines, objectives and safety options have been selected, the full process (iterative as needed) for the design and the assessment of the retained safety architecture (including the safety analysis[59]) can be summarized as in Table 1-1.

The ISAM methodology

The full set of above steps can be achieved with the help of the Integrated Safety Assessment Methodology (ISAM) methodology, developed within the context of the Generation IV Risk and safety Working Group (GIF/RSWG) [15].

The methodology consists of five distinct analytical tools, each of which can be used to answer specific kinds of safety-related questions with different degrees of detail, and at different stages of design maturity.

Although individual analytical tools can be selected for individual and exclusive use, the full value of the integrated methodology is derived from using each tool, in an iterative manner and in combination with the others, throughout the development cycle.

Figure A2-1 details the overall task flow of the ISAM and indicates which tools are intended for use in each phase of Generation IV system technology development.

Each analysis tool is briefly described in the following [15].

[59] Following the indications of IAEA [4], the safety assessment is "*the systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design of the plant. This would include also the requirements set by the operating organization and the regulators. Safety assessment includes, but is not limited to, the formal safety analysis*".

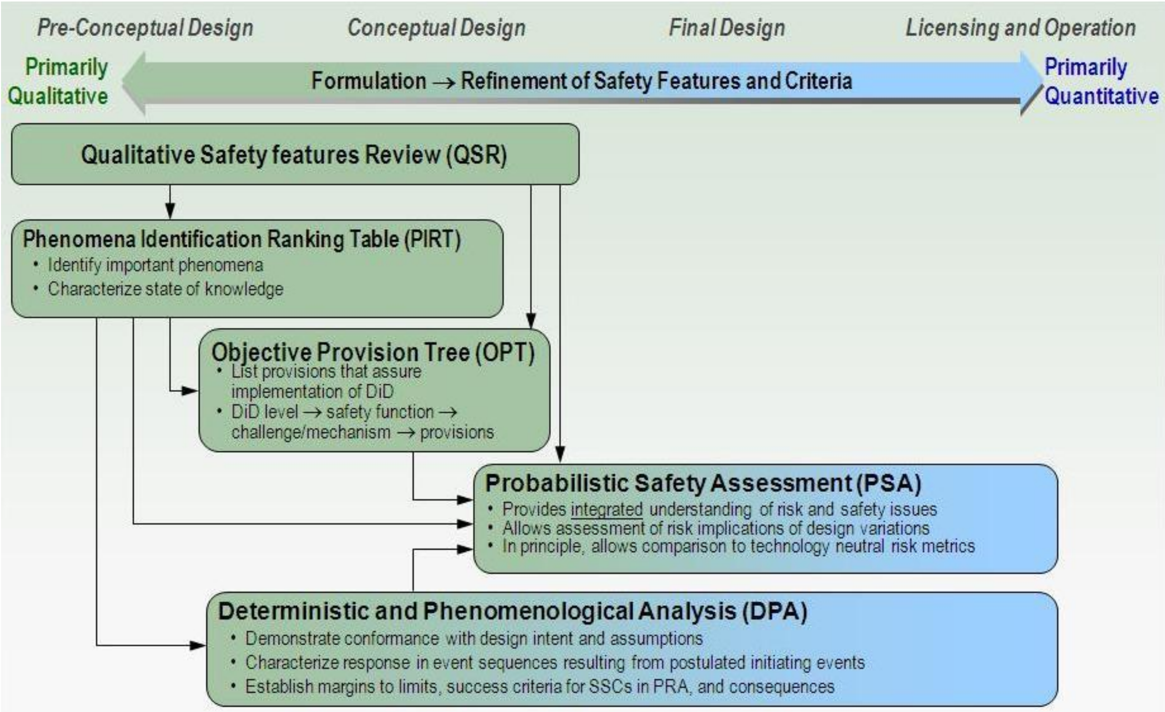


Figure A2-1 ***Proposed GIF Integrated Safety assessment Methodology (ISAM) Task Flow*** **[15]**

- *Qualitative Safety features Review (QSR)*

The QSR provides a systematic means of ensuring and documenting that the evolving Gen IV system concept of design incorporates the desirable safety-related attributes and characteristics that are identified and discussed within the significant references for principles, requirements and guidelines (IAEA, GIF, INPRO, etc.). The QSR provides a useful means of shaping designers' approaches to their work to help ensure that safety truly is "built-in, not added-onto" since the early phases of the design of Gen IV systems. The QSR serves as a useful preparatory step for other elements of the ISAM by promoting a richer understanding of the developing design in terms of safety issues or vulnerabilities.

- *Phenomena Identification and Ranking Table (PIRT)*

The PIRT technique has been widely applied in both nuclear and non-nuclear applications. As applied to Gen IV nuclear systems, the PIRT is used to identify a spectrum of safety-related phenomena or scenarios that could affect those systems, and to rank order those phenomena or scenarios on the basis of their importance (often related to their potential consequences), and the state of knowledge related to associated phenomena (i.e., sources and magnitudes of phenomenological uncertainties). The method relies heavily on expert elicitation, but provides a discipline for identifying those issues that will undergo more rigorous analysis using the other tools of ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT cf. below) analyses, and the Probabilistic Safety Analysis (PSA). The PIRT is particularly helpful in defining the course of accident sequences, and in defining safety system success criteria. The PIRT is essential in helping to identify areas in which additional research may be helpful to reduce uncertainties.

- *Objective Provision Tree (OPT)*

Following the logic illustrated by the Figure 4-1, the purpose of OPT is to ensure and document the provision of essential “lines of protection” to ensure successful prevention, control or mitigation of phenomena that could potentially damage the nuclear system. As such it can be considered as an innovative mean to represent the whole safety architecture.

There is a natural interface between the OPT and the PIRT in that the PIRT identifies phenomena and issues that could potentially be important to safety, and the OPT focuses on identifying design provisions intended to prevent, control, or mitigate the consequences of those phenomena.

The OPT can be extremely useful in helping to focus and structure the analyst’s identification and understanding of possible initiators and mechanisms of abnormal conditions, accident phenomenology, success criteria, and related issues.

- *Deterministic and Phenomenological Analyses (DPA)*

Conventional deterministic and phenomenological analyses, including the due consideration for the uncertainties, will be used to perform the quantitative analysis which supports the development and the sizing of the safety architecture. They will feed the PSA as an essential input to quantify the results. DPA is used from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Generation IV system.

- *Probabilistic Safety Analysis (PSA)*

The PSA is a widely accepted, integrative method that is rigorous, disciplined, and systematic, and therefore it forms the principal basis of the ISAM. PSA can only be meaningfully applied to a design that has reached a sufficient level of maturity and detail. Thus, PSA is performed and iterated beginning in the late pre-conceptual design phase, and continuing until the final design stages.

In fact, as the concept of the “living PSA” is becoming increasingly accepted, the RSWG advocates the idea of applying PSA at the earliest practical point in the design process, and continuing to use it as a key decision tool throughout the life of the plant or system.

Although the other elements of the ISAM have significant value as stand-alone analysis methods, their value is enhanced by the fact that they serve as useful tools in helping to prepare for and to shape the PSA once the design has matured to a point where the PSA can be successfully applied.

Safety assessment and verification: the role of the ISAM tools

Table A-1 resumes - roughly - the crosscutting relationships between, on one side, the steps of the design / assessment process as described above and, on the other side, the different tools of ISAM.

The table content demonstrates the integrated character of the ISAM tools versus the safety assessment objective but, in particular, it shows the specific an complementary role of the deterministic tools (PIRT, OPT and DPA) and that of the probabilistic assessment (PSA).

Table A-1 ***Relationships between the steps for the design and assessment of the SA and the role of the different tools of ISAM***

	QSR	PIRT	OPT	DPA	PSA
Regulatory Framework (Goals, objectives, principles, requirements, guidelines)	✓				
Selection of Safety Options and provisional Provisions		✓	✓	✓	✓
1. *Compliance / consistency of the design options with the principles, requirements and guidelines*	✓				
2. *Identification, prioritization and correction (if feasible) of discrepancies between design options with the principles, requirements and guidelines,*	✓	✓	(✓)[60]	(✓)[35]	(✓)[35]
3. *Identification of challenges to the safety functions,*		✓	✓		
4. *Identification of mechanisms (initiating events) and selection of significant (envelope) plants conditions to be considered for the design basis,*		✓	✓	✓	(✓)[61]
5. *Selection and categorization of representative design extension conditions (without and with core melting; DEC A & DEC B with the WENRA terminology) to be considered for the design basis*		✓	✓	✓	(✓)[36]
6. *Selection of external events that exceed the design basis and for which safety systems are designed to remain functional both during and after the external event*		✓		✓	(✓)[36]
7. *Identification of plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated*		✓		✓	✓[62]
8. *Identification and selection of needed provisions, implementation within the corresponding “layers of provisions” for the different levels of the DiD*	✓	✓	✓		
9. *Design and sizing of the provisions,*			✓	✓	✓[63]
10. *Response to transients (safety analysis),*				✓	✓
11. *Final assessment for a safety architecture that should be:*					
○ *Exhaustive,*		✓	✓		
○ *Progressive,*			✓	✓	✓
○ *Tolerant,*				✓	✓
12. *Forgiving,*				✓	✓
○ *Balanced.*					✓

---

[60] While QSR and PIRT are identified as the main ISAM tools for this step, the outcomes of other ISAM tools can used in successive iterations.

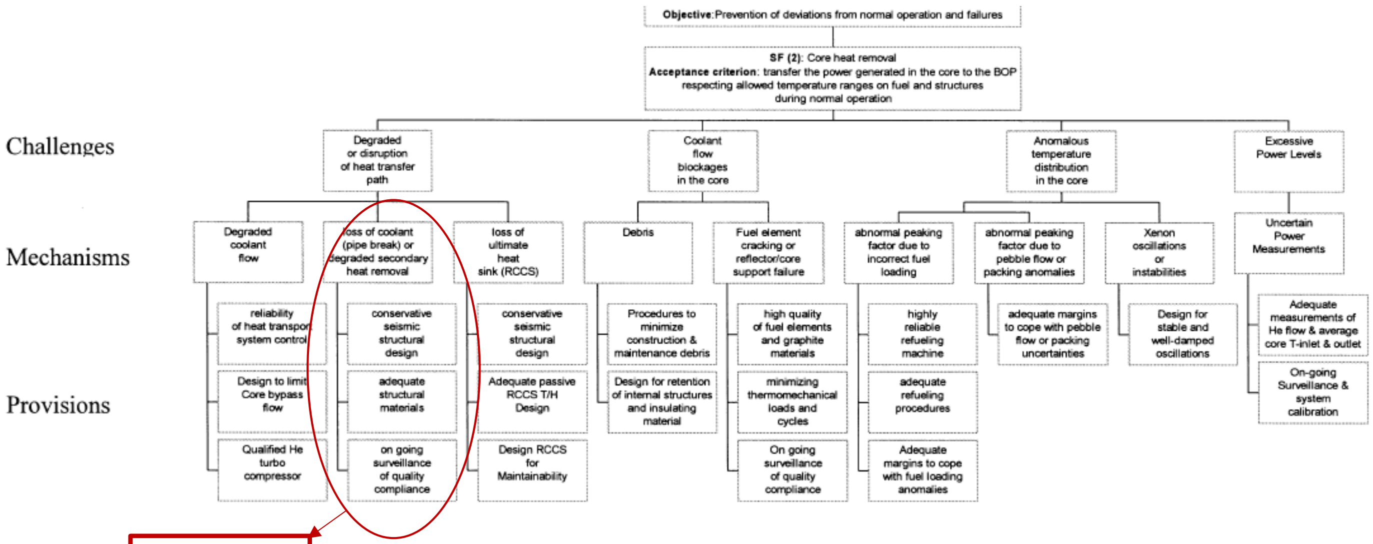
[61] The contribution to this step is essentially deterministic even if it is recognized that probabilistic assessment can help, for example, for the identification of complex events / sequences which probability of occurrence justify their consideration for the design and / or for the categorization of the selected initiating events..

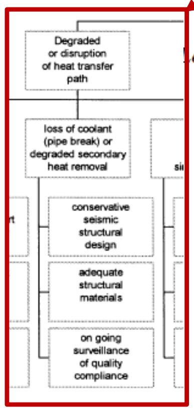
[62] The role of probabilistic studies is important even if not sufficient for the demonstration of the practical elimination

[63] While the design and sizing of the provisions will be essentially deterministic, the probabilistic studies will help guaranteeing the requested reliability

APPENDIX 2 – SUCCINCT ANALYSIS OF THE OPT IN IAEA TECDOC 1366 [8] – EVENT TREES FOR THE PSA

N.B. The following trees are taken from the IAEA TECDOC 1366
The « layers of provisions » which are identified for the « loss of coolant » conditions are put in exergue





Level 1 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.

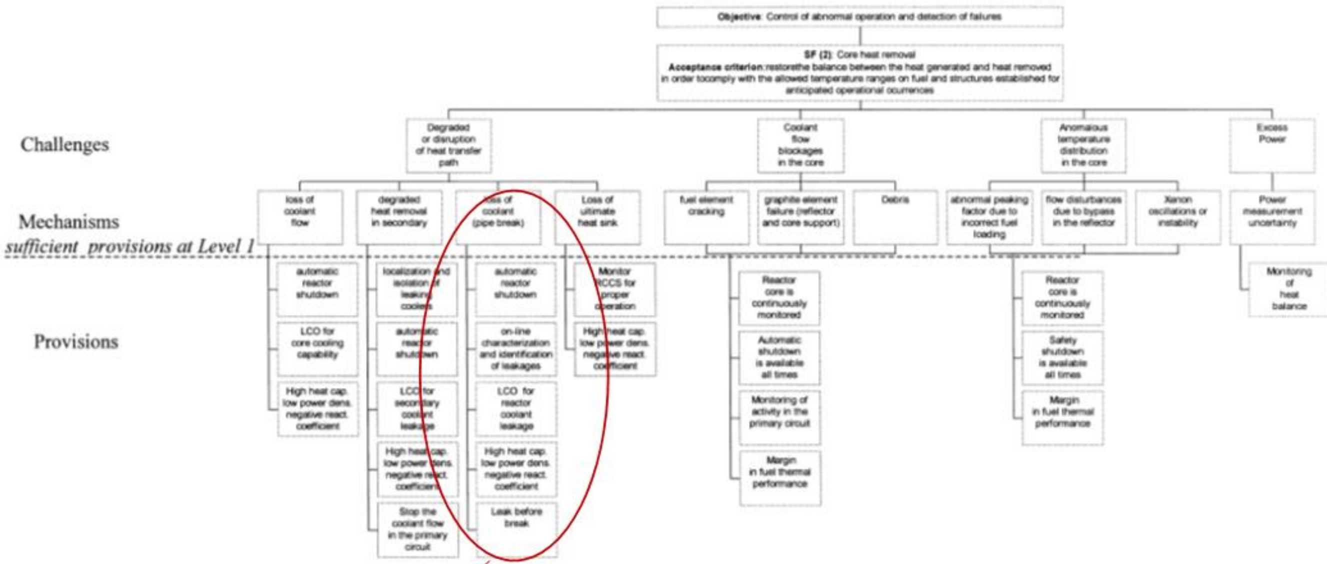
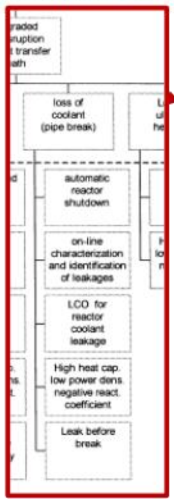


Fig. 12. MHTGR Level 2 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.



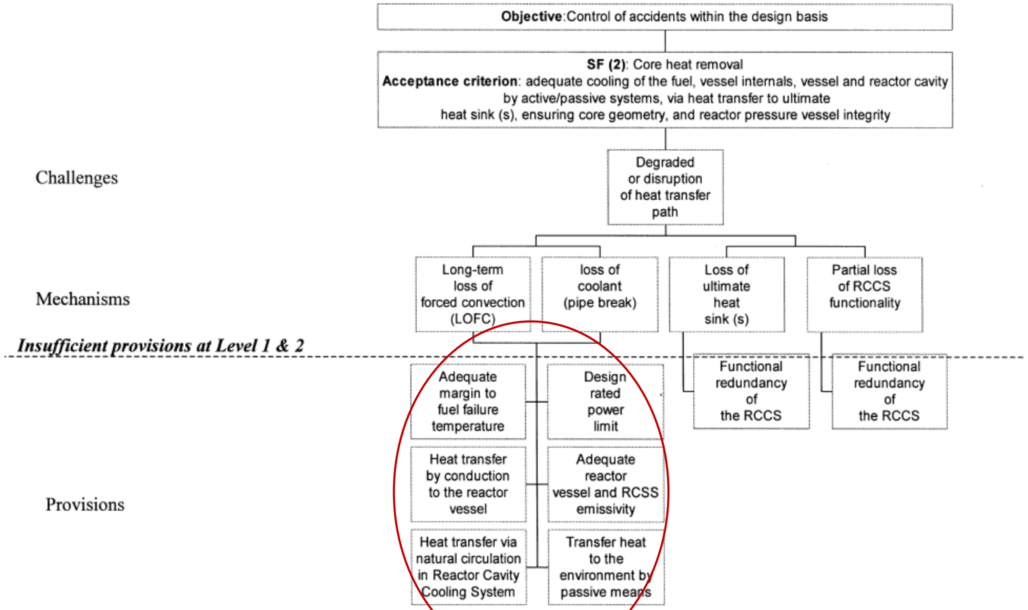
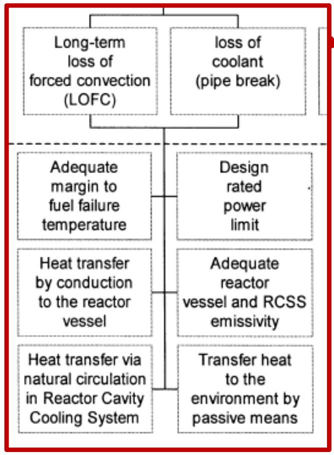


Fig. 15. MHTGR Level 3 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.



N.B. This Trees should be completed with one or two other trees (level 3b) to consider the possibility for the « multiple failures »

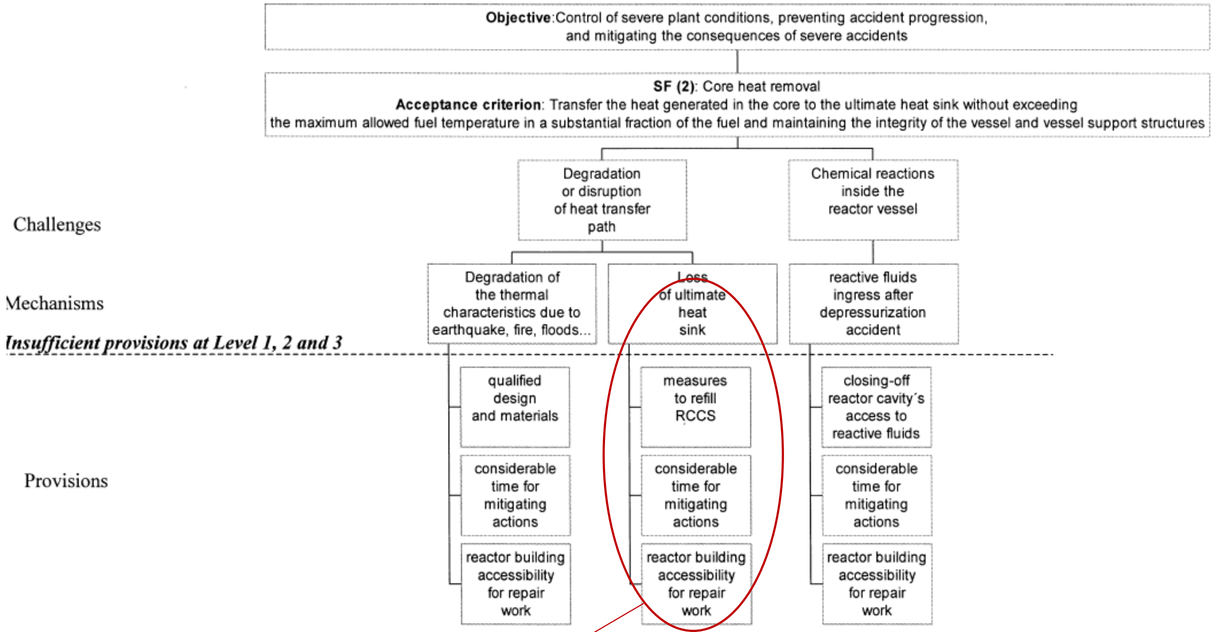
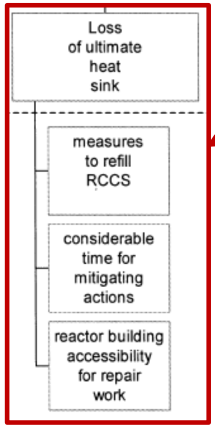


Fig. 18. MHTGR Level 4 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.



N.B. This tree for the 4th level should be completed to take explicitly into consideration the possibility of degradation of the DHR path. The « loss of ultimate sink » is likely not sufficient to represent the different configuration.

Example of Event Tree organized following the structure of the Defense in depth.