

"NUCLEAR FISSION"
Safety of Existing Nuclear Installations

Contract 605001

<p align="center">Recommendations on Extended PSA and its Use in Decision Making</p>



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

<p align="center">Reference ASAMPSA_E Technical report ASAMPSA_E/WP30/D30.6/2016-28 Reference IRSN PSN/RES/SAG/2016-0234</p>
--

A. Wielenberg (GRS), E. Cazzoli (CCA), S. la Rovere (NIER), C. Hasnaoui (AREXIS), H. Löffler (GRS), S. Potemski (NCBJ), J. Vitazkova (CCA), G. Fiorini (NIER), E. Raimond (IRSN)




Period covered: from 01/07/2013 to 31/12/2016		Actual submission date: 20/07/2016
Start date of ASAMPSA_E: 01/07/2013		Duration: 42 months
WP No: 30	Lead topical coordinator : A. Wielenberg	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

	<p>Advanced Safety Assessment Methodologies: extended PSA</p>	
--	---	--

ASAMPSA_E Quality Assurance page

Partners responsible of the document : GRS, IRSN	
Nature of document	Technical Report
Reference(s)	Technical report ASAMPSA_E/WP 30/D30.6/2016-28 Rapport IRSN-PSN-RES/ SAG/2016-0234
Title	Recommendations on Extended PSA and its Use in Decision Making
Author(s)	A. Wielenberg (GRS), E. Cazzoli (CCA), S. la Rovere (NIER), C. Hasnaoui (AREXIS), H. Löffler (GRS), S. Potempski (NCBJ), J. Vitazkova (CCA), G. Fiorini (NIER), E. Raimond (IRSN)
Delivery date	01-07-2016
Topical area	Extended PSA, Risk-informed Decision Making
For Journal & Conf. papers	No
<p><u>Summary :</u></p> <p>In a perspective of extended PSA applications, the report D30.6 summarizes the main findings of WP30 on</p> <ul style="list-style-type: none"> the lessons of the Fukushima accident for PSA, identifying initiating events and hazards, risk measures, the link between PSA and the DiD principles. <p>Finally, the report discusses the use of insights from extended PSA for risk-informed decision making (RIDM).</p>	

Visa grid			
	Main author(s) :	Verification	Approval (Coordinator)
Name (s)	Andreas Wielenberg	Horst Löffler	E. Raimond
Date	2016-07-15	2016-07-14	2016-07-15
Signature			

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
Rev. 0		A. Wielenberg	All	Initial version
Rev. 1	October 2015	A. Wielenberg	All	Update to status of WP 30.
Rev. 2	February 2016	E. Cazzoli, S. la Rovere, G. Fiorini, J. Vitazkova, A. Wielenberg	All except section 1	Integration of first contributions
Rev. 3	May 2016	H. Löffler, A. Wielenberg	Most	Integration of topic report results, and RIDM section
Rev. 4	23-06-2016	H. Löffler	Most after 4	summarize findings
Rev. 5	15-07-2016	E. Raimond	All	<p>Final approval review, editorial modifications and few proposals in the findings.</p> <p>Important: the report has been delivered very late in the ASAMPSA_E project and this Rev. 5 cannot reflect fully the ASAMPSA_E partner's experience.</p> <p>The report, which includes extracts from other deliverables, needs to be further improved by considering additional opinions and examples (for example of IRIDM applications or cost-safety benefits methods).</p> <p>At this stage, it is mainly a basis for discussions. During the review of this report, the executive summary shall be discussed and completed.</p>

LIST OF DIFFUSION

European Commission (Scientific Officer)

Name	First name	Organization
Passalacqua	Roberto	EC

ASAMPSA_E Project management group (PMG)

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

REPRESENTATIVES OF ASAMPSA_E PARTNERS

Name	First name	Organization
Grindon	Liz	AMEC NNC
Mustoe	Julian	AMEC NNC
Cordoliani	Vincent	AREVA
Dirksen	Gerben	AREVA
Godefroy	Florian	AREVA
Kollasko	Heiko	AREVA
Michaud	Laurent	AREVA
Hasnaoui	Chiheb	AREXIS
Hurel	François	AREXIS
Schirrer	Raphael	AREXIS
De Gelder	Pieter	Bel V
Gryffroy	Dries	Bel V
Jacques	Véronique	Bel V
Van Rompuy	Thibaut	Bel V
Cazzoli	Errico	CCA
Vitázková	Jirina	CCA
Passalacqua	Roberto	EC
Banchieri	Yvonnick	EDF
Benzoni	Stéphane	EDF
Bernadara	Pietro	EDF
Bonnevialle	Anne-Marie	EDF
Brac	Pascal	EDF
Coulon	Vincent	EDF
Gallois	Marie	EDF
Henssien	Benjamin	EDF
Hibti	Mohamed	EDF
Jan	Philippe	EDF
Lopez	Julien	EDF
Nonclercq	Philippe	EDF
Panato	Eddy	EDF
Parey	Sylvie	EDF

Romanet	François	EDF
Rychkov	Valentin	EDF
Vasseur	Dominique	EDF
Burgazzi	Luciano	ENEA
Hultqvist	Göran	FKA
Karlsson	Anders	FKA
Ljungbjörk	Julia	FKA
Pihl	Joel	FKA
Loeffler	Horst	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	GRS
Tuerschmann	Michael	GRS
Wielenberg	Andreas	GRS
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Serrano	Cesar	IEC
Apostol	Minodora	ICN
Nitoi	Mirela	ICN
Groudev	Pavlin	INRNE
Stefanova	Antoaneta	INRNE
Andreeva	Marina	INRNE
Petya	Petrova	INRNE
Armingaud	François	IRSN
Bardet	Lise	IRSN
Baumont	David	IRSN
Bonnet	Jean-Michel	IRSN
Bonneville	Hervé	IRSN
Clement	Christophe	IRSN
Corenwinder	François	IRSN
Denis	Jean	IRSN
Duflot	Nicolas	IRSN
Duluc	Claire-Marie	IRSN
Dupuy	Patricia	IRSN
Durin	Thomas	IRSN
Georgescu	Gabriel	IRSN
Guigueno	Yves	IRSN
Guimier	Laurent	IRSN
Lanore	Jeanne-Marie	IRSN
Laurent	Bruno	IRSN
Pichereau	Frederique	IRSN
Rahni	Nadia	IRSN
Raimond	Emmanuel	IRSN
Rebour	Vincent	IRSN
Sotti	Oona	IRSN
Volkanovski	Andrija	JSI
Prošek	Andrej	JSI
Alzbutas	Robertas	LEI
Matuzas	Vaidas	LEI
Rimkevicius	Sigitas	LEI
Häggström	Anna	LRC
Klug	Joakim	LRC
Kumar	Manorma	LRC
Olsson	Anders	LRC
Borysiewicz	Mieczyslaw	NCBJ
Kowal	Karol	NCBJ
Potemski	Slawomir	NCBJ
La Rovere	Stephano	NIER
Vestrucci	Paolo	NIER
Brinkman	Hans (Johannes L.)	NRG

Kahia	Sinda	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Morandi	Sonia	RSE
Caracciolo	Eduardo	RSE
Dybach	Oleksiy	SSTC
Gorpinchenko	Oleg	SSTC
Claus	Etienne	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Grondal	Corentin	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Oury	Laurence	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Yu	Shizhen	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	TUS
	Kaleychev	TUS
Holy	Jaroslav	UJV
Hustak	Stanislav	UJV

Jaros	Milan	UJV
Kolar	Ladislav	UJV
Kubicek	Jan	UJV
Decker	Kurt	UNIVIE
Halada	Peter	VUJE
Prochaska	Jan	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

GLOSSARY

Definitions of terms used in the report.

Consequence

In terms of risk analysis, consequence denotes certain aspects describing the end state of sequences in the risk model. In that sense, consequence is synonymous to risk metric. For practical purposes, e.g. “core damage” and “large release” are typical consequences.

Frequency

Frequency in this report is the measure for the rate of an event, ideally being constant over time. The dimension would be 1/s. For PSA, frequencies are often given as 1/yr. If a probability over a time period scales (approximately) linearly with the duration of that time period, it can be treated as a frequency for most practical purposes, hence e.g. core damage frequency.

Likelihood

Likelihood is used in this report as a convenient generalization of probability, probability over a time period, and frequency.

Probability

Probability in this report denotes a (dimensionless) measure that can take values between 0 and 1. It describes the likelihood that an event will happen.

Probability can be related to a certain time frame, e.g. a year or a month, or may be specific to a certain condition, e.g. per demand. If a probability is not scaling linearly with time (e.g. because it is per demand), then time averaging using the time at risk can give misleading results.

Risk

Risk is defined relative to hazards or accidents. A hazard is something that presents a potential for health, economical or environmental harm. Risk associated with the hazard is a combination of the probability (or frequency) of the hazardous event and the magnitude of the consequences. The consequences can be represented in several dimensions. A usual engineering definition of risk associated with an event i is:

$\text{Risk}(\text{event } i) = \text{“the probability of an event } i\text{”} \times \text{“the consequences of an event } i\text{”}$. [69], cf. [5]

Risk accepting

Risk accepting or risk seeking is used to describe a decision maker with a convex expected utility function in expected utility function. For example, a risk accepting decision maker will accept an unfair gamble (e.g. play roulette) if there is a small probability for a very large gain. A risk accepting decision maker would prefer an alternative with a small likelihood for large gains over a decision with small gains with high certainty given the same utility. Conversely, a risk accepting decision maker will accept a catastrophic loss predicted with a very

small probability if there are small benefits with a high probability even if the overall utility is negative.

Cf. [88] and related links.

Risk aggregation

Risk aggregation describes the process of integrating results from risk measures for different sequences in a risk model. If the sequences are connected to different consequences and thus risk over different consequences is aggregated, some kind of conversion of the different risk measures has to be applied. Taking into account that different outcomes for risk measures are subject to different expected utilities by decision makers, risk aggregation needs to be handled with care.

Risk averse

Risk averse is used to describe a decision maker with a concave expected utility function in expected utility function. For example, a risk averse decision maker would decline any unfair gamble (i.e. never play roulette). A risk averse decision maker would prefer decisions with small but certain benefits over decisions with large but unlikely benefits given the same utility. Conversely, a risk averse decision maker would prefer to exclude catastrophic losses even if unlikely irrespective of potential benefits. Cf. [88] and related links.

Risk metric and measure

“In the context of risk measurement, a risk metric is the concept quantified by a risk measure.” [88]. The risk metric is a feature or property of the risk model like e.g. a consequence, a transition between two states of the risk model, or an indicator derived from another risk measure. The risk measure includes in addition the quantification procedure for the risk metric. Risk measures are used for the representation, discussion, and interpretation of PSA results. For risk measures like core damage frequency, conditional failure probability of a system, or basic event importance for CDF to be used, the risk model has to support the respective risk metrics. However, under the ASAMPSA_E project the two terms risk metrics and risk measures have been used without distinction. For this reason, in this report, the term risk measure will be used as a more comprehensive term even if only the risk metric is meant. The term risk metric will be used if specifically the metric aspect is addressed or if there would otherwise be ambiguities. cf. [5]

Risk neutral

Risk neutral is used to describe a decision maker with a linear utility function in expected utility theory. Cf. [88] and related links.

Sequence

A sequence describes the development of a specific event scenario from an initiating event to an end state (consequence) in a risk model. Using the common event tree description of risk models, a sequence is a specific branch in an event tree.

Utility

Utility is used in this report in the sense of expected utility theory. It describes the expected value of a decision alternative to the decision maker taking into account the likelihood for the different potential outcomes of that alternative.

One simple example would be the probability weighted net return on investment (in an economics area). Cf. [88]

Validity

Validity describes whether the risk measure is in line with the assumptions made and the calculation approach applied in the risk model (predictive validity), and if the risk metric adequately reflects an aspect of the analysed risk and provides relevant information for decisions on risk (content validity). Cf. [5]

EXECUTIVE SUMMARY

/This should be carefully discussed during the review process/ Existing experience of practical use of IRIDM process shall be commented.

Introduction

The ASAMPSA_E project has investigated the concept of extended PSA (cf. [1]) and its implications for PSA modelling and PSA methods. Within WP30, several specific issues were discussed in more detail and dedicated reports were published. In report D30.2 [2] the authors have looked at available information about the accident at the Fukushima Daiichi power plant from the point of view of PSA and at recent PSA models for NPP in general. Report D30.3 [3] investigated the approach for identifying initiating events and hazard scenarios for an extended PSA. The authors have derived recommendations for a comprehensive screening methodology. The subject of report D30.4 [4] was the link between assessments of the appropriate realization of the defence-in-depth (DiD) concept and extended PSA. The authors have described which PSA insights can be used for DiD assessments and provide recommendations for appropriate risk measures and on structuring of PSA models to support DiD assessments. Report D30.5 [5] has investigated risk measures for an extended L1 L2 PSA. The authors discuss the validity of commonly used risk metrics and provide recommendations on the use of risk measures for screening, for the development of PSA models, and for supporting decision making.

The present report D30.6 has two main objectives: firstly to integrate the conclusions derived in the aforementioned reports and secondly, to discuss the use of insights from extended PSA for risk-informed decision making (RIDM).

Initiating events identification for extended PSA

The following refined methodology for initiating events identification, screening and bounding analysis for an extended PSA consists of four major steps and is further developed in section 3:

1. Comprehensive identification of events and hazards and their respective combinations applicable to the plant and site,
2. Initial frequency claims for events and hazards and their respective combinations applicable to the plant and the site,
3. Impact analysis and bounding assessment for all applicable events and scenarios. Events are either screened out from further more detailed analysis, or are assigned to a bounding event (group), or are retained for detailed analysis,
4. Probabilistic analysis of all retained (bounding) events or groups at the appropriate level of detail.

Probabilistic safety objectives

The formulation or acceptance of safety objectives is in the responsibility of authorities which are in charge of public safety while the safe operation of NPPs is the responsibility of utilities. The report discusses this safety objectives topic but the proposed considerations shall not interfere with these responsibilities.

On the basis of [5], in section 4, risk measures are recommended for L1 and L2 PSA each, and quantitative safety objectives are discussed in section 7.

For L1 PSA, the “fuel damage frequency (FDF)” is considered as a useful measure. It contains the well-known “core damage frequency”, but in addition extends to all other potential locations in a site where fuel damage could occur. Furthermore, the “radionuclide mobilization frequency” is suggested, taking into account accidents inducing radioactive releases without fuel melt (for example, primary circuit water release in case of SGTR for PWRs).

The quantitative objectives for FDF should, of course, be consistent with the established CDF figures. Therefore, as a first step of introducing FDF, the existing CDF objectives can be directly applied to FDF. This is more than just a formal step, since it means, for example, taking into account the spent fuel on the site in addition to the core.

As a second step, in a perspective of harmonization, it is recommended that the organizations involved agree on a common definition of fuel damage. In a third step, attempts should be made to arrive at a harmonized safety objective for FDF: it seems that 1 E-5/year (for all initiating events) could be the order of magnitude for such a safety objective, based on a compilation of present figures. **But the main point is that such a safety objective for FDF should cover each and every initiating event (internal and external), and all sources of fuel (in particular core and SFP) and all units on a site.** Therefore, even if the figure itself may be not much more stringent than existing values, the inclusion of all relevant aspects means a significant challenge for PSA analysis and plant design.

For L2 PSA there is already a widespread good practice to identify the frequency of the loss of containment functions. The application of this measure is further encouraged, with the following remarks.

It is recommended to distinguish the possible containment failure modes, depending on the NPP design, especially:

- intact containment with design basis leakage,
- intact containment with filtered venting,
- loss of containment function due to a leak or rupture of the containment structure (after a short term (e.g. energetic) phenomena or a slow phenomena (e.g. basemat penetration by the corium),
- loss of containment function due to failure of containment isolation systems (e.g. open ventilation systems, open hatches),
- loss of containment function due to bypass through interfacing systems (for BWR including non-isolated break of feedwater or steam lines outside of the containment),
- loss of containment function due to bypass through steam generator tube leak (PWR only).

One purpose of L2 PSA shall be to verify the efficiency of SAM strategies to maintain the confinement function during the severe accident progression. Using quantitative objectives for the conditional probability for the loss of containment function under the condition of fuel damage (from all potential sources, including the containment of the SFP) can be helpful for this purpose, for example:

- for existing plants where SAM strategies have been developed for fuel damage conditions, a conditional probability of less than 10% for the loss of containment function could be a reasonable objective
- for new plants that include SAM strategies in the initial design, such objective could be reduced to 1%.

For such an application of L2 PSA, appropriate success criteria for SAM strategies can be derived: for example, for successful filtered containment venting with intact containment, or for the use of mobile equipment for the NPP

long term accident management (if procedures exist and are routinely tested). This will highlight solutions to manage accidents where equipment needed for both accident prevention and mitigation is not available (due to long term station blackout for example). Indirectly, such application of L2 PSA will facilitate to examine quantitatively the independence between accident prevention provisions and accident mitigation provisions (see discussion on DiD below).

Measures of the “total risk” are discussed in the report based on L2 PSA results. This total risk can be calculated by aggregating the risk due to all event sequences into a single metric by summing up all activity releases multiplied by their respective frequencies. This is meaningful for the extended PSA concept but needs to have such an extended PSA available. A suggestion for a quantitative total risk target is provided in this report.

Extended PSA and defence in depth (DiD) concept

Keeping in mind the complementary objectives of DiD and PSA, it is recommended that DiD implementation and PSA are developed independently of each other. However, beyond this basic concept of independence there are a few issues which establish links between DiD and PSA (section 5):

- PSA should be structured in such a way that the individual levels of DiD can be identified ,
- DiD as well as PSA have their own concepts for including or dismissing events or phenomena from their respective analyses ; it is not recommended to harmonize these features ,
- the evolution of the DiD concept is not related to the progress in PSA methods,
- if PSA shows that a particular level of DiD does not contribute significantly to reducing risk, or if PSA indicates that even without a particular level of DiD risk targets can be met, there are arguments to relieve DiD requirements for this particular plant; on the other hand, if PSA indicates a high risk, it is advisable to improve the design, possibly by strengthening the application of the DiD principles.

In order to define a way to go beyond the above considerations, further investigations have been developed during the project about the specific roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations.

The common expression “risk informed decision making” captures very well that decision making will have to consider many issues, PSA being just one of them. Implicit and explicit utility considerations on decision alternatives will necessarily have a strong subjective component. Basically, the decision maker is faced with the question of how to combine different values into a single decision. Section 8 of this report provides suggestions how to do this in a logical and comprehensible way. From the PSA point of view, it is adequate to mention that PSA methods are flexible enough to provide the decision maker with almost all technical evaluations which he might ask for. It is nevertheless prudent that decision makers are aware of the strengths and weaknesses of PSA and seek support from PSA experts, especially to discuss whether the PSA status is consistent with its application to support decision-making.

ASAMPSA_E PARTNERS

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

1	Institute for Radiological Protection and Nuclear Safety	IRSN	France
2	Gesellschaft für Anlagen- und Reaktorsicherheit mbH	GRS	Germany
8	Cazzoli Consulting	CCA	Switzerland
17	NCBJ Institute	NCBJ	Poland
20	NIER Ingegneria	NIER	Italy
28	AREXIS S.A.R.L.	AREXIS	France

CONTENT

MODIFICATIONS OF THE DOCUMENT	3
LIST OF DIFFUSION	4
Glossary	6
Executive Summary	9
ASAMPSA_E Partners	12
Content.....	13
Abbreviations	15
1 Introduction.....	16
1.1 Operational Understanding of Risk for Nuclear Power Plants	16
1.2 Capabilities and Limitations of PSA models	17
1.3 Structure of the Report	18
2 Summary of the Lessons Learned from the Fukushima Dai-ichi accident	19
3 Recommendations on Identifying Initiating Events and Hazards for an Extended PSA	22
3.1 General considerations for initiating events selections	23
3.2 Screening criteria.....	24
3.2.1 Qualitative screening criteria	24
3.2.2 Quantitative screening criteria	25
3.3 Plant response analysis, hazards impact analysis and bounding analysis.....	27
3.3.1 General consideration	27
3.3.2 Applicability analysis.....	27
3.3.3 Impact analysis.....	28
3.3.4 Plant response analysis for combinations of hazards including less intense scenarios	33
3.3.5 Bounding analysis	33
3.4 Selection of the individual internal initiating events to be considered in a single unit PSA	35
3.5 Selection of the individual internal hazards scenarios to be considered in a single unit PSA.....	36
3.6 Selection of the individual external hazards scenarios to be considered in a single unit PSA	39
3.7 Selection of the combined/correlated hazards scenarios in a single unit PSA	44
3.8 Selection of initiating events for multi-units, multi-sources PSA.....	45
4 Recommendations on Risk Measures for an Extended PSA	49
4.1 Risk Measures for an Extended Level 1 PSA.....	50
4.2 Risk Measures for an Extended Level 2 PSA.....	51
4.2.1 Measure for loss of containment function.....	51
4.2.2 L2 PSA total risk measure	52
5 Recommendations on the Link between Defence-in-Depth and Extended PSA	53
6 Evolutions of Risk Assessment and Risk-informed Decision Making	57

6.1 The PSA assessment of DiD by NIER	57
6.2 Common Risk Target by CCA	63
6.2.1 CCA's Total risk measure definition and risk target.....	64
6.2.2 Common Risk Target and analysis of results and decision making	65
6.2.3 Common Risk Target and severe accident management.....	67
7 Safety Objectives for an Extended PSA	69
7.1 Safety objectives from existing PSA Compiled by OECD/NEA.....	69
7.1.1 Summary of a NEA survey from 2009	69
7.1.2 Summary of a NEA survey from 2012	72
7.2 Recommended Safety Objectives for Level 1 PSA Risk Measures	74
7.3 Recommended Safety Objectives for Level 2 PSA Risk Measures	75
7.3.1 Measure for loss of containment function.....	76
7.3.2 L2 PSA total risk measure	77
8 Improving Decision Making Using Extended PSA Results	77
8.1 Current Understanding of RIDM Approaches	77
8.2 Extensions of RIDM Approaches.....	79
8.2.1 Practical approach to the implementation of integrated RIDM process.....	79
8.2.2 Some insights from NASA's RIDM Handbook.....	83
8.3 Additional Remarks on RIDM Approaches.....	88
8.4 As Low As Reasonably Achievable and Extended PSA Results.....	91
9 Summary	92
9.1 Introduction	92
9.2 Identifying Initiating events and hazards.....	92
9.3 Recommendations on Risk Measures and safety objectives for an Extended PSA	94
9.4 The Link between Defence-in-Depth and Extended PSA.....	95
9.5 Improving Decision Making Using Extended PSA Results	96
10 List of References.....	98
11 List of Tables.....	103
12 List of Figures	103

ABBREVIATIONS

CCF	Common cause failure
CDF	Core damage frequency
CFF	Containment Failure Frequency
CERP	Conditional early release probability
CLRP	Conditional Large Release Probability
DBA	Design basis accident
DiD	Defence in depth
DSA	Deterministic Safety Analysis
EOP	Emergency operating procedures
ERF	Early release frequency
FDF	Fuel damage frequency
HRA	Human reliability analysis
IE	Initiating event
IRIDM	Integrated risk informed decision making
LRF	Large release frequency
NPP	Nuclear power plant
PSA	Probabilistic Safety Analysis (L1, L2, L3 : level 1, 2, 3).
PDSF	Plant damage state frequency
PIE	Postulated initiating event
PSA	Probabilistic safety assessment
RIDM	risk informed decision making
RMF	Radionuclide mobilization frequency
RR	Research reactor
SAMG	Severe accident management guidelines
SFPDF	Spent fuel pool damage frequency
SSC	Systems, structures and components
VTA	Value tree analysis

1 INTRODUCTION

The ASAMPSA_E project has investigated the concept of extended PSA (cf. [1]) and its implications for PSA modelling and PSA methods. Within WP30, several specific issues were discussed in more detail and dedicated reports were published. In report D30.2 [2] the authors have looked at available information about the accident at the Fukushima Daiichi power plant from the point of view of PSA and at recent PSA models for NPP in general. This led to the identification of several areas where probabilistic methods should be enhanced in light of extended PSA. The respective lessons learned were transferred to more than 80 specific recommendations. Report D30.3 [3] investigated the approach for identifying initiating events and hazard scenarios for an extended PSA. The authors have derived recommendations for a comprehensive screening methodology. The subject of report D30.4 [4] was the link between assessments of the appropriate realization of the defence-in-depth (DiD) concept and extended PSA. The authors have described which PSA insights can be used for DiD assessments and provide recommendation for appropriate risk measures and on structuring of PSA models to support DiD assessments. Report D30.5 [5] has investigated risk measures for an extended L1 or L2 PSA. The authors discuss the validity of commonly used risk metrics with regard to certain aspects of risk and provide recommendations on the use of risk measures for screening, for the development of PSA models, and for supporting decision making. The implications of multi-unit, multi-source PSA models are explicitly considered.

This report has two main objectives. Firstly, this report aims at integrating the recommendations derived in the aforementioned reports under explicit consideration of insights in other activities of the ASAMPSA_E project and by reflecting PSA end user's needs as documented in the respective ASAMPSA_E survey [6]. To this end, this report includes sections on the recommendations from topical reports D30.3 to D30.5 [3], [4], [5]. These recommendations are then refined based on overall insights of the ASAMPSA_E project, on feedback from PSA end-users and other stakeholders, and on the discussion in this report.

Secondly, this report discusses the use of insights from extended PSA for risk-informed decision making (RIDM). This is an extension of previous activities. To this end, this report briefly presents the general framework for RIDM as it is currently understood and discusses upcoming enhancements and developments for RIDM approaches. Moreover, strengths and limitations of current PSA models and in particular of the extended PSA approach are briefly presented. Against this background, the second main objective of this report is to identify recommendations on the use of extended PSA for RIDM.

In order to set the stage for the remainder of the report, some important issues have to be briefly mentioned.

1.1 OPERATIONAL UNDERSTANDING OF RISK FOR NUCLEAR POWER PLANTS

Following D30.5 [5], we present the following remarks.

There are multiple aspects of risk. This applies to nuclear power plants and other facilities. The discussion in this report is limited to the specific aspect of risk as described by the fundamental safety objective in IAEA SF-1 [9], as referenced in [5], p. 4:

“The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.”

Thus, the risk investigated in this report is the risk of failing to meet this objective. More specifically, the report will focus on the risk of significant damages outside of the plant boundary, i.e. accidental releases with potential of affecting a large number of people and a significant part of the vicinity of the plant for an extended period of time.

Following the ASAMPSA2 guidelines, [7], we employ the following definition of risk.

Risk is defined relative to hazards or accidents. A hazard is something that presents a potential for health, economical or environmental harm. Risk associated with the hazard is a combination of the probability (or frequency) of the hazardous event and the magnitude of the consequences. The consequences can be represented in several dimensions. A usual engineering definition of risk associated with an event i is:

Risk(event i) = “the probability of an event i ” x “the consequences of an event i ”.

With D30.5 [5] the authors define risk measures and risk metrics as follows.

“In the context of risk measurement, a risk metric is the concept quantified by a risk measure.” [69]. The risk metric is a feature or property of the risk model like e.g. a consequence, a transition between two states of the risk model, or contribution to other risk measures. The risk measure includes in addition the quantification procedure for the risk metric. Risk measures are used for the representation, discussion, and interpretation of PSA results. For risk measures like core damage frequency, conditional failure probability of a system, or basic event importance for CDF to be used, the risk model has to support the respective risk metrics. However, under the ASAMPSA_E project the two terms risk metrics and risk measures have been used without distinction. For this reason, in this report, the term risk measure will be used as a more comprehensive term even if only the risk metric is meant. The term risk metric will be used if specifically the metric aspect is addressed or if there would otherwise be ambiguities.

The annex of D30.5 [5] gives additional theoretical background for the interested reader.

1.2 CAPABILITIES AND LIMITATIONS OF PSA MODELS

One commonly stated objective of PSA for NPP is to quantify the risk of NPP as defined above in a realistic or best-estimate manner. To this end, analysts develop a complex logical model of the development of scenarios which could end in accidental states and releases to the environment. Respective methods are described in guidelines and requirements, e.g. in SSG-3 [10] for L1 PSA and SSG-4 [11] for L2 PSA. Incidentally, the ASAMPSA_E project aims to enhance these methods. Depending on the scope, level of detail and level of conservatism employed for the PSA model, PSA can provide quantitative results on the risk profile of the plant, the relevance of safety features in terms of risk, or the importance of potential weaknesses in terms of risk. Detailed PSA models,

particularly for internal events, have reached a rather high degree of maturity and have significant capabilities in this regard.

Nonetheless, even an extended PSA produced to the state-of-the-art and incorporating the ASAMPSA_E recommendations would have several important and fundamental limitations. Importantly, PSA analysts have to use simplifying and conservative assumptions just to construct a logical plant model (e.g. on accident sequences, success criteria, severe accident phenomena, definition of basic events, etc.). Sequences are then formulated based on enveloping scenarios even for internal events PSA. Other commonly applied modelling elements like human reliability analysis (HRA), common cause failure (CCF) assessment, or plant response to hazard impact introduce further simplifications based on enveloping boundary conditions. Moreover, different parts of the PSA model will be developed to different levels of detail and conservatism, depending on their risk contribution, the resources needed for the development, and the availability or lack of knowledge on relevant phenomena and plant behaviour. In addition, there are likely parts of the risk which are, either intentionally or due to lack of knowledge, not included in the PSA model. These observations are in principle applicable to all kinds of PSA models, even considering advanced approaches as dynamic PSA, fuzzy probability approaches, or multi-state Markov-process modelling.

These limitations are important for the interpretation of recommendations in this report. Since PSA models require resources, which could be used for other worthy purposes (e.g. plant safety upgrading), insights from PSA models and in particular from refinements of PSA models should provide added value. We emphasize that PSA analysts have to determine whether more detailed PSA models can provide relevant contributions to decision makers or whether PSA models with a higher degree of conservatism would be sufficient to resolve the issue.

1.3 STRUCTURE OF THE REPORT

The remainder of this report is organised as follows. In section 2, we repeat the summary of the report on lessons learned for PSA from the Fukushima Daiichi accident D30.2 [2] and provide additional explanations on the interpretation of our recommendations. In section 3, we present the recommendations on identifying initiating events and hazards based on D30.3 [3]. In section 4, recommendations on risk measure for extended PSA based on the results in D30.5 [5] are given. The following section 5 summarizes the recommendation on the use of PSA for DiD assessments based on D30.4 [4]. The subsequent section 6 discusses selected issues for the evolution of safety assessment and risk informed decision making, which are not covered by the preceding sections, and which have been discussed within the ASAMPSA_E project. Thereafter, in section 7 we discuss safety objectives on the risk measures presented in section 4, both for L1 and L2 PSA risk measures. This discussion will also consider the implications of an eventual L3 PSA, although no criteria related to L3 PSA will be stated. In section 8, we present the current status on RIDM approaches, discussion potential enhancements and extensions of RIDM, especially in light of extended PSA and give recommendations on the use of extended PSA results in actual RIDM applications. All sections consider the findings of the report on lessons learned for PSA from the Fukushima Daiichi accident D30.2 [2], PSA end-user expectations from D10.2 [6] and other input and comments related to the project activities.

2 SUMMARY OF THE LESSONS LEARNED FROM THE FUKUSHIMA DAI-ICHI ACCIDENT

In the report on lessons learned from the Fukushima Dai-ichi accident for PSA, D30.2 [2], the ASAMPSA_E project has provided the following summary.

“The Fukushima Dai-ichi accident is a [...] sequence of equipment, planning and institutional failures resulting in releases of radioactive materials, following the [Great East Japan Earthquake and the subsequent tsunami(s)]” [70], p. 1. Although the seismic hazard was considered both in the site evaluation and design of the Fukushima Dai-ichi NPPs, the impact from the earthquake on 11 March 2011 exceeded the licensing based design basis ground motion. More importantly, although the tsunami hazard was considered both in the site evaluation and design of the Fukushima Dai-ichi NPPs, the related risk was underestimated. Subsequent additional protective measures taken as result of a re-evaluation after 2002 were insufficient to cope with the tsunami run-up values on 11 March 2011 and related phenomena (hydrodynamic forces, debris impact) [71]. Therefore, the plants were not able to withstand the tsunami impact.

In [the D30.2] report, the implications from the Fukushima Dai-ichi accident for L1 and L2 PSA and to decision making using PSA results have been investigated in the framework of the ASAMPSA_E project. Since the scope of PSA in Japan in general as well as for the Fukushima Dai-ichi units did not extend to the relevant scenarios, direct lessons to be learned on these issues are limited. Therefore, the authors have used their experience on the current status of L1 and L2 PSA models worldwide and in Europe as well as the insights gained from the ASAMPSA_E questionnaire for identifying further gaps PSA methodologies and for derived related conclusions and recommendations.

[...]

In view of Fukushima Dai-ichi accident, the existing (Level 1 and Level 2) PSAs for NPPs manifest specific insufficiencies about the identification of rare events and their combinations. Efforts should be put mainly on the improvement of the adequacy of criteria for the identification of initiators, including rare events and their combinations, of the assessment of their frequency of occurrence versus severity and of the models for components/structures failure. More generally, initiating events should be systematically determined for all operation modes and relevant sources of radionuclides, and include all hazard impact with a special focus on low probability/high impact events, which can significantly challenge the safety concept of the plant and thus may give rise to cliff-edge effects. Specific to hazards, this includes the systematic extension of the PSA scope to beyond design basis hazard scenarios (at frequencies below $\sim 10^{-4}$ per year) as well as combinations of hazards events with other events, which includes correlated hazards as well as uncorrelated combinations with sufficient probability. Internal and external hazards shall include natural and man-made hazards that originate externally to both the site and its processes. The list of external hazards shall be as complete as possible. Justification shall be provided on its completeness and relevance to the site.

Where the results of engineering judgement, deterministic and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations shall be considered in the PSA in principle. A systematic check of dependencies, taking account of all correlation mechanisms like source correlated hazards or consequential failures shall be performed. The combined impact on the plant shall be investigated.

The screening process shall be established in a way that ensures that no relevant risk contributor is omitted. Respective screening criteria should be commensurate to overall PSA results and ensure that low probability/high impact events are not screened out. To that effect, a set of suitable risk metrics and threshold values (including adequate Level 1 and Level 2 metrics) should be defined. All arguments in support of the screening process shall be justified.

Similarly, PSA Level 1 end states at the interface to the PSA Level 2 should be transferred to and treated within Level 2. Specifically, PSA Level 1 states with containment failure prior to core damage, e.g. due to hazard impact, should routinely be transferred.

During the development of accident sequence models for a PSA and for reliability assessments of systems, components, and operator actions best estimate boundary conditions should be used to the extent practicable. Specifically, analysis times for scenarios as well as mission times for safety functions should be extended until a defined stable or an accidental state has been reached as demonstrated with appropriate justification. PSA models should systematically consider dependencies between systems affecting safety function availability, including the effect of non-safety systems. Particularly for the accidental phase, the analysis should be extended to likely detrimental or aggravating actions, which operators or crisis management staff might erroneously derive based on their knowledge, existing SAMG and the available information during the accident. Particularly for PSA Level 2, modelling of releases up to adequate release categories should always be performed and reflected in the development of the accident progression event tree. Moreover, release pathways in addition to aerial release like water, ground should be considered and modelled as appropriate. Containment failure and containment failure modes need to be treated comprehensively for the different accidental scenarios. All relevant release pathways, including those opened e.g. by hazard impact, should be part of the model.

The probabilistic assessment of EOP and any accident management procedures/measures should systematically consider accessibility and operability of equipment as well as feasibility of measures in case of hazard impacts. Especially, severe accident management measures and guidelines should be checked with PSA methods on reliability, for identifying weaknesses in procedures as well as vulnerabilities of the plant and potentials for improvements. For longer-term scenarios, likely repair actions should be included in the PSA models as well.

Another important field is the assessment of human reliability (HRA) for the purposes of PSA. HRA needs to include a more comprehensive and realistic assessment of the effect of hazards on human performance. Despite numerous HRA methods being available, there is a lack of methods for the assessment of knowledge-based actions like e.g. recovery action, of action in high-stress situation like e.g. operability under accidental conditions, and of potentially aggravating actions during and before the event. Particularly with regard for HRA for PSA Level 2, it is necessary to consider performing shaping factors like exposure to high radiation fields, actions with protective equipment, and long term effects like fatigue or the effect of shift changeover. Moreover, the impact of multiple layers of decision makers on accident management should be assessed.

PSA models for multi-unit sites should systematically include relevant dependencies on the systems levels, e.g. via shared support systems or buildings, as well as dependencies on the accident sequence level, e.g. via

the impact of a severe accident in one unit on measures or systems in another unit, into their PSA models. In addition, shared staff resources, mobile equipment, etc. have to be considered. This might require dedicated human reliability analysis. For adequately covering complex scenarios simultaneously affecting several units, site risk PSA models should be developed.

Another important challenges in light of the Fukushima Dai-ichi accident pertains to the assessment of the adequacy of DiD. PSA results and insights should be used complementary to deterministic approach to assess the reliability and independence of measures on the different levels of DiD. Particularly, PSA should be used to assess and further strengthen measures for design extension conditions (DiD Level 4). DiD assessments should cover all operating modes and internal as well as external hazards.

The insights in this report confirm that safety related decision making should be made within a risk-informed context, encompassing deterministic, probabilistic and other information. The fundamental approach used for decision making should be the continuous improvement of plant safety to the extent reasonably achievable [73]. In that sense, “even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures to lower the risk further should be implemented.” [74], p. 32. Thus, PSA results should be used to systematically identify plant vulnerabilities for all scenarios which are not deemed to be practically eliminated, and to demonstrate the effectiveness of potential plant improvements.

Risk-informed decision making should consider the risk profile of the plants based on sets of PSA risk measure/metrics for Level 1 and Level 2, which are understood and presented as uncertainty distributions. These should be accompanied with sensitivity analyses demonstrating the influence of different important sources of uncertainty. Risk-informed decision making should consider always potential long-term consequences of accidental releases. Moreover, the decision making should take into account uncertainty assessments on safety margins, particularly those to known or suspected cliff-edge effects.

In summary, the Fukushima Dai-ichi accident justifies the basic assumption of the ASAMPSA_E project of extending the scope of PSA to include all operating modes, all events and hazards, and all relevant potential sources like e.g. the spent fuel pool. It has to be acknowledged that extended PSA models, which cover all the scenarios and events recommended above, will require a lot of work on the development of efficient PSA methods, generation of (plant-specific) data, further research on such diverse areas as human reliability, geosciences, and severe accident phenomena, and on the improvement of PSA models themselves. In this sense, the PSA community is faced with a series of complex and difficult problems. “But the fact that this problem¹ is complex can no longer be an excuse for doing nothing.” [71]. The ASAMPSA_E project will tackle the aforementioned issues during the remainder of the project.”

With respect to the aforementioned summary and with respect to the 87 specific recommendations documented in D30.2 [2], the following comments on their proper interpretation are added here.

¹ The remark was in reference to gun control issues in the U.S.A after the Newtown massacre.

The recommendations are often developed in light of an “ideal” PSA model, which aims at modelling the risk from NPP at a high level of accuracy. Depending on the intended use of PSA insights, applicable regulation, and stakeholder interests, this might not be the applicable objective for a specific PSA. Therefore, all recommendations have to be interpreted in light of the objectives of the PSA and its intended use, e.g. in risk-informed decision processes.

In addition, the ASAMPSA_E guidances often recommend to (systematically) consider a certain aspect or to extend the scope of the PSA (modelling). This does not imply a call for the development of specific, detailed, and comprehensive probabilistic models for these issues. As with all PSA modelling, the starting point needs to be a systematic assessment of the relevance of the respective issues. This initial step already provides added value. If the issues are potentially relevant, the screening should be continued with an initial, simplified approach. The need for further, more detailed modelling needs to be judged against the results of the PSA as well as PSA objectives.

Similarly, if we recommend to include certain aspects, for which PSA can contribute addition insights, within a risk-informed decision making process, this does not change that the first question to be answered always needs to be: is that PSA information relevant to the issue to be decided and also to the responsible decision maker(s). Only if both conditions are fulfilled, further consideration should be given to the kind of information provided to the decision maker, the scope and level of detail of PSA analyses, and the appropriate risk measures and safety objectives.

3 RECOMMENDATIONS ON IDENTIFYING INITIATING EVENTS AND HAZARDS FOR AN EXTENDED PSA

Within ASAMPSA_E, the deliverable D30.3 [3] on the methodology for selecting initiating events and hazards in an Extended PSA has been produced. The identification of all initiating events, hazards (internal or external) and their combinations, which contribute to the risk induced by a NPP (or several NPPs on a nuclear site) connected to its environment, is a major task to be done during the development of an extended PSA.

The report [3] tries to discuss relevant methodologies for this purpose. It includes considerations on:

- the existing basic approach for the identification of initiating events and hazards in PSA (screening methodologies),
- the practices in countries and proposed by international standards, especially from IAEA,
- the appropriate risk metrics and screening thresholds to be used in the process of initiating events and hazards selection for an extended PSA,
- the link between deterministic and probabilistic approaches for the selection of initiating events,
- the screening of high impact events, possibly correlated, associated to a low frequency of occurrence, but that can induce major consequences on a NPP,
- the specificities of hazards screening.

From these considerations, the report [3] proposes a methodology to select initiating events and hazards for the development of an extended PSA. The following sections summarize the relevant statements of [3].

3.1 General considerations for initiating events selections

Initiating event identification and selection (screening “in” or “out”) for an extended PSA have to consider the objectives for which the PSA is produced. These objectives should help defining:

1. the aspects of risk which are relevant and for which the PSA model should provide results,
2. the risk measures that are relevant in interpreting PSA results,
3. the values of risk criteria for relevant risk measures, to which the extended PSA results should be compared,
4. an acceptable scope, level of details, and level of conservatism for the PSA.

These objectives may differ for a NPP during design or operation phases.

The screening approach for an extended PSA is based on the following assumptions on PSA scope:

1. the risk is (or will be) described by L1 and L2 PSA,
2. the risk measures for reporting PSA results for the unit and the site (if applicable) may differ depending on the PSA application but it should include:
 - a. core damage/fuel damage frequency as the main L1 PSA results,
 - b. As a minimum for L2 PSA results, the large release frequency and the early release frequency measures,
 - c. Preferably for the L2 PSA results, the frequencies of an appropriate number of release categories in order to calculate a meaningful risk profile.

A reasonable approach is to introduce progressively the sources of risk in the PSA model and to select the relevant internal initiating events and hazard scenarios:

1. start with internal initiating events screening and PSA model development,
2. continue with internal hazard scenarios and integration into PSA model,
3. extend by external hazard scenarios,
4. complement with combinations of hazards and correlated hazards,
5. complete by extension to multi-units and multi-sources considerations.

This approach assumes that a PSA model for a specific hazard scenario will benefit from the use of the available internal events PSA. Conceptually, each hazard scenario will be an initiator for an initiating event directly challenging some safety functions.

The screening entails the following major steps.

For all operating states and all relevant sources on the site:

1. identification of possible initiating events, hazard scenarios, and combinations thereof,
2. plant response analysis and suitable grouping of initiating events or hazard scenarios to a representative group,
3. for each representative group, bounding analysis consisting of
 - a. qualitative plant response,

- b. quantitative assessment of the likelihood of the scenario, of its consequences for the plant,
4. definition of a set of initiating events and hazard scenarios for extended PSA analysis.

The next sections discuss some good practices for each step of the selection of extended PSA initiating events.

3.2 SCREENING CRITERIA

The ASAMPSA_E report D30.2 [2] includes the following recommendations on screening criteria.

“[S]creening criteria should be commensurate to overall PSA results and ensure that low probability/high impact events are not screened out. To that effect, a set of suitable risk metrics and threshold values (including CDF and LRF) should be defined.”

“The screening of initiating events for detailed consideration in the PSA should be performed not only based on PSA Level 1 risk metrics but also on PSA Level 2 risk metrics like e.g. different release categories, including at least one risk metric for large releases and one for early releases. Screening thresholds on the risk measures for the Level 2 risk metrics should be defined and justified. Initiating events (including hazard scenarios) should only be screened out from the PSA, if they are screened out based on Level 1 and on Level 2 risk metrics. In addition, if a PSA Level 3 is intended, the screening process should include Level 3 risk metrics and thresholds as well.”

In addition, any screening procedure should be consistent with the respective goals set out by WENRA, which state for new reactor designs that “accidents with core melt which would lead to early or large releases have to be practically eliminated” [74], p. 24, and for existing reactors that “any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable” [78], p. 23.

The recommendations given below are based on these ideas.

3.2.1 QUALITATIVE SCREENING CRITERIA

With regard to qualitative screening criteria that can be used to screen out scenarios from an extended PSA application of the following criteria appear clearly to be a good practice:

1. the event poses no challenge to safety systems,
2. the event is bounded by another initiating event or the induced accident scenario is already included in the PSA (from other causes) (in that case, there is no need for a specific development of the PSA but its probability shall be considered in conjunction with another event (or group)),

If the event (external hazard) has the potential to induce catastrophic levels of destruction on the plant and regional scale offsite consequences such scenarios cannot be screened out from the extended PSA. Such scenario should be subject to the need for practical elimination.

The following qualitative screening criteria may be less relevant:

1. the event is very slow in development and fully efficient protection can be put in place on the NPP against the event;
an explicitly bounding assessment shall be performed for the traceability of screening process and emphasize in PSA approach the importance of the “fully efficient protection”. This information can be used during NPP normal operation (maintenance, tests for the protection ...),
2. the event has a very low frequency of occurrence (e.g. 10^{-7} / yr;
this is actually not a qualitative but a quantitative screening criterion and should be treated as such,
3. the event has a low frequency of occurrence and several trains of relevant safety systems are available. This is an implicit bounding assessment; an explicit bounding assessment would improve the traceability of screening process.

3.2.2 QUANTITATIVE SCREENING CRITERIA

The following refined methodology for initiating events identification, screening and bounding analysis for an extended PSA consists of four major steps

1. comprehensive identification of events and hazards and their respective combinations applicable to the plant and site,
2. initial frequency claims for events and hazards and their respective combinations applicable to the plant and the site,
3. impact analysis and bounding assessment for all applicable events and scenarios. Events are either screened out from further more detailed analysis, or are assigned to a bounding event (group), or are retained for detailed analysis,
4. probabilistic analysis of all retained (bounding) events at the appropriate level of detail.

Numerical probabilistic safety targets are applied differently depending on countries. Interpretation of quantitative screening criteria may also differ from one country to the other. Nevertheless the following approach for defining quantitative screening criteria (from [3]) for the selection of PSA initiating events is proposed as a good practice.

1. Based on regulatory acceptance criteria or established international guidance for CDF/FDF (e.g. 10^{-5} /yr) and LRF/LERF, the maximum screening quantitative criteria shall be set to 1 % of that value. This results in the following minimum criteria:
 - a. $FDF_{event} < 10^{-7}$ /yr
($RMF_{event} < 10^{-7}$ /yr)
 - b. $LRF_{event} < 10^{-8}$ /yr
 - c. $ERF_{event} < 10^{-8}$ /yr
($LERF_{event} < 10^{-8}$ /yr)
2. If L1 and L2 PSA results are already available, then the above limits shall be reduced to 1 % of the overall PSA results (if relevant) or kept unchanged.

- a. $FDF_{event} < 1\% FDF_{overall}$ if $< 10^{-7}$ /yr
($RMF_{event} < 1\% RMF_{overall}$ if $< 10^{-7}$ /yr)
 - b. $LRF_{event} < 1\% LRF_{overall}$ if $< 10^{-8}$ /yr
 - c. $ERF_{event} < 1\% ERF_{overall}$ if $< 10^{-8}$ /yr
($LERF_{event} < 1\% LERF_{overall}$ if $< 10^{-8}$ /yr)
3. An initiating event of hazard scenario should be screened out from extended PSA detailed analysis, only if it can be screened out against all quantitative screening criteria,
 4. Very low frequency events associated to potential major consequences are often associated to high uncertainties; a prudent approach shall be applied and possibilities to reinforce the plant defences shall be kept open independently of the extended PSA considerations,
 5. Bounding analysis to estimate the criteria above shall be preferred during the screening approach ;
 6. The bounding analysis shall consider both single unit (source) and multi units (sources) ; the same numerical criteria shall be applied for a single and multi-units site ;
 7. A more precise analysis is needed for events which cannot be appropriately represented by a probability per year (typically reactor refuelling phase or seasonal effects) ; in that case, the maximum probability value for that event within the year shall be preferred when applying quantitative screening criteria.

Explanation of the point 7: an important remark relates to the differences between events treated properly by frequency of occurrence (per year) and events properly treated by a probability of occurrence within a year. For the former, the probability for the occurrence of the event is distributed uniformly over time and the event probability scales inversely with the reference time period, i.e. $T_2 \cdot p_{T_1} = T_1 \cdot p_{T_2}$. For the latter, the event might happen with a certain probability p in a time interval ΔT within a year. Obviously, the “event frequency” does not change for different reference intervals, if these intervals cover ΔT , i.e. $p = p_{T_2} = p_{|\Delta T|} \Delta T \subset \{0, T_1\}$, $\Delta T \subset \{0, T_2\}$.

It is recommended performing screening based on time-averaged FDF/CDF in general but this is not applicable for events which are properly described as a probability per year. Salient examples of these types of events include internal initiating events specific to refuelling operation or other shutdown operating states. For hazard scenarios, these type of events are relevant e.g. to hazards for which the frequency of occurrence strongly varies over a year, e.g. due to seasonal variations. Rescaling those probability-per-year types of events to an observation period of one year is not appropriate for screening purposes. In these cases, it can be more appropriate to use instead the maximum probability value for that event within the year²

If there are indications of significant risk peaks already during screening a more detailed analysis of the scenario is recommended, since it might be related to a potential weakness in the safety design of the plant.

The ASAMPSA_E project acknowledges that low screening values pose a significant challenge to PSA methods and data and might well go beyond the bounds of values, which can be sensibly supported by current knowledge. The

² Conceptually, the check is then against peak FDF(t), LRF(t), and ERF(t). However, an explicit calculation of time-dependent risk measures is not recommended, since this needs to rely on detailed models. For additional discussion on time-dependent risk measures, see D30.5.

ASAMPSA_E project points out that current operating experience and knowledge usually limits frequency estimates for single events and phenomena to values in the range of $1 \cdot 10^{-4}$ to $1 \cdot 10^{-7}$ /yr. Using statistical methods like extreme value statistics to extend limited data far outside of the reference time frame is fraught with large uncertainties and might produce arbitrary results. Such extensions by several orders of magnitude are therefore not encouraged by the ASAMPSA_E project. Instead, available data for the site have to be completed by using regional data and by evaluating historical data or paleogeological information. Since rare mechanisms and phenomena, which could result in severe hazard impacts, might be missing from the available observations altogether, these should be complemented by investigations of such potential mechanism and phenomena. These investigations will often require dedicated simulation models, calculations or expert judgement.

3.3 PLANT RESPONSE ANALYSIS, HAZARDS IMPACT ANALYSIS AND BOUNDING ANALYSIS

3.3.1 GENERAL CONSIDERATION

Plant response analysis is an essential task for the screening of initiating events and hazard scenarios as well as the subsequent development of probabilistic model, both in bounding analysis and in more detailed probabilistic modelling. The overall objectives of plant response analysis are to identify if the safety of the plant (i.e. safety of the fuel or of other sources) is challenged by the event or scenario under investigation, which fundamental safety functions are challenged either directly or by consequential effects, and if provisions for safety functions (SSC, barriers, other features) are effective or not. For hazards scenarios, hazard impact analysis describes the specific aspect of plant response after hazard effects within the plant.

Plant response analysis makes use from all available sources of information about the (transient) behaviour of the plant from deterministic assessments of PIE, deterministic hazard assessments, and existing PSA models.

For screening purposes and for bounding analysis, plant response analysis may rely on conservative assumptions and expert judgement, where specific information on plant behaviour is not readily available in order to limit analysis effort. For detailed PSA model development, plant response analysis is based on plant specific accident sequence analysis.

In the following is a summary of plant response and hazard impact analysis for the screening of external hazard scenarios. The concepts presented are broadly applicable to internal initiating events and internal hazards, even if it is a well-established technique.

3.3.2 APPLICABILITY ANALYSIS

The first step in the screening of external hazards relates to applicability. Analysts need to identify those potential single or combined external hazards that are not relevant to the nuclear power plant and to the site due to site characteristics (e.g. tsunamis usually cannot affect plants located far away from seas and oceans). Use is made of

the results of site investigation and evaluation to screen out hazards not applicable to the site. Expert judgement will play an important role.

3.3.3 IMPACT ANALYSIS

3.3.3.1 Approach

A more detailed deterministic impact assessment is performed for hazards that could not be screened out since they are applicable. The purpose of screening by impact analysis is to eliminate all those potential external events from the initial list of external hazard scenarios that do not have the potential to induce any transient on the plant, i.e. the maximum credible impact caused by an external hazard scenario does not induce any of the internal initiating events of the PSA or any additional initiating events previously not considered in the internal events PSA.

In general, the following two criteria are applied for screening by impact analysis:

1. Severity: the effects of the event are not severe enough to cause damage to the plant, since it has been designed for loads with similar or higher strength due to other event scenarios.
2. Predictability: the event is very slow in developing, and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate and timely response without notably jeopardizing safety.

3.3.3.2 Load parameters

With regard to the first criterion, the most important parameters which best represent the load induced by an external hazard should be specified [10]. All parameters specified for the hazards should be taken into account in performing the impact analysis.

Examples of external event scenarios and associated load parameters are listed below ³:

- 1) external explosion:
 - a. maximum pressure wave [kPa];
 - b. maximum heat flux [W/m^2];
 - c. peak ground velocity (due to vibratory ground motion) [m/s];
 - d. maximum momentum of generated missiles [kg m/s];
 - e. maximum concentration of a toxic substance for a certain exposure duration [ppm/hour].
- 2) external fire:
 - a. maximum heat flux [W/m^2];
 - b. maximum concentration of a toxic substance for a certain exposure duration [ppm/hour]
- 3) extreme wind:
 - a. maximum gust of wind (related to a 2 second period) [m/s];
 - b. maximum of 10 minute average wind speed [m/s].

³ See [D21.3] for a more comprehensive list.

- 4) extreme air temperature:
 - a. maximum and minimum instantaneous temperature [$^{\circ}\text{C}$];
 - b. maximum and minimum average temperature for a certain duration (e.g. daily or weekly average temperature) [$^{\circ}\text{C}$].
- 5) extreme precipitation:
 - a. maximum precipitation intensity for a certain duration (e.g. 10, 20, 60 minute or daily) [mm/min].
- 6) extreme snowfall:
 - a. maximum thickness of snow [cm];
 - b. maximum snow water equivalent [mm/cm].
- 7) lightning:
 - a. peak value of lightning current [kA];
 - b. maximum steepness of the lightning current [kA/s];
 - c. maximum charge of the lightning current [kAs];
 - d. maximum specific energy of the lightning current [MJ/Ω].

3.3.3.3 Maximum impact

The maximum impact that can develop in the vicinity of the site due to an external event (or combination of events) should be determined for the purposes of impact screening. This should be based on reasonably conservative assumptions on those factors that determine the harmful effects of an initiating accident (e.g. assumed maximum freight in a transportation accident). Besides the maximum load induced by the event at the location of the source, the maximum impact on the plant is also assessed and used during screening. These two quantities, i.e. the maximum load at the source and the maximum load that can impact on the plant can be considered identical for most natural events (e.g. extreme wind), but they are usually different for man-made events (e.g. accidents during railway transport). The distance between the event location and the plant, the characteristics of propagation, spread and decay should be taken into consideration to determine the impact on the plant.

3.3.3.4 Maximum credible impact

If engineering estimates prove insufficient for screening, a more detailed analysis should be done as part of bounding analysis and the event should not be screened out at this stage. The maximum load on the plant induced by an external event applicable to the site under realistically possible boundary conditions is called maximum credible impact.

The assessment of the maximum credible impact induced by most man-made external events can be based on site-specific geographical data. Typically, a limiting value can be determined for those parameters of the source that are relevant for the impact (e.g. energy) irrespective of the occurrence frequency of the event. For instance, the maximum pressure wave due to a road transport accident can be assessed by taking into consideration the following:

- 1) substances transported by trucks on roads near the plant (based on transportation records),

- 2) maximum allowed cargo for each substance relevant for the roads in the vicinity of the site (based on national or regional regulations on transport),
- 3) physical-chemical characteristics of the substances transported,
- 4) site specific meteorological data for the assessment of environmental spread,
- 5) geographical data around the site (e.g. topography, terrain).

Estimating the maximum credible impact for a hazard or hazard scenario can be done by expert judgement, informed by all available information including hazard frequency curves. The maximum credible impact should be estimated in a conservative way. If the hazard scenario cannot be screened out in that it does not pose a challenge to the safety of the plant, it should be retained for bounding assessment.

3.3.3.5 Comparison of the maximum credible impact with existing protections

By comparing the maximum credible impact of an external hazard with existing protection of the relevant safety functions enables to decide if the external hazard can be screened out or not. For this reason the protection of the safety functions against the loads induced by external hazards has to be assessed. This is done by assembling all relevant design basis data for the SSCs affected by the external event. In some cases, especially for plants in operation, the information needed for the assessment may be incomplete. Consequently, deterministic screening criteria for certain impacts may be difficult to set. Use should be made of expert opinion on the protection against certain impacts (e.g. heat flux, pressure wave, missile penetration, etc.).

3.3.3.6 Exceedance frequency curves for the maximum credible impact

For many natural hazards screened in as applicable, a maximum impact at the site cannot be determined independent of the occurrence frequency or exceedance frequency. In these cases, the magnitude of hazard impact is effectively not bounded by physical effects or site-specific properties (e.g. tsunami height due to asteroid impact for coastal sites or earthquake magnitude for seismically active regions). Then, a maximum credible impact needs to be determined with explicit reference to frequency of exceedance curves with a reasonably small frequency threshold. This threshold will depend on screening criteria, and might be in the range of $10^{-7}/y$ to $10^{-8}/y$ or even below for PSA. If the analysts cannot demonstrate that the safety of the plant is not challenged by using such assumptions, the respective hazard should be treated by bounding assessment (see below). Often, design basis values are set at exceedance frequencies of $10^{-4}/y$ or $10^{-5}/y$. and the main difficulty for the PSA development is to determine the exceedance frequency curve in the range $10^{-8}/y$ to $10^{-4}/y$.

If a frequency value (or range) for the hazard is set, then the maximum probable impact can be assigned to the load parameter value (or range) of the frequency of exceedance curve. Often, the parameter at the median (“best-estimate”) value of the curve is taken. However, uncertainty bands should be considered at least as sensitivity cases. Defining maximum credible impact for this frequency value (range) at a high percentile (e.g. 95%) of uncertainty bands is recommended. This approach is meaningful if the region of interest of the hazard frequency curve can be determined without excessive uncertainty.

The hazard can be screened out due to impact if the safety of the plant is not challenged by the maximum credible impact (obtained from the low frequency part of the exceedance frequency curve). In that case, the frequency threshold for maximum credible impact (if applicable) shall be consistent with the quantitative screening criteria (see section 3.2.2).

3.3.3.7 Multiple impacts, secondary impact analysis on plant structures and systems

Many external events have more than one harmful effect, including secondary effects, too. For instance, a transportation accident may have simultaneous effects like pressure wave, heat flux, missile impact, release of toxic gases, etc. Furthermore, external fire, external explosion and release of toxic gases can be additional consequences (secondary effects) of an aircraft crash. These complex impacts may have more serious consequences than the individual ones; therefore they should also be taken into consideration.

In order to support the screening investigations in this regard, the Fault Sequence Analyzer method can be useful. This approach or similar analyses can provide valuable insights about potentially challenging combinations of hazard impacts for a specific hazard scenario.

All safety related plant areas affected by the external hazard scenario in question should be mapped for the purposes of plant response analysis in the initial screening phase. In general, the effects induced by external events belong to one or more of the following categories:

- 1) failure of structures: the external event may affect the structures by direct pressure (e.g. wind or snow load), pressure waves (e.g. explosion), ground shakes (e.g. explosion, earthquake), etc., so that the structures and/or the related safety functions are degraded or damaged. The following effects of area events are particularly noteworthy.
 - a. external flooding: undermining of buildings or structures, consequently disabling the safety functions contained.
 - b. Internal and external fire: extreme direct heat flux may destroy/degrade structures.
- 2) Failures in systems: the external event induces failures in systems or components that lead to challenges of plant safety. The following systems are particularly relevant.
 - a. failure of HVAC (Heating, Ventilation, Air Conditioning) system: the external event may affect HVAC functions and may cause partial or total loss of safety systems or components relying on heating or cooling.
 - b. failure of ultimate heat sink: the external event may affect the ultimate heat sink, consequently it may cause partial or total loss of cooling water supply for safety systems.
 - c. electric: the external event may generate electrical or magnetic fields, which may potentially affect transmission of power supply or control signals to safety systems.
 - d. failure of power supply: the external event affects the offsite power and may cause total or partial loss of offsite power or other power supply faults.
- 3) Spreading via failed barriers: Due to failures or unavailability of (designed) barriers, hazard effects spread into the plant leading to challenges to other structures (see the first item) or systems and components (see the second item). This is particularly relevant for flooding and fire hazard events.

- 4) Spreading via systems and components: due to effects in systems or components, which were not designed against (the magnitude of) hazard impact, hazard effects spread into the plant leading to challenges to other structures or systems. One salient example would be the HVAC system, which can spread the effects of fire and flooding scenarios.
- 5) Other direct impact: in a few cases, the event may have such effects that are not covered by the general categories above (e.g. plant isolation/limited accessibility, freezing).

3.3.3.8 Impact analysis on plant personnel

The existing guidance documents focus primarily on the impact of external events on systems, structures and components, without much consideration to effects that may influence the ability of the plant personnel to respond correctly in a timely manner.

The impacts of an external event on plant personnel working open air at a nuclear site as well as the habitability within building enclosures of a nuclear power plant due to toxic gases, heat flux or radiological consequences of accidents at nearby nuclear installations are of high importance. The aforementioned impacts on the plant personnel should be taken into consideration during plant response analysis for initial screening. This is particularly relevant, if the hazard scenario prevents necessary operator actions that are needed to bring and maintain the plant in a stable safe condition.

The accessibility of the plant as well as the conditions and the allowable time for working open air at the site should be evaluated for certain hazards. In general, protective measures are applied to reduce harmful effects on the plant personnel. These measures and their effectiveness shall be taken during screening. For that purpose the design basis loads of the protective measures are compared with the loads induced by the given (external) hazard scenario.

The consequences of accidents with toxic effects, heat flux or radiological effects at nearby nuclear installations should be taken into consideration in order to ensure the habitability of vital service areas within the building enclosures needed to maintain the safe conditions of the nuclear power plant. A significant reduction in health effects can be achieved by using sufficient air filtration and cleaning systems. Therefore, appropriate positioning and orientation of the air filtration equipment also helps to limit the health effects from inhalation within the plant buildings. Furthermore, the exposure time of the operating personnel can be limited by strictly controlling the allowable time at work.

Besides relevant design data, plant response information regarding an (external) hazard event scenario includes data on protective measures and administrative procedures. The protection may include special protective measures and protection features applied to prevent structures as well as of active or passive safety functions and the related plant systems. Also, early protective or mitigating human actions to prevent plant transients due to an external event, as defined in safety and operating procedures, need to be considered, if the development of the hazard scenario is slow and grace time is large. Measures requiring operator actions should not be credited for impact screening, if these actions are needed in the short or medium term. This aspect should be considered during bounding assessment.

3.3.4 PLANT RESPONSE ANALYSIS FOR COMBINATIONS OF HAZARDS INCLUDING LESS INTENSE SCENARIOS

Plant response analysis is also applicable to combinations of hazards. Usually, correlated hazards have to be evaluated, since most of the hazards without any correlation can be screened out on the basis of event frequency. Combined hazards may have either the same types of impact as individual hazards, but they can also impose different effects on the plant.

If the effects are the same, the maximum credible impact is determined by the summation of the effects induced by the multiple hazards that belong to the combination. If there are different effects, then all types of impacts should be taken into consideration as complex effects.

Impact analysis for screening should not only consider rare, high impact events, but also less intense scenarios at or even below design basis values, as these might be relevant in combinations with other events. This effect has been observed for cases, where the provision of safety functions for one challenge depends on components that are not designed against impacts of the other.

One example can be the combination of a below DBE earthquake with very high temperatures. If the ventilation systems are not seismically qualified, they will likely fail for earthquake impacts even below the DBE threshold. As a consequence, temperatures in the I&C cabinets and other safety-related rooms will soon exceed their design values, leading to a high likelihood for the unavailability of multiple safety functions.

The Fault Sequence Analyzer approach (or equivalent approach) may give valuable information on potentially critical impact scenarios and can thus inform impact screening as well as bounding analysis.

3.3.5 BOUNDING ANALYSIS

Bounding analysis describes that task of estimating, with conservative approach, initiating event and hazard scenario frequencies as well as the respective conditional failure probability of plant safety provisions.

[10] (IAEA SSG-3) specifies (with respect to hazards) the following.

“8.7 The bounding estimations should be based on models and data that are either realistic or demonstratively conservative. Such models and data include:

- (a) Assessment of the frequency of hazards (i.e. estimations of the frequency of exceedance of particular intensities);*
- (b) Analysis of the impact of hazards on the plant (i.e. loads associated with the hazard);*
- (c) Analysis of the plant response (i.e. fragilities);*
- (d) Level 1 PSA models and data, etc., for the plant.”*

The bounding analysis is an important element for reducing the number of internal initiating events which need to be analysed in more detail.

Bounding analysis for screening is usually inherently based on expert judgement. Experts need to use all available information on events, hazards, and plant response, using sources from deterministic analysis, probabilistic evaluations, operating experience, siting, simulation models, etc. These are then translated in to claims on frequencies and conditional probabilities. Justifying these claims in a traceable manner but explaining the underlying reasoning, providing supporting arguments, and linking to available evidence is good practice.

As with every expert judgement, only generic guidance can be provided. The following recommendations are proposed:

- bounding analysis for screening needs to be demonstrably conservative; this prevents scenarios to be screened out with potentially relevant contributions to risk,
- bounding analysis can be made at different levels of sophistication; particularly for initial screening, (very) conservative estimates are acceptable; such values could be based on a high confidence of a small value type of approach or could correspond to a 95% percentile of the (possibly unknown) distribution at a confidence level of 95%,
- in order to limit the amount of initiating events and hazard scenarios for a more detailed analysis, more realistic bounding estimates can be necessary; such estimates can be
 - a. based on conservatively estimated mean values for frequencies or probabilities,
 - b. based on simplified probabilistic models;
analysts could make separate (bounding) estimates for the failure probability of different (groups of) safety functions, barriers, related plant compartments, or other provisions available to control the scenario,
 - c. with regard to hazard scenarios, simplified probabilistic modelling can include separate estimations on the conditional probabilities for hazard impact propagation, consequential effects, triggering of initiating events, and protection measures,
- estimations based on simplified probabilistic modelling need to critically examine:
 - a. potential common cause failures
 - b. boundary conditions (e.g. impact of hazard effects)
 - c. interactions and interdependencies with other units.
 - d. shared systems and resources; if they cannot (simultaneously) supply all relevant demands from the connected units, they should be assumed to be unavailable for bounding assessment as default assumption,
- bounding analysis for hazards needs to be based on their impact characteristics.

For some hazards like e.g. internal fire, specific bounding analysis approaches have already been developed.

Bounding analysis should be made in a progressive manner.

- 1) the first step will be the estimation of the frequency of occurrence of the initiating event or hazard scenario; at this step, the conditional probabilities for severe consequences (whatever they may be) should be assumed to be 1,

- 2) if the event or scenario cannot be screened out on frequency alone (a quite common case), estimates on the L1 PSA risk metric, i.e. FDF and possibly RMF, have to be made with an adequate level of sophistication (see above). At this stage, CLRP and CERP should be assumed to be 1,
- 3) if the event or scenario cannot be screened out because it fails the Level 2 criteria, additional estimates on CLRP and CERP with an adequate level of sophistication have to be made.

During bounding analysis, the analyst might notice that the scenario under consideration can be reasonably assigned to an already existing initiating event or hazard scenario group based on plant response analysis. This option should be preferred, especially if there is a detailed PSA models available for that group.

Bounding analysis should allow for demonstrating that certain events are extremely unlikely to develop into a large release or an early release scenario. This provides valuable justification to decision makers and stakeholders that low probability/high consequence events have been comprehensively identified so traceability is crucial. Importantly, using bounding analysis for the assessment of a scenario does not remove the need for practical elimination of a sequence with unacceptable risk.

For screening purposes, bounding assessment related to site risk measures should not be necessary. Claims for each unit from bounding assessment should be added up to arrive at site-level risk contributions from bounding assessment.

3.4 SELECTION OF THE INDIVIDUAL INTERNAL INITIATING EVENTS TO BE CONSIDERED IN A SINGLE UNIT PSA

The screening process for internal initiating events is an established practice for current PSA. For the identification of initiating events, the following approaches [10] can be used in general:

- a) list of initiating events, either from other existing PSA or recommended in standards and guides;
- b) evaluation of operating experience events, and events specific to spent fuel pool;
- c) bottom-up analysis approaches like hazard and operability (HAZOP) studies or failure mode and effects analysis (FMEA);
- d) master logic diagrams which develops a plant level logic structure whose basic input events are the initiating events, for identifying failures leading to challenges of normal operation;
- e) evaluation of the plant safety analysis report and other deterministic analyses on design and beyond design basis accidents.

The plant systems and major components should be systematically reviewed to see whether any of the failure modes could lead directly or in combination with other failures, to significant disturbances of plant operation, requiring operation of mitigating systems. Partial failures of systems need also to be considered as well.

There is a lot of experience in the PSA community on the spectrum of internal initiating events for all operating modes relevant for the different NPP designs. Therefore, comments are provided only on some specific aspects relevant for the proposed screening approach for an extended PSA.

First, the screening for an extended PSA may assume significantly lower quantitative screening thresholds than established practices. Therefore, internal initiating events, which have been screened out from more detailed

assessment may need to be re-assessed. This particularly includes a check of screening out internal events against the recommended L2 PSA screening risk measures.

Regarding internal initiating events screening against L2 PSA risk measures, particular attention should be given to IE-specific boundary conditions or unavailabilities relating to the containment function of the NPP. For example, event scenarios, which are inherently intertwined with an open containment or a containment isolation failure, are potentially significant contributors to LRF and ERF scenarios. Such boundary conditions can also originate from different operating modes, e.g. shutdown states with and without an open containment.

Based on the ASAMPSA_E investigation of the link of DiD and PSA (cf. ASAMPSA-E deliverable D30.4 [4]), the spectrum of internal initiating events screened for PSA should be cross-checked against the list of PIE for deterministic safety assessment. Particularly PIE classified as DEC events can complement the spectrum of initiating events for PSA and vice versa.

Another link between deterministic and probabilistic assessment approaches lies in determination of initiating event frequency. Obviously, this determination should come from the same data and results should not be inconsistent.

For internal initiating events, frequency estimates down to the range of about 10^{-6} /yr can often be justified based on operating experience, by extrapolation of operating experience, or by combination of operating experience with modelling assumptions. In these cases, uncertainty bands for the respective values are usually limited (to about an order of magnitude at most).

However rarer events pose significant challenges to analysts. Extrapolations from available data (e.g. by extreme value statistics) may lead to results with excessively large uncertainty bands. In these cases, the ASAMPSA_E project recommends as far possible combining available data with event model information (e.g. structural integrity assessments and simulations) and adjusting results based on expert judgement. Especially for screening purposes, conservative estimates of event frequencies are sufficient. Therefore, using conservative point estimate values based on a high probability that the actual frequency value is lower should be considered as an approach. Direct estimations - even based on expert judgement - of the 95% percentile at a 95% uncertainty level for the event frequency will likely lead to results at an appropriate level of accuracy and conservatism for screening. Such estimations can then be refined, if a more stringent treatment of the event either in bounding analysis or in a detailed PSA is merited based on its contribution to the risk measures of interest.

The internal events screening needs to include the spent fuel pool, if not separated from the reactor core in a specific facility. The spectrum of initiating events affecting the SFP needs to entail reactivity accident scenarios as well as loss of fuel cooling scenarios. To the extent that a PSA models still has to be developed, the deterministic safety case for the SFP will provide valuable insights on initiating events for the different operating modes.

3.5 SELECTION OF THE INDIVIDUAL INTERNAL HAZARDS SCENARIOS TO BE CONSIDERED IN A SINGLE UNIT PSA

There is established internal hazard screening guidance available from several sources, e.g. SSG-3 [10] or the ASME PSA guide [79]. Internal hazards scenarios to be considered include

- (a) Internal fires;
- (b) Internal floods;
- (c) Heavy load drop;
- (d) Turbine missiles;
- (e) Internal explosions” [10], p. 65.

Detailed PSA investigations have been performed in particular for internal fire and internal flooding scenarios, with respective guidance on specific screening available. Nonetheless, several remarks and recommendations with respect to the proposed screening approach for an extended PSA can be made.

The aforementioned internal hazards can be extended by several addition classes like e.g. electromagnetic interference or collapse of structures as mentioned for deterministic internal hazards assessment. or from country presentations, cf. e.g. sections 5.1.1, 5.2.6, or 5.2.7 in [5]. A systematic approach similar to the approach for internal initiating events identification needs to identify those scenarios, which induce a challenge to plant safety, i.e. an internal initiating event. For the further analysis, consequential and secondary failures of the internal hazard have to be considered.

The screening approach for an extended PSA assumes that an internal initiating events PSA for the reactor core and for the spent fuel pool (if applicable) is available to inform the screening. Consequently, internal hazards PSA should be extended to the SFP.

Based on experience, single internal hazards other than internal fire and internal flooding have either been screened out from further consideration or assessed with bounding assessment approaches. This is mainly due to the observation that these other internal hazards either do not (easily) trigger events that lead to fuel damage states (due to reactivity accidents or excess cladding temperature) or that the resulting scenarios are enveloped by existing internal initiating events with significantly larger IE frequencies.

In view of the proposed screening approach and the quantitative screening criteria, it is recommended that internal hazard screening needs to be extended with regard to the following aspects:

- consideration of internal hazards originating from outside of the unit but from inside of the plant or site perimeter; this should include the following effects, which can basically be treated like other (external) man-made hazards,
 - a. fires at other installations on the site like e.g. hydrogen or hydrocarbon fuel storage facilities,
 - b. flooding originating from installations on the site like e.g. leakages from water storage tanks or fire protection systems,
 - c. explosions originating at other installations on the site, e.g. a hydrogen gas explosion after a generator blowout,
 - d. missiles originating at other installations on the site like e.g. a turbine missile from another NPP on the site. Note: Such a missile might be screened out for the originating installation,
 - e. electromagnetic interference from other sources on the site, e.g. due to welding work near the affected unit,
 - f. hazardous gas releases from other installations on the site, e.g. hydrogen releases during a severe accident in another unit (multi-unit effect),

- g. accident level radiological releases from other installations on the site (multi-unit effect).
- consideration of effects on containment function availability with respect to L2 PSA screening measures,
 - combination of internal hazard scenarios and independent or correlated internal initiating events,
 - extension to the internal hazard scenarios affecting the spent fuel pool.

With respect to the determination of internal hazard scenario frequencies, basically the same comments as for internal initiating events apply. To the extent sensible, internal hazard scenario frequencies should be based on (mostly generic) operating experience. This should be combined with expert judgement using also information for deterministic hazard assessment specific simulation models, as appropriate and available. Such generic operating experience is available in particular for internal fire and also for internal flooding (from component integrity data bases). For other internal hazards, it is assumed that there is a dearth of generic information on such frequencies, as these are commonly screened out from further detailed analysis.

It has to be emphasized that certain internal hazards are strongly dependent on time. For example, internal fire initiators are known to be more likely during shutdown operation due to respective work. High energy faults of components (power switches as well as pressure vessels) will depend on the component being in operation. For screening purposes, internal hazard scenarios that strongly depend on time should be treated as “probability per year” types of events. In that case, the peak probability value over a representative time interval should be assumed for screening purposes.

The proposed screening approach for extended PSA requires the consideration of very rare events. Initiating frequencies of such rare events (e.g. significantly below 10^{-6} /yr) will be hard to justify with a best-estimate approach. For screening purposes, it is recommended using conservative point estimate values based on expert judgement. Such estimations can then be refined, if a more stringent treatment of the event either in bounding analysis or in a detailed PSA is merited based on its contribution to the risk measures of interest.

Internal hazard scenarios need to be mapped to initiating events. This requires the consideration of the effects of the initiator event on the plant. Plant response analysis needs to consider the resilience of the plant (i.e. its SSC) against hazard impact as well as the spreading of the hazard and its consequential effects (salient examples: fire and flooding). It has to be pointed out that this necessitates a bounding assessment for internal hazard scenarios. PSA analysts have to propose claims on two important aspects:

- 1) conditional probability for the failure of provisions against potential spreading and other consequential effects of the scenario,
- 2) conditional probability of triggering an initiating event.

Due to the large number of potential initiators (e.g. rooms with a high fire load and prone to internal fire), effective bounding assessment is an essential task for internal hazards PSA. Moreover, grouping internal hazards scenarios, that have not been screened out (as not challenging plant safety), into enveloping hazard scenario groups will be needed. This will significantly reduce the number of detailed PSA models.

In addition, the deterministic analysis of internal hazard should result in a comprehensive protection concept with efficient protection measures. Internal hazards screening should confirm the effectiveness of the deterministic

protection concept. If more than a limited number of internal hazard scenarios are identified for detailed probabilistic assessment, it is recommended to revisit the deterministic assessment and protection concept.

Finally, it has to be pointed out that a number of internal hazards are rather unlikely to get relevant with respect to the FDF risk measures. A prominent example would be heavy load drop damaging a number of fuel elements in the spent fuel pool (without impairing fuel cooling). Another example would be a high energy fault damaging the radioactive waste treatment system. For such scenarios, screening against the proposed radionuclide mobilization frequency risk measure should be considered. For further multi-source considerations, see section 3.8

3.6 SELECTION OF THE INDIVIDUAL EXTERNAL HAZARDS SCENARIOS TO BE CONSIDERED IN A SINGLE UNIT PSA

Improving hazard identification for PSA is one of the main lessons learned from the Fukushima Dai-ichi accident. The following recommendations from the report ASAMPSA D30.2 [2] are particularly relevant.

“Site specific hazard identification has to be systematically extended to scenarios in the design extension conditions range [...], especially for the purposes of an extended PSA.”

“All natural hazards that might affect the site shall be identified; a wide spectrum of rare events should be assessed.” [78]

“It has been recognized that current methods as well as data used for determining frequency vs. likelihood curves for a lot of hazards are limited in their validity and often fraught with high uncertainties. Methods for treating correlated (hazard) events - if available at all - are usually not mature. Consequently, this is identified as a field for additional research [...].”

“The screening process should consider justifiable frequencies for the hazards of relatively high magnitude even if they have never been observed in the past in the plant vicinity. The impact of correlated hazards should be carefully considered.”

“Screening criteria should include suitable risk metrics for covering accidental release risk like e.g. large release frequency or conditional containment failure probability.”

“Screening should be done by combining fixed threshold values (e.g. for frequency of exceedance) with criteria relative to the risk level of the plant (e.g. using metrics like CDF, LRF, CCFF, etc.).”

External hazards screening for a specific site should start from a comprehensive list and narrow this down in the further steps of screening. The report ASAMPSA_E D21.2 [80] provides a comprehensive list of natural and man-made hazards that can serve as a good starting point. In addition, the operational history of the plant in question and of similar plants should be reviewed to search for any events involving functional degradation or unavailability of systems due to external events which should be added to the list. The publicly accessible databases that contain summaries of accidents and near misses that have occurred in hazardous processes around the world should be consulted. The report ASAMPSA_E D10.3 [81] summarizes external hazards with high amplitude that have affected NPP in operation.

The first step in the screening of external hazard will be applicability screening. Analysts need to identify those hazards that are not relevant to the nuclear power plant and to the site due to site characteristics (e.g. tsunamis usually cannot affect plants located far away from seas and oceans). Hazards can be screened out as not applicable because

- 1) the hazard is not applicable to the site due to physical, geological or other properties,
- 2) the hazard does not challenge the safety of the plant.

Applicability screening should initially be performed using a maximum (credible) impact and needs input from plant response analysis.

With respect to the actual determination of frequency of exceedance curves for single hazards or combinations of hazards, the reader is referred to the hazard-specific ASAMPSA_E topical reports.

The determination of frequency of exceedance curves for hazards will require input from (several) subject matter experts on the respective hazards. Moreover, it is a well-known problem that the amount of data particularly on rare, high amplitude hazard events is often severely limited. Current operating experience and knowledge often limits frequency estimates for single events and phenomena to values in the range of $1 \cdot 10^{-4}$ to $1 \cdot 10^{-7}$ /yr. Using statistical methods like extreme value statistics to extend limited data far outside of the reference time frame is fraught with large uncertainties and might produce arbitrary results. Such extensions by several orders of magnitude are therefore not encouraged. Instead, available data for the site have to be completed by using regional data and by evaluating historical data or paleogeological information. Since rare mechanisms and phenomena, which could result in severe hazard impacts, might be missing from the available observations altogether, these should be complemented by investigations of such potential mechanism and phenomena. These investigations will often require dedicated simulation models, calculations or expert judgement.

One essential step after the determination of frequency of exceedance curves (with respect of characteristic hazard impact parameters like e.g. peak ground acceleration or flooding height) is the subdivision into more specific hazard scenarios based on the characteristics of the plant. The partitioning should be informed by plant response and hazard impact analysis, design values of SSC regarding different impacts, deterministic assessment results, other hazard PSA results, etc. as appropriate.

The subdivisions need to be made in light of important thresholds of the plant with regard to the impact parameter. Important limiting thresholds for screening will be the following:

- 1) minimal hazard impact magnitude with challenges to plant safety (trigger for an AOO type of event),
- 2) design basis hazard impact magnitude for design basis accident conditions,
- 3) (maximum) hazard impact magnitude assumed for design extension conditions,
- 4) hazard impact magnitude with an assumed cliff-edge to catastrophic failure.

Usually, (single) external hazard impact is characterized by a single impact parameter. If, however, a set of impact parameters needs to be used (e.g. precipitation, wind speed, humidity, etc. for extreme weather), this subdivision needs to be made on the set of relevant impact parameters.

As an example is discussed severe weather impact due to heavy snow. Usually the plant will cope with a certain snow weight on buildings and snow levels on the plant site without significant impairments to safety systems or adverse effects on operational systems, no event is triggered. This relates to the first alternative, the risk is covered by the general risk of the plant. In case of more severe snow up to design basis limits, a shutdown and likely loss of offsite power will be the main probable consequence of the scenario. For beyond design basis snow loads, safety-important equipment will be rendered unavailable, for example (e.g. EDG air intakes covered by snow) and emergency measures might no longer be possible. Based on plant response analysis, a maximum impact level needs to be determined⁴. Excessive snow loads could potentially lead to catastrophic building collapse (e.g. the reactor building) with catastrophic off-site consequences.

Based on the frequency of the occurrence curve (often a cumulative distribution), a bounding estimate frequency for the respective subset has to be determined. The specific hazard scenario is then described by enveloping impact parameters and the assigned frequency value.

The bulk of the frequency distribution will usually fall within the first two classes or even below. Moreover, these two classes can often be screened out for further detailed analyses by (cf. section 3.2.1) the following criteria:

- 1) the event poses no challenge to safety systems,
- 2) the event is bounded by another initiating event,
- 3) the scenario is already captured in the PSA model as an intermediary state⁵.

The group corresponding to impact magnitude related to a catastrophic cliff-edge effect can often be screened out from further detailed analysis because:

- 1) such hazard impact magnitudes are not physically possible for the hazard source under consideration,
- 2) such hazard impact magnitudes are not applicable to the site,
- 3) the estimated frequency for such hazard impact magnitudes is significantly below quantitative screening values and thresholds for practical elimination.

It is emphasized that application of the latter criterion includes these hazard scenarios into the overall PSA results.

The next step consists of identifying initiating events triggered by the specific hazard scenarios. When identifying internal initiating events for hazard scenarios during screening for a hazard PSA, analysts should have access to the internal events L1 and L2 PSA for all operating states for the plant and, if applicable, for the site. The PSA model should cover the spent fuel pool and other major sources for fuel damage, as applicable. If this is not the case, it is recommended to check hazard screening results as the internal events PSA models become available. For the

⁴ It is noted that this impact magnitude might have been defined as maximum credible impact based on practical elimination reasoning in deterministic safety analysis.

⁵ This situation might arise if external hazard initiators or conditional probabilities are already considered in the (internal events) PSA model, e.g. via initiating event fault trees.

identification of initiating events and unavailabilities of safety-related SSC, so-called “hazard equipment lists” are an essential tool.

“Probabilistic hazards analysis routinely maps the hazard impact on the plant to initiating events for an (internal) accident sequence model, which is usually already present in the PSA” [2], p. 19. For that mapping, insights from plant response analysis and bounding analysis will be essential. The following cases can be distinguished⁶:

1. the hazard scenario contributes to an initiating event which is already modelled in the PSA, and is not altering any other conditions assumed in the internal events analysis. Analysts need to check that not only L1 PSA but L2 PSA boundary conditions are identical or at least comparable between the internal IE and the hazard scenario. Based on the screening approach, the hazard scenarios should be grouped into the initiating event group. Salient examples include loss of off-site power (heavy snow, lightning, etc.) scenarios. Analysts need to check if these events are covered by the operating experience used for the determination of (internal) initiating events frequency. However, grouping hazard scenarios with very different ranges of uncertainty - regarding frequency of occurrence as well as plant impact and accident development - should be avoided to the extent sensible.

Hazard-specific contributions can be derived from importance values for PSA end results. There is no need for additional modelling.

2. the hazard scenarios induce an (internal) initiating event but with different boundary for the L1 or L2 PSA model. Then, the hazard scenario should be linked to the existing IE, with appropriate boundary conditions. Further consequences of hazard impact (e.g. common cause failures) relevant to the event tree or fault tree modelling can then be considered by setting appropriate boundary conditions on the availability of required safety functions and accident management measures. This standard approach is well described in SSG-3 [10].

Depending on the overall PSA structure, modelling practices, and the modelling tool, either the hazard event scenario is added to the (set of) initiators treated in the event tree together with the respective boundary conditions. Alternatively, the existing event tree/fault tree model is copied, linked to the hazard scenario as an initiator and the respective boundary conditions are set to the model. Whether hazard scenario specific boundary conditions or effects are considered via setting logic switches or by adapting the actual fault tree/event tree structure e.g. by adding additional (scenario-specific) basic events depends on the overall modelling approach.

3. if the set of internal initiating events does not include a suitable initiator and accident sequence (event tree) model that can be mapped to the hazard scenario, a new IE should be defined. In any case, analysts will have to model the accident development and systems analysis under scenario-specific conditions as it is done for internal events (cf. SSG-3 [10]). The Fukushima accident highlighted the need for defining initiating events for risk sources other than the core (as the spent fuel pool) and systematically mapping hazards to those initiating events for full power as well as low power and shutdown operations.

⁶ It should be noted that simplified probabilistic assessment approaches are already covered under bounding assessment as described in section 3.3.

For screening purposes, this initial mapping to initiating events and the associated bounding analysis will often be sufficient. If hazard scenarios might be screened out from further analysis due to initial mapping and respective bounding analysis, analysts need to check for the following.

- 1) A hazard scenario might trigger several (distinct) initiating events with different probabilities. The screening needs to ensure that at least bounding assumptions on the triggered event, the overall conditional probability, and consequences with respect to Level 1 and Level 2 risk measures have been made.
- 2) If the hazard scenario triggers a “near miss”, i.e. there is only a (weak) line of defence left to prevent core damage or (assuming the use of a PSA model) there are minimal cuts triggered by the hazard scenario and its enveloping boundary conditions that include only one additional, non-consequential failure.

If hazards screening is iterated in order to reduce the scope of detailed analysis, a refinement of the hazard scenario subdivisions can be considered. Depending on further subdivisions of hazard impact magnitude, different boundary conditions, conditional failure probabilities, and eventually consequences can be justified as bounding estimates. Such subdivisions can be based e.g. on components operability limits, assuming that:

- SSCs will fail if the loads (acceleration, vibration, humidity, temperature, etc.) exceed the design loads
- SSCs will remain operational if the loads are below the design loads
- all equipment located inside damaged buildings/structures or close to the failed structures will be inoperable
- human actions are successful if they are performed from a location not affected by the hazard and with pathways available after the hazard occurrence

The principles for internal initiating events grouping can be transferred to hazard scenarios. In order to reduce the amount of detailed analysis, a hazard scenario group with enveloping boundary conditions and impact characteristics can be defined. The grouping should not be overly conservative and it shall be made in such a way that hazard scenarios assigned to the group would induce the same or a reasonably similar plant response with regard to same success criteria on the frontline systems, challenges to plant operators, and plant damage states for L1 and L2 PSA. In particular, it should be checked if the accident progression after the initiating event will trigger the same mitigating systems and with the same (or less onerous) success criteria. Moreover, the availability and operability of safety systems and support systems, grace periods and requirements on operators should be similar or less onerous than those of the bounding event.

It is emphasized that the process for the identification and mapping of internal events triggered by hazard scenarios, the grouping and/or partitioning of hazard scenarios with regard to mapped internal events, the identification and establishment of boundary conditions on the internal events assigned to each hazard scenario, and the development of a model for an extended PSA is to be understood as an iterative process.

No hazard-specific screening criteria are recommended. Since external hazards are usually affecting the site, site-PSA considerations play a role. For discussion on combinations of hazards and correlated hazards, see the next section.

3.7 SELECTION OF THE COMBINED/CORRELATED HAZARDS SCENARIOS IN A SINGLE UNIT PSA

With regard to the selection of combinations of external as well as internal hazards and correlated hazards and internal events, the following recommendations from the report ASAMPSA D30.2 [2] are particularly relevant.

“A realistic set of combinations of hazards should be identified on the basis of a list of individual internal and external hazards, before the application of any screening criteria.

It should be done through a systematic check of dependencies, by identifying:

- *hazards occurring at the same time and in the same conditions (e.g. winds and snow);*
- *hazards and other internal events occurring at the same time (e.g. if a hazard situation persists);*
- *external hazard inducing other external hazards (e.g. seismically induced tsunami) ;*
- *external hazard inducing internal hazards (e.g. seismically induced internal fires);*
- *internal hazard inducing other internal hazards (e.g. internal floods induced by missiles).” [2], p. 13*

“The screening process should consider justifiable frequencies for the hazards of relatively high magnitude even if they have never been observed in the past in the plant vicinity. The impact of correlated hazards should be carefully considered.” [2] p. 15

The scope of hazard screening needs to be comprehensive. The ASAMPSA_E project has drawn up a list of external hazards, including man-made hazards, which by themselves or as combinations can apply to the site of a nuclear installation. The correlations between hazards can lead to the following categories of combinations:

- causally connected hazards where one hazard may cause another hazard; or where one hazard is a prerequisite for a correlated hazard,
- associated hazards which are probable to occur at the same time due to a common root cause.

The causality dependence can be divided into 2 categories:

- causality dependence between the specific hazard and the external natural hazards group,
- causality dependence of specific hazard with the man-made hazards group.

With respect to internal hazards, the analysis has to be extended to consider the following issues:

- internal hazard scenarios are triggered as a consequence of external hazard impact (e.g. external flooding entering the reactor building),
- internal hazard scenarios triggered on the site but not in the unit or for the source currently analysed,
- internal initiating events, for which probability of occurrence correlates with the hazard scenario frequencies. (e.g. a LOOP scenario might be more likely due to high grid load in conjunction with a heat wave or during the hurricane season).

As a first step, PSA analysts should develop a matrix of all reasonable (bounding) combinations of hazards deemed applicable to the site. Quantitative screening thresholds should be applied. Such a matrix needs to consider all hazards, even if they have been screened out individually (for not challenging the plant or based on bounding analysis). The screening of combinations should not only consider rare, high impact events, but also less intense scenarios at or even below design basis values, as these might be relevant in combinations with other events. One salient example would be the combination of high external temperatures with a design basis earthquake, which

was identified as a contributor for a NPP, since ventilation systems were not qualified for earthquake impact and the subsequent temperature increase in safety related buildings would impair safety-related I&C.

For each entry in that matrix, an enveloping set of maximum (credible) impact characteristics needs to be defined. It then has to be checked if this enveloping set of impact characteristics would challenge the safety of the plant. The results of an investigation following the Fault Sequence Analysis (FSA) method or similar approaches will be invaluable for that purpose.

If combinations are identified as potentially applicable and relevant for the plant, the further screening will follow the concepts outlined in sections 3.6, 3.5, and 3.4 in [2].

Screening of combinations of external and internal hazards for PSA is a field with need for further research. This applies in particular to the determination or bounding estimation of adequate frequency of occurrence or conditional probability values for combined/correlated hazard scenarios. The same considerations as for rare external hazards apply. Regional frequency approaches as described in ASAMPSA_E report on flooding PSA are a good way to enlarge the data basis.

Finally, the screening of combinations of hazards needs to efficiently use strategies for grouping hazard scenarios for specific combinations into enveloping hazard scenario groups. However, grouping hazard scenarios that are very different in terms of levels of uncertainty on frequency of occurrence or hazard impact and accident development should be avoided to the extent possible. The use of bounding assessment will be essential for limiting the amount of cases for a more detailed analysis.

3.8 SELECTION OF INITIATING EVENTS FOR MULTI-UNITS, MULTI-SOURCES PSA

The report ASAMPSA D30.5 [5] includes a discussion of risk measures for multi-unit and multi-source PSA (site-level PSA). Based on this discussion, the following important conclusions can be drawn:

- site level risk measures can be defined by extending common unit- or source level risk measures; specifically, risk measures recommended for screening can be extended to the site level,
- site-level risk results can be estimated from unit- or source-level risk measures,
- as corollary, initiating events and hazard scenarios that are screened in based on unit- or source-level risk measures are also screened in based on the respective site level risk measures,
- for the recommended risk measures and given the recommended quantitative screening, the following observations can be made:
 - a. events and scenarios not screened in based on FDF for any unit or source will not be screened in on FDF_{site} ,
 - b. events and scenarios not screened in based on LRF or ERF or RMF for any unit or source are for practical purposes also not screened in based on LRF_{site} or ERF_{site} or RMF_{site} ; deviations would result from multi-source release scenarios, for which all single-source releases are below the release threshold for those three risk measures, but the combined releases are above; since release estimates during screening shall be adequately conservative, this possibility will not be relevant in practice,

- it follows that all events and scenarios screened in for site-level risk measures will be screened in based on one unit- or source-specific screening risk measure; consequently, no screening specific to site-level risk measures will be necessary.

Importantly, this discussion rests on the assumption that unit- or source-level PSA results adequately consider all site-level effects. Consequently, if screening for hazard scenarios (external but also internal) for an extended (i.e. in this case site-level) PSA is to be performed, PSA analysts should have access to a comprehensive site-level internal initiating events L1 and L2 PSA for all operating states and all sources.

The following comments are due regarding site-level PSA:

- for each screened in event and scenario, PSA analysts need to check during the development of the probabilistic model if and which multi-unit or multi-source aspects have to be included in the PSA model; some remarks and recommendation on that task are provided below,
- the identification process of initiating events and hazard scenarios needs to consider shared systems and connections between units and sources for determining if they can trigger an initiating event for each single unit or source,
- the issue of how to structure a site-level PSA model is still subject to research since only limited practical experience has been gained so far; generally speaking, site-level models can be constructed from existing single unit/single source models, if the separation between the units/sources is highly effective (physical separation, no shared or interconnected systems, including operating systems, dedicated control rooms, dedicated severe accident installations and resources, etc.) ; otherwise, an integrated, site-level model will be needed ;
since external hazard scenarios are often affecting multiple units (and sources), dedicated site-level models are particularly relevant for these scenarios.

The screening approach for a multi-unit, multi-source PSA is basically similar to the screening approach for a single unit as discussed in the previous sections. The following comments and recommendations on specific aspects for site-level PSA screening are given:

- obviously, internal initiating events have to be identified for each unit and source ; the scope of an internal initiating events site PSA consists of the set of initiating events for each unit/source,
- similarly, internal hazard are basically related for each individual unit; relevant releases from one unit (or source) should be considered as a potential (external) hazards for other units/sources; the set of internal hazard scenarios for a site-level PSA consists of the set of internal hazard scenarios for each unit/source,
- external hazard scenarios are basically events affecting the site; consequently, external hazard scenarios (or combinations of external hazards with other events) should be screened in for detailed site-level modelling if they are screened in for any one unit or source.

Bounding assessment needs to consider multi-unit/multi-source aspects:

- systems and other provisions or resources providing safety functions to more than one unit or sources should be assumed to be unavailable, if they cannot provide simultaneous demands from all connected units or sources simultaneously,

- if shared or interconnected systems or other provisions providing safety functions to more than one unit can fail due to hazard impact, propagation of hazards from any one unit, or due to consequential effects from internal initiating events or internal hazard at any one unit/source or due to external hazards, these should be assumed to be unavailable for every unit for all relevant cases per default,
- if the propagation of internal or external hazard impacts or effects of consequential failures from one unit/source to another unit/source cannot be excluded with a high degree of certainty, it should be assumed to occur for bounding assessment by default.

More realistic bounding assessments should be well justified.

These recommendations should be applied for bounding assessment of each individual unit/source, irrespective of whether the development of a site-level PSA model is intended or not.

For the development of a multi-unit and multi-source (site-level) PSA model, PSA analysts have to identify the relevant events and scenarios affecting multiple units or sources at the same time.

Multi-unit accident sequences may be caused by two classes of initiating events:

- Common-Cause Initiators (CCIs): initiators that simultaneously challenge all of the units at the site; CCIs include initiators that are caused by external hazards (e.g. earthquakes, severe weather).
- Single-Unit Initiators (SUIs): Initiators that occur at one unit. SUIs generally include initiators caused by internal hazards such as internal events (e.g. loss of main feedwater, loss of coolant accidents), internal floods, and internal fires. SUIs may cause multi-unit accidents due to cross-unit dependencies such as shared support systems, spatial interactions (e.g., internal flood and internal fire propagation pathways), common cause failures or operator actions.

In addition, PSA analysts need to identify further dependencies between the units/sources in order to decide on the need for a (dedicated) site-level modelling.

Six main dependence classifications are identified [79]:

- initiating events,
- shared connections,
- identical components,
- proximity dependencies,
- human dependencies, and
- organizational dependencies.

The next table represents the matrix showing the classification scheme and systems with respect to L1 PSA considerations potentially affected [46].

Table 1. Classification of dependencies in L1 PSA

Accident Sequence Classifications	Definition	Potential Systems Belonging to Classification
Initiating Events	Single events that have the capacity to affect multiple units	Loss of Offsite Power, Loss of Ultimate Heat Sink, seismic event (including seismically-induced tsunami), external fire, external flood, hurricane, high wind, extreme temperature
Shared Connections	Links that physically connect SSCs of multiple units	Reactor pool, chilled water system, BOP water system, spent fuel pool cooling system, circulating water system, reactor component cooling water system, high, medium and low voltage AC distribution systems
Identical Components	Components with same design, operations or operating environment	Safety DC electrical and essential AC distribution system, reactor module bay, containment, decay heat removal system, emergency core cooling system, non-safety instrumentation and control, chemical volume and control system, power conversion system
Proximity Dependencies	A single environment has the potential to affect multiple units	Reactors, ultimate heat sink, containment, non-safety DC electrical and essential AC distribution system, control room HVAC
Human Dependencies	A person's interaction with a machine affects multiple units	Shared control room, operator staffing more than one reactor
Organizational Dependencies	Connection through multiple units typically by a logic error that permeates the organization	Same vendor for safety and non-safety system valves, consolidated utility ownership of multiple nuclear power plant sites, decision-maker overseeing more than one reactor or more than one operator

It should be noted that the examples given need to be extended to L2 PSA considerations, i.e. dedicated severe accident management equipment, effects of radioactive releases of one unit on others, hydrogen hazard, etc. Therefore, any comprehensive screening for an extended PSA depends on the understanding of all interdependencies between the different units/sources. Therefore, the identification of SSC and other provisions that might be relevant for multiple units/sources is an essential step. To this end, a combination of the following approaches can be recommended:

- evaluation of deterministic safety demonstrations related to multi-unit effects,
- evaluation of deterministic hazard impact analyses,
- dedicated failure mode and effects analysis of SSC and other provisions on the site looking for effects on multiple units,
- evaluation of (existing) single-unit PSA models for minimum cuts sets that are (largely) the same for more than one unit or of existing PSA modelling on multi-unit issues.

This information needs to be gathered into a comprehensive list of SSC and other provisions potentially affecting multiple units/sources with regard to the six dependency classifications defined above. Based on such information, the list of events, hazards and combinations thereof can be checked for those events which potentially affect multiple units.

Every multi-unit PSA is also a multi-source PSA. A quite common multi-source PSA is a PSA for the reactor core and the spent fuel pool. The screening approach for a multi-source PSA is basically identical to the multi-unit approach described above. Therefore multi-source aspects are included in the text above as applicable. Issues connected to multi-source PSA are still a field of research and there is few good practices available to the ASAMPSA_E project

(apart from extension of the PSA to include the SFP). However, some remarks specific to multi-source PSA can be made with respect to the proposed screening approach:

1. the identification of initiating events and hazard scenarios for non-fuel type sources has to be performed along the lines described in sections 3.4, 3.5, 3.6, 3.7; the identification process should use as failure criterion for determining a potential challenge to plant safety the definition of the RMF metric: if an event or scenario and its further development in plant response analysis might challenge the first boundary design to contain the source, the event or scenario should be considered during screening.
2. qualitative screening criteria defined in section 3.2.1 are fully applicable to screening for a multi-source PSA,
3. for non-fuel sources, the RMF risk measure (cf. also D30.5 [5]) is recommended for L1 PSA;
typical sources in a NPP include radioactive waste treatment facilities, waste conditioning facilities, and on-site interim storage facilities,
Analysts should be aware that RMF is intended to generalize the CDF/FDF metric. Therefore, CDF/FDF is a subset of RMF; respective CDF/FDF contributions from bounding assessment and more detailed PSA models should be treated as contributions to overall RMF results,
4. RMF is also recommended as a L1 PSA risk measure for capturing scenarios with (significant) mechanical damage to fuel rods without excessive fuel heat-up not captured by the FDF metric; such scenarios are particularly relevant for some internal hazard impact scenarios like e.g. heavy load drop or accidents during on-site transport of spent fuel,
5. no specific and additional L2 PSA risk measures are defined for multi-source PSA screening; releases from sources other than fuel should be converted to equivalent releases of the representative isotopes for LRF and ERF.

For sites with multiple units, scenarios with potential accidental releases representative of severe accidents in more than one unit might be of specific interest. As explained above, such release scenarios would be captured by the proposed screening approach. Nonetheless, very large (e.g. from a spent fuel pool) releases might be of specific interest in order to screen in specific scenarios for more detailed analysis, even though they have been screened out based on LRF. For this purpose, using a variant of the LERF metric, the very large release frequency (VLRF), by defining a very large release threshold, can be recommended.

4 RECOMMENDATIONS ON RISK MEASURES FOR AN EXTENDED PSA

Within ASAMPSA_E a deliverable on risk metrics has been developed [5]. This report contains a sophisticated evaluation of about 17 different risk metrics for L1 PSA and about 12 for L2 PSA. This large number is already an indication that the selection of proper risk metrics is not trivial, and very often PSA results are difficult to interpret if the underlying motivations are not clear. A key concern is that “risk” is not, in itself, a well defined concept. For example, risk can be understood as the frequency of core damage, but also as the probability to permanently evacuate a certain area around the installation. Depending on the stakeholder (e.g. utility or plant-external emergency teams) and its responsibilities, all the different metrics have their reasons. When in the

present document only a small selection of recommended risk metrics is provided in the sections to follow, this is by no means to be understood as a suggestion to dismiss other risk metrics if they are considered useful.

On the other hand, PSA analyses often are targeted by the rightful criticism that the results are difficult to understand. This is not so much a concern for L1 PSA with the established core damage frequency (although PSA experts very well know about the insufficiency of this concept), but it is valid for L2 PSA. Even the common “large early release frequency” turns out to be far from a harmonized concept. Therefore, the recommendations below (from [5]) try to establish metrics which should be applied in all PSA to get a common ground for methodology, general safety assessment and better acceptance of PSA. They are not intended to supersede other metrics.

4.1 RISK MEASURES FOR AN EXTENDED LEVEL 1 PSA

The Level 1 risk metric has to be defined as those end states of the L1 PSA model, which are classified as accidental. In that sense, the risk metric aggregates over the plant damage state metric(s), which are assigned to the accidental end-states of the L1 PSA.

From the review of widely used risk measures, fuel damage frequency (FDF) measure, defined as a loss of integrity of fuel elements on the site, which has the potential for an accident-level release, provides a more general notion of a L1 PSA end state than other direct risk measures as CDF. CDF, which should be understood as a fuel damage state affecting fuel elements located in the reactor core, is considered as a subset of FDF. Similarly, risk measures related to other locations than the core as SFPDF are also subset of the FDF risk measure. FDF is a direct risk measure that encompasses all these secondary risk measures. Moreover, the FDF measure needs to be consistent with the plant damage state measure(s) (PDSF) it shall aggregate.

FDF risk measure has the following limitations. It does not distinguish between severity of core damage (extent of damage to fuel rods) beyond the defining threshold for fuel damage and it does not preserve (or provide) information on fuel damage characteristics in light of expected releases (e.g. time of fuel damage onset, extent of fuel damage, status of barriers and safety systems, etc.).

Because the main risk measures for L1 PSA like e.g. core damage frequency or fuel damage frequency are not well suited for describing several scenarios which might lead to a significant release of radionuclides into the plant as a starting point for a L2 PSA, a new metric, “Radionuclide Mobilization Frequency, RMF” ([5]), addresses these issues. This risk metric is defined as a loss of the design basis confinement for a source of radionuclides, leading to an unintended mobilization of a significant amount of radionuclides with the potential for internal or external release, e.g. more than 1 TBq I-131 or equivalent⁷. The threshold value and its reference radionuclide (or radionuclides) have to be adjusted to the facility under consideration and the objectives of the study. The RMF conceptually aggregates rather diverse sequences in terms of consequences into one common risk measure (figure

⁷ The proposed threshold value has been set to 1 % of the lower end 100 TBq I-131 limit for an accidental level release (INES 5) defined in the INES manual. This assumes that short-term consequences are of interest. For long-term consequences, a threshold based on e.g. Cs-137 should be selected. .

of merit). While this is one of its advantages, its simplicity limits its suitability for understanding the actual risk profile with regard to the fundamental safety objective.

The RMF was developed during the ASAMPSA_E project. The RMF risk measure is recommended to be used for an extension and generalization of the established CDF and FDF risk measures to a multi-source PSA. It is therefore a suitable and above all complementary risk measure for an extended PSA that addresses potential sources on the site in addition to fuel in the reactor and spent fuel. Currently, no applications of RMF are known, and there is no consensus on the threshold value and its reference isotopes. However, the RMF generalizes the CDF and FDF risk measures to a comprehensive L1 PSA risk measure for a multi-source PSA. This risk measure can also contribute to the verification of the low probability of events that would induce off-site protective measure without core melt.

4.2 RISK MEASURES FOR AN EXTENDED LEVEL 2 PSA

The sections in [5] on possible risk metrics for level 2 PSA provide a comprehensive summary on this topic. Although existing PSA at maximum only partly apply the many options for different risk metrics, there is a large choice of metrics available. This wide selection of risk metrics is also applicable for extended PSA.

It is of interest to have not only a single value presenting the total risk (whatever that may be), but to be able to determine the contribution of initiating events (e.g. external hazards) and different plant operation states and particular SSCs. This requirement is not at all specific for extended PSA; it is comparable to providing the risk contributions from different issues in traditional PSA.

The risk metrics applied in an extended PSA for a multi-unit site should be identical with the conventional risk metrics. The risk of each individual unit at a particular site should be given, and also the cumulative risk for all units on a site. Of course one could imagine complicated risk patterns from multi-unit sites. The accidents in Fukushima Dai-ichi are a striking example for different accident evolutions initiated by the same external hazard in different reactor blocks on the same site. But again, this does not necessarily call for additional or modified risk metrics. In principle, the different release histories from different reactor blocks are comparable to a sequence of release episodes from a single reactor. It has to be conceded that calculating these risks from multi-unit sites are really challenging, but there is no reason for introducing additional risk metrics or dismissing other metrics which have been in use in conventional PSA.

From the various metrics discussed in [5], the following are recommended as particularly suited for characterizing L2 PSA results. For the specific advantages of these metrics see the pertinent parts in section [5].

4.2.1 MEASURE FOR LOSS OF CONTAINMENT FUNCTION

There is already a widespread good practice in L2 PSA to identify the frequency of the loss of containment functions. The application of this measure is further encouraged, with the following comment:

It is recommended to at least distinguish:

- intact containment with design basis leakage,
- intact containment with filtered venting,
- loss of containment function due to a leak or rupture of the containment structure,
- loss of containment function due to failure of containment systems (e.g. open ventilation systems, open hatches),
- loss of containment function due to bypass through interfacing systems (for BWR including non-isolated break of feedwater or steam lines outside of the containment),
- loss of containment function due to bypass through steam generator tube leak (PWR only).

It may be interesting to introduce an additional metric, which has similarity to the well-known core damage frequency (CDF) concept of L1 PSA : a “Containment Failure Frequency” (CFF). The CFF would comprise all sequences where the containment function is lost - whatever the reason.

4.2.2 L2 PSA TOTAL RISK MEASURE

Depending on judgments involving also non-scientific considerations, the “total risk” of any installation can be defined in very different ways, e.g. in loss of value (of the plant and for the environment), or in health effects - which in themselves are far from being a precise category (e.g. distinguish long-term health effects from short-term health effects). The present document is about L2 PSA, and therefore the “total risk” which is proposed here is related to L2 PSA issues.

L2 PSA should provide a total risk measure as an overall complement to the many other risk measures under consideration. This can be done by integrating the risk due to all event sequences into a single metric by summing up all activity releases multiplied by their respective frequencies. Technically, this is an easy task for a present-day L2 PSA which has all accident sequences and release categories with their respective source terms available. When documenting the PSA, the contributions of interest to the total risk measure (e.g. specific initiating events, failure of particular SSCs, and potential of SAMs for reducing the total risk) should be indicated. Based on this information, it is possible to assess whether the design is well balanced, or whether particular improvements should be considered.

Another attractive feature which comes with a single value for the total risk is the possibility to compare it to a risk target. Without such a single value, having just a set of several different L2 PSA result characteristics, it is difficult to define a consistent set of various targets for the different result characteristics. Unfortunately, the PSA community is far from having consensus on what might be the proper harmonized total risk measure suggested above. It is recommended that pertinent groups precisely define the appropriate metrics (e.g. the isotopes to be considered, or the introduction of a parameter representing health effects for the individual isotopes). Once such a metric is defined it can be completed by pertinent risk targets. A suggestion for such a target is provided in section 7.3.

5 RECOMMENDATIONS ON THE LINK BETWEEN DEFENCE-IN-DEPTH AND EXTENDED PSA

Report D30.4 [4] is dedicated to the investigation of the link of Probabilistic Safety Assessment (PSA) and assessment with respect to the Defence-in-Depth (DiD) concept for NPP.

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

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

As an introduction to the topic, the paper on peculiar roles of DiD and PSA in NPP [92] states the following:

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

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

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

...

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

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

The main focus in report [4] is on the discussion of how an "extended PSA" can be used to verify the adequacy of the application of the defence-in-depth concept. In line with other activities of the ASAMPSA_E project, the report treats mainly L1 PSA and Level 2 issues.

In section 2, the report [4] reminds the most important aspects of the current understanding of the DiD concept and discusses important links to PSA in general and extended PSA in particular. Based thereon, several specific issues are identified for further investigation. Section 3 treats the link between the initiating event determination for an extended PSA, intermediate PSA results and the classification of potential initiating events (PIE) for DiD assessments. Section 4 is dedicated to classification schemes for systems, structures, and components (SSC), the reliability of engineered safety functions and the links to PSA. Complementary, in section, the report looks at

requirements on PSA models to facilitate DiD-related assessments and other important DiD-related issues not previously discussed. Finally, in section 6 conclusions and recommendations are provided.

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

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

Trying to do PSA assessments of DiD poses several specific challenges:

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

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

In the analysis of compliance with DiD, PSA can be an excellent tool to verify the independence of provisions on different levels of DiD. PSA used in the process of assessing compliance with DiD and determining the requirements for reliability of normal operation and safety systems, should be of sufficient scope and follow the current state of the art in PSA technology. A full scope PSA including all operational modes and events (i.e. an extended PSA as understood by the ASAMPSA_E project) is usually required. Level 1 PSA is needed to assess compliance with Level 3 of DiD and specify requirements for reliability parameters. Level 2 PSA is needed to evaluate compliance with Level 4 of DiD.

Simplistically, one can consider that the solution is to represent, for a given initiator and for a given safety function, the safety architecture through different levels of defence in depth, and for each DiD level, to consider

all the provisions that make up the "layers of provision" expected to achieve the safety function under consideration. The event tree is built with nodes that correspond to different levels of defence in depth. For each level, i.e. for each node, the fault tree applied to the layer of corresponding provisions establishes the probability of success or failure of the DiD level. Of course the reality is more complex because it is important to consider, with the PSA, the possibilities of partial failures for the layers of provisions and to integrate the mutual dependencies between different safety functions.

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

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

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

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

- discussion and recommendations in [4] are largely at a conceptual level ; this is partly due to the lack of previous investigations into the subject and partly due to a lack of practical implementations and feedback on good practices in the PSA community; therefore, specific guidance on how to do practical modelling of PSA with a view to do DiD assessments could be a subject for subsequent work;
- PSA models often have been produced without the specific objective of assessing the implementation of DiD by DiD levels; therefore, existing PSA models would have to be modified to comply with the

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

In order to define a way to go beyond the above considerations and overcome the highlighted limits, further investigations have been developed during the project about the peculiar roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations. An additional report [76] describes the proposed process and tools (see section 6.1). All the proposals are based on consolidated terminology and shared concepts and consistent with the (IAEA) Safety Fundamentals, Safety Requirements and process for the Safety assessment. Further activities are required in order to finalize the proposal, mainly about the criteria and metrics to be adopted and the development of practical applications. See related remarks in the following section 6.1.

6 EVOLUTIONS OF RISK ASSESSMENT AND RISK-INFORMED DECISION MAKING

Within the ASAMPSA_E project, several ideas for the evolution of safety assessment and risk informed decision making approaches were discussed. These concepts and ideas are presented in this section.

6.1 THE PSA ASSESSMENT OF DID BY NIER

NIER has presented several ideas which are also related to the further development of risk-informed decision making and the use of PSA. This section briefly summarizes the respective sections of [76].

NIER recognizes that *“[d]eterministic and probabilistic approaches [...] 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.”*

NIER emphasizes that *“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 performances to keep the consequences of the event under examination allowable, and 2) reliability of the layers of provisions which perform the requested mission.”* [74] NIER puts the DiD concept at the center of their proposals and state that *“[t]he 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.”* [74].

This is summarized in Fig. 1 for the whole process for the assessment of the DiD with the support of the PSA.



The commonly accepted deterministic analysis concept should be complemented by the following probabilistic considerations [76].

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.

[...]

From a probabilistic point of view, discussing about orders of magnitude, as indicated in the INSAG-12 [77], the objective is a frequency of severe damage to the plant (e.g. core melting) lower than $\sim 10^{-5}$ /reactor year (CDF, equivalent L1 PSA) all initiators considered and combined [...]. This objective shall be correlated with a further reduction of a factor 10 - ($10^{-5} > 10^{-6}$ reactor year) [...] usually endorsed by regulators -, for the unacceptable offsite consequences [...], all events considered and combined (equivalent L2 PSA). 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 + loss of containment function $\Rightarrow 10^{-6}$ / 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, on 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."

As practical guidance to designers, NIER states a “fraction of 10^{-7} per reactor year, per family of initiators and per function”.

“The management of Severe Accident with core degradation”

“[I]t 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.”

“Events, conditions or sequences practically eliminated”

Finally, initiators, situations or sequences that lead to intolerable large or early releases in the environment, and for which it is not reasonable to implement provisions for management of their consequences, should be identified and “practically eliminated”. To achieve this objective, the loss of provisions performing safety function whose failure can cause these intolerable effects, should be significantly lower than 10^{-7} /reactor year [...], even if this “cut off value” cannot be used alone to justify the practical elimination [...].”[76]

In addition to probabilistic considerations, the safety assessment should also take into account the following qualitative objectives.

“Robustness”

“[T]he notion of “robustness” is systematically evoked both for the design and for the assessment of the safety architecture [...]. This notion cannot be reduced, but envelops, the request for “simplicity” of the safety architecture [...] and to the meeting of values / figures consistent with the quantitative safety objectives, even if these figures are extremely low.”

“Exhaustiveness”

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.”

“Progressiveness character”

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.”

“Tolerant character

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.”

“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 order priority - inherent characteristics of the plant, passive systems or systems operating continuously in the necessary state, systems that need to be brought into operation, procedures.”

“Balanced character

The Balance 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 the damaged plant states.” [76]

In [76], the authors explain how these aspects can be considered in the PSA assessment and how PSA insights can be used to evaluate these aspects. Moreover, the authors explain how an Objective Provision Tree (OPT) approach can be used for a standardized representation of the safety architecture and how to implement this with a view to DiD. They also discuss how a “Lines of Protection” (LOP) approach, which consists of simplified and bounding probabilistic considerations, can be applied for assessing a design. This is summarized in Fig. 2. Based on these consideration, event trees can be derived along the lines of DiD. Fig. 3 illustrates this concept.

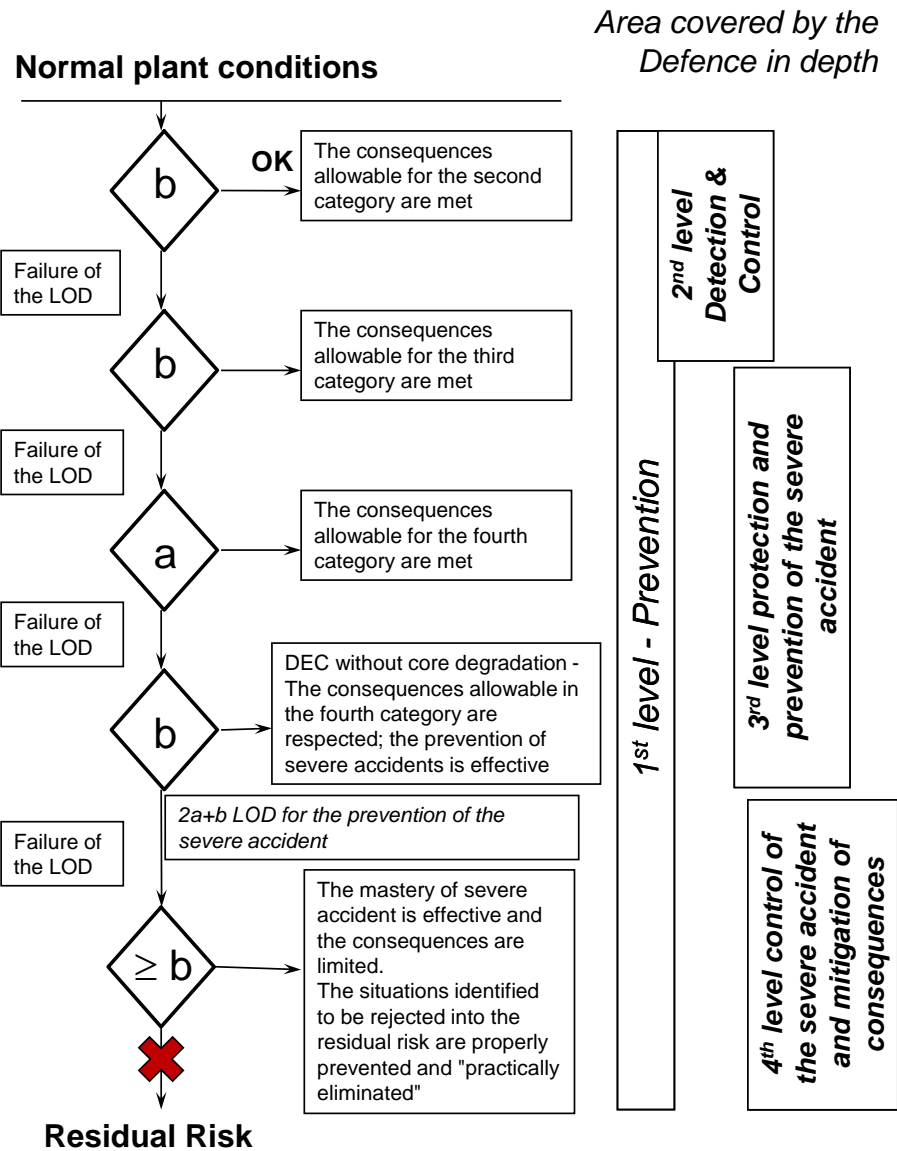


Fig. 2 Principles for the Lines of Defence methodology [76]

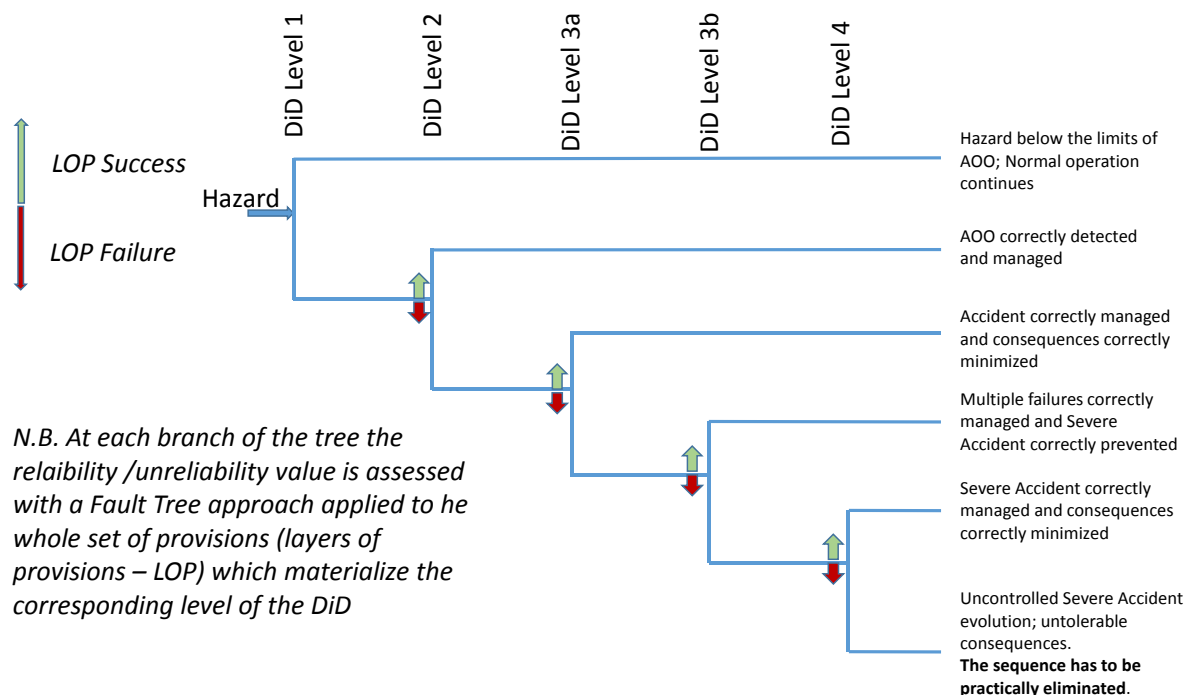


Fig. 3 Example of Event Tree organized following the structure of the DiD [76]

Based on this approach, the results of the design process can then be transferred to the risk space and checked for acceptable results and if risk is as low as reasonably achievable (ALARA). “The overall intent is illustrated schematically in Fig. 4. It shows that, for a given initiating event whose consequences are potentially unacceptable, design provisions are implemented⁸:

- to keep or make the consequences acceptable with regard to the likelihood of the initiating event they are requested to control; [...] and /or
- to decrease the likelihood of the accidental sequence; [...].”

⁸ For initiating events which consequences are very low there is no need for mitigation measures; the implementation of provisions to limit the consequences is not necessary.

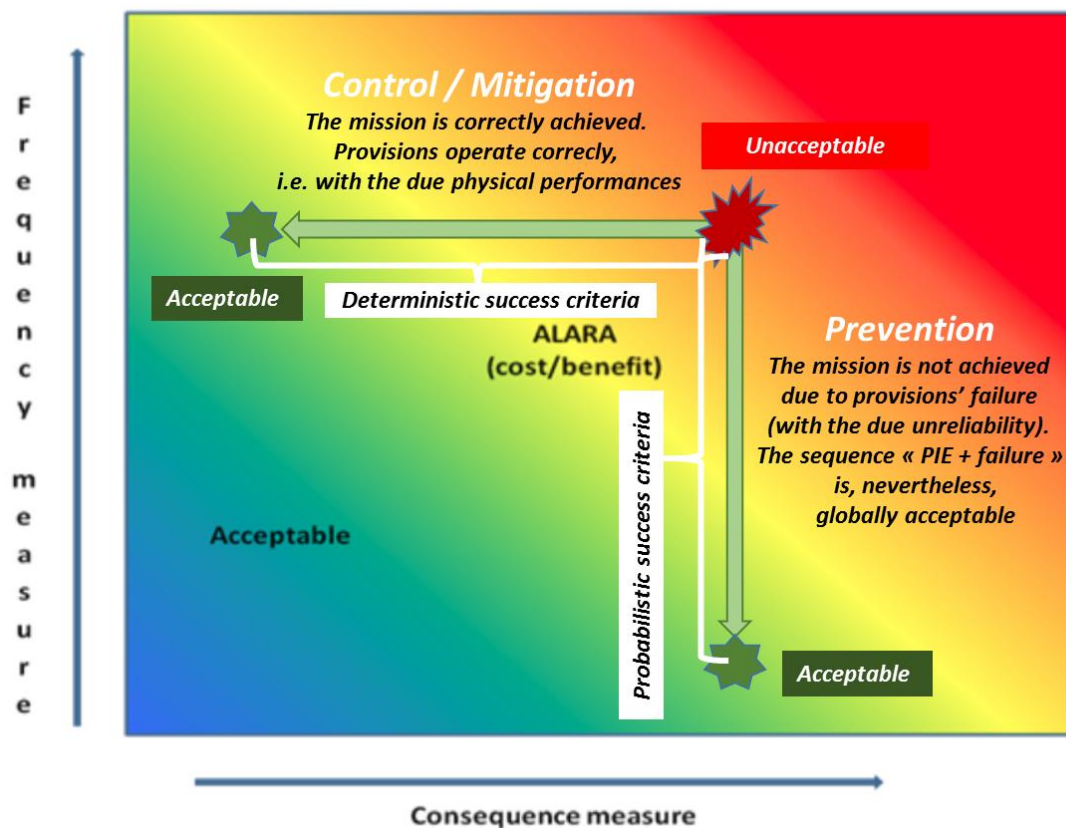


Fig. 4 Risk space and deterministic / probabilistic success criteria [76]

6.2 COMMON RISK TARGET BY CCA

CCA states that the major deficiency of current “safety objectives” and also so called “risk metrics” is that all of them are relative only in the sense that, while allowing for some comparison about risks, they are not developed to judge the overall risk of an NPP. According to CCA this is because they either represent just one component of the risk (mostly frequency, rarely consequences), or they are limited to some calculations assessing partial results, but not the total risk (which is the objective of PSA).

Additionally, parameters and acceptance values for safety objectives are country-dependent and they may differ by orders of magnitude or by definition, or “PSA objective”.

The IAEA definition of risk is usually implemented as a product of frequency and consequences. Considering recent research in the field of risk measures and nuclear safety, CCA developed a Common Risk Target (CRT) methodology and respective acceptance criteria. The basic concept was developed within the ASAMPSA2 project [7] and was further developed and published as scientific work in Nuclear Engineering and Design [49]. The CRT methodology and risk parameters make use of the IAEA INES scale [75].

The approach has the potential for the use as a common, harmonized and usable valid criterion for risk assessment. The numerical value(s) proposed in the method are suggested as a “target” to strive for in order to minimize all risks, and not as a “regulatory limit”. The target represents the practical tool for NPP safety evaluation including analysis of results and decision making. The method evaluates risk of releases by grouping results according to releases graded by INES scale, and the results can be related or converted in first approximation to absolute consequences in number of potential deaths, lost land, etc.

6.2.1 CCA'S TOTAL RISK MEASURE DEFINITION AND RISK TARGET

The ASAMPSA_E report on risk metrics D30.5 [5] discusses “integral risk measures” for L2 PSA. The common idea behind these approaches is aggregating risk over the different release categories into one figure of merit that reflects both the frequency of the respective sequence (or release category) and the consequence. It can be defined as:

$$\text{Total risk} = \sum_i f_i \cdot c_i$$

Where:

- i is the i^{th} release mode (class, sequence, source term),
- f_i is the maximum frequency per year of the i^{th} release mode, and
- c_i is the consequence in Bq of ^{131}I equivalent (cf. e.g. INES Manual [75]) for the i^{th} release mode.

With this definition of total risk [49] and the requirement of the constant total risk, CCA proposes to use a CRT parameter for a single unit site:

$$\text{ICRT} = 200 \times \text{FDFmax TBq of I-131 equivalent per year}$$

where

ICRT is Individual Common Risk Target (ICRT) of a single unit on the site with no significant contribution to already accepted other industrial risks

FDFmax is individual Fuel Damage Frequency maximum of a single unit per reactor year corresponding to a high level confidence safety limit of risk with no significant contribution to already accepted other industrial risks

Currently used limits do not consider higher number of units on a site, the issue that arose after the Fukushima accident. CCA offers solution of this problem with UCRT parameter (Universal CRT) which is supposed to be used for multi-unit sites by involving integrated site risk analysis. Single source initiators may cause multi-unit accidents due to cross-unit dependencies such as shared support systems, spatial interactions (flood propagation pathways) etc, common cause failures, or operator actions. It also offers the solution of the problem of common cause initiators challenging simultaneously units at multi-unit site (earthquakes, external floods, severe weather) [93]. Still keeping in mind the requirement of the constant total risk, the UCRT is as follows:

$$\text{UCRT} = \sum_m \text{IR}_m + \sum_n \text{Rccf-n}$$

where

m is number of units in the site,

n is number of possible combinations of common cause failures of the units,

IR is the individual risk of a single unit calculated using CRT method as described above,

Rccf-n is the risk of one common cause combination calculated for common cause initiators for more units using CRT method as described above (Details see [49]).

6.2.2 COMMON RISK TARGET AND ANALYSIS OF RESULTS AND DECISION MAKING

Decision should be made what investment should be realized to improve safety.

The reason, why this criterion is supposed to be better suited for risk analyses than currently used objectives is that it allows for decision making through proper analysis of results. The problem is that results are currently mostly given in form only of frequencies.

A simple example is given here of the potential for misinterpretation of risk results using current practices:

One of the results of L1 PSA is the set of minimal cutsets contributing to total CDF, which in the interface between L1 and L2 PSA are regrouped as individual accident sequences into PDSs (groups of sequences with “expected similar consequences”). One of the requirements of the IAEA followed by the CRT parameter is that “the plant risk should be balanced” - i.e. no sequence should have a significant contribution to total risk (cf. INSAG-12 [77]).

Let us suppose that in PSA results there are two PDSs only⁹:

1. Current practice is - results show frequency and the analysis of results is done with respect to frequency looking at PDS only:

PDS	fraction of CDF
1	30%
2	70%

According to this representation the conclusion I is that PDS 2 is “worse” with the contribution of 70% to total CDF (extrapolating the results even further to containment failure modes).

However:

2. Looking in more detail into the results we can see following:

In point 1 we considered CDF only, not frequency of releases. In case we take into account frequency of releases instead of frequency of core damage, we may arrive at a different conclusion:

PDS	fraction of CDF	fraction of LERF
1	30%	70%
2	70%	30%

According to these numbers, the conclusion is that PDS1 is “worse”.

3. Looking even further into the results we can see following:

⁹ In the following examples, only fractions of total results are used. Readers should be aware that in general e.g. total CDF and total LERF are not the same. The example makes implicit assumptions on reasonable values.

In 1 and 2, we considered frequencies only, not risk of releases. In case we take into account risk of releases (i.e. e.g. factoring in the magnitude of the different releases) instead of frequency of core damage/releases only, we may get different conclusion:

PDS	fraction of CDF	fraction of LERF	risk of releases
1	30%	70%	10%
2	70%	30%	90%

According to this representation, the conclusion is that PDS 2 is worse.

4. Looking further into the results taking into account also composition of PDSs, we may see the following:

PDS	Number of sequences	fraction of CDF	fraction of LERF	RISK of releases
1	10	30%	70%	10%
2	1000	70%	30%	90%

Assume the number of sequences in PDS1 shall be 10, but in PDS2 1000. It means that, if we simplify the situation in the first iteration by assuming that each sequence in every PDS has equal contribution, one sequence from PDS 1 has a contribution to total CDF of 3% while one sequence from PDS 2 has a contribution to total CDF of 0.07%. It would follow that each sequence from PDS 1 contributes about 40 times more in terms of “risk”, having individually a much more significant (4000% comparing with sequences from PDS 2) contribution to total CDF.

Taking into account CDF only, according to this “risk” model, PDS1 is “worst”; or rather a particular sequence from PDS1 with a contribution of 3% to CDF. The sequences from PDS 1, having equal contribution to CDF may have different contribution to LERF - maybe one of them close to 70%. Thus the model would show the worst sequence from PDS1 with significant contribution to LERF but from the point of view of contribution to final risk of releases the contribution it might be negligible.

Of course this may happen also with sequences from PDS2. A seemingly negligible sequence from PDS2 with 0.07% contribution to CDF may have up to 30% contribution to LERF and may also become significant from the point of view of contribution to total risk in terms of CRT, or the significant sequence may be some other sequence having negligible contribution to both CDF and LERF respectively, but significant contribution to total risk of releases.

In practice, PDSs consist of various sequences having different weights as far as contribution to CDF, LERF and risk of releases. Thus, we can see that it is necessary to analyse the PSA results properly to get a realistic figure about the impact of sequences/systems/failures to overall risk of releases, which we identify as the measure relevant for judging the safety of a plant. Therefore, PSA cannot stop at evaluating the individual components of “risk” (be they frequency, releases, consequences).

CCA further explains that in most of the current practice, PSA was able to identify the potential major contributors to “risk”, but decision making would not really be able to decide whether to concentrate efforts in finding ways to reduce the “risks” (should we first look at why accident in PDS1 occur before we look at the reasons for accidents that belong to PDS2?). Nevertheless, according to the logic imposed by the risk

representation as “frequency first”, efforts would likely concentrate on reducing the probability that accidents belonging to PDS2 would occur (and according to CCA this is the common occurrence).

CCA’s conclusion from the example above is that, focusing on frequency only, it is not unlikely that conclusions as far as significant contributors to final risks are wrong, and thus also related recommendations towards plant improvements are wrong. Thus, not only the financial resources invested into improvements based on these conclusions may be not optimal, but also the changes/investments may have marginal impact on safety/risk. Therefore, the core damage frequency and the large (early) release frequency figures of merit alone as risk metrics are not sufficient from the point of view of plant safety judgement and potential recommendations towards improvements.

6.2.3 COMMON RISK TARGET AND SEVERE ACCIDENT MANAGEMENT

The application of definitions of safety targets based on the LRF/LERF concept is well established. The application, however, is often limited to risk reduction only for large releases, i.e., only for the releases that would result in risk of individual “early” offsite consequences, and especially “individual early” death, unless the definition of “large” is much more restrictive.

The definition of targets based on the INES scale, according to CCA, provides a more powerful tool, which can also be used for applications to Severe Accident Management (SAM).

The following example for the use of the CRT was helpful for decision making about the installation and operation of a venting system in a PWR for improving the safety of the plant, again the main question being about the right investment.

The issue for the plant in question was that a filtered containment venting had been already installed, and the PSA showed a very marginal risk reduction due to this system. One reason was the large uncertainty connected with hydrogen combustion at the time of venting, especially related to a potential for detonation in the venting system scrubbing tank or at the exit of the system (a stack). This would have resulted in relatively large source terms due to failure of the filtration system. At the time, only sensitivity analyses had been performed to calculate the risk reduction, and if the LERF concept had been applied, the results would not have shown any advantage for venting because the sequences needing venting would not have fallen into the class of “Early” even without venting.

On the other hand, if the concept proposed in this work (the “CRT”) had been applied from the onset, a clearer response had been given. This is illustrated in Fig. 5. The safety targets defined here can be displayed in a line of constant risk (the red line in the figure). When a data point lies to the right of this curve, the result can be considered “unsafe”. The red circle represents the risk of late containment failure without the venting system. After the venting system is implemented, three outcomes are possible.

Blue triangle 1: Release due to venting

Blue triangle 2: Failure of the venting system and late containment failure.

Blue triangle 3: Hydrogen combustion due to venting and failure of the venting system.

It can be seen that when the venting option alone is implemented, there is some risk reduction because the risk from accidents with late containment failure (LCF) diminishes. However, one component of risk (“Hydrogen combustion due to venting”) remains to the right of the iso-risk curve and therefore the remaining risk is not deemed acceptable, still.

On the other hand, if an effective hydrogen reduction method is provided (e.g. by igniters and/or recombiners) as shown in green triangle, then the risk component due to hydrogen combustion would be basically eliminated and then the implementation of venting would have been recognized as clear-cut “fail safe”. There would be no discussion with respect to the advantages of additionally installing hydrogen reduction systems at the plant in conjunction with the containment venting system. Note that since this safety targets related technique was not available at the time, discussions on hydrogen control in relation to a venting strategy continued for several years after the PSA was concluded. Similar examples could be given to show effectiveness of SAM measures, and also for prioritization of actions in the actual SAM guidelines.

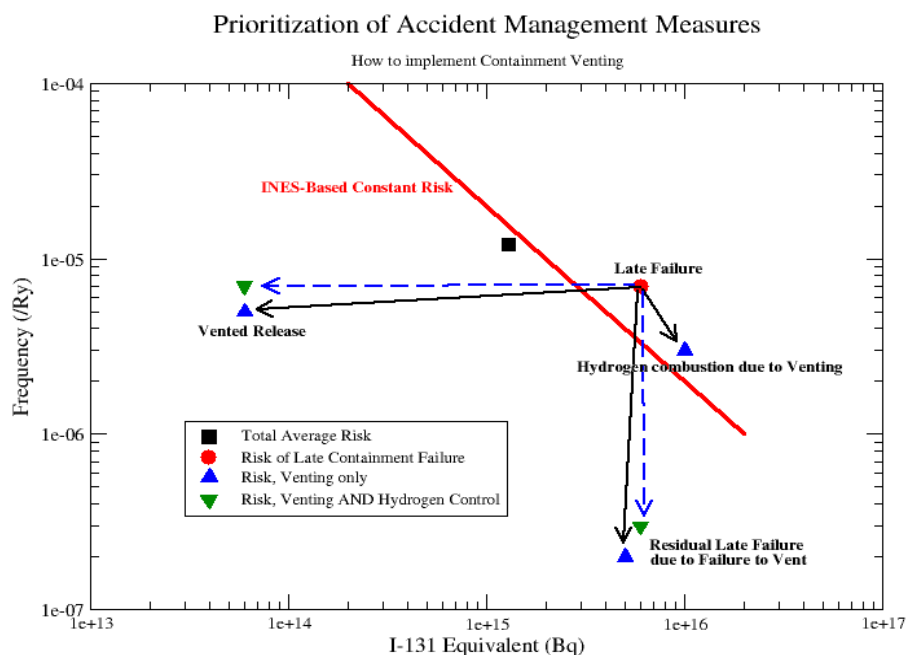


Fig. 5 Example of the possible use of INES-Based safety targets for prioritization of SAM actions

7 SAFETY OBJECTIVES FOR AN EXTENDED PSA

The definition or acceptance of safety objectives is in the responsibility of authorities which are in charge of public safety and the safe operation of NPPs is the responsibility of the utilities. The present document has been written by a group of technical experts which do not claim to have the respective authority. All the following statements should be seen with this background.

7.1 SAFETY OBJECTIVES FROM EXISTING PSA COMPILED BY OECD/NEA

7.1.1 SUMMARY OF A NEA SURVEY FROM 2009

In the ASAMPSA_E deliverable [5] a large number of risk metrics is compiled. For several of them safety objectives have been defined by various organizations, or for particular purposes. The NEA-document “Probabilistic Risk Criteria and Safety Goals” [19] contains a compilation of 19 answers from different organizations. Answers have been received from 13 nuclear safety organizations (Canada, Belgium, Chinese Taipei, Finland, France, Hungary, Japan, Korea, Slovakia, Sweden, Switzerland, UK and USA) and 6 utilities (Hydro-Québec, Fortum, OKG, Ontario-Power-Generation, Ringhals and TVO). Most of the following text is taken from [19].

The criterion core damage frequency is used by most of the respondents. However, the definition of the criterion differs considerably with the reactor’s technology. For instance, for reactors of CANDU type, the core damage is defined as loss of structural integrity of more than one fuel channel. Some countries have very precise technical definitions of CDF, e.g. defining core damage as local fuel temperature above 1204 °C, i.e., the limit defined in section 1b of 10 CFR 50.46 (Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors). Other countries have more general definitions referring, for instance to prolonged core uncover or long-term cooling. Requirements for new plants are typically stricter (in terms of frequency) than for existing ones, and are mandatory as opposed to indicative. For instance, in Switzerland and Finland it is required by regulation that the applicant for a permit to build a new nuclear power plant shall demonstrate that the core damage frequency is below 1 E-5 per year. Fig. 6 summarizes numerical criteria defined for core damage. The values associated with CDF vary from 5 E-4 per year to 1 E-5 per year. When indicated, this spread is reduced when considering new plants where all respondents but 2 set the CDF to 1 E-5.

The values associated to releases frequency show a wider spread, from 1 E-5 per year to 1 E-7 per year. As for the CDF, the spread is reduced when considering new plants, where all respondents but one set the LRF (or LERF) to 1 E-6 per year. It has to be noted that the results are highly related to the scope and detail of the reference PSA, so the numerical values cannot be compared without a complete definition of the scope covered by the PSA.

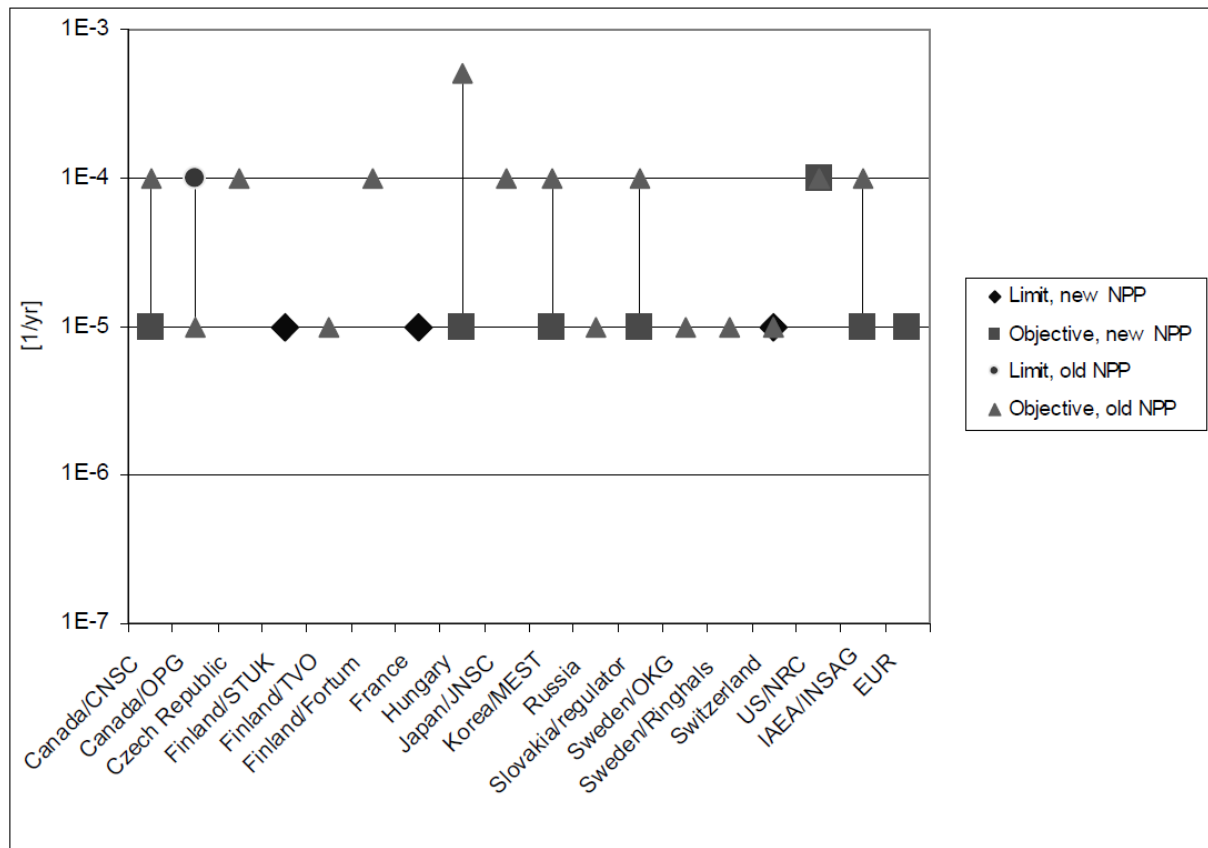


Fig. 6 Numerical criteria defined for Core Damage [76]

There is both a considerably larger variation in the frequency limits for large releases, and very different answers to the question of what constitutes an unacceptable release. As with the CDF, the magnitudes are sometimes based on IAEA safety goals suggested for existing plants, i.e., on the level of 1 E-5 per year (IAEA-INSAG-12). However, most countries seem to define much stricter limits, between 1 E-6 per year and 1 E-7 per year.

The definition of what constitutes an unacceptable release differs a lot, and there are many parameters involved in the definition, the most important ones being the time, the amount and the composition of the release. Additionally, other aspects may be of interest, such as the height above ground of the point of release. The underlying reason for the complexity of the release definition is largely the fact that it constitutes the link between the L2 PSA results and an indirect attempt to assess health effects from the release. However, such consequence issues are basically addressed in L3 PSA, and can only be fully covered in such an analysis.

The release for which a numerical criterion is given is also defined in several different ways:

- large release: this is defined as an absolute magnitude of activity and isotope released, e.g., 100 TBq of Cs137,
- large early release: these definitions are more qualitative, e.g., “Large off-site releases requiring short term off-site response,” “Significant, or large release of Cs137, fission products before applying the offsite protective measures,” “Rapid, unmitigated large release of airborne fission products from the containment to the environment, resulting in the early death of more than 1 person or causing a severe social effect.”

- small release: CNSC from Canada has set criteria both for large and small release. A small release is defined as a release of 1000 TBq of I131
- unacceptable consequence ; this is a French definition which is fully open and rather old (1977) ; today, for France, EDF proposes numerical targets case by case for applications (e.g a criteria “50 mSv at 500 m” has been used to identify “large release” situations for the EPR licensing in France). These targets are consistent with the qualitative objective “consequences limited in space and time”). containment failure: the Japanese Nuclear Safety Commission proposes a criterion for containment failure frequency; in Finland, STUK had defined, in the first version of the Guide YVL-2.8, a probabilistic criterion for containment isolation failure (conditional failure probability); this is a requirement that aims at assuring the robustness of the defence-in-depth.

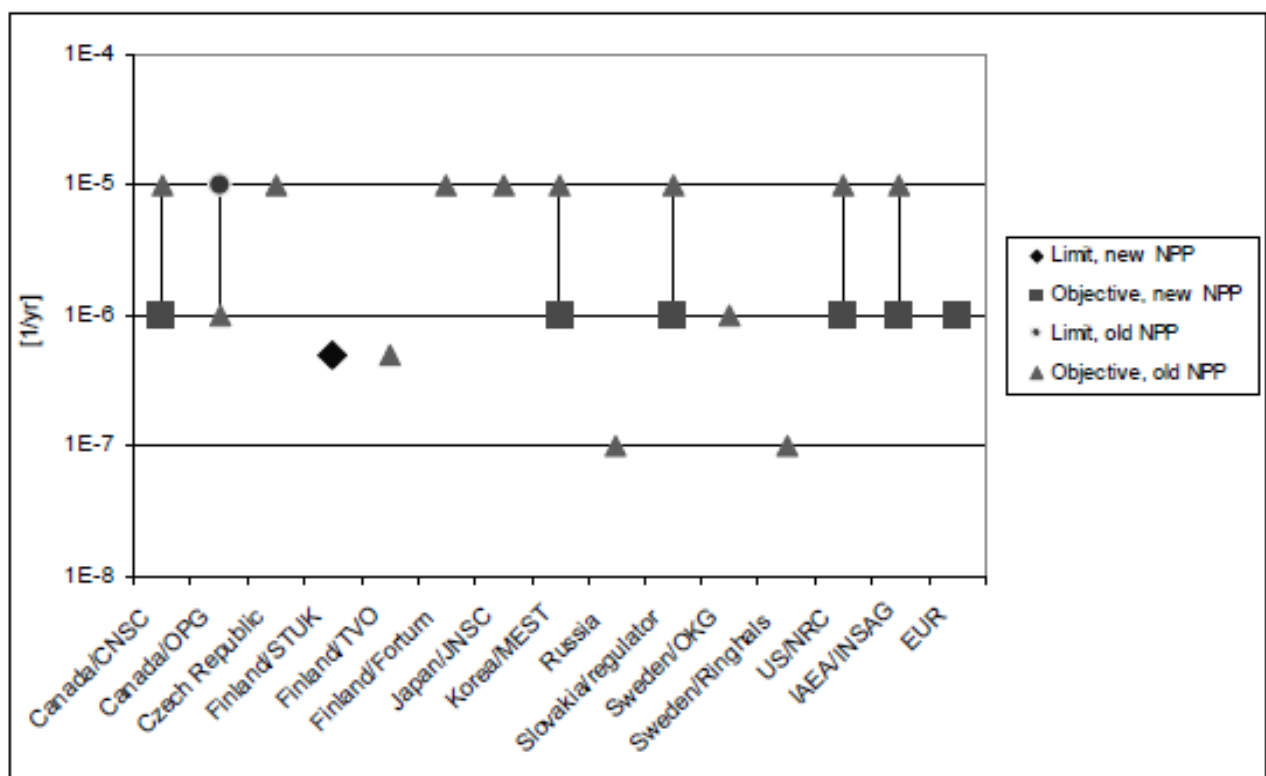


Fig. 7 Numerical criteria defined for large release. (Definition and timing of “large release” varies) [19]

Fig. 7 summarizes numerical criteria defined for large release frequency. The definition for “large release” is not the same for all organizations. However, it can be seen that objectives vary from 1 E-7/year to 1 E-5/year, which is a quite large spread, larger than for core damage frequency.

In the USA, the NRC expects new or advanced nuclear power plants to present a higher level of severe accident safety performance consistent with the NRC’s Severe Accident Policy Statement.

	CDF	LERF	Conditional Containment Failure Probability
Operating Plants & License Renewal	<1E-04	<1E-05	n/a
New Plants	<1E-04	<1E-06	<0.1

7.1.2 SUMMARY OF A NEA SURVEY FROM 2012

Report [93] provides a description of the PSA activities in the NEA member countries at the time of the report writing at the end of 2010. An evolution occurred in the definition of safety criteria. Generally the safety criteria for new plants are more demanding (concerning numerical value and/or requirements) than for existing plants. In general, the expectation is that the target/objective for the level of risk from a new plant should be about an order of magnitude lower than for existing plants for which a PSA is available. Some countries use the numerical criteria as an orientation and as an indicative figure (Czech Rep., France, India, UK), whereas some countries have identified the safety criteria only for the new build (Canada, Finland, Slovenia, Switzerland).

In some countries, the numerical criteria are derived from the high level metrics, i.e., the qualitative safety objectives such as the individual risk and/or societal risk, whereas in some other countries, the safety goals were adopted by the regulatory bodies or the licensees from IAEA (IAEA-INSAG-12) or from published documents by other bodies.

In most of the countries in which numerical safety criteria have been defined, the latter have been defined as a “target”, an “objective” or a “goal” where the recommendation is that the risk should be lower than the prescribed value with no guidance given on what action needs to be taken if it is exceeded. However, the UK uses a comprehensive framework for defining the risk criteria. For each of the risk measures addressed, two numerical values are defined: a Basic Safety Limit (BSL) above which the risk would be unacceptably high; and a Basic Safety Objective (BSO) below which the risk is broadly acceptable. It is noted that these criteria are not legal limits but are guidance, and are used by the regulator to inform the depth of assessment a particular issue is subject to.

Some countries (Canada, USA) have defined qualitative individual risk criteria so that individual members of the public are provided a level of protection from the consequences of nuclear power plant operation such that there is no significant additional risk to the life and health of individuals.

For the contributing countries the numerical criteria for core damage frequency are shown in the following table from [93].

Table 2. Summary of numerical criteria for CDF [93]

TABLE 3-1: Summary of numerical criteria defined for core damage frequency			
Country	Organization	Frequency	Notes
USA	Regulator	10^{-4} /r.y	Objective
UK ⁴	Regulator	10^{-4} /r.y 10^{-5} /r.y	Limit Objective
Taiwan	Licensee	10^{-5} /r.y	Limit
Switzerland	Law	10^{-5} /r.y	Limit for new plants Objective for existing plants
Sweden	Law	Licensee 10^{-5} /r.y – level 1 studies	Objective This is a criterion or safety goal established by the licensees, for CDF from level 1 PSA's.
Slovak Rep	Regulator	10^{-4} /r.y 10^{-5} /r.y	Objective for existing plants Objective for new build
Slovenia	Regulator	10^{-4} /r.y 10^{-5} /r.y	Objective for existing plants Objective for new build
Netherlands	Regulator	10^{-4} /r.y 10^{-6} /r.y	Limit for existing plants Limit for new plants
Italy	Regulator	10^{-5} to 10^{-6} /r.y	Objective
Hungary	Regulator	10^{-5} /r.y	Objective
France	Regulator	10^{-6} /r.y	Objective related to shutdown state
France/Germany	Designers of EPR	10^{-6} /r.y	Objective
Finland	Regulator	10^{-5} /r.y	Objective for new build
Czech Rep	Licensee	10^{-4} /r.y 10^{-5} /r.y	Objective for existing plants Objective for new plants
Canada	Regulator	10^{-5} /r.y	Limit for new plants
	Licensee	10^{-4} /r.y 10^{-5} /r.y	Limit for existing plants Objective for existing plants

The numerical criteria for large early release frequency are shown in Table 3-4 of [93].

Table 3. Summary of numerical criteria for L(E)RF [93]

TABLE 3-4: Summary of numerical criteria defined for large (early) release frequency				
Country	Organization	Risk metric	Frequency	Notes
UK	Regulator	10^4 TBq I131, or 200 TBq Cs137 or other isotopes	10^{-4} /yr 10^{-5} /yr	Limit Objective
Taiwan	Licensee	Not defined	10^{-6} /yr	Objective
Sweden	Licensee	> 0.1% of core inventory	10^{-7} /yr	Objective This is a criteria or safety goal established by the licensees, for L(E)RF from level 2 PSAs.
Slovak Rep	Regulator	Not defined	10^{-5} /yr	Limit for existing plants
		Not defined	10^{-6} /yr	Limit for new build
Slovenia	Regulator	Not defined	5×10^{-6} /yr	Limit for existing plants
		Not defined	10^{-6} /yr	Limit for new build
Japan	Regulator	Containment failure	10^{-5} /yr	Objective
France	Regulator	Unacceptable consequences	10^{-4} /yr 10^{-5} /yr	Objective
France/Germany	Designer of EPR	Not defined	Neg ⁵	Objective
Finland	Regulator	100 TBq Cs137	5×10^{-7} /yr	Objective for new builds
Czech Republic	Licensee	Not defined	10^{-5} /yr	Objective for existing plants
			10^{-6} /yr	Objective for new plants
Canada	Regulator	100 TBq Cs137	10^{-6} /yr	Objective for new plants
	Licensee	>1% Cs137 >1% Cs137 \\	10^{-5} /yr 10^{-6} /yr	Limit for existing plants Objective for existing plants

7.2 RECOMMENDED SAFETY OBJECTIVES FOR LEVEL 1 PSA RISK MEASURES

This chapter tries to discuss possibilities to harmonize safety objectives for L1 PSA risk measures using the extended PSA concept.

In the ASAMPSA_E deliverable [5], two L1 PSA risk measures have been recommended: fuel damage frequency FDF and radionuclide mobilization frequency RMF.

Fuel damage frequency (FDF) measure, defined as a loss of integrity of fuel elements on the site, which has the potential for an accident-level release, provides a more general notion of a L1 PSA end state than other direct risk measures as CDF. CDF affecting fuel elements located in the reactor core is considered as a subset of FDF. Similarly, fuel damage related to other locations than the core (e.g. spent fuel pool) are also subset of the FDF risk measure. FDF can also be readily applied to multi-unit sites

Is it possible and useful to harmonize quantitative objectives for FDF ?

The quantitative objective for FDF should, of course, be consistent with the established CDF figures. Therefore, as a first step of introducing FDF, the existing CDF objectives should be directly applied to FDF. This is more than just a formal step, since it means taking into account the spent fuel on the site in addition to the core.

As a second step, in a perspective of harmonization, it is recommended that the organizations involved agree on a common definition of fuel damage. From a technical point of view it is meaningful to establish a link to the damage of fuel cladding. Fuel cladding damage could either be defined as cladding rupture, releasing part of the contained activity; or it could be defined as a deformation (ballooning) which would obstruct cooling channels.

In a third step, attempts should be made to arrive at a common safety objective for FDF: from Table 2, it seems that 1 E-5/year (for all initiating events) could be an order of magnitude of such common safety objective. **But the main point is that such common safety objective for FDF should cover each and every initiating event (internal and external), and all sources of fuel (in particular core and SFP) and all units of a site.** Therefore, even if the figure itself may be not much more stringent than existing values, the inclusion of all relevant aspects means a significant challenge for PSA analysis and plant design.

Because the main risk measures for L1 PSA like e.g. core damage frequency or fuel damage frequency are not well suited for describing several scenarios which might lead to a significant release of radionuclides into the plant as a starting point for a L2 PSA, a new metric, “Radionuclide Mobilization Frequency, RMF” (see section 2.17 in [5]), addresses these issues. This risk metric is defined as a loss of the design basis confinement for a source of radionuclides, leading to an unintended mobilization of a significant amount of radionuclides with the potential for internal or external release.

Since RMF is a new metric, there is no recommendation available about a pertinent quantitative safety objective. The threshold value and its reference radionuclide (or radionuclides) have to be adjusted to the facility under consideration and the objectives of the study.

The RMF risk measure is recommended to be used for an extension and generalization of the established CDF and FDF risk measures to a multi-source PSA. It is therefore a suitable and above all complementary risk measure for an extended PSA that addresses potential sources on the site in addition to fuel in the reactor and spent fuel. Currently, no applications of RMF are known, and there is no consensus on the threshold value and its reference isotopes. In any case, CDF and FDF is a subset of RMF.

7.3 RECOMMENDED SAFETY OBJECTIVES FOR LEVEL 2 PSA RISK MEASURES

In the ASAMPSA_E deliverable [5] two L2 PSA risk measures have been recommended:

- containment failure frequency (CFF),
- level 2 total risk measure.

7.3.1 MEASURE FOR LOSS OF CONTAINMENT FUNCTION

There is already a widespread good practice in L2 PSA to identify the frequency of the loss of containment functions. The following modes of loss of containment function should be distinguished [5]:

- intact containment with design basis leakage,
- intact containment with filtered venting,
- loss of containment function due to a leak or rupture of the containment structure,
- loss of containment function due to failure of containment systems (e.g. open ventilation systems, open hatches),
- loss of containment function due to bypass through interfacing systems (for BWR including non-isolated break of feedwater or steam lines outside of the containment),
- loss of containment function due to bypass through steam generator tube leak (PWR only).

The contribution of each of these modes of loss of containment function to the total conditional probability (as defined above) shall be identified in the PSA documentation.

It is recommended to introduce a “Containment Function Failure Indicator” which would comprise all sequences where the containment function is lost - whatever the reason.

The containments of almost all existing NPPs were not designed against accidents with fuel melting. Therefore, it would be inappropriate for such plants to define very low conditional probabilities for containment failure. Nevertheless, for the protection of people and environment, some efficiency of the containment against severe accident effects is expected. This leads to the following recommendation for existing plants:

- for existing plants the conditional probability for the loss of containment function under the condition of fuel damage (from all potential sources, including the containment of the SFP) must not exceed 10%. (Successful filtered containment venting with intact containment is not considered as loss of containment function).

Future plants will have to include better management of fuel damage. They are e.g. equipped with melt retention devices (core catchers), alternative containment cooling systems or with procedures to prevent high pressure core melts. Therefore, it is justified to recommend a better containment performance as follows:

- for new plants the conditional probability for the loss of containment function under the condition of fuel damage (from all potential sources, including the SFP) must not exceed 1%. (Successful filtered containment venting with intact containment is not considered as loss of containment function).

For such an application of L2 PSA, appropriate success criteria for SAM strategies can be derived: for example, for successful filtered containment venting with intact containment, or for the use of mobile equipment for the NPP long term management (if procedures exist and are routinely tested). This will highlight solutions to manage accidents where equipment needed for both accident prevention and mitigation are not available (due to long term station blackout for example). Indirectly, such application of L2 PSA will conduct to examine quantitatively the independence between accident prevention provisions and accident mitigation provisions (see discussion on DiD).

7.3.2 L2 PSA TOTAL RISK MEASURE

Level 2 PSA should provide a total risk measure as a complement to the many other risk measures under consideration. This can be done by integrating the risk due to all event sequences into a single metric by summing up all activity releases multiplied by their respective frequencies [5]. Technically, this is an easy task for a present-day L2 PSA which has all accident sequences and release categories with their respective source terms available.

In section 6.2 CCA provides a suggestion for a safety objective as follows:

$$\text{Total risk} = \sum_i f_i \cdot c_i$$

Where:

- i is the i^{th} release mode (class, sequence, source term),
- f_i is the maximum frequency per year of the i^{th} release mode, and
- c_i is the consequence in Bq of ^{131}I equivalent (cf. e.g. INES Manual [75]) for the i^{th} release mode.

With this definition of total risk, CCA proposes to use a common risk target (CRT) objective :

for single unit site (Individual CRT):

$$ICRT = 200 \times FDF_{\max} \text{ TBq of I-131 equivalent per year}$$

for multi-unit site (universal CRT):

$$UCRT = \sum m IRm + \sum n Rccf-n$$

The derivation of this objective is given in detail in [49] and will not be repeated here.

The CRT objective as defined above fits to the other recommendations in the present document. Its application would probably not lead to inconsistencies with other types of objectives. If a total risk measure is deemed useful for decision making and / or communication of PSA results, the common risk as defined above should be applied.

8 IMPROVING DECISION MAKING USING EXTENDED PSA RESULTS

8.1 CURRENT UNDERSTANDING OF RIDM APPROACHES

The basic approach to risk-informed decision making (RIDM) is well described in INSAG-25 [12]. Fig. 8 illustrates the integrated RIDM approach as defined in INSAG-25.

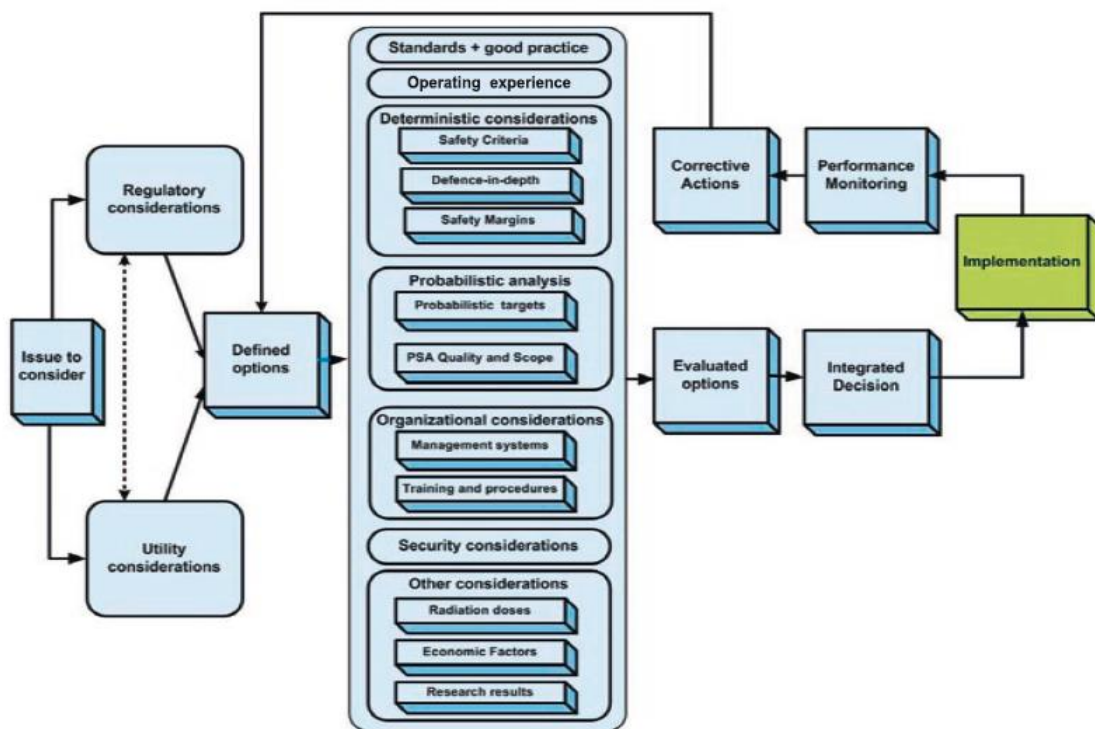


Fig. 8 Key elements of integrated RIDM approach from INSAG-25 [12], p. 6

Following D30.5 [5], we point out to the following limitations on any decision making problem. *There is no common understanding on the correct (or even appropriate) approach to decision making regarding risk in the scientific community as well as with actual end-users [58]. Depending on the subject matter to decide and the role and the interest of the decision maker or stakeholder, different approaches to decision making are advocated or rejected [28], [31], [52], [53], [58], [60], [13]. Moreover, the acceptability of these approaches to the stakeholders or the society obviously depends on the culture of the society in question and the specific values and beliefs on risk acceptance on a personal and societal level [64]. For the purpose of the ASAMPSA_E project, work on the ethical or legal or theoretical foundations of decision making [23], [55], [56], [57], [58] is clearly out of scope, as is a discussion on cultural influences.*

It is important to note that the aforementioned issues have important implications for the recommendations contained in this report. Decision makers are influenced by factors that transcend natural science and cannot be resolved in a strictly objective manner in this sense. Consequently, implicit and explicit utility considerations on decision alternatives will necessarily have a strong subjective component. Furthermore, the relevance of information, e.g. from PSA, the acceptability of certain kinds of risks, and finally the adequacy of risk measures to support decisions will depend on the decision maker. In the end, the decision maker has to decide which aspects of risk and thus which risk measures are relevant for each alternative. This is illustrated in Fig. 9. Therefore, the recommendations in this report have to be understood as options for decision makers. The authors have identified these approaches as suitable for a wide range of typical situations and believe that they will help to select the best decision alternative. The recommendations should not be interpreted as a fixed set of rules which can be applied to every situation. Similarly, they might lead to results which decision makers do not agree with. Thus, even if decision makers follow the recommendations in this report, they should be free to select alternative

approaches as they see fit. This has to be acknowledged by PSA analysts, which use this report to prepare information for decision makers. It is therefore essential that PSA analysts and decision makers agree on the scope of PSA assessments at an early stage.

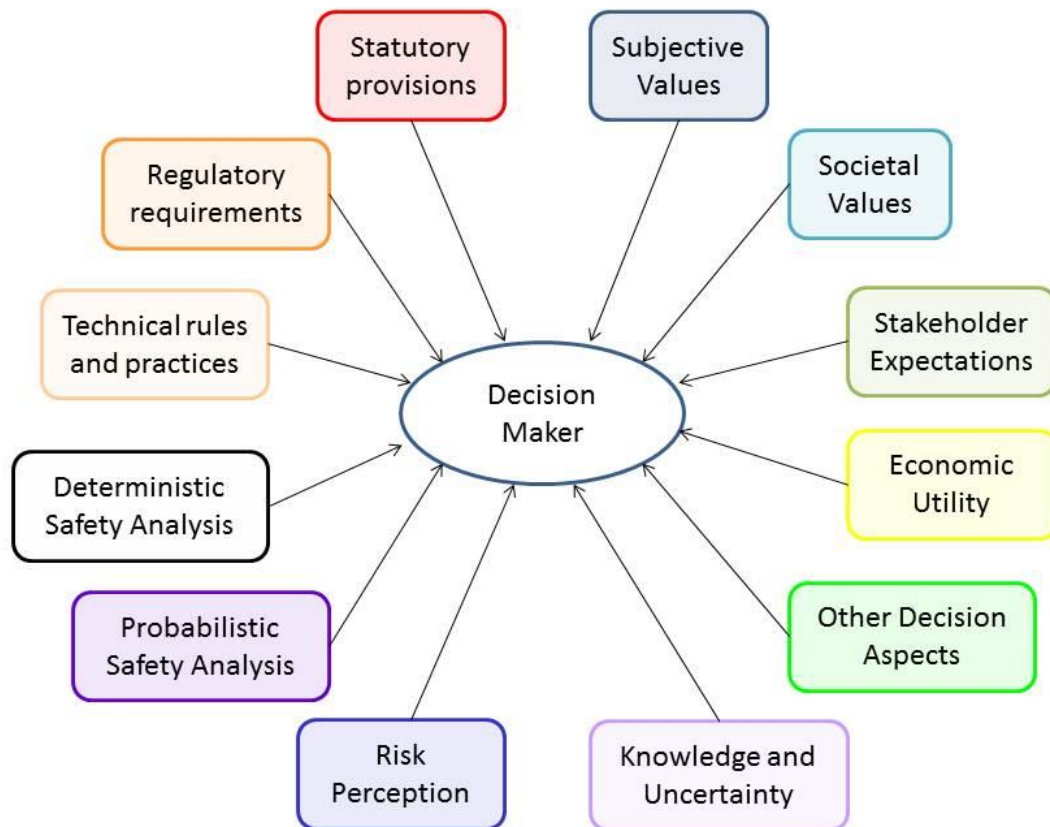


Fig. 9 Selected Influencing Inputs to a Decision Maker

8.2 EXTENSIONS OF RIDM APPROACHES

The following additions and recommendations on RIDM approaches have been discussed during the project.

8.2.1 PRACTICAL APPROACH TO THE IMPLEMENTATION OF INTEGRATED RIDM PROCESS

/Exchanges of experience from the ASAMPSA_E partners is missing here/ An example can be found in section 6.2.3. The report shall be completed as far as possible before the end of the project/ typically : cost vs safety benefits methods could be presented/

In this section a short description of possible practical approach for the implementation of IRIDM process is given based on paper [82]. In order to select optimal options from possible decision strategies, in IAEA guidelines it is proposed to calculate the score of the option k by the following formula:

$$S_k = \sum_i W_i \cdot s_{ik}$$

where W_i are the weighting factors for inputs i (corresponding to different types of risk), while s_{ik} describes an impact of option k on input i .

The weights are assigned basing on engineering judgement with the range from the most negative to the highest positive impact (for example from -10 to 10, or from 0 to 10). This process can be quite subjective, therefore the methodology based on Value Tree Analysis (VTA) has been proposed in [82].

Implementation of VTA consists of the following steps [83]:

1. structuring - definition of concepts, identifying objectives, alternatives, creating a hierarchical model of objectives, recognizing attributes for objectives,
2. decision criteria/attributes - problem framing and defining value dimensions,
3. value comparisons - prioritisation of objectives,
4. sensitivity - usually related to what-if analysis,
5. learning - reformulating the problem, return to the beginning and generation of compromise alternatives.

The first of this methodology step is to construct the value tree diagram - an example of such graph is presented on Fig. 10. The diagram contains the following elements:

- IRIDM inputs: typically DSA, PSA and economy aspects, but any other element can be included;
- set of attributes important for each IRIDM input;
- possible strategies to be analysed and scored in the IRIDM process.

Assignment of weights for IRIDM inputs can be organized in the form of facilitated workshop, in which wide spectrum of stakeholders can participate (like representatives of regulatory body and operator, experts, local administration). When a compromise is reached in the process of prioritisation of the IRIDM inputs, a relative importance of i -th input is expressed by weight W_i .

The attributes can be identified by a group of experts and the prioritisation of these attributes is done by assigning weight A_{ij} for each j -th attribute of the i -th input. There are several techniques for performing such assignment [82], [83]. This leads to the following formula for assignment of the score for option k :

$$S_k = \sum_i W_i \cdot \sum_j A_{ij} \cdot s_{ijk}$$

where the s_{ijk} factor describes how the implementation of option k -th would affect the attribute j of input i .

As far as deterministic attributes are considered they should describe crucial parameters and performance of the nuclear installation, important for safety e.g. maximum peak cladding temperature or its maximum oxidation. These limits cannot be exceeded in any case because it would lead to the failure of important systems or components of the installation.

The PSA margins can be defined as the difference between the legally binding PSA goals acceptable to the regulatory body and the values of the risk parameters calculated for the specified plant. Thus, the PSA attributes could cover the following goals [84], [85]:

- core damage frequency ($\leq 1\text{E-}5$ per year),
- probability for radioactivity release ($\leq 1\text{E-}6$ per year),
- shut down system unavailability ($\leq 1\text{E-}6$ per demand),

- engineered safety systems unavailability ($\leq 1\text{E-}3$ per demand),
- individual risk of fatality ($\leq 1\text{E-}6$ per year),
- frequency of doses (≤ 1 mSv per year).

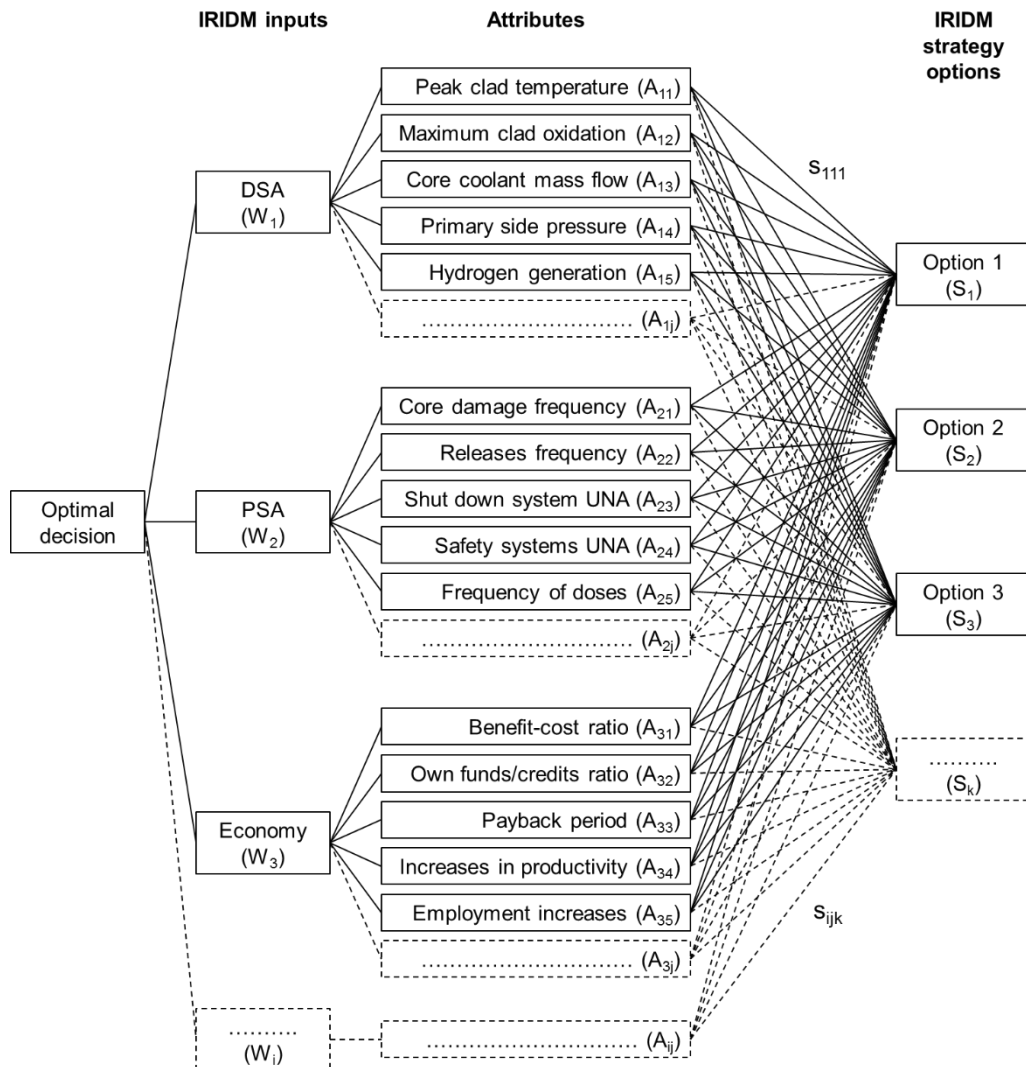


Fig. 10 Simplified value tree diagram developed to support decision-making on nuclear safety [82].

In this respect it should be mentioned that in order to verify the interest of the probabilistic goals, the OECD Nuclear Energy Agency (NEA) has prepared a questionnaire addressed to nuclear safety organizations and regulatory bodies all over the world [19]. Some prioritization can be proposed basing on the received answers:

- core damage frequency (16 respondents confirmed importance),
- release frequency (14 respondents),
- frequency of doses (4 respondents),
- individual risk of fatalities (3 respondents),
- safety systems unavailability (2 respondents).

In order to estimate s_{ijk} the value function v can be applied. In general it can be defined as a function of x given by the formula:

$$x = \frac{x^a - x^f}{x^a - x^i},$$

where x^a is the acceptable value of the considered parameter, which cannot be exceeded (for example due to the official regulations, safety goals or internal policy of the operator). The variables x^i and x^f describe the initial (actual) value of the parameter and its final value (after implementation of k -th decision option), respectively. Assuming that x^a is higher than x^i , which means that the actual state of the installation is in compliance with the requirements, one can evaluate different decision options by calculation of x^f . When safety issues are considered the x value describes how the safety margins would be changed by implementation of different decision options. In general, when $x > 1$ the implementation of particular decision has a positive effect on the considered parameter by increasing the safety margins. When $0 < x < 1$ the decision would change the considered parameter negatively. For $x < 0$ the particular decision cannot be implemented because of exceeding the acceptance criteria. If $x = 1$ no change is expected after the decision implementation.

Hence, the range of x should be chosen at first, e.g.:

- $x_{min} = 0$ - correspond to reducing the safety margins to minimum acceptable level,
- $x_{max} = 1.5$ - significant improvement in the safety margins.

Then, the value $v(x)$ can be fixed for the two extreme points, e.g.:

- $v(x_{min}) = 0$ - the limit of acceptance,
- $v(x_{max}) = 1$ - the very best case.

Next, the shape of the curve should be specified in order to describe the relation between the x value and the s_{ijk} factor estimated by $v(x)$. When any changes in the lower region of the parameter x space are more important to the decision makers than the changes of the same size in the upper region the concave curve should be chosen (Fig. 11). Such a situation usually takes place when the safety margins are considered. If the safety margins are appropriate then the decision makers are rather interested in keeping their current values than to increase them. Consequently, those options which do not change the current values of the safety margins have a relatively high score $v(x = 1.0) = 0.9$. Moreover, in this particular case the value of $v(x = 1/2)$ was fixed for 0.75 (on Fig. 11), which means that the safety margins reduced by half are still good enough. It should be stressed that this parameter can be controlled by the decision makers by changing the initial shape of the value function.

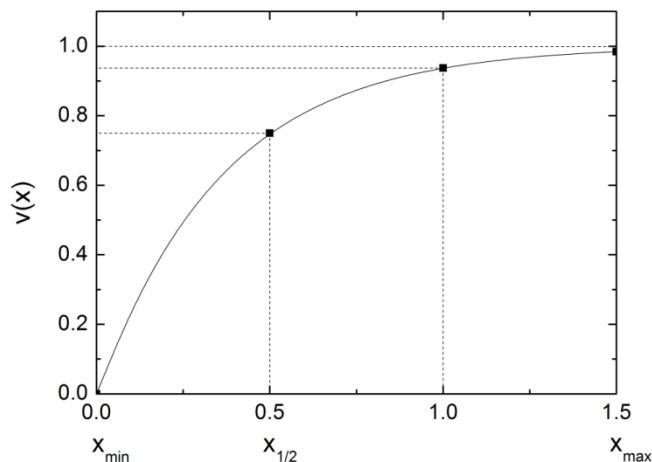


Fig. 11 Example of the concave value function $v(x)$ [82]

In general, a value function of different shape can be applied for each measurable attribute considered during the IRIDM process. Simple evaluation techniques can be also utilised for estimating s_{ijk} factors.

To summarize application of VTA makes the IRIDM process well-structured and easier to implement because of clear definitions of considered attributes, their safety margins and the goals to be achieved.

Comment : practical experience of application of such IRIDM methodology could be discussed here (examples are welcome).

8.2.2 SOME INSIGHTS FROM NASA'S RIDM HANDBOOK

The Risk Informed Decision Making Handbook by NASA [86] is focused on the design process relevant to NASA's missions (i.e. often spacecrafts) and the link to NASA's Continuous Risk Management (CRM) process. With regard to RIDM concepts, it contains some relevant insights that can and should be transferred to RIDM for NPP.

First of all, NASA's RIDM Handbook [86] clearly describes role and responsibilities in the RIDM process (during design), cf. Fig. 12. Importantly, risk analysts are responsible for providing the analysis of risks identified and comprehensively documenting that analysis. Risk analysts will need to rely on subject matter analysts for constructing and quantifying risk models. However, objectives will be set externally from all stakeholders (both internal as project manager and also relevant decision makers as well as external as e.g. Congress). A decision makers will select an alternative for implementation (as the design) based on the results of a deliberation process, his decision preferences and valuations, and in coordination with (external) safety authorities.

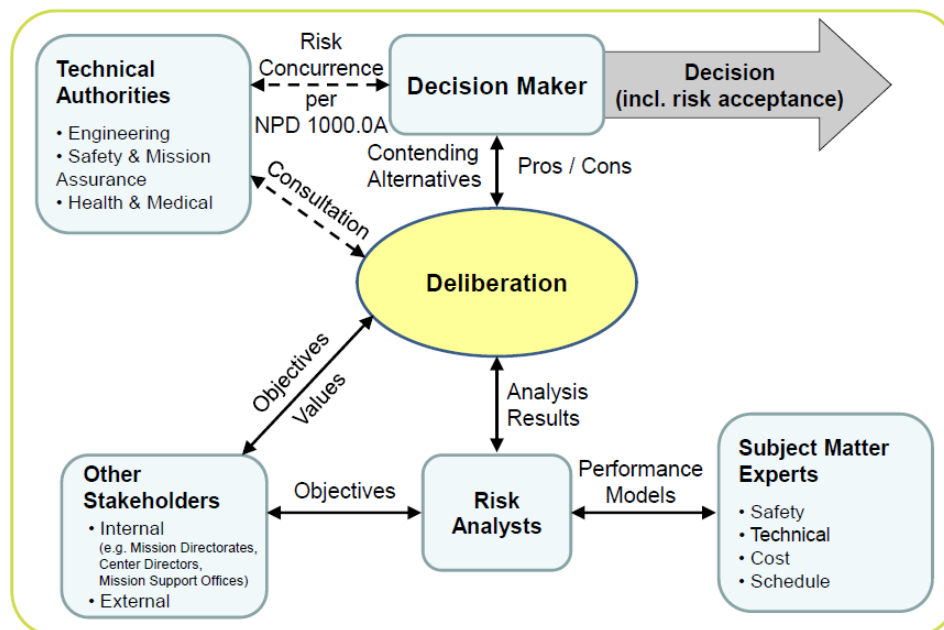


Fig. 12 Roles in RIDM [86], p. 8

For the design, NASA's RIDM Handbook [86] specifically mentions that a hierarchy of (design) objectives should be developed, cf. Fig. 13. Each of the objectives and sub-objectives then needs to be linked to performance measures

and performance objectives (including acceptance criteria on performance measures), cf. Fig. 14. It should be noted that this step represents the decision making aspects illustrated in Fig. 8 and Fig. 10. Moreover, the objectives tree with associated performance measures and acceptance criteria is conceptually related to the “objective provision tree” discussed in the supplemental publication for D30.4 [76] for assessing DiD.

With regard to performance measures, these include risk measures as discussed e.g. in the risk metrics report D30.5 [5], e.g. if the risk of “loss of mission” is investigated. Performance measures for NASA, however, are a broader concept and include also performance characteristics of (main) components like e.g. the operational thrust of a rocket engine or the assured mission time of an emergency oxygen supply system. Conceptually, if all components perform as designed and meet all performance objectives, the requested outcome for the mission will be achieved. Therefore, if a design solution can meet required performance objectives, mission designers as well as component designers have to commit to achieve performance measure with a sufficient degree of certainty. These threshold values, meeting performance objective, then become performance commitments. Obviously, there will be differences between design solutions in their ability to meet or exceed performance objectives. This can then drive the risk-informed design optimisation, which is out of scope for this discussion.

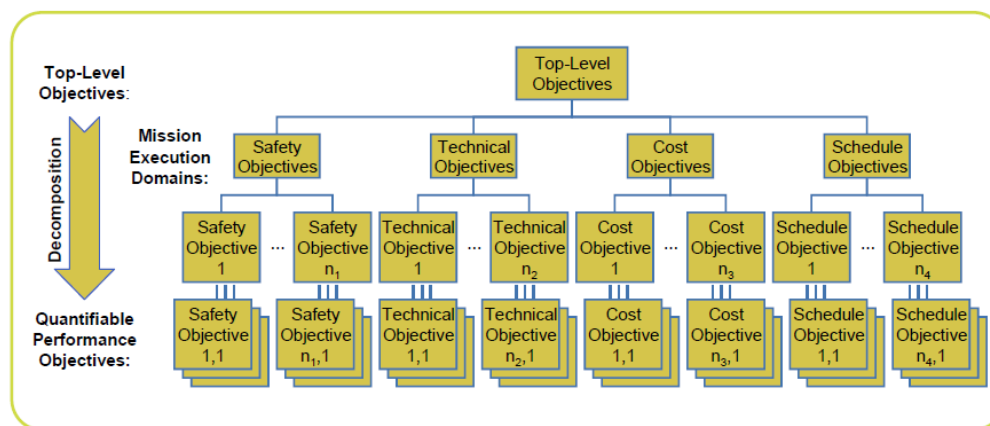


Fig. 13 Hierarchy of Objectives in the Design Process [86], p. 34

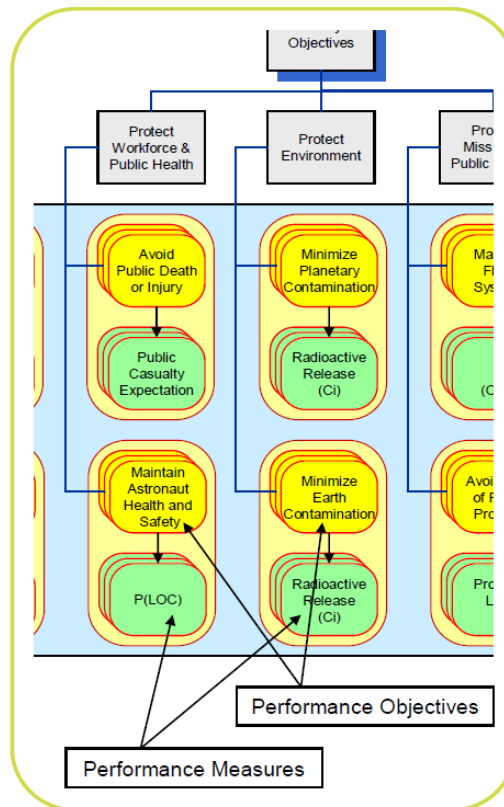


Fig. 14 Performance objectives and performance measures [86], p. 40

Importantly, each performance commitment corresponds to an accepted level of risk (cf. Fig. 15), as a component or sub-component not meeting its specified performance will impact (and should increase) the risk of not meeting essential mission objectives, including the risk of “loss of mission” or “loss of life”. These risk measures broadly correspond to core damage or large release (frequency) risk measures for NPP. Depending on the criticality of the component not meeting its required performance, there will be different degrees of relevance for overall outcomes (denoted here as high, moderate to low). When determining performance commitments (i.e. acceptance criteria), this criticality needs to be recognized and factored into the safety margins for setting these thresholds. Indeed, NASA’s RIDM Handbook recommends to use a risk normalization procedure [86] in order to establish performance commitments consistent with their relevance to risk. Moreover, the Handbook specifically points out that the risk tolerance of decision makers and participants in the deliberation process needs to be reflected in risk tolerances and consequentially in safety margins for the different performance measures.

With a view to the current state of the art of PSA models for NPP, it has to be recognized that this complex relationship between the risk of not meeting performance criteria and the resultant impact on a risk measure like core damage is commonly treated in a bounding and conservative manner: The component or redundant train is assumed to be failed “entirely”. There often is at least a distinction between different failure modes, as relevant, e.g. “failure to start” or “failure to operate” on the component level. The uncertainty distributions assigned to the relevant reliability parameters (e.g. failure rate distribution) and the resultant uncertainty distributions on component reliability conceptually correspond to performance measure distributions as depicted below. However,

as there are no formal reliability requirements for specific safety systems (e.g. the ECCS), corresponding performance commitments are often not defined for NPP¹⁰.

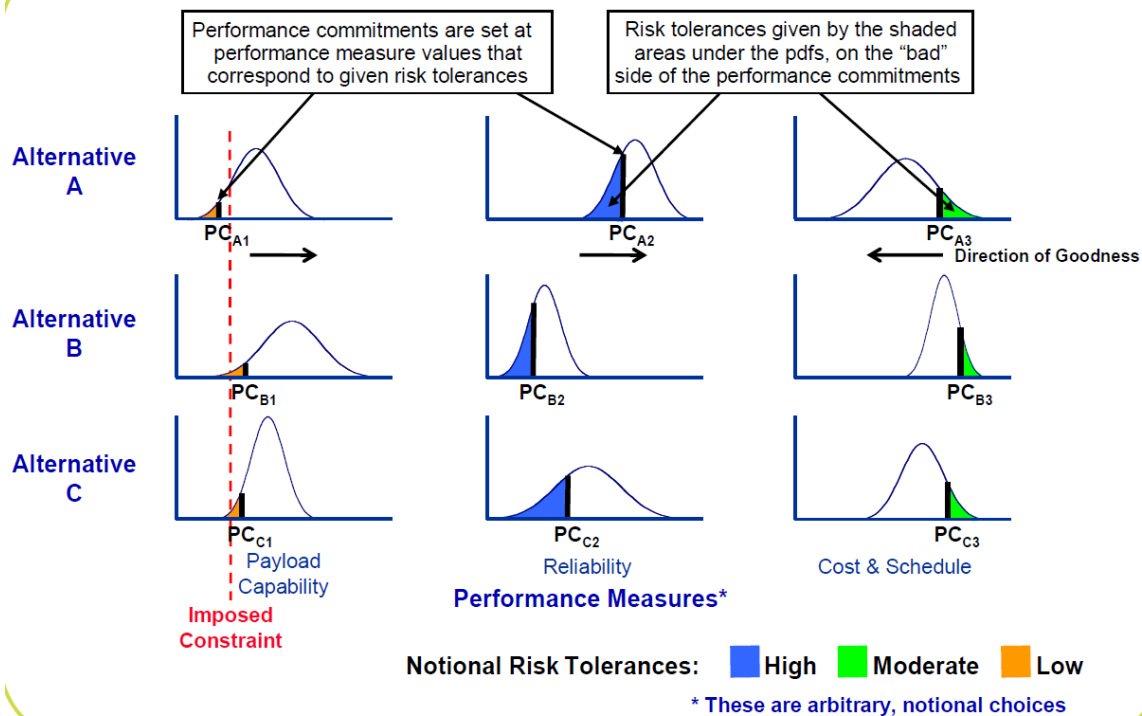


Fig. 15 Performance measures and performance commitments in RIDM [86], p. 76

An important insight from the discussion so far is the following: RIDM on a complex system like a NPP typically rests on a rather large number of aspects as e.g. indicated in Fig. 10. NASA's RIDM Handbook [86] clearly explains that all these aspects of the decision (termed performance measures and related objectives or commitments) are uncertain and contribute (to some extent) to certain aspects of the relevant risk(s). Moreover, there is - once acceptance criteria have been established - an accepted level of risk relevant to all these aspects. For RIDM on NPP, it is important to recognize that aspects of uncertainty and risk also (and systematically) apply to deterministic risk assessments, the meeting of regulatory expectations and legal requirements, radiation protection, work place safety, etc. RIDM processes for NPP should recognize these uncertain and risk relevant aspects of the decision maker's input. Their related uncertainty and their contribution to other aspects of risk (e.g. in terms of CDF) should be considered and discussed at least in a qualitative manner. In this respect, RIDM is substantially more comprehensive than simply the utilisation of PSA results to inform decisions.

NASA's RIDM Handbook also discusses how to actually achieve at a decision. NASA states: "*The RIDM process invests the decision-maker with the authority and responsibility for critical decisions. While ultimate responsibility for alternative selection rests with the decision-maker, alternative evaluation can be performed*

¹⁰ Deterministic design rules call for reliable systems, and implementation of DiD and established good design practice often achieve high reliability systems even without explicit risk targets. There are, however, some examples where the design of NPP has been influenced by meeting specific risk targets set by the designers. These have been targets on CDF but also targets on system reliability for relevant sequences.

within a number of deliberation forums that may be held before the final selection is made. As partial decisions or –down-selects may be made at any one of these deliberation forums, they are routinely structured around a team organizational structure identified by the decision-maker.” [86], p. 78. This central role of the decision maker, which ensures that authority and responsibility are clearly assigned to the same person, is an important aspect for any RIDM approach.

NASA’s RIDM Handbook [86] continues with a procedural discussion of how a decision may be reached in a deliberative (and iterative) process. Some important aspects driving decisions are mentioned. These include e.g. inferior performance in key areas, risk of exceptionally high or poor performance, and sensitivity to risk tolerance. However, Ref. [86] also specifically mentions subjective judgements and backgrounds of decision makers. Moreover, Ref. [86] states that risk analysts have to clearly present their risk assessment results. In light of the central position of the decision maker, his input e.g. via the deliberation process but also in earlier phases, is important to the analysis and the results presentation. Ref. [86] briefly discussed different means and tools of presenting risk information, which have been successfully applied previously. However, NASA’s RIDM Handbook does not recommend specific presentation tools over others or recommends relative weightings for risk aggregation. From the context it is obvious that this lies in the authority of decision makers.

One final important insight is related to the transition from RIDM to CRM. NASA’s RIDM Handbook [86] explains that, conceptually, after selection of a decision alternative, performance commitments and their associated risk levels become reliability and risk targets for RCM. Conversely, insights from the continuous risk management of existing projects will be fed back into the RIDM process. Most evidently, this is the case if an additional RIDM process for the same project is initiated, e.g. for a backfitting measure or a re-evaluation (re-baselining). But previous experiences from CRM also feed back into RIDM projects for new projects. It has to be recognized that the influence of previous experiences by decision makers on their decisions should not be underestimated. The relationship is summarized in Fig. 16.

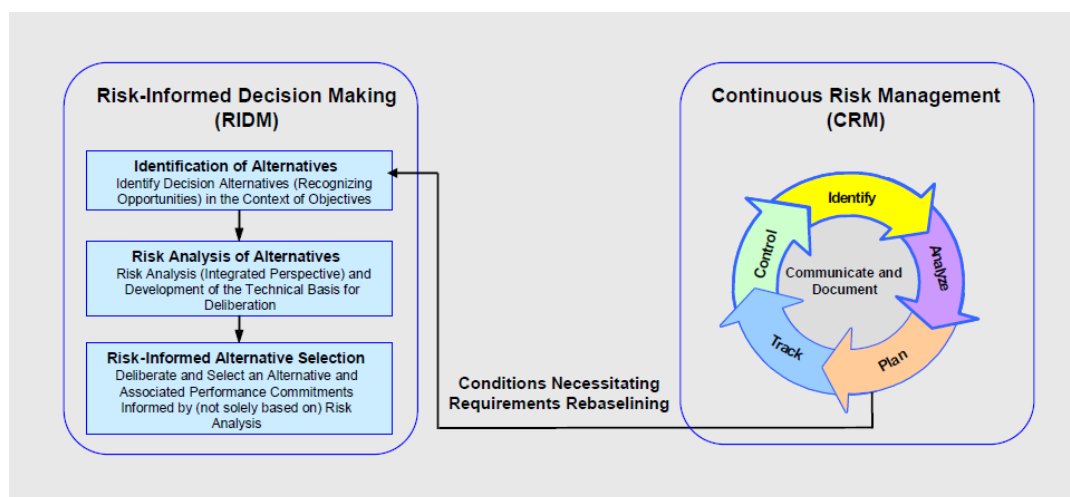


Fig. 16 Relationship of RIDM and CRM, [86], p. 25

8.3 ADDITIONAL REMARKS ON RIDM APPROACHES

In the following, several specific issues related to risk informed decision making for NPP are discussed. Most of these remarks apply to all RIDM using PSA and are thus general. To the extent applicable, there will be comments on those aspects specific to the use of extended PSA.

For PSA practitioners, aggregating risk is an evident concept. Basically, computing e.g. FDF or LRF results for a NPP amounts to aggregating the risk over all sequences ending in fuel damage or large release, respectively. The basic assumption is that - using Boolean algebra as needed - frequency values or minimum cut sets can be simply “summed up”. While mathematically well defined, this rests on an important assumption: that all the risks thus “summed up” have the same detriment to the decision maker. Recurring to section 8.2.1 above, the same value function $v(x)$ (cf. Fig. 11) needs to be applicable to all sequences. (In decision making theories, this value function is also called utility function.) In practice, PSA analysts often do not consider the value function and simply assume it as unity.

However, when aggregating risk for different outcomes, value functions will become relevant. It is important to notice that for PSA of NPP, sequences ending in e.g. fuel damage do represent widely different outcomes e.g. with respect to off-site consequence. Similarly, it is by no means self-evident that the risk of a major accident due to a human error, due to a technical failure of the plant, and due to extreme external hazard impact should be judged with the same disutility - for installations other than NPP materialization of the first is often sanctioned by authorities whereas materialization of the latter is judged to be part of the accepted risk, even if consequences are the same. It is important to be aware that the choice of value functions for aggregating risks influences the eventual decision between different alternatives at least as much as the actual results of a PSA investigation. Given the importance of choosing value functions for risk aggregation and decision making, some additional remarks and words of caution are in order.

1) The choice of value function entails subjective preferences

Risk-informed decision making for NPP should extend (principally) to a number of aspects, including PSA results (cf. e.g. Fig. 8, Fig. 10). However, there is no “objective” or commonly acceptable way of identifying and justifying decision criteria and the different weightings of decision aspects (i.e. value functions). Personal convictions of the decision maker, including ethical considerations and societal influences, but also personal understanding and acceptance of (specific) risks as well as previous experiences related to risk aspects will play an important role (cf. also Fig. 9).

As RIDM aims at providing a structured and traceable process, factors influencing the choice of value functions should be made explicit to the extent practicable. To this end, a deliberative process as described by NASA (cf. section 8.2.2) will be helpful.

This observation is also the basis for the following comment.

2) The decision maker is responsible for selecting value functions.

As the RIDM process aims at integrating information from several disparate areas (in principle), it should be oriented towards working in a team. At the end, however, there needs to be a decision for a specific alternative. Good practice in business organization calls for the congruence of authority to make and accountability for the decision. In addition, responsibility for the decision needs to be clearly assigned. In practice, there will often be one individual in an organization (typically with managerial responsibilities) that

actually takes and shall be accountable for a decision.

The decision makers (or a panel with that authority) need to be responsible for specifying their acceptance criteria (below those mandated by law or regulation), their risk acceptance levels, and ultimately their value functions.

Subject matter analysts, as e.g. PSA experts, should be aware of this responsibility. They should therefore seek guidance from responsible decision makers on their preferences on PSA related information, including relevant risk metrics, risk aggregation approaches and presentation of results and their uncertainty. During deliberation, PSA analysts should forward their understanding of the relative importance of risk aspects (i.e. value functions and risk aggregation) and ask for guidance by decision makers.

3) Different stakeholders will have different objectives and will thus advocate different value functions.

Obviously, objectives of stakeholders will influence their preferred choice for “value functions”. Examples would be that plant managers will tend to focus on plant availability vs. cost considerations as these are relevant for their daily business. For people living in the vicinity of the plant, operational as well as accidental releases or the impact from overland grid lines might be more relevant than cost considerations. And to persons far away from a NPP, accidental level releases might be the focus of concern.

Based on these remarks, specific advice on how to assign value functions to aggregate risks from different risk determined in a PSA is hard to give. Moreover, specific advice on how decision makers should weigh PSA inputs compared to other aspects of a decision is quite impossible for the authors of the present document. Therefore, this report will refrain from doing so.

A further important remarks pertains to the actual decision making process. Usually, decision makers will only develop a formal weighting of different aspects of a decision and assign specific value function (cf. section 8.2.1) if they feel that this provides additional value. If a decision can be arrived at with less onerous methods at a comparable level of (subjective) certainty, such approaches will be preferred.

The important aspect for a successful RIDM process is that these choices of decision makers are made explicit and can be traced to the eventual decision. To this end, a documented deliberation process is recommended.

In the following, some additional remarks related to decision making and the use of (extended) PSA are made.

1. The role of uncertainty

Detailed PSA results are usually uncertainty distributions for a specific risk measure like e.g. RMF. Often, the range of uncertainty, e.g. the range between the 5% percentile and the 95% percentile exceeds one order of magnitude. For an extended PSA, which also considers effects of extreme external hazard impacts, including combinations of hazards, the uncertainty ranges associated with these results might be even broader than two or three orders of magnitude.

Simultaneously, in most cases only mean values (or other point values) are reported as main inputs from decision making.

Obviously, if a (strongly) non-linear value function (cf. e.g. Fig. 11) is applied to a certain risk metric, than the result will be (very) sensitive to the choice if it is applied to a mean value or to the full

uncertainty distribution. Therefore, risk analysts should take care when aggregating risks that come with widely disparate uncertainty distributions. It is recommended to seek guidance from decision makers on the appropriate procedure. Moreover, PSA analysts and decision makers should be aware of this potential issue when using aggregated risk measure like e.g. the integral risk measure for L2 PSA discussed in section 4.2.

Furthermore, current research into decision making under uncertainty emphasizes the relevance of uncertainty for decision making, cf. e.g. [27]. Importantly, decision makers should include information on associated uncertainty into their considerations and weighting in order to arrive at decisions that are stable against variations of parameters within the respective uncertainty ranges.

An obvious advantage of PSA is that there is an inherent mechanism for determining and reporting uncertainty information. It should be recognized that all other decision aspects are similarly uncertain (cf. e.g. section 8.2.2).

2. One recommendation after the Fukushima-Daiichi accident was that special attention should be paid to low probability, high impact scenarios (cf. e.g. section 2 and D30.2 [2]). This includes e.g. retaining such scenarios during screening of a PSA for further more detailed investigations. However, there is also an aspect related to decision making. The implicit assumption often associated with that recommendation is that proper consideration of the potential high consequences of such a low probability event would lead to a mitigation of risks. And it is further assumed that such consideration would also extend to available safety margin and potential cliff-edge effects. Moreover, sometimes the “precautionary principle” is invoked to justify mitigation measures for such scenarios, particularly if there is a large degree of uncertainty.¹¹

Referring to the discussion above, the consideration of such low probability/high impact scenarios in decision making depends on the choice of value functions by the decision maker. Moreover, it will depend on the decision maker’s preferences for treating uncertainty in decision making. Therefore, PSA analysts should seek guidance on how this aspect of the risk should be captured in risk measures and presented for decision making.

3. Risk aggregation for extended PSA

An extended PSA aims at determining risk for all relevant sources on the plant. Conceptually, this also includes sources like e.g. radwaste treatment facilities (cf. also [87]). The RMF metric has been proposed to provide a metric to capture accidental level releases from such sources in addition to the reactor core and the SFP. However, for these non-reactor sources the maximum accidental level of release as well as the mobility of potential releases will differ from e.g. severe core melt accident releases. PSA analysts should be aware of this when aggregating risks in order to not mask the risk profile of the plant. PSA analysts should therefore seek guidance from decision makers on their preferences on risk aggregation and the set of relevant risk measures on this aspect.

¹¹ It should be recognized that the precautionary principle is strongly criticized by some experts while it is emphatically advocated by others.

8.4 AS LOW AS REASONABLY ACHIEVABLE AND EXTENDED PSA RESULTS

One widely accepted concept in the field of nuclear safety is to reduce risks as low as reasonably achievable (ALARA), cf. Principle 5 of SF-1 [9]. There are some (country-specific) versions of this approach, e.g. to reduce risks as low as reasonably practicable (ALARP) [18] based on the wording of applicable legislation in the UK. The overall requirement to optimize the level of protection is applicable for all phases of a NPP life cycle and all relevant risk, i.e. nuclear (reactor) safety as well as radiation protection. Specific investigations whether the safety architecture achieves ALARA are often associated with licensing of the plant, periodic safety reviews or license renewal, and potentially major safety improvement campaigns.

A decision whether the risk is as low as reasonably achievable will often require that several options in addition to the reference design or reference procedure are identified and assessed (cf. e.g. [7]). That identification process might be driven by the evaluation of relevant good practice realized for other plants or in mature designs; lessons learned from operating experience should be taken into account as well. The further assessment then should determine the benefits and detriment of the different options (cf. e.g. [7], [90]). Thus, the demonstration of ALARA often amounts to performing a RIDM process (see the sections above). It is important to acknowledge that acceptance criteria (or rather decision criteria) are different between countries and usually influenced by the relevant original legislation, legal and regulatory precedent, and also more general societal positions on risk acceptance and regulatory burden.¹²

Availability of an extended PSA, as described by the ASAMPSA_E project, can provide additional benefits to ALARA investigations compared to less comprehensive PSA models. Specifically, the extended scope of PSA allows for using PSA results from well-developed models for questions related e.g. to sources other than the reactor core, to interactions between the site and its environment, or related to multi-unit considerations. In addition, the extended scope of the PSA models will allow for a better understanding of the risk profile of the plant and site, thus bringing additional value to ALARA investigations. While the ASAMPSA_E project was focused on PSA up to Level 2(+) and accidental level releases, the concept of extended PSA can also be applied to PSA Level 3 and to the inclusion of a determination of on-site doses to workers for all types of events. In this way, PSA information can serve as one important input for a wide range of ALARA considerations (cf. e.g. [18], [87], [91]).

In summary, the use of an extended PSA in ALARA investigations using a RIDM framework is strongly recommended by the ASAMPSA_E project. However, no specific guidance is given on related decision making criteria.

¹² The question if value for money is demonstrated by multiplying the value at risk with frequencies from PSA and checking if that exceeds the costs, or if gross disproportionality between costs and benefits is the guiding principle, or if the relevant, proven state of technology with relevant safety benefits form the basis of the decision will not influence the generic process and the assessment process very much, however it will play a major role in the actual decision.

9 SUMMARY

9.1 INTRODUCTION

The ASAMPSA_E project has investigated the concept of extended PSA (cf. [1]) and its implications for PSA modelling and PSA methods. Within WP 30, several specific issues were discussed in more detail and dedicated reports were published. In report D30.2 [2] the authors have looked at available information about the accident at the Fukushima Daiichi power plant from the point of view of PSA and at recent PSA models for NPP in general. Report D30.3 [3] investigated the approach for identifying initiating events and hazard scenarios for an extended PSA. The authors have derived recommendations for a comprehensive screening methodology. The subject of report D30.4 [4] was the link between assessments of the appropriate realization of the defence-in-depth (DiD) concept and extended PSA. The authors have described which PSA insights can be used for DiD assessments and provide recommendation for appropriate risk measures and on structuring of PSA models to support DiD assessments. Report D30.5 [5] has investigated risk measures for an extended PSA for L1 and L2 PSA. The authors discuss the validity of commonly used risk metrics with regard to certain aspects of risk and provide recommendations on the use of risk measures for screening, for the development of PSA models, and for supporting decision making.

This present report D30.6 has two main objectives. Firstly, this report aims at integrating the recommendations derived in the aforementioned reports under explicit consideration of insights in other activities of the ASAMPSA_E project and by reflecting PSA end user's needs as documented in the respective ASAMPSA_E survey [6]. To this end, this report includes sections on the recommendations from topical reports D30.3 to D30.5 [3], [4], [5]. These recommendations are then refined based on overall insights of the ASAMPSA_E project, on feedback from PSA end-users and other stakeholders, and on the discussion in this report.

Secondly, this report discusses the use of insights from extended PSA for risk-informed decision making (RIDM). This is an extension of previous activities. To this end, this report briefly presents the general framework for RIDM as it is currently understood and discusses upcoming enhancements and developments for RIDM approaches.

9.2 IDENTIFYING INITIATING EVENTS AND HAZARDS

The ASAMPSA_E report D30.3 [2] includes the following recommendations on screening criteria.

"[S]creening criteria should be commensurate to overall PSA results and ensure that low probability/high impact events are not screened out. To that effect, a set of suitable risk metrics and threshold values (including CDF and LRF) should be defined."

"The screening of initiating events for detailed consideration in the PSA should be performed not only based on L1 PSA risk metrics but also on L2 PSA risk metrics like e.g. different release categories, including at least one risk metric for large releases and one for early releases. Screening thresholds on the risk measures for the Level 2 risk metrics should be defined and justified. Initiating events (including hazard scenarios) should only be screened out from the PSA, if they are screened out based both on Level 1 and on Level 2 risk metrics. In addition, if a PSA Level 3 is intended, the screening process should include Level 3 risk metrics and thresholds as well."

In addition, any screening procedure should be consistent with the respective goals set out by WENRA, which state for new reactor designs that *“accidents with core melt which would lead to early or large releases have to be practically eliminated”* [74], p. 24, and for existing reactors that *“any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable”* [78], p. 23.

The following refined methodology for initiating events identification, screening and bounding analysis for an extended PSA consists of four major steps and is further developed in section 4:

1. comprehensive identification of events and hazards and their respective combinations applicable to the plant and site,
2. initial frequency claims for events and hazards and their respective combinations applicable to the plant and the site,
3. impact analysis and bounding assessment for all applicable events and scenarios; events are either screened out from further more detailed analysis, or are assigned to a bounding event (group), or are retained for detailed analysis,
4. probabilistic analysis of all retained (bounding) events at the appropriate level of detail.

Numerical probabilistic safety targets are applied differently depending on countries. Interpretation of quantitative screening criteria may also differ from one country to the other. Nevertheless an approach for defining quantitative screening criteria (from [3]) for the selection of PSA initiating events is proposed in section 4.

Plant response analysis is an essential task for the screening of initiating events and hazard scenarios as well as the subsequent development of probabilistic model, both in bounding analysis and in more detailed probabilistic modelling. The overall objectives of plant response analysis are to identify if the safety of the plant (i.e. safety of the fuel or of other sources) is challenged by the event or scenario under investigation, which fundamental safety functions are challenged either directly or by consequential effects, and if provisions for safety functions (SSC, barriers, other features) are effective or not. For hazards scenarios, hazard impact analysis describes the specific aspect of plant response after hazard effects within the plant.

In general, the following two criteria are applied for screening by impact analysis:

1. severity: the effects of the event are not severe enough to cause damage to the plant, since it has been designed for loads with similar or higher strength due to other event scenarios,
2. predictability: the event is very slow in developing, and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate and timely response without notably jeopardizing safety.

Bounding analysis should allow for demonstrating that certain events are extremely unlikely to develop into a large release or an early release scenario. This provides valuable justification to decision makers and stakeholders that low probability/high consequence events have been comprehensively identified so traceability is crucial.

9.3 RECOMMENDATIONS ON RISK MEASURES AND SAFETY OBJECTIVES FOR AN EXTENDED PSA

The definition or acceptance of safety objectives is in the responsibility of authorities which are in charge of public safety and the safe operation of NPPs is the responsibility of the utilities. The report discusses this safety objectives topic but the proposed considerations shall not interfere with these responsibilities.

Within ASAMPSA_E a deliverable on risk metrics has been developed [5]. On this basis, in section 4 risk measures are recommended for L1 and L2 PSA each, and quantitative safety objectives are provided in section 7.

For L1 PSA, the fuel damage frequency is considered a useful measure. It contains the well-known core damage frequency, but in addition reflects all other potential locations in a site where fuel damage could occur. Furthermore, the radionuclide mobilization frequency is suggested, taking into account also radioactive material (e.g. filter contents) in order to capture all potential sources completely.

Few comments are made with a perspective of safety objectives harmonization. The quantitative objective for FDF should, of course, be consistent with the established CDF figures. Therefore, as a first step of introducing FDF, the existing CDF objectives should be directly applied to FDF. This is more than just a formal step, since it means taking into account the spent fuel on the site in addition to the core.

As a second step, in a perspective of harmonization, it is recommended that the organizations involved agree on a common definition of fuel damage. From a technical point of view it is meaningful to establish a link to the damage of fuel cladding. Fuel cladding damage could either be defined as cladding rupture, releasing part of the contained activity; or it could be defined as a deformation (ballooning) which would obstruct cooling channels.

In a third step, attempts should be made to arrive at a common safety objective for FDF: from Table 2, it seems that 1 E-5/year (for all initiating events) could be an order of magnitude of such common safety objective. **But the main point is that such common safety objective for FDF should cover each and every initiating event (internal and external), and all sources of fuel (in particular core and SFP) and all units of a site.** Therefore, even if the figure itself may be not much more stringent than existing values, the inclusion of all relevant aspects means a significant challenge for PSA analysis and plant design.

Because the main risk measures for L1 PSA like e.g. core damage frequency or fuel damage frequency are not well suited for describing several scenarios which might lead to a significant release of radionuclides, a new metric, “Radionuclide Mobilization Frequency, RMF” (see section 2.17 in [5]), addresses these issues. This risk metric is defined as an unintended mobilization of a significant amount of radionuclides with the potential for internal or external release.

For L2 PSA there is already a widespread good practice to identify the frequency of the loss of containment functions. The application of this measure is further encouraged, with the following remark:

It is recommended to at least distinguish:

- intact containment with design basis leakage,
- intact containment with filtered venting,
- loss of containment function due to a leak or rupture of the containment structure (after a short term (e.g. energetic) phenomena or a slow phenomena (e.g. basemat penetration by the corium),

- loss of containment function due to failure of containment isolation systems (e.g. open ventilation systems, open hatches),
- loss of containment function due to bypass through interfacing systems (for BWR including non-isolated break of feedwater or steam lines outside of the containment),
- loss of containment function due to bypass through steam generator tube leak (PWR only).

For existing plants the conditional probability for the loss of containment function under the condition of fuel damage (from all potential sources, including the containment of the SFP) should not exceed 10%. Future plants will have to demonstrate better management of fuel damage. It is justified to recommend a better containment performance as follows: For new plants the conditional probability for the loss of containment function under the condition of fuel damage (from all potential sources, including the SFP) must not exceed 1%. (Successful filtered containment venting with intact containment is not considered as loss of containment function).

For such an application of L2 PSA, appropriate success criteria for SAM strategies can be derived: for example, for successful filtered containment venting with intact containment, or for the use of mobile equipment for the NPP long term management (if procedures exist and are routinely tested). This will highlight solutions to manage accidents where equipment needed for both accident prevention and mitigation are not available (due to long term station blackout for example). Indirectly, such application of L2 PSA will facilitate to examine quantitatively the independence between accident prevention provisions and accident mitigation provisions.

Depending on judgments involving also non-scientific considerations, the “total risk” of any installation can be defined in very different ways, e.g. in loss of value (of the plant and for the environment), or in health effects. The present document is about L2 PSA, and therefore a “total risk” is proposed here in section 6.2 related to L2 PSA issues. It should be considered as an overall complement to the many other risk measures under consideration. This total risk can be calculated by integrating the risk due to all event sequences into a single metric by summing up all activity releases multiplied by their respective frequencies. An attractive feature which comes with a single value for the total risk is the possibility to compare it to a risk target. Without such a single value, having just a set of several different L2 PSA result characteristics, it is difficult to define a consistent set of various targets for the different result characteristics. Unfortunately, the PSA community is far from having consensus on what might be the proper harmonized total risk measure. It is recommended that pertinent groups precisely define the appropriate metrics (e.g. the isotopes to be considered, or the introduction of a parameter representing health effects for the individual isotopes). A suggestion for such a common risk target is provided in section 7.3. The derivation of this objective is given in detail in [49] and will not be repeated here.

9.4 THE LINK BETWEEN DEFENCE-IN-DEPTH AND EXTENDED PSA

Keeping in mind the complementary objectives of DiD and PSA, it is recommended that DiD and PSA be developed independently of each other. If a NPP could demonstrate that it follows all applicable DiD rules, and if an independent PSA confirms a low risk of this plant, there would be a well-founded confidence in an adequate level of safety for this plant. If, on the other hand, PSA identifies a high or unbalanced risk profile for the plant, there

are doubts as to whether the current application of the DiD concept is sufficient and additional safety provisions are expected. This impact of PSA is now included in the DiD concept, as a complement for the design.

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

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

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

- discussion and recommendations in [4] are largely at a conceptual level; this is partly due to the lack of previous investigations into the subject and partly due to a lack of practical implementations and feedback on good practices in the PSA community; therefore, specific guidance on how to do practical modelling of PSA with a view to do DiD assessments could be subject to subsequent work;
- PSA models often have been produced without the specific objective of assessing the implementation of DiD by DiD levels; therefore, existing PSA models would have to be modified to comply with the recommendations of this report.

In order to define a way to go beyond the above considerations and overcome the highlighted limits, further investigations have been developed during the project about the specific roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations. An additional report [76] describes the proposed process and tools (see section 5.1.3).

9.5 IMPROVING DECISION MAKING USING EXTENDED PSA RESULTS

The common expression “risk informed decision making” captures very well that decision making will have to consider many issues, PSA being just one of them. Decisions are influenced by factors that transcend natural science. Consequently, implicit and explicit utility considerations on decision alternatives will necessarily have a

strong subjective component. Furthermore, the relevance of information, e.g. from PSA, the acceptability of certain kinds of risks, and finally the adequacy of risk measures to support decisions will depend on the decision maker. In the end, the decision maker has to decide which aspects of risk and thus which risk measures are relevant for each alternative.

Basically, the decision maker is faced with the question of how to combine different values into a single decision. Section 8.2 provides suggestions how to do this in a logical and comprehensible way. Specific advice on how to assign value functions to aggregate risks from different sources determined in a PSA is hard to give. Moreover, specific advice on how decision makers should weigh PSA inputs compared to other aspects of a decision is quite impossible for the authors of the present document. Therefore, this report will refrain from doing so.

From the PSA point of view, it is adequate to mention that PSA methods are flexible enough to provide the decision maker with almost all technical values which he might ask for. This covers information about the plant (e.g. frequency of various plant damage states), environmental data (e.g. frequency of different source terms) and health effects (e.g. frequency of radiation exposure to the public). It is nevertheless prudent that decision makers are aware of the strengths and weaknesses of PSA and seek support of PSA experts, especially to discuss whether the PSA status is consistent with its application to support decision-making.

10 LIST OF REFERENCES

- [1] “Advanced Safety Assessment : Extended PSA”, ASAMPSA_E Description of Work, 2013, Grant agreement 605001
- [2] ASAMPSA_E, “Lessons of the Fukushima Dai-ichi accident for PSA”, ASAMPSA_E D30.2. January 2015, Technical report ASAMPSA_E/WP30/D30.2/2015-08, Reference IRSN PSN-RES/SAG/2015-00025
- [3] ASAMPSA_E, “Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA”, ASAMPSA_E D30.3, Technical report ASAMPSA_E/WP30/D30.3/2016-13
- [4] ASAMPSA_E, “The Link between the Defence-in-Depth Concept and Extended PSA”, ASAMPSA_E D30.4, Technical report ASAMPSA_E/WP30/D30.4/2016-26-Reference IRSN PSN/RES/SAG/2016-209
- [5] ASAMPSA_E, “Risk Metrics and Measures for an Extended PSA”, Technical report ASAMPSA_E/WP30/D30.5/2016-17 Reference IRSN PSN/RES/SAG/2016-00171
- [6] ASAMPSA_E, “Synthesis of the initial survey related to PSAs End-Users needs”, ASAMPSA_E D10.2, January 2015, Technical report ASAMPSA_E/WP10/D10.2/2014-05, Reference IRSN PSN-RES/SAG/2014-00193
- [7] ASAMPSA2, Best-Practices Guidelines for L2PSA Development and Applications, Volume 1 - General, Technical report ASAMPSA2/WP2-3-4/D3.3/2013-35, IRSN-PSN/RES/SAG 2013-0177, dated 2013-04-30.
- [8] ASAMPSA2, Best-Practices Guidelines for L2PSA Development and Applications, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs, Extension to Gen III reactors, Technical report ASAMPSA2/ WP2-3-4/D3.3/2013-35, IRSN-PSN/RES/SAG 2013-0177, dated 2013-04-30.
- [9] International Atomic Energy Agency (IAEA), “Fundamental Safety Principles”, Safety Fundamentals No. SF-1, November 2006
- [10] International Atomic Energy Agency (IAEA), “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-3, April 2010
- [11] International Atomic Energy Agency (IAEA), “Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-4, May 2010
- [12] International Atomic Energy Agency (IAEA), “A Framework for an Integrated Risk Informed Decision Making Process” , report by the International Nuclear Safety Group, INSAG-25, May 2011
- [13] International Atomic Energy Agency (IAEA), “Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status”, IAEA-TECDOC-1436, February 2005
- [14] U.S. Nuclear Regulatory Commission, “A Proposed Risk Management Regulatory Framework”, NUREG-2150, April 2012
- [15] U.S. Nuclear Regulatory Commission, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-informed Decisionmaking”, draft report for comment, NUREG-1855, Rev. 1, March 2013
- [16] Himanen, R. et al., “Risk-informed Regulation and Safety Management of Nuclear Power Plants - on the Prevention of Severe Accidents”, Risk Analysis, Vol. 32, No. 11, 2012, p. 1978 - 1993
- [17] Kadak, A.C., T. Matsuo, “The Nuclear Industry’s Transition to Risk-informed Regulation and Operation in the United States”, Reliability Engineering and System Safety, Vol. 92, (2007), p. 609-618
- [18] Health and Safety Executive (HSE), “Reducing Risks, Protecting People, HSE’s Decision-Making Process”, HSEBooks, 2001

- [19] OECD Nuclear Energy Agency, “Probabilistic Risk Criteria and Safety Goals”, NEA/CSNI/R(2009)16, December 2009
- [20] Abrahamsen, E.B., T. Aven, “On the Consistency of Risk Acceptance Criteria with Normative Theories for Decision-making”, Reliability Engineering and System Safety, Vol. 93, (2008), p. 1906-1910
- [21] Apostolakis, G., “Safety Goals and Risk-Informed Regulation at the U.S. NRC”, Presentation to Canadian Nuclear Safety Commission, Ottawa, Canada, January 2014
- [22] Autoridad Reguladora Nuclear, “Criterios Radiológicos Relativos a Accidentes en Reactores Nucleares de Potencia”, Revisión 2, AR 3.1.3, 2002
- [23] Aven, T., “On the Ethical Justification for the Use of Risk Acceptance Criteria”, Risk Analysis, Vol. 27, Issue 2, (2007), p. 303-312
- [24] Aven, T., B. Heide, “Reliability and Validity of Risk Analysis”, Reliability Engineering and System Safety, Vol. 94, (2009), p. 1862-1868
- [25] Aven, T., “On How to Define, Understand and Describe Risk”, Reliability Engineering and System Safety, Vol. 95, Issue 6 (2010), p. 623-631
- [26] Aven, T., “The Risk Concept - Historical and Recent Development Trends”, Reliability Engineering and System Safety, Vol. 99, (2012), p. 33-44
- [27] Aven, T., “Foundational Issues in Risk Assessment and Risk Management”, Risk Analysis Vol. 32, Number 10, 2012, p. 1647 - 1656
- [28] Aven, T. B.S. Krohn, “A New Perspective on How to Understand, Assess and Manage Risk and the Unforeseen”, Reliability Engineering and System Safety, Vol. 121, (2014), p. 1-10
- [29] Ball, D.J., J. Watt, “Further Thoughts on the Utility of Risk Matrices”, Risk Analysis, Vol. 33, No. 11 (2013), p. 2068 - 2078
- [30] Borgonovo, E., G.E. Apostolakis, “A New Importance Measure for Risk-informed Decision Making”, Reliability Engineering and System Safety, Vol. 72, (2001), p. 193-212
- [31] Cox, L.A., “Does Concern-Driven Risk Management Provide a Viable Alternative to QRA?”, Risk Analysis, Vol. 27, Issue 1, (2007), p. 27-43
- [32] Cox, L.A., D.A. Popken, “Some Limitations of Aggregate Exposure Metrics”, Risk Analysis, Vol. 27, Issue 2, (2007), p. 439-445
- [33] Cox, L.A., “What’s Wrong with Risk Matrices”, Risk Analysis Vol. 28 No. 2 (2008), p. 497-512
- [34] Cheok, M.C., G.W. Parry, R.R. Sherry, “Use of Importance Measures in Risk-informed Regulatory Applications”, Reliability Engineering and System Safety, Vol. 60, (1998), p. 213-226
- [35] Hirst, I.L., D.A. Carter, “A ‘Worst Case’ Methodology for Obtaining a Rough but Rapid Indication of the Societal Risk from a Major Accident Hazard Installation”, Journal of Hazardous Materials A92 (2002), p. 233-237
- [36] Holmberg, J., M. Knochenhauer, “Probabilistic Safety Goals Phase 3 - Status Report”, NKS-195, July 2009
- [37] Johansen, I.L., M. Rausand, “Risk Metrics: Interpretation and Choice”, in: IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Hong Kong, December 2012
- [38] Johansen, I.L., M. Rausand, “Foundations and Choice of Risk Metrics”, Safety Science, Vol. 62, (2014), p. 386-399

- [39] Jonkman, S.N., P.H.A.J.M. van Gelder, J.K. Vrijling, “An Overview of the Quantitative Risk Measure for Loss of Life and Economic Damage”, Journal of Hazardous Materials A99 (2003), p. 1-30
- [40] Jonkman, S.N., A. Lentz, J.K. Vrijling, “A General Approach for the Estimation of Loss of Life due to Natural and Technological Disasters”, Reliability Engineering and System Safety, Vol. 95, (2010), p. 1123-1133
- [41] Kaplan, S., B.J. Garrick, “On the Quantitative Definition of Risk”, Risk Analysis, Vol. 1 No. 1 (1981), p. 11-27
- [42] Paté-Cornell, M.E., “Uncertainties in Risk Analysis”, Reliability Engineering and System Safety, Vol. 54 Issue 2-3, December 1996, p. 95-111
- [43] Paté-Cornell, E., “On ‘Black Swans’ and ‘Perfect Storm’: Risk Analysis and Management When Statistics are Not Enough”, Risk Analysis Vol. 32, No. 11, 2012, p. 1823 - 1833
- [44] Prem, K.P., D. Ng, H.J. Pasman, M. Sawyer, Y. Guo, M.S. Mannan, “Risk Measures Constituting a Risk Metrics which Enables Improved Decision Making: Value-at-Risk”, Journal of Loss Prevention in the Process Industries, Vol. 23 (2010), p. 211-219
- [45] Sagi, G., “A new Approach to Reactor Safety Goals in the Framework of INES”, Reliability Engineering and System Safety, Vol. 80, Issue 2, (2002), p. 143 - 161
- [46] Schroer, S., M. Modarres, “An Event Classification Schema for Evaluating Site Risk in a Multi-unit Nuclear Power Plant Probabilistic Risk Assessment”, Reliability Engineering and System Safety, Vol. 117 (2013), p. 40-51
- [47] Van der Borst, M., H. Schoonakker, “An Overview of PSA Importance Measures”, Reliability Engineering and System Safety, Vol. 72 (2001), p. 241-245
- [48] Vasseur, D, M. Llory, “International Survey on PSA Figures of Merit”, Reliability Engineering and System Safety, Vol. 66, (1999), p. 261-274
- [49] Vitázkova, J., E. Cazzoli, “Common Risk Target for Severe Accidents of Nuclear Power Plants based on IAEA INES Scale”, Nuclear Engineering and Design, Vol. 262 (2013), p. 106-125
- [50] Vrijling, J.K, W. van Hengel, R.J. Houben, “A Framework for Risk Evaluation”, Journal of Hazardous Materials, Vol. 43 (1995), p. 245-261
- [51] Einarsson, S., A. Wielenberg, “Vorschlag für eine bundeseinheitliche Anwendung von IRIDM-Verfahren bei sicherheitstechnischer Entscheidungsfindung”, GRS-A-3666, Cologne, September 2012
- [52] NASA, “Risk Management Handbook”, Version 1.0, NASAA/SP-2011-3422, November 2011
- [53] Grechuk, B. M. Zabarankin, “Risk Averse Decision Making under Catastrophic Risk”, European Journal of Operational Research, Vol. 239 (2014), p. 166-176
- [54] Cha, E.J., B.R. Ellingwood, “The Role of Risk Aversion in Nuclear Plant Safety Decisions”, Structural Safety Vol. 44 (2013), p. 28-36
- [55] Ersdal, G., T. Aven, “Risk Informed Decision-making and its Ethical Basis”, Reliability Engineering and System Safety, Vol. 93, (2008), p. 197-205
- [56] Hartford, D.N.D., “Legal Framework Considerations in the Development of Risk Acceptance Criteria”, Structural Safety, Vol. 31 (2009), p. 118-123
- [57] Tversky, A., D. Kahneman, “Advances in Prospect Theory: Cumulative Representation of Uncertainty”, Journal of Risk and Uncertainty, Vol. 5 (1992), p. 297-323

- [58] Berg, M. et al., “Risikobewertung im Energiebereich”, Polyprojekt Risiko und Sicherheit Dokumente Nr. 7, Zürich, 1995
- [59] Lind, N.C. (ed.), “Technological Risk”, Proceedings of a Symposium on Risk in New Technologies 15 December 1981, University of Waterloo, Waterloo, Ontario, 1982
- [60] U.S. NRC, “White Paper on Risk-informed and Performance-based Regulation”, SECY-98-144, March 1999
- [61] Bundesministerium für Umwelt und Naturschutz (BMU), “Sicherheitsanforderungen an Kernkraftwerke” of 22 November 2012 (BANz AT 24.02.2013 B3)
- [62] International Atomic Energy Agency (IAEA), “Safety Assessment for Facilities and Activities”, General Safety Requirements Part 4, No. GSR Part 4, May 2009
- [63] ISO, “ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for Management Systems”, ISO/TC 176/SC 2/N 544R3, 2008
- [64] Wint, S.M.E., “An Overview of Risk”, RSA Risk Commission, ca. 2006
- [65] Kim, S.K., Song, O., “A MAUT Approach for Selecting a Dismantling Scenario for the Thermal Column in KKR-1”, Annals of Nuclear Energy, Vol. 36 (2009), p. 145-150
- [66] Artzner, P., J. Eber, D. Heath, “Coherent Measures of Risk”, Mathematical Finance, Vol. 9, No. 3 (1999), p. 203-228
- [67] Frittelli, M., E.R. Gianin, “Putting Order in Risk Measures”, Journal of Banking and Finance 26 (2002), p. 1473-1486
- [68] Cox, L.A., “Why Risk is Not Variance: An Expository Note”, Risk Analysis, Vol 28 (2008), p. 925-928
- [69] Wikimedia Foundation, “Risk metric” , version 7 December 2014, http://en.wikipedia.org/wiki/Risk_metric
- [70] Woody Epstein, A Probabilistic Risk Assessment Practitioner looks at the Great East Japan Earthquake and Tsunami, <http://woody.com/wp-content/uploads/2011/06/A-PRA-Practitioner-looks-at-the-Great-East-Japan-Earthquake-and-Tsunami.pdf>
- [71] IAEA, Mission Report - The Great East Japan Earthquake Expert Mission - IAEA International Fact Finding Expert Mission Of The Fukushima Dai-ichi NPP Accident Following The Great East Japan Earthquake And Tsunami, 24 May - 2 June 2011
- [72] B. Obama, “Remarks by the President in a Press Conference” from 19 December 2012, Press Office of the White House, December 2012 (published online)
- [73] European Atomic Energy Community, Food and Agriculture Organization of the United Nations, International Atomic Energy Agency, International Labour Organization, International Maritime Organization, OECD Nuclear Energy Agency, Pan American Health Organization, United Nations Environment Programme, World Health Organization, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006)
- [74] WENRA, “Safety of New NPP Designs, Study by Reactor Harmonization Working Group RHWG”, March 2013
- [75] IAEA, OECD/NEA, “INES The International Nuclear and Radiological Event Scale User’s Manual, 2008 Edition”, Vienna, amended version March 2013
- [76] Fiorini, G., S. de la Rovere, The PSA assessment of Defense in Depth Memorandum and proposal, Supporting material to ASAMPSA_E D30.4, May 2016,
- [77] INSAG, Basic Safety Principles for Nuclear Power Plants; 75-INSAG-3 Rev. 1 - INSAG-12; 1999

- [78] Western European Nuclear Regulators Association (WENRA), “WENRA Safety Reference Levels for Existing Reactors”, September 2014
- [79] The American Society of Mechanical Engineers, “Standard for probabilistic risk assessment for nuclear power plant applications”, ASME RA-S-2002, 2002 with addenda ASME RA-Sa-2003 and ASME RA-Sb-2005
- [80] Decker, K., H. Brinkmann, List of External Hazards to be Considered in Extended PSA, ASAMPSA_E D21.2, December 2014
- [81] ASAMPSA_E, “Report on external hazards with high amplitude that have affected NPP in operation (in Europe or in other countries)”, ASAMPSA_E D10.3, January 2016
- [82] M. Borysiewicz, K. Kowal, S. Potemski, An application of the value tree analysis methodology within the integrated risk informed decision making for the nuclear facilities, Reliability Engineering and System Safety 139, pp. 113-119, 2015
- [83] Mustajoki J, Hamalainen RP. Web-HIPRE: Global decision support by value tree and AHP analysis. INFOR 2000;38(3):208-220.
- [84] Berg HP. Quantitative safety goals and criteria as a basis for decision making. Reliability: Theory & Applications 2010;17(2):62-78.
- [85] International Atomic Energy Agency. Safety margins of operating reactors. Analysis of uncertainties and implications for decision making. IAEA-TECDOC-1332, Vienna: IAEA; 2003.
- [86] National Aeronautics and Space Administration, NASA Risk Management Handbook, NASA/SP-2011-3422, November 2011
- [87] Office for Nuclear Regulation, Probabilistic Safety Analysis, NS-TAST-GD-030 Revision 4, June 2013
- [88] Wikimedia Foundation, Expected Utility Hypothesis , last accessed 14 June 2016, http://en.wikipedia.org/wiki/Expected_utility_hypothesis
- [89] Health and Safety Executive (HSE), Policy and guidance on reducing risks as low as reasonably practicable in Design, June 2003, <http://www.hse.gov.uk/risk/expert.htm>
- [90] Health and Safety Executive (HSE), Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable, December 2001 <http://www.hse.gov.uk/risk/expert.htm>
- [91] Office for Nuclear Regulation, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Revision 0, November 2014
- [92] G.L. Fiorini, S. La Rovere, P. Vestrucci, “Peculiar Roles of the Defense in Depth and the Probabilistic Safety Assessment in NPP Safety Performances Optimization”, ICAPP2015, May 3-6, 2015
- [93] OECD Nuclear Energy Agency, “Use and Development of Probabilistic Safety Analysis”, NEA/CSNI/R(2012)11, December 2012

11 LIST OF TABLES

Table 1.	Classification of dependencies in L1 PSA.....	48
Table 2.	Summary of numerical criteria for CDF [93]	73
Table 3.	Summary of numerical criteria for L(E)RF [93]	74

12 LIST OF FIGURES

Fig. 1	Steps for the PSA assessment of DiD and details [76]	58
Fig. 2	Principles for the Lines of Defence methodology [76]	61
Fig. 3	Example of Event Tree organized following the structure of the DiD [76]	62
Fig. 4	Risk space and deterministic / probabilistic success criteria [76]	63
Fig. 5	Example of the possible use of INES-Based safety targets for prioritization of SAM actions	68
Fig. 6	Numerical criteria defined for Core Damage [76]	70
Fig. 7	Numerical criteria defined for large release. (Definition and timing of “large release” varies) [19]	71
Fig. 8	Key elements of integrated RIDM approach from INSAG-25 [12], p. 6.....	78
Fig. 9	Selected Influencing Inputs to a Decision Maker	79
Fig. 10	Simplified value tree diagram developed to support decision-making on nuclear safety [82].....	81
Fig. 11	Example of the concave value function $v(x)$ [82]	82
Fig. 12	Roles in RIDM [86], p. 8.....	83
Fig. 13	Hierarchy of Objectives in the Design Process [86], p. 34	84
Fig. 14	Performance objectives and performance measures [86], p. 40.....	85
Fig. 15	Performance measures and performance commitments in RIDM [86], p. 76	86
Fig. 16	Relationship of RIDM and CRM, [86], p. 25	87