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

"NUCLEAR FISSION"
Safety of Existing Nuclear Installations

Contract 605001

Guidance for Decision Making based on Extended PSA

Volume 1 – Summary report

Reference ASAMPSA_E



Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 1

Reference IRSN/PSN-RES/SAG/2017-00016

H. Löffler (GRS), M. Kumar (LR), E. Raimond (IRSN)

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

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

	<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/WP30/D30.7/2017-31 volume 1 Reference IRSN/PSN-RES/SAG/2017-00016
Title	Guidance for Decision Making based on Extended PSA Volume 1 - Summary report
Author(s)	H. Löffler (GRS), M. Kumar (LR), E. Raimond (IRSN)
Delivery date	31-12-2016
Topical area	Extended PSA, Risk-informed Decision Making
For Journal & Conf. papers	No
<p><u>Summary :</u></p> <p>This report of ASAMPSA_E project is a summary report of the WP30 activities which were intended to develop guidance on decision-making process based on extended PSA results, when the PSA scope has been extended to all sources of radioactivity, all internal and relevant external events.</p> <p>It summarizes the ASAMPSA_E recommendations on :</p> <ul style="list-style-type: none"> - the lessons of Fukushima Dai-ichi accident for PSA, - the risk metrics, - the method for identifying Initiating Events and Hazards for an Extended PSA (screening), - the link between extended PSA and the defense-in-depth concept. <p>The report then provides some general considerations on application of extended PSA results, criteria that can be applied and also some difficulties inherent to the status of extended PSAs.</p>	

Visa grid			
	Main author(s) :	Verification	Approval (Coordinator)
Name (s)	H. Löffler	E. Raimond	E. Raimond
Date	2017-03-19	2017-04-29	2017-04-29

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
1	2016-10-05	H. Löffler	all	First proposal for the structure of document, based on D30.6
2	2017-03-19	H. Löffler	Ch 4	Ch 4 is completed using [4]
3	2017-03-20	M. Kumar	Ch 1 to 3	Ch 1 to 3 are completed using [2] and [3].
4	2017-03-22	E. Raimond	Ch 5	Ch 5 is completed using [5]. The initial structure of report is modified: ch.6 is added and appendixes are created.
5	2017-03-29	E. Raimond	Ch 7,8,9	Creation of concluding sections. This version is sent to the partners for final remarks.
6	2017-04-29	E. Raimond	All	Updated from received comments (mostly JSI, A. Prošek, GRS, A. Wielenberg).

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	LR	WP22 coordinator until 2015-10-31
Kumar	Manorma	LR	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
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
Hage	Michael	GRS
Loeffler	Horst	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	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	LR
Klug	Joakim	LR
Kumar	Manorma	LR
Olsson	Anders	LR
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
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

Frequency

Frequency in this report is the measure for the rate of an event, ideally being constant over time. 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.

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:

$\text{Risk}(\text{event } i) = \text{“the probability of an event } i\text{”} \times \text{“the consequences of an event } i\text{”}$. [85], cf. [9]

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.

Risk metric and measure

“In the context of risk measurement, a risk metric is the concept quantified by a risk measure.” [99]. 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. [4].

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. [99]

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
5	Lloyd's Register	LR	Sweden
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
ASAMPSA_E Partners	7
Content	8
Abbreviations	10
1 Introduction	11
2 High level / general considerations	12
2.1 Risk for Nuclear Power Plants.....	12
2.2 Capabilities and Limitations of PSA models	12
2.3 Lessons learned from the Fukushima Dai-ichi accident	13
3 Identifying Initiating Events and Hazards for an Extended PSA.....	17
4 Risk Measures for an Extended PSA.....	24
4.1 Risk Metrics for an extended Level 1 PSA.....	24
4.2 Risk Metrics for an extended Level 2 PSA.....	25
5 Link between Defence-in-Depth and Extended PSA.....	28
6 Safety Objectives for an Extended PSA	32
6.1 Safety objectives from existing PSA compiled by OECD/NEA.....	32
6.1.1 Summary of a NEA survey from 2009	32
6.1.2 Summary of a NEA survey from 2012	35
6.2 Discussion on Safety Objectives for extended Level 1 PSA Risk Measures	37
6.3 Discussions on Safety Objectives for extended Level 2 PSA Risk Measures.....	38
6.3.1 Measure for loss of containment function	38
6.3.2 CRT: an example of L2 PSA total risk criteria	39
7 PSA applications and role of extended PSA.....	41
7.1 Summary	41
7.2 The main application of the PSA is for design evaluation.....	42
7.3 PSA is also used to enhance the management of the potential accidents and their consequences.	43
7.4 PSA insights are important to optimize plant operation and make sure that important SSCs are properly managed.	44
7.5 PSA contributes to plant operating experience analysis	45
7.6 The risk information provided by the PSA is increasingly being used by regulatory authorities in planning their activities.....	46
7.7 Application of Extended PSA Results for Risk reduction “As Low As Reasonably Achievable”	47
8 Limits for extended PSA development and applications	48
9 Conclusion	49

10 List of References.....	50
11 List of Tables.....	56
12 List of Figures	56
Appendix 1 - Current Understanding of RIDM Approaches	57
Appendix 2 - INSAG-25 (IAEA)	58
A.2.1 Extensions of RIDM Approaches	59
A.2.1.1 Practical approach to the implementation of integrated RIDM process	59
A.2.1.2 Some insights from NASA's RIDM Handbook.....	61
Appendix 3 - Vulnerability of NPPs according to recent IAEA TECDOC	65
Appendix 4 - The PSA assessment of DiD.....	67
Appendix 5 – Example for the “CRT” application.....	71

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.

“An extended PSA (probabilistic safety assessment) applies to a site of one or several Nuclear Power Plant(s) (NPP(s)) and its environment. It intends to calculate the risk induced by the main sources of radioactivity (reactor core and spent fuel storages, other sources) on the site, taking into account all operating states for each main source and all possible relevant accident initiating events (both internal and external) affecting one NPP or the whole site.”

The partners involved in the ASAMPSA_E work package WP30 have examined general issues for extended PSAs development and applications.

- In report D30.2 [2], the authors have looked at available information about the accident at the Fukushima Dai-ichi 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 87 specific recommendations on L1 PSA, L2 PSA and use of PSA results in decision making.
- The report D30.7 volume 2 [3] investigates the approach for identifying initiating events and hazard scenarios for an extended PSA and have derived recommendations for a comprehensive screening methodology.
- The report D30.7 volume 3 [4] has investigated risk measures for an extended L1 and L2 PSA. The authors discussed 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.
- The report D30.7 volume 4 [5] discusses 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. The report D30.7 volume 5 provides additional views from one of the ASAMPSA_E partner [6].

This report aims firstly at integrating the recommendations derived in the aforementioned ASAMPSA_E reports, and secondly, at discussing the use of insights from extended PSA in risk-informed decision making (RIDM). Among other issues, the state of the art PSA, uncertainty about initiating events, and problems associated with multi-unit sites are addressed.

It takes into account the End-Users comments on a previous version (D30.6) discussed during the ASAMPSA_E end-users workshop [8], and also some ongoing work at IAEA on the high level considerations on safety requirements and role of PSA in fulfilling such requirements, e.g. IAEA TECDOCs in decision making and safety goals.

2 HIGH LEVEL / GENERAL CONSIDERATIONS

2.1 RISK FOR NUCLEAR POWER PLANTS

There are multiple aspects of risk for nuclear power plants, but the discussion here is limited to the specific aspect of risk as described by the fundamental safety objective in IAEA SF-1 [13], as referenced in [4], 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 [9], the following definition of risk is applied:

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”.

2.2 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 [16] for L1 PSA and SSG-4 [17] for L2 PSA. 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. Consequently, PSA results are routinely taken into account in decision making processes.

Nonetheless, even an extended PSA produced with the state-of-the-art and incorporating all the ASAMPSA_E recommendations would have several important and fundamental limitations. Importantly, PSA analysts have to use simplified 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 often based on enveloping boundary conditions. Moreover, the different parts of the PSA model may be developed with different levels of detail and conservatism, depending on their risk

contribution, the resources available for the development, and the availability or lack of knowledge on relevant phenomena and plant behaviour.

In addition, some parts of the risk may be, 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 development requires significant 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. PSA analysts together with other stakeholders should determine whether more detailed or additional PSA models can provide relevant contributions to decision makers or whether existing or simple PSA models with a higher degree of conservatism are sufficient to resolve the issues.

2.3 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)” [86], 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) [87]. 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 [13]. 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.” [89], 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 problem is complex can no longer be an excuse for doing nothing.” [87]. The ASAMPSA_E project will tackle the aforementioned issues during the remainder of the project.”

Comments

The purpose of D30.2 [2] listed recommendations is not to put too much burden on the PSA role, but to stress that PSA is an important tool for assessing the nuclear safety aspects that need further improvements. The Table 1 below provides a list of PSA issues (relevant to ASAMPSA_E project scope) identified in [2] and related recommendations for PSA Level 1, Level 2 and use of PSA results:

Table 1. Distribution of recommendations in D30.2 [2] from the Fukushima Dai-ichi accident

PSA Issues		Level 1 PSA recommendations	Level 2 PSA recommendations	Use of PSA results recommendations	Total
INITIATING EVENTS AND LOW PROBABILITY/HIGH IMPACT EVENTS (and combination of rare events)	HAZARDS IDENTIFICATION FOR PSA	1 to 9			9
	CORRELATION OF HAZARDS	10			1
	EXTERNAL HAZARDS SCREENING	11 to 14	44, 49		6
	EXTERNAL HAZARDS ASSESSMENT	15 to 19			5
	EXTERNAL HAZARDS AND INITIATING EVENTS	20 to 22	43, 45 to 48, 50, 51		10
SYSTEMS RELIABILITY AND CONDITIONAL UNAVAILABILITY FOR THE DID LEVELS	SYSTEMS RELIABILITY	23 to 26	52 to 59		12
	MODELING AND ASSESSMENT ISSUES	27 to 33	60 to 69		17
EMERGENCY OPERATING PROCEDURES, SEVERE ACCIDENT MANAGEMENT PROCEDURES/GUIDELINES AND EVENT SPECIFIC BOUNDARY CONDITIONS		34, 35	70 to 73		6
HUMAN RELIABILITY ASSESSMENT AND EVENT SPECIFIC BOUNDARY CONDITIONS		36 to 42	74 to 78		12
USE OF PSA RESULTS IN DECISION MAKING				79 to 87	9
Total recommendations					87

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.

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 guidance's 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 the ASAMPSA_E project recommends to include certain aspects, for which PSA can contribute additional 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 IDENTIFYING INITIATING EVENTS AND HAZARDS FOR AN EXTENDED PSA

The report D30.7 volume 2 [3] provides in-depth discussions of the methodologies to be applied to identify Initiating Events and Hazards to be considered in an Extended PSA. This is a key activity to extend reasonably the content of PSAs. The summary of this report is provided hereafter.

From an industrial end-user perspective, the screening process must be effective enough to be able to identify rapidly key predominant hazards eligible to extended PSA analysis. This is paramount to enable industrial end-user to better focus resources and direct them to address issues that present the highest significance to NPP Risks and Safety. The following provide some envelope good practices for each step of the selection of extended PSA initiating events. From an industrial end-user perspective, each step must be adapted and simplified where necessary and justified.

The major steps for initiating events identification

Based on the discussion in the previous section, the following refined methodology for initiating events identification, screening and 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. Qualitative screening criteria will be applied.*
- 2. Initial (possibly conservative) frequency claims for events and hazards and their respective combinations applicable to the plant and the site. Quantitative screening criteria will be applied.*

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. If required, refinement of screening by comparison of bounding analyses results against detailed PSA results.

The main qualitative and quantitative screening criteria

The proposed screening approach for an extended PSA recommends using the following qualitative screening criteria.

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.
3. The event (external hazard) has the potential to induce catastrophic levels of destruction on the plant and regional scale offsite consequences.

The following quantitative screening criteria, relative to overall PSA results for the respective risk measures are proposed.

1. Based on regulatory acceptance criteria or established international guidance for CDF/FDF (e.g. $10^{-5}/a$ for new reactors) and LRF/LERF, the maximum screening quantitative criteria shall be set to 1 % of that value. This results in the following minimum criteria:
 - a. $FDF_{event} < 10^{-7}/a$
($RMF_{event} < 10^{-7}/a$)
 - b. $LRF_{event} < 10^{-8}/a$
 - c. $ERF_{event} < 10^{-8}/a$
($LERF_{event} < 10^{-8}/a$)
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 $< 10^{-7}/a$
($RMF_{event} < 1\% RMF_{overall}$ if $< 10^{-7}/a$)
 - b. $LRF_{event} < 1\% LRF_{overall}$ if $< 10^{-8}/a$
 - c. $ERF_{event} < 1\% ERF_{overall}$ if $< 10^{-8}/a$
($LERF_{event} < 1\% LERF_{overall}$ if $< 10^{-8}/a$)
3. An initiating event or hazard scenario should be screened out from extended PSA detailed analysis, only if it can be screened out against all quantitative screening criteria.
4. Bounding analysis to estimate the criteria above shall be preferred during the screening approach.
5. 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.
6. Very low frequency events associated to potential major consequences are often associated to high uncertainties. Pessimistic bounding analyses or mean values of distributions may lead to results which violate the quantitative criteria above. If they are screened out nevertheless, a prudent approach shall

be applied and possibilities to reinforce the plant defences shall be kept open independently of the extended PSA considerations. The extended PSA should clearly identify such events and how they are addressed.

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.

The whole process

The identification of internal initiating events as well as internal and external hazard scenarios needs to be as comprehensive as possible. The identification process should follow a systematic approach, use all relevant and available information on the plant and its environment, and be documented in a traceable manner. Guides like IAEA SSG-3 [16] provide solid high-level guidance on this issue.

Important recommendations for the screening of internal initiating events and hazard scenarios for an extended PSA are the following:

1. Grouping of internal initiating events and hazard scenarios into representative groups plays an important role during screening.

Events and scenarios should be grouped into one bounding group only if they have similar properties in terms of accident development up to fuel damage, accident progression after fuel damage up to release categories, and relevant accident mitigation measures.

The grouping of events should consider uncertainties and levels of conservatism associated with frequency determination and bounding assessments. As far as practicable, grouped events and scenarios should be comparable in this regard. Importantly, the results for initiating frequency and the bounding scenario should not be distorted by combining e.g. a moderately frequent event with small uncertainty bounds with a rare event with excessive uncertainty bounds.

To the extent practicable, the implications of each event or scenario with regard to several sources in one unit (e.g. reactor core and spent fuel pool) or for the site in case of a multi-unit site should be considered.

Grouping of similar events and scenarios should be preferred to screening them out individually based on bounding assessment from a more detailed probabilistic assessment.

2. Bounding assessment is an essential step in the screening process for limiting the number of cases for more detailed probabilistic modelling. Bounding assessment is based on plant response analysis and hazard impact analysis. Bounding assessment used all relevant information sources on the plant and its behaviour in response to the analysed event or scenario.

Claims made based on expert judgement during bounding assessment shall be demonstrably conservative. Estimations should be made consecutively on initiating event or hazard scenario frequency, conditional probabilities to FDF or RMF, and conditional probabilities to LRF and ERF.

Bounding assessments for internal and external hazard scenarios should make use of internal initiating event PSA models.

Bounding assessment for multi-unit and multi-source PSA should make conservative failure assumptions on shared systems and the propagation of hazard effects through shared systems and other connections.

3. *Screening of internal initiating events and internal hazard scenarios should be made specific for the respective unit or source. A site-model should then be developed from those events screened in for each unit or source.*

Screening for external hazard scenarios should be done based on the specific units or sources. If an external hazard scenario is screened in for any unit or source, it should be treated for all units or sources in the site-level PSA model by more detailed probabilistic modelling.

4. *Plausible combinations of applicable hazard scenarios with other independent or correlated external or internal hazards or internal initiating events need to be screened separately, even if the individual event or hazard has already been screened out (except if it is not applicable to the site).*
5. *Applicability screening for hazard scenario (as well as each combination of hazards), PSA analysts should make claims on the maximum credible impact. The ASAMPSA_E project recommends that maximum credible impact is determined based on reasonable physical, geophysical, and chemical assumptions on the source of the hazard, without explicit consideration on the likelihood of such a scenario.*
6. *Particularly for external hazards, a partitioning of the hazard frequency curve in a small number of subgroups based on one representative hazard impact parameter of a set of such parameters will be necessary. The partitioning should consider design basis thresholds for hazard impact, design extension condition analysis assumptions on beyond design basis impacts, and impact parameter values for a potential cliff-edge to catastrophic failures.*
7. *Results from an analysis following the Fault Sequence Analysis method or similar approaches can provide valuable input for the screening of internal and external hazards and their combinations.*
8. *Screening for non-fuel sources should use the RMF as PSA Level 1 risk measure. The identification process of events and scenarios challenging non-fuel type sources can be based on the RMF metric definition as a potential challenge to the first barrier designed to contain the respective source.*
9. *Screening on the recommended release metrics LRF and ERF should be focused on aerial release. Analysts need to confirm if aqueous release or release into the ground are relevant release paths.*
10. *For the construction of site-level PSA models, further screening needs to be performed on those events and scenarios for which a dedicated site-level PSA will be necessary. Although this is not formally part of the screening for an extended PSA but rather an issue of how to construct a multi-unit, multi-source PSA model, we have provided selected recommendations in section 6.8 [of [3]].*

Bounding estimates on the screening risk measures (i.e. FDF, RMF, LRF, and ERF) for each event and scenario should be understood to be part of overall PSA results. Insights from bounding analysis and potential vulnerabilities of the plant discovered during the screening process should be documented and treated in the further PSA process.

The screening process is inherently iterative in order to limit the number of cases for more detailed PSA models. If the number of screened in scenarios is large it could be necessary to set priorities for the detailed PSA models and bounding could be useful for that purpose. The overall approach to the determination of initiating events for an extended PSA can be summarized for internal events PSA in Fig. 1. The extension of the approach to hazard scenarios is depicted in Fig. 2.

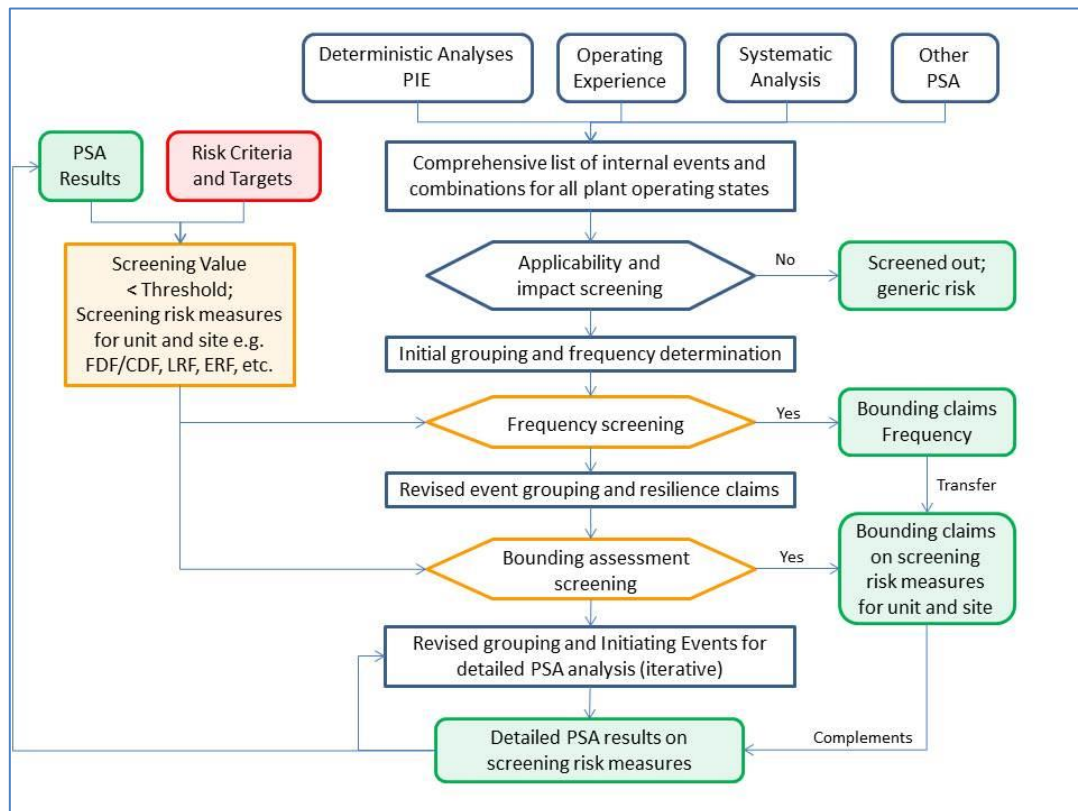


Fig. 1 Screening approach to internal events

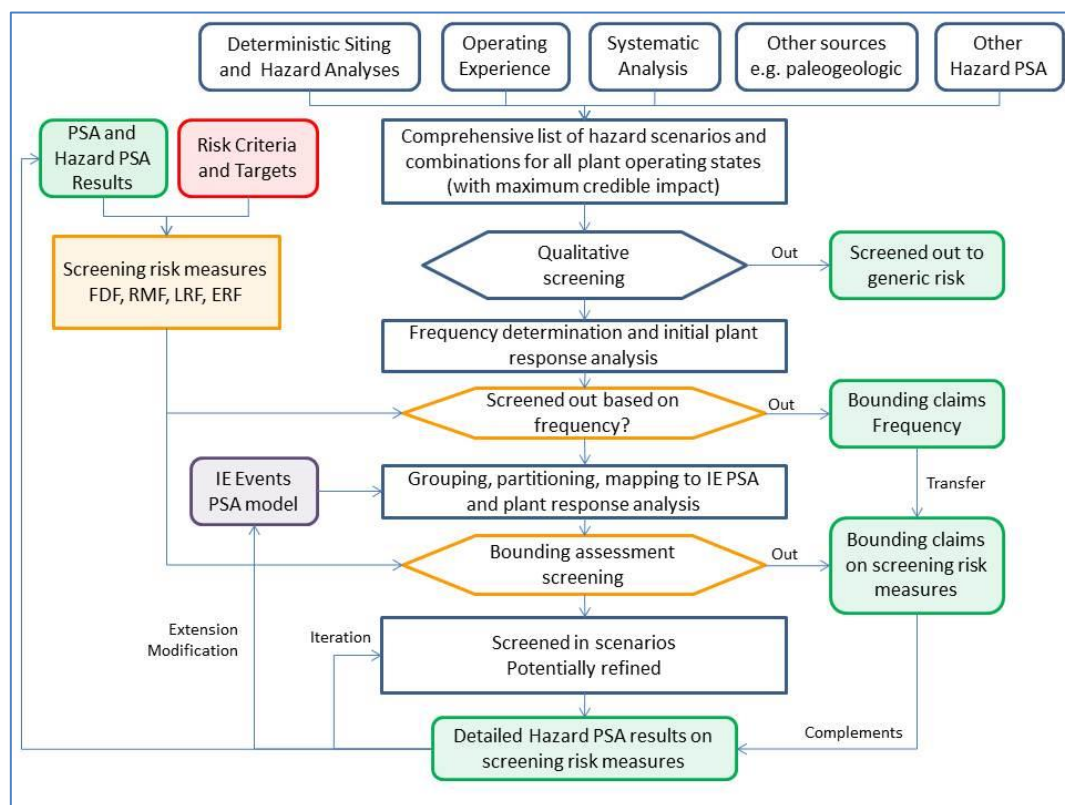


Fig. 2 Extension of screening approach to hazard scenarios

Remarks regarding PSA quality

Systematic use of quantitative bounding assessment in the screening for an extended PSA is seen as good practice.

- *Explicit bounding assessment rules necessarily limit the risk of neglecting specific aspects of the event and its impact on the plant, especially regarding severe accident scenarios. PSA analysts should be encouraged to propose specific claims (at the appropriate level of conservatism and detail) and provide supporting arguments.*
- *The quantitative bounding assessment, irrespective whether by expert judgement or by using simplified conservative assessment models, is seen as a valid probabilistic assessment approach. To that end, bounding assessments have to be traceable.*
- *Having claims and supporting arguments significantly improves the traceability of the screening process and thus contributes to the review of the PSA, both internally as well as by regulatory bodies.*

Towards detailed PSA models?

There is no sharp dividing line between progressively more refined bounding assessment and the development of a more detailed PSA model. The transition is gradual and depends, amongst others, on the availability of assessment methods, available data, and the scope and level of detail of existing PSA modelling for this and similar events or scenarios. As a general guidance, probabilistic assessment leaves the area of bounding assessment, if results should be reported with uncertainty bounds.

The development of detailed PSA models may require further iteration steps for screened-in initiating events or hazard scenario groups. Depending on the risk measures specified for PSA Level 1, PSA Level 2, and possible PSA Level 2+ results, there can be additional constraints on the grouping of events and scenarios, because initially grouped scenarios have dissimilar properties with respect to these additional (aspects of) risk measures. Then, PSA analysts need to de-aggregate the respective groups.

Moreover, bounding assessment results from screening have to be forwarded to overall PSA results and need to be compared with the more detailed results, based on the risk measures defined for detailed PSA investigations. The risk measure for detailed PSA investigations may address additional characteristics and aspects of accident sequences, not covered by the screening risk measures. For the comparison of detailed PSA results and bounding assessment results, the latter should be assigned to the worst applicable category. For example, if the FDF measure is differentiated by the aspect of time to fuel damage, all bounding assessments should be assigned to the subcategory representing the earliest fuel damage by default. Assigning results to a less severe subgroup should be justified by targeted or refined bounding assessment.

Detailed analysis of hazards scenarios should follow a graded approach as well. The level of effort and the level of conservatism should be commensurate to the overall contribution of the scenarios to relevant risk measures, to the knowledge available on the hazard, its frequency, and its impact on the plant and site, and to the relevance of respective PSA results to decision makers and other stakeholders. A too high level of detail and complexity could lead to PSA models that are very difficult to build and to use for practical applications.

In order to have a better understanding of the quality of the quantitative results of the screening process, PSA analysts should aggregate the bounding assessment claims on FDF, RMF, LRF, and ERF over all screened-out events. These should then be compared to the respective PSA results from more detailed analysis.

- If the aggregated claims for FDF, RMF, LRF, and ERF are below 10% of the respective total results from more detailed PSA, no further refinement of a comprehensive screening process is necessary. Such a result should be seen as an indicator for a PSA which can not only support risk-informed decisions in general but also decisions with respect to the risk profile of the plant in most cases.*
- If the aggregated claims for FDF, RMD, LRF, and ERF are below the respective total results from more detailed PSA, analysts should consider*
 - a. if bounding assessments can be refined or*
 - b. if certain events should be considered for a detailed PSA investigation. Single events can be prioritized by the contribution of their claims to the aggregated claims.*

Such a result should be seen as an indicator for a sound PSA, which can support risk-informed decision making. However, decisions with respect to the risk profile of the plant merit explicit consideration of screened-out events.

- If the aggregated claims for FDF, RMF, LRF or ERF are larger than the respective results from more detailed PSA but less than 10 times larger, analysts should at least refine bounding assessments for important events or scenarios. Alternatively, important events or scenarios should be considered for a detailed PSA investigation.*

Such a result should be seen as an indicator for an acceptable PSA. While the PSA can support risk-informed decision making in principle, the impact of screened-out events merits explicit consideration. Decisions on the risk profile of the plant might be significantly impacted by screened-out events.

- If the aggregated claims for FDF, RMF, LRF or ERF are larger than 10 times the respective results from more detailed PSA, the screening should be refined. Important events should be considered for detailed PSA investigations.*

Such a result should be seen as an indicator for a screening process which should be improved. The PSA might be able to support risk-informed decision making, but lack of knowledge about the risk of the plant will reduce the validity of PSA insights and might reduce its range of applicability.

Link with the situations that should be practically eliminated (if applicable)

If the concept of practical elimination is applied in the NPP safety demonstration, then the PSA analysts shall make the link between initiating events selection for extended PSA and the situations that are considered to be practically eliminated explicit. They should verify that these situations contribute negligibly to the overall risk.

4 RISK MEASURES FOR AN EXTENDED PSA

Many risk measures have been discussed in the ASAMPSA_E report on risk metrics for extended PSA [4] with the aim of being complete and well founded. However, in practice there is no lack in availability of risk metrics, but there is a need for the harmonized selection of such metrics. Therefore, to be practical and in order to contribute to harmonization of PSA application, just four risk metrics are recommended in the present section: Two for PSA level 1 and level 2 each.

In general, L1 PSA risk metrics assess the risk within a plant, whereas L2 PSA risk metrics are related to risks of releases to the environment around the plant, which reflect the requirement of fundamental safety objective - to protect people and the environment from harmful effects of ionizing radiation under to all circumstances that give rise to radiation risks.

4.1 RISK METRICS FOR AN EXTENDED LEVEL 1 PSA

The Level 1 risk metric has to be defined as those end states of the L1 PSA model that 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, FDF (fuel damage frequency) 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 PSA Level 1 end state than other direct risk measures as CDF. CDF that 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", 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 Equivalent¹. 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 mobilized activity into one common risk measure

¹ The proposed threshold value has been set to 1 % of the lower end 100 TBq I-131 Equivalent limit for an accidental level release (INES 5) defined in the INES manual [90]. This assumes that short-term consequences are of interest. For long-term consequences, a threshold reflecting e.g. Cs-137 should be selected. .

(figure of merit). While this is one of its advantages, it similarly limits its suitability for understanding the actual risk profile with regard to the challenge to the environment.

The RMF was proposed 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 a 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.

It must be pointed out, though, that the RMF risk measure is not well suited for understanding the risk profile of e.g. an NPP in operation. It should be complemented by e.g. CDF/FDF as a L1 PSA risk measure. FDF would be the recommended metric in this case.

4.2 RISK METRICS FOR AN EXTENDED LEVEL 2 PSA

The pertinent sections in the ASAMPSA_E report on risk metrics for extended PSA [4] on possible risk metrics for L2 PSA provide a comprehensive summary on this topic. (see also the ASAMPSA2 report [9]).

The metrics discussed in [4] are the following:

- Large Release Frequency (LRF),
- Early Release Frequency (ERF),
- Large Early Release Frequency (LERF),
- Release Categories Frequency (RCF),
- Frequency of Loss of containment functions,
- “Kinetics Based” Release Categories,
- Functional and Phenomena Based Risk Metric,
- Absolute Severity Metric,
- Integral Risk or Total Risk Measures.

Each metric has interest even if there is no harmonization in the details of application (for example for the definition of what is “early” or “large”), nevertheless the choice should be consistent with the application of L2 PSA for protection of population and environment.

Before providing recommendations for suitable Level 2 PSA metrics, the following remarks on multi-unit issues are due. It is of interest to not only have just one single value representing the total risk (whatever this may be) from the set of units on the site, 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 risk metrics provided for individual units. 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 in different reactor blocks on the same site initiated by the same external hazard. 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 is really challenging, but there is no reason for introducing additional risk metrics or dismissing other metrics which have been proposed for single unit PSA.

From the various metrics discussed in the ASAMPSA_E report on risk metrics for extended PSA [4], the following are recommended as particularly suited for characterizing L2 PSA results.

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 for core melt sequences:

- 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 compile the different containment failure modes into an additional metric called “Containment Failure Frequency” (CFF). CFF has similarity to the well-known core damage frequency (CDF) concept of L1 PSA. The CFF would comprise all sequences where the containment function is lost - whatever the reason.

PSA Level 2 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 section is about L2 PSA, and therefore the “total risk” which is proposed here is related to L2 PSA issues, i.e. radioactive releases to the environment.

The total risk measure should be seen as an optional 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 could be an easy task for L2 PSAs which have 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.

The attractive feature which comes with a single value for the integral risk is the possibility to compare it to a risk target. It allows for “rational” decision making and for the identification of an “optimal decision” in principle. 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 risk measure. It is recommended that pertinent working 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 and accepted by decision makers it can be completed by pertinent risk targets.

Section 6.3.2 and appendix 4 provides an example application of a “total risk” metric with a common risk target (CRT).

5 LINK BETWEEN DEFENCE-IN-DEPTH AND EXTENDED PSA

This section provides the general conclusions and recommendations coming from the ASAMPSA_E report D30.7 volume 4 [5] about the link between the Probabilistic Safety Assessment (PSA) and the Defence-in-Depth (DiD) concept for NPP, with specific focus on the capability of an “extended PSA” to support the assessment of DiD.

The identification of the Postulated Initiating Events (PIEs) is the initial step of a safety analysis. Thus, it is also a cornerstone in the application of the DiD concept. Some main recommendations were specified discussing (in Section 3 [of [5]]) the link between PIE in Deterministic Safety Assessment (DSA) and Initiating Event (IE) in PSA:

- *from the point of view of risk, there is no need to make distinctions between initiators/scenarios as design basis, design extension conditions and beyond design or even severe accident;*
- *the analysts should be aware that, from historical evidence, actual severe accidents (i.e. design extension conditions with core degradation) happened more often than predictions;*
- *the analysts should be aware that the original sets of DBAs were postulated as “enveloping accidents” by nuclear engineers more than 50 years ago based on the knowledge and consensus at the time;*
- *the quantitative references for the frequency of occurrence stated in the SSG-2 [15] should be considered as indicators rather than fixed limits; some harmonization are still needed between these thresholds and some historical assumptions and recent safety criteria/design objectives (e.g. practical elimination);*
- *the list of IE of an extended PSA, including internal events, hazard event groups, combination events, should be checked against the list of PIE for deterministic safety analyses;*
- *before any comparison with the IE in PSA, the basic scenario for the PIE (e.g. loss of feedwater, small LOCA), the related boundary conditions (e.g. loss of offsite power) and concurrent failures assumed in the DSA should be clearly understood;*
- *the frequency values assumed for PIE in DSA should be consistent with the related IE frequency or intermediate or final results of the PSA model, as applicable;*
- *the consistency between the data sources used for the estimation of the IE frequency (value or distribution) in PSA and the classification of PIE should be checked.*

The classification of Systems, Structures, and Components (SSCs) and their assignment to different levels of DiD is an essential aspect of the implementation of the DiD concept. Some recommendations were specified discussing (in Section 4 of [5]) the process and criteria for the classification of SSCs and the reliability of provisions implementing safety functions:

- *for the classification of SSCs it is recommended to apply deterministic methodologies and to complement them by probabilistic safety assessment;*
- *PSA information should be used through the approach endorsed by the US NRC [24], [25] or similar approaches based on the importance measures estimated for the SSCs with reference to the PSA Level 1 (CDF) and PSA Level 2 risk measures;*
- *the assessment of the reliability of the provisions (including SSCs) achieving the safety functions does not require different methods or risk measures for an extended PSA to be used for the assessment of DiD;*
- *a more systematic use of the information coming from PSA is recommended in risk-informed decision making on the adequate reliability of systems, and structures (i.e. including passive safety features) and, more*

generally, the safety related provisions; the measure should be their conditional failure probability / availability.

The main issues related to the DiD concept, including the structure of the levels of DiD, and the essential requirement about their independence, and the need(s) for the safety and DiD assessments, have been introduced in Section 2 [of [5]].

The need for the assessment of DiD is explicitly recognized by the GSR Part 4 (Rev1) [18], which defines the context for the safety assessment of a nuclear installation, encompassing DiD concept and the PSA approach, enhancing their complementarity and detailing the objective to be pursued.

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

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

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

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

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

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

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

methods for some human actions, large requirement of resources, etc.), motivating a specific work for their improvement, are not related to DiD issues.

At this regard, the DiD assessment as preconized by the GSR Part 4 (Rev.1) [18] could be inscribed in the Integrated Risk Informed Decision Making Process, where the PSA can play an essential role, without the need to define specific assessment process and criteria.

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

First of all, the existing PSA models have been often produced without the specific objective to assess the implementation of DiD. This is partly due to the lack of previous investigations into the subject and partly due to the lack of practical implementations and feedbacks about good practices in the PSA community.

If the PSA is used with this particular objective, its results should be presented and exploited in such a way that the contribution of each level of DiD to the overall safety can be checked and potential weaknesses identified. Specifically, the PSA should be properly structured in order to provide results that can be correlated with the performances (capability, reliability and robustness) required to the levels of DiD and have a sufficient scope.

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

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

Additionally:

- the different progressive levels of DiD and the associated plant conditions do not easily map to the traditional PSA end states (e.g. CDF and release categories) and, on their side, initiating events could be assimilated to the failure of a given level of the DiD; at this regard, there is a considerable debate in the community about which initiating events, boundary conditions, safety functions and other elements of a PSA should be assigned to which level of DiD;
- the best-estimate approach typically used in PSA is not immediately compatible with the (conservative, safety case oriented) deterministic approach for a DiD assessment; on the other hand, taking into account uncertainties and assessing their contribution is now essential to any safety assessment.
- non-safety systems should be considered in the PSA, but they are usually neglected in the DSA;
- the comparison between the IE in PSA (with related frequency of occurrence) and the classification of PIE could be difficult mainly because of the (potential) different grouping of events and the different assumptions on boundary conditions and concurrent failures in PSA and DSA;

- a PSA model for the assessment of DiD could require additional data if they are not already included in the existing non-full scope PSA models (e.g. about initiating events and SSCs failure at the DiD level 2);
- deterministic analyses (DSAs) often assume certain boundary conditions to occur simultaneously at the time of the PIE occurrence, without considering their likelihood; differently, they are usually addressed in the PSA with their conditional probabilities, giving less conservative estimation.

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

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

The work done by SSM ([34], [35], [36]) could be the starting point for future work (see §5.1 [of [5]]).

An additional report [6] has been developed during the ASAMPSA_E project about the peculiar roles of the DiD concept and PSA approach for the optimization of the safety performances of nuclear installations. It describes the process and tools proposed for the DiD assessment through PSA (see §5.3 [of [5]]). All the proposals are based on consolidated terminology [21] and shared concepts ([13], [14], [89], [92], [22], [26], [27]) and are consistent with process for the Safety assessment defined by the IAEA [18] and with the approach proposed by SSM. Further activities, including practical applications, are required in order to finalize the proposals.

By summarizing, the present report provides elements to feed the thoughts about the optimization between the contributions of DiD and PSA to guarantee the safety assessment of the installation, but further discussion and practical experiences (e.g. benchmarking²) are needed to achieve consensus on objectives, scope and approaches for the use of PSA in the assessment of DiD concept and to develop a practical guideline.

² For instance, it would be necessary to extract from a complete existing PSA a self-supporting portion (e.g., the full set of plausible sequences from a given initiator event) and then to check if and how the (intermediate and final) results available provide the answers required for the assessment of DiD. In parallel, the safety architecture (i.e. the portion involved in the selected sequences of events) should be represented according to the principles of DiD, e.g. through the Objective Provisions Tree methodology, and the PSA (fault tree - event tree) model developed coherently with this representation. The solution of the model and the comparison of results (and embedded information for the DiD assessment) with the ones coming from the existing PSA could provide answers to the open questions (mainly, about the need of a different structure of the probabilistic model).

6 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.

6.1 SAFETY OBJECTIVES FROM EXISTING PSA COMPILED BY OECD/NEA

6.1.1 SUMMARY OF A NEA SURVEY FROM 2009

In the ASAMPSA_E deliverable [4] 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” [33] 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 [33].

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. 3 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.

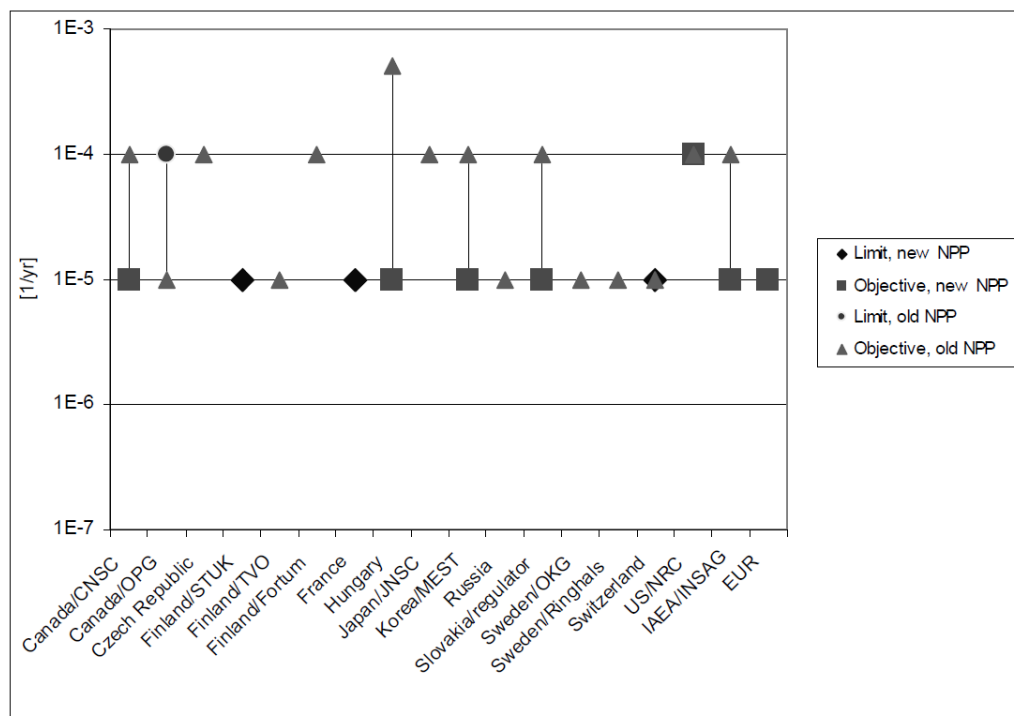


Fig. 3 Numerical criteria defined for Core Damage [33]

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.

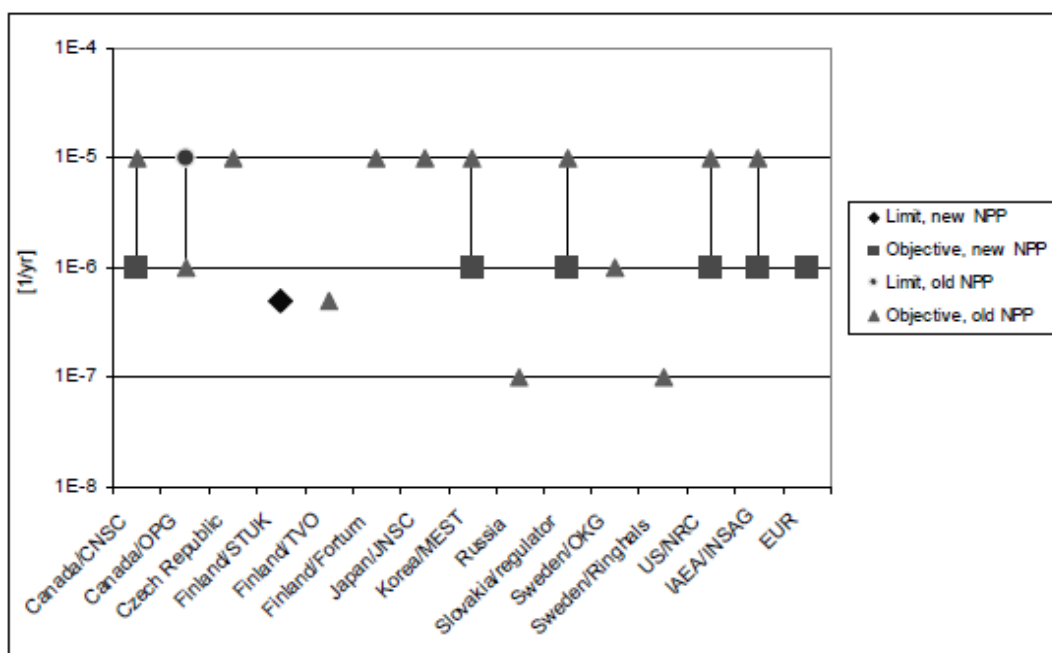


Fig. 4 Numerical criteria defined for large release. (Definition and timing of “large release” varies) [33]

Fig. 4 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.

Table 2. US-NRC probabilistic criteria [33]

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

6.1.2 SUMMARY OF A NEA SURVEY FROM 2012

Report [104] 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 [104].

Table 3. Summary of numerical criteria for CDF [104]

TABLE 3-1: Summary of numerical criteria defined for core damage frequency			
Country	Organization	Frequency	Notes
USA	Regulator	10^{-4} /r.y	Objective
UK ⁺	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^{-3} /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	Objective for existing plants

Slovenia	Regulator	10^{-5} /r.y	Objective for new build
		10^{-4} /r.y	Objective for existing plants
		10^{-5} /r.y	Objective for new build
Netherlands	Regulator	10^{-4} /r.y	Limit for existing plants
		10^{-6} /r.y	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	Objective for existing plants
		10^{-5} /r.y	Objective for new plants
Canada	Regulator	10^{-5} /r.y	Limit for new plants
	Licensee	10^{-4} /r.y	Limit for existing plants
		10^{-5} /r.y	Objective for existing plants

The numerical criteria for large early release frequency are shown in table below (Table 3-4 of [104]).

Table 4. Summary of numerical criteria for L(E)RF [104]

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	10^{-5} /yr	Limit for existing plants
		>1% Cs137 \\	10^{-6} /yr	Objective for existing plants

6.2 DISCUSSION ON SAFETY OBJECTIVES FOR EXTENDED 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 [4], 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 3, it seems that $1 \cdot 10^{-5}$ /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 [4]), 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.

6.3 DISCUSSIONS ON SAFETY OBJECTIVES FOR EXTENDED LEVEL 2 PSA RISK MEASURES

In the ASAMPSA_E deliverable [4] two L2 PSA risk measures have been recommended in addition to LERF or LRF which are already commonly applied (see section 4.2 or section 6.1):

- containment failure frequency (CFF),
- L2 PSA total risk measure.

The following subchapters provide two examples of safety objectives for these risk measures.

6.3.1 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 (see the modes of loss of containment function that should be distinguished for LWRs in section 4.2).

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).

6.3.2 CRT: AN EXAMPLE OF L2 PSA TOTAL RISK CRITERIA

In the framework of ASAMPSA_E, 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 should be 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 [9] and was further developed and published as scientific work in Nuclear Engineering and Design [66]. The CRT methodology and risk parameters make use of the IAEA INES scale [90].

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.

In the method, the risk is proposed to be calculated 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 [90]) for the i^{th} release mode.

With this definition of total risk CCA proposes to use common risk target (CRT) parameter for a single unit site (see [4] or [66]):

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

where

- ICRT is the Individual Common Risk Target (ICRT) of a single unit on the site with no significant contribution to other already accepted industrial risks (200 TBq I-131 equivalent corresponds to INES5 lower level of releases),
- 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 other already accepted industrial risks.

This approach has also the potential to be extended to multi-units risks (see [4] or [66]).

According to CCA, the CRT objective as defined above fits with other types of objectives (see discussion in [4]) and if a total risk measure is deemed useful for decision making and / or communication of PSA results, the common risk as defined above could be applied. Appendix 4 provides an example of application.

7 PSA APPLICATIONS AND ROLE OF EXTENDED PSA

PSA applications are part of a very large topic. The compilation and comparison of practices is periodically done by the NEA/CSNI Risk working group (WG-RISK). The last existing compilation is the report “Use and Development of Probabilistic Safety Assessment - An Overview of the situation at the end of 2010” [104]. This report is a useful source of information from member countries of OECD, even if provided before the Fukushima Dai-ichi accident.

Such a complete review could not be done in the ASAMPSA_E project so the next 6 chapters (§7.1 to §7.6) remind the conclusions of the NEA/CSNI report [104] on PSA application and propose some additional considerations on extended PSA developed during the ASAMPSA_E project. The following chapters introduce complementary considerations.

7.1 SUMMARY

[From NEA/CSNI/R(2012)11, ch 7, [104]]

PSA is used as a decision support tool to enhance a plant's design and operation. The benefits of such applications are of two types:

- *Safety benefits with measured risk reduction or improved safety focus; and*
- *Operational benefits with plant flexibility or complexity reduction.*

In a risk informed decision process, PSA insights are used together with other relevant information such as engineering judgment or regulatory requirements. The decisions must be made so that defense-in-depth is always assured and the safety margins are maintained.

[From ASAMPSA_E]

The ASAMPSA_E has revealed that the scope of existing PSA was still limited but many organizations are now completing these PSAs.

Extended PSA shall in near future:

- help identifying additional enhancement of plant's design and operation, typically for the protections against internal/external hazards, for the simultaneous management of reactor and spent fuel pool systems in complex situations or for multi units site management provisions,
- bring a better probabilistic justification of the relevance of existing provisions against accidents,
- bring a better probabilistic justification for decisions related to plant flexibility or complexity reduction.

After the Fukushima Dai-ichi accident, plants reinforcements have been decided to face extreme hazards, long term loss of ultimate heat sink, long term loss electrical power supply or severe accident.

These reinforcements were rarely based on results from PSAs (often not available). Nevertheless, development of extended PSA will contribute a posteriori to the verification that these new provisions are appropriate (reduction of measured risk, CDF or FDF, better design balance, absence of design weakness, ...).

7.2 THE MAIN APPLICATION OF THE PSA IS FOR DESIGN EVALUATION

[From NEA/CSNI/R(2012)11, ch 7, [104]]

The insights from the PSA have been used in combination with the insights from the deterministic analysis in a risk-informed approach. The PSA has been used to:

- *identify the dominant contributions to the risk (CDF and LERF);*
- *identify weaknesses in the design and operation of the plant; and*
- *determine whether the design is balanced.*

This has been done during periodic safety reviews for existing plants. There are many instances of where the PSA has identified weaknesses where plant improvements have been made. For example, the PSAs carried out in France for shutdown conditions identified significant contributions to the risk related to excessive drainage of the primary circuit during mid-loop operation and of heterogeneous boron dilution that could lead to a reactivity accident.

It is still often the case that, during the lifetime of the plant, the scope of the PSA that is carried out has increased - for example the PSA has been extended to include external hazards, cover low power and shutdown conditions, and extend the analysis to a Level 2 PSA. This identifies additional weaknesses that need to be addressed and many improvements have led to enhanced plant capability to respond to external events (such as earthquakes and floods) which can be important contributors to total plant risk.

The PSA has also been used to provide risk information in making the decisions on issues that have arisen such as: increasing the time between refueling outages; and increasing the power level of the core.

The PSA has proved to be a useful and versatile tool supporting the decision-making process in the following cases: assessing safety aspects of some backfits; and considering equipment innovations or other design or operation changes of existing plants. The review of proposed alternative options is often done as part of a cost-benefit approach. For some countries, PSA insights are also used to support life extension for existing operating plants.

Now, PSA is an important part of the design and the licensing processes of new plants. For example, for European Pressurized water Reactor (EPR) Flamanville 3, PSA contributions addressed the following items among others:

- *designing and optimizing the facility during the design phase and life of the site; and*
- *confirm the balanced risk profile of the design.*

In the USA, the Design Certification application for a light-water reactor design must contain a final safety analysis report (FSAR) that includes a description and analysis, based on PSA, of design features for the prevention and mitigation of severe accidents.

[From ASAMPSA_E]

These conclusions of WG-RISK are obviously still valid with the perspective of extended PSA. The following general statements can be proposed.

- an extended PSA can bring attention on additional safety issues,
- a larger scope of PSA content shall increase the validity of the application of cost-benefits approach in decision making process but it has to be considered in applications that conservatisms or uncertainties are not equivalent in all parts of an extended PSA (see remark 2 of section 8),
- concerning the main PSA applications identified by WG-RISK here (identify the dominant contributions to the risk (CDF and LERF), identify weaknesses in the design and operation of the plant; and determine whether the design is balanced), extended PSA shall bring additional information on beyond design conditions (for example on rare high amplitude initiating events) and help discussing conditions where both DiD level 3 (accident prevention) and 4 (accident mitigation) are threatened. This should provide a better confirmation of the balanced risk profile of the design. On this issue, the ASAMPSA_E project has concluded on the interest of global risk metrics that combine all causes of accidents, their frequencies and their consequences ($Total\ risk = \sum_i f_i \cdot c_i$), see above. It can appear that a low frequency accident is “risk dominant” due to the amplitude of the accident consequences if the DiD level 3 and 4 fail. This topic shall be a major concern for the development and the use of extended PSAs. Of course, a global risk metric is very sensitive to the quality/degree of conservatism in the model (see remark 2 of section 8).

7.3 PSA IS ALSO USED TO ENHANCE THE MANAGEMENT OF THE POTENTIAL ACCIDENTS AND THEIR CONSEQUENCES.

[From NEA/CSNI/R(2012)11, ch 7, [104]]

Often, the Level 2 PSA has been used to identify accident management measures that could be carried out to mitigate the effects of a severe accident. This has led to the implementations of generic or plant-specific Severe Accident Management Guidelines (SAMG) to guide operators in the event of a severe accident. An example of this is the Level 2 PSA for the Bruce B NPP in Canada, which provides a framework for the development of specific SAMG. Other examples are given by Mexico and Japan, and are also presented in the proceedings of a workshop organised by WGRISK jointly with WGAMA [7].

The source terms and frequencies produced by the Level 2 PSA have been used as the basis for emergency planning. In Canada, the regulator (CNSC) is promoting the use of PSA insights in defining the strategies to cope with the consequences of severe accidents. In Mexico, PSA was used to plan the emergency scenario for the evaluation of the External Radiological Emergency Procedures.

As operators are a key element in the defense in depth, their training on emergency operating procedures (EOPs) is very important. The PSA is being used at a number of plants to provide an input into the training program of plant staff. The aim is to focus the training on risk significant systems/ structures/ components, accident scenarios, maintenance activities, etc. In particular, the PSA is being used to identify risk significant scenarios to use in simulator training. An example of this is the training of critical human interventions contributing to the CDF identified by unit specific PSA models for the Dukovany NPP in Czech Republic. Risk Monitors are also being

used in training since they give a very direct indication of how activities being carried out on the plant affect the risk.

[From ASAMPSA_E]

The ASAMPSA_E project has specifically addressed partially this issue in the report “Verification and improvement of SAM strategies with L2 PSA” [106]. Several design options are available for severe accident management strategies and L2 PSA can usefully be applied to determine an optimal one.

In the future, multi-units L2 PSA should bring some additional inputs to this topic.

Regarding the emergency preparedness activities, the extended PSA results shall bring additional information whether the possible consequences increase with external events for a single reactor and SFP (or a site) and consequently whether there is a need to adapt emergency preparedness activities to those new consequences.

7.4 PSA INSIGHTS ARE IMPORTANT TO OPTIMIZE PLANT OPERATION AND MAKE SURE THAT IMPORTANT SSCS ARE PROPERLY MANAGED.

[From NEA/CSNI/R(2012)11, ch 7, [104]]

The PSA has been used, along with the deterministic insights, to identify the systems important to safety and these have been monitored using an enhanced surveillance program. The same approach has also been used to identify the active components that need to be given special attention as part of the program for the management of ageing. In Switzerland for example, a component is regarded as significant to safety when one of the following relations applies for CDF (core damage frequency), FDF (fuel damage frequency) or LERF (large early release frequency): $FV \geq 1E-3$ or $RAW \geq 2$, where FV is the Fussell-Vesely and RAW the Risk Achievement Worth importance measure. The guidance for combining both probabilistic and deterministic insights to group SSCs into four categories is given in the Nuclear Energy Institute (NEI) document NEI 00-04, “10 CFR 50.69 SSC Categorization Guideline.” In Japan, the new inspection system for NPPs started in January 2010 introducing the following three elements: new maintenance program, root cause analysis of events, and comprehensive plant performance assessment. Importance of systems and functions reviewed on the basis of both PSA findings and deterministic considerations was ranked into class 1 to 4 and nonclass.

The Technical Specifications define the Limiting Conditions for Operation (LCOs), the Allowed Outage Times (AOTs) and the Surveillance Test Intervals (STIs). In the past these have been based on deterministic considerations. In many countries the PSA has been used to justify and optimize the LCOs, AOTs and STIs. The PSA has also been used to justify an exemption from a Technical Specification. PSA has been used for identifying situations in which the plant shutdown could cause higher risk than continuing power operation and fixing the failures. For example, if systems used for decay heat removal are seriously degraded (CCF), it may be safer to

continue operation than to shutdown the plant immediately, although shutdown may be required by the current Technical Specifications.

Where the PSA that has been carried out addresses both operation at power and low power and shutdown conditions, it has been used as part of the justification for moving some of the maintenance activities from being carried out during plant shutdown to being carried out during power operation. This has the economic benefit of shortening the refueling outages without leading to a significant increase in the risk. Nevertheless, the risk increase due to maintenance and test activities must be kept to an acceptable level. This is often done with use of Risk Monitors. They are now in operation at a very large number of plants and this is one of the most widely accepted PSA applications. They are being used on a day to day basis in making decisions on plant safety issues relating to maintenance activities. They have generally been introduced to provide a tool for addressing maintenance rules e.g. the US rule 50.65 (a)(4). The Risk Monitors are used:

- to avoid simultaneous components unavailability that would lead to a high point-in-time risk;
- to plan the maintenance outages over a period of time to minimize any risk increases; and
- to monitor the plant performance over time by addressing the cumulative risk.

There are a number of Risk Monitor software packages that are commercially available such as the Safety Monitor, EOOS, and RiskWatcher. In addition, other software packages have been produced and are in use in some countries - for example, the Taipower Integrated Risk Monitor (TIRM-2) in Taiwan and the Essential System Outage Program (ESOP) in the UK.

To optimize pipes inspection programmes, Risk-Informed In-Service Inspection is being carried out for a number of plants. Both the Westinghouse and the EPRI methodologies are being applied. The U.S. NRC has also approved RI-ISI programmes based, in part, on ASME Code Case N-716 identifying segments that are generically considered high-safety-significant (HSS). A flooding PSA is then used to identify any additional, plant specific HSS segments.

[From ASAMPSA_E]

This topic has not been discussed in the ASAMPSA_E project because “extended PSAs” are not yet a common practice, and insights related to plant operation and SSCS management are not yet available. Nevertheless PSA scope extension may modify some conclusions of PSA applications described above. This topic may need additional considerations.

7.5 PSA CONTRIBUTES TO PLANT OPERATING EXPERIENCE ANALYSIS

[From NEA/CSNI/R(2012)11, ch 7, [104]]

The analysis of operating events using the PSA is carried out in many countries as part of the analysis of operating experience. The process usually involves a deterministic screening process to identify the significant events and

the PSA is then used to determine the extent to which safety margins were reduced. This indicated the relative seriousness of the event. For example, the U.S. NRC uses PSA models to support decisions regarding the appropriate response to a reported incident. The value of Conditional Core Damage Probability (CCDP) is considered when determining the type of inspection team to send.

PSA results may also be used to set up performance indicators regarding plant safety. For example, the Mitigating Systems Performance Index is proposed to follow safety systems unavailability in the US plants. In Canada, the PSA model is used to derive reliability models for the important systems in order to report on the reliability of these systems.

[From ASAMPSA_E]

This topic was not discussed formally during the ASAMPSA_E project. Nevertheless it seems clear that an extended PSA, if available, should lead to a better diagnostic on the relative seriousness of an event. Other considerations (like simplicity of the PSA model) can also be important in such activity.

7.6 THE RISK INFORMATION PROVIDED BY THE PSA IS INCREASINGLY BEING USED BY REGULATORY AUTHORITIES IN PLANNING THEIR ACTIVITIES

[From NEA/CSNI/R(2012)11, ch 7, [104]]

This includes:

- the prioritization of inspection tasks so that they focus on risk significant issues;*
- determining the significance of inspection findings; and*
- the response to non-compliances.*

An example of this is the Reactor Oversight Program (ROP) carried out by US NRC. Similar processes to this are carried out in other countries.

In Finland, the decommissioning-related risks are analyzed by the regulator (STUK) to ensure risk-informed NPP decommissioning.

A risk informed approach is used in a number of countries as an input to changing the regulations. In the USA, this approach has been used to change the regulations relating to: fire protection, combustible gas control, emergency core cooling system requirements and pressurized thermal shock.

Details of how these changes were made are given in the country responses (see Appendix B [of [104]]).

[From ASAMPSA_E]

Extended PSA, if available, could obviously be useful for the regulatory authorities in planning their activities.

7.7 APPLICATION OF EXTENDED PSA RESULTS FOR RISK REDUCTION “AS LOW AS REASONABLY ACHIEVABLE”

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 [13]. There are some (country-specific) versions of this approach, e.g. to reduce risks as low as reasonably practicable (ALARP) [32] 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. 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. Thus, the demonstration of ALARA often amounts to performing a RIDM process. 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.³

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.

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.

³ 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.

8 LIMITS FOR EXTENDED PSA DEVELOPMENT AND APPLICATIONS

At the end of the ASAMPSA_E project it would be unreasonable to recommend routine development and application of so call extended PSA. The following remarks, coming from the exchanges with the PSA End-Users [8] or [107] can be formulated.

Remark 1

An extended PSA is still an objective to be reached and today no NPPs site has a PSA that covers:

- all reactors initial state,
- all sources of radioactivity
- all possible type of initiating events (internal and external)
- multi-unit accident management

This questions both the regulators and the operators on the relevance of existing PSA. In any case, there is a large space for PSA developments.

Remark 2

The ASAMPSA_E project recommends, among other metrics, calculating “global risk metrics” with extended PSA. Unfortunately, the data quality of the different parts of a PSA can be highly heterogeneous. For rare natural events (high magnitude earthquake frequency, correlated extreme weather conditions ...) the uncertainties on initiating events frequencies are expected to be very large.

For some PSA End-Users, it is more relevant to separate clearly the PSAs (internal events PSA for reactor and spent fuel storage, earthquake PSA, flooding PSA, fire PSA, extreme weather PSA,...) and analyse independently the lessons of each part of the extended PSA.

The uncertainties in PSA have always been an issue for the PSA development, result communication and applications for decision-making. Their quantification needs in general a very high level of expertise but the remaining uncertainties must be acknowledged and taken into account.

Remark 3

For natural hazards, the geosciences may not yet provide good solutions to calculate frequency and features of rare natural events for PSA, for example:

- earthquake predictions are mainly based on seismic historical data and on limited views on possible active faults displacement,
- extreme weather conditions are identified as a possible significant contributor to the risk of accident but limited methodologies are available to assess the frequencies of the worst cases (combined / correlated events).

Geosciences progresses for rare extreme natural events modelling are highly desirable for “routine” application in PSAs.

Remark 4

For external hazards, the “extended” PSA analyst shall consider a global picture with the neighbouring threats around the site (cliff-edge for flooding (sea, river, dam failure, rain impacts, combination), other industrial facilities, transports, dam, ...). Simplified approach may be relevant to get first insights.

Remark 5

Following PSA End-Users recommendations, the ASAMPSA_E partners have considered earthquake, flooding, extreme weather, lightning, biological hazards, aircraft craft and man-made hazards. For all these hazards, it appears that methodologies for hazards impacts assessment were available (e.g fragility curves) except for (beyond design) lightning impact assessment.

Lightning impact is not considered in general in PSA and the risk significance of lightning and methodologies to address it, remains an open issue.

Remark 6

Following PSA End-Users opinions, 2 objectives can be considered for screening:

- to identify the hazard events that contribute to the risks,
- to identify the hazard events for which it is useful to develop a PSA

During the screening process, it can be concluded that a hazard event is “risk significant” but that a PSA development is not relevant, for example in case of low data quality. In that case, this should be indicated in the PSA summary report and some NPP reinforcements may be discussed without any PSA contribution. The appendix 2 provides information on an IAEA TECDOC on assessment of vulnerabilities of operating nuclear power plants to extreme external events.

9 CONCLUSION

The report provides an overview of the considerations in the ASAMPSA_E project for extended PSA applications and decision-making.

It appears that screening methodology is an area where harmonization of practices is possible. Concerning risk metrics, safety objectives formulation, verification (with PSA) the defence-in-depth concept, many differences can exist depending on the countries or stakeholders.

There are also limitations in the state-of-art technology and knowledge to develop extended PSA, but when examining the PSA applications at a general level for NPPs safety improvements, development of extended PSA, as far as possible, is expected to improve the quality of PSA applications and of risk informed decision making.

10 LIST OF REFERENCES

- [1] “Advanced Safety Assessment : Extended PSA”, ASAMPSA_E Description of Work, 2013, Grant agreement 605001
- [2] ASAMPSA_E D30.2, “Lessons of the Fukushima Dai-ichi accident for PSA”, Technical report ASAMPSA_E/WP30/D30.2/2017-32, Reference IRSN PSN-RES/SAG/2017-00021, January 2017
- [3] ASAMPSA_E D30.7 volume 2, “Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA”, Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 2, Reference IRSN PSN-RES/SAG/2017-00017, January 2017
- [4] ASAMPSA_E, “Risk Metrics and Measures for an Extended PSA”, Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 3 Reference IRSN PSN-RES/SAG/2017-00018
- [5] ASAMPSA_E D30.7 volume 4, “The Link between the Defence-in-Depth Concept and Extended PSA”, Technical report ASAMPSA_E/D30.7/2017-31 volume 4-Reference IRSN PSN/RES/SAG/2017-00019
- [6] ASAMPSA_E D30.7 volume 5, “The PSA assessment of Defense in Depth - Memorandum and proposals, Technical report ASAMPSA_E/D30.7/2017-31 volume 5 - Reference IRSN PSN/RES/SAG/2017-00020
- [7] 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
- [8] ASAMPSA_E, “Synthesis report of the End-Users survey and review of ASAMPSA_E guidance, and final workshop conclusions. Identification of follow-up useful activities after ASAMPSA_E”, Technical report ASAMPSA_E/WP10/D10.5/2017-40, IRSN PSN-RES/SAG-2017-00003
- [9] 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.
- [10] 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.
- [11] ASAMPSA_E, List of External Hazards to be Considered in Extended PSA, ASAMPSA_E D21.2, December 2014, Decker, K., H. Brinkmann
- [12] 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
- [13] International Atomic Energy Agency (IAEA), “Fundamental Safety Principles”, Safety Fundamentals No. SF-1, November 2006
- [14] International Atomic Energy Agency (IAEA), “Safety of Nuclear Power Plants: Design”, Specific Safety Requirements No. SSR-2/1 (Rev. 1), Vienna 2016
- [15] International Atomic Energy Agency (IAEA), “Deterministic Safety Analysis for Nuclear Power Plants”, Specific Safety Guide No. SSG-2, December 2009.
- [16] 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
- [17] 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
- [18] International Atomic Energy Agency (IAEA), “Safety Assessment for Facilities and Activities”, General Safety Requirements Part 4 No GSR Part 4 (Rev. 1), Vienna 2016

- [19] 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
- [20] International Atomic Energy Agency (IAEA), “Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status”, IAEA-TECDOC-1436, February 2005
- [21] International Atomic Energy Agency (IAEA), “Terminology Used in Nuclear Safety and Radiation Protection”, IAEA Safety Glossary, 2007 Edition, June 2007.
- [22] U.S. Nuclear Regulatory Commission, “A Proposed Risk Management Regulatory Framework”, NUREG-2150, April 2012
- [23] U.S. Nuclear Regulatory Commission, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-informed Decision Making”, draft report for comment, NUREG-1855, Rev. 1, March 2013
- [24] US NRC, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance”, RG 1.201 Rev. 1, May 2006.
- [25] U.S. NRC, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors”, 10 CFR 50.69, 2004.
- [26] GIF/RSWG/2007/002/Rev.1 - Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems; November 2008.
- [27] GIF/RSWG/2010/002/Rev.1 - An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems; June 2011.
- [28] 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
- [29] 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
- [30] Kuzmina, I., A. Lyubarskiy, M. El-Shanawany, “An Approach for Systematic Review of the Nuclear Facilities Protection against the Impact of Extreme Events”, Nordic PSA Conference, Castle Meeting 2011, September 2011
- [31] Kuzmina, I., A. Lyubarski, P. Hughes, J. Klügel, T. Koslik, V. Serebrjakov, “Fault Sequence Analysis Method to Assist in Evaluation of the Impact of Extreme Events on NPP“, Nordic PSA Conference - Castle Meeting 2013, April 2013
- [32] Health and Safety Executive (HSE), “Reducing Risks, Protecting People, HSE’s Decision-Making Process”, HSEBooks, 2001
- [33] OECD Nuclear Energy Agency, “Probabilistic Risk Criteria and Safety Goals”, NEA/CSNI/R(2009)16, December 2009
- [34] P. Hellström, “DiD-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA”, SSM 2015:04, January 2015.
- [35] Holmberg, J., J. Nirmark, “Risk-informed Assessment of Defence in Depth, LOCA Example, Phase 1: Mapping of Conditions and Definition of Quantitative Measures for the Defence in Depth Levels”, Rev. 0, SKI report 2008:33, February 2008.
- [36] Hellström, P. M. Knochenhauer, R. Nyman, “SSM Research Project on Defence-in-Depth PSA - Assessing Defence-in-Depth Levels with PSA Methods” in: 10th International Probabilistic Safety Assessment and Management Conference (PSAM10), 2010.

- [37] 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
- [38] Apostolakis, G., "Safety Goals and Risk-Informed Regulation at the U.S. NRC", Presentation to Canadian Nuclear Safety Commission, Ottawa, Canada, January 2014
- [39] Autoridad Regulatoria Nuclear, "Criterios Radiológicos Relativos a Accidentes en Reactores Nucleares de Potencia", Revisión 2, AR 3.1.3, 2002
- [40] Aven, T., "On the Ethical Justification for the Use of Risk Acceptance Criteria", Risk Analysis, Vol. 27, Issue 2, (2007), p. 303-312
- [41] Aven, T., B. Heide, "Reliability and Validity of Risk Analysis", Reliability Engineering and System Safety, Vol. 94, (2009), p. 1862-1868
- [42] Aven, T., "On How to Define, Understand and Describe Risk", Reliability Engineering and System Safety, Vol. 95, Issue 6 (2010), p. 623-631
- [43] Aven, T., "The Risk Concept - Historical and Recent Development Trends", Reliability Engineering and System Safety, Vol. 99, (2012), p. 33-44
- [44] Aven, T., "Foundational Issues in Risk Assessment and Risk Management", Risk Analysis Vol. 32, Number 10, 2012, p. 1647 - 1656
- [45] 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
- [46] Ball, D.J., J. Watt, "Further Thoughts on the Utility of Risk Matrices", Risk Analysis, Vol. 33, No. 11 (2013), p. 2068 - 2078
- [47] 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
- [48] Cox, L.A., "Does Concern-Driven Risk Management Provide a Viable Alternative to QRA?", Risk Analysis, Vol. 27, Issue 1, (2007), p. 27-43
- [49] Cox, L.A., D.A. Popken, "Some Limitations of Aggregate Exposure Metrics", Risk Analysis, Vol. 27, Issue 2, (2007), p. 439-445
- [50] Cox, L.A., "What's Wrong with Risk Matrices", Risk Analysis Vol. 28 No. 2 (2008), p. 497-512
- [51] 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
- [52] 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
- [53] Holmberg, J., M. Knochenhauer, "Probabilistic Safety Goals Phase 3 - Status Report", NKS-195, July 2009
- [54] 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
- [55] Johansen, I.L., M. Rausand, "Foundations and Choice of Risk Metrics", Safety Science, Vol. 62, (2014), p. 386-399
- [56] 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

- [57] 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
- [58] Kaplan, S., B.J. Garrick, "On the Quantitative Definition of Risk", Risk Analysis, Vol. 1 No. 1 (1981), p. 11-27
- [59] Paté-Cornell, M.E., "Uncertainties in Risk Analysis", Reliability Engineering and System Safety, Vol. 54 Issue 2-3, December 1996, p. 95-111
- [60] 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
- [61] 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
- [62] 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
- [63] 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
- [64] Van der Borst, M., H. Schoonakker, "An Overview of PSA Importance Measures", Reliability Engineering and System Safety, Vol. 72 (2001), p. 241-245
- [65] Vasseur, D, M. Llory, "International Survey on PSA Figures of Merit", Reliability Engineering and System Safety, Vol. 66, (1999), p. 261-274
- [66] 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
- [67] Vrijling, J.K, W. van Hengel, R.J. Houben, "A Framework for Risk Evaluation", Journal of Hazardous Materials, Vol. 43 (1995), p. 245-261
- [68] Einarsson, S., A. Wielenberg, "Vorschlag für eine bundeseinheitliche Anwendung von IRIDM-Verfahren bei sicherheitstechnischer Entscheidungsfindung", GRS-A-3666, Cologne, September 2012
- [69] NASA, "Risk Management Handbook", Version 1.0, NASAA/SP-2011-3422, November 2011
- [70] Grechuk, B. M. Zabaranin, "Risk Averse Decision Making under Catastrophic Risk", European Journal of Operational Research, Vol. 239 (2014), p. 166-176
- [71] Cha, E.J., B.R. Ellingwood, "The Role of Risk Aversion in Nuclear Plant Safety Decisions", Structural Safety Vol. 44 (2013), p. 28-36
- [72] Ersdal, G., T. Aven, "Risk Informed Decision-making and its Ethical Basis", Reliability Engineering and System Safety, Vol. 93, (2008), p. 197-205
- [73] Hartford, D.N.D., "Legal Framework Considerations in the Development of Risk Acceptance Criteria", Structural Safety, Vol. 31 (2009), p. 118-123
- [74] Tversky, A., D. Kahneman, "Advances in Prospect Theory: Cumulative Representation of Uncertainty", Journal of Risk and Uncertainty, Vol. 5 (1992), p. 297-323
- [75] Berg, M. et al., "Risikobewertung im Energiebereich", Polyprojekt Risiko und Sicherheit Dokumente Nr. 7, Zürich, 1995

- [76] Lind, N.C. (ed.), “Technological Risk”, Proceedings of a Symposium on Risk in New Technologies 15 December 1981, University of Waterloo, Waterloo, Ontario, 1982
- [77] U.S. NRC, “White Paper on Risk-informed and Performance-based Regulation”, SECY-98-144, March 1999
- [78] Bundesministerium für Umwelt und Naturschutz (BMU), “Sicherheitsanforderungen an Kernkraftwerke” of 22 November 2012 (BAnz AT 24.02.2013 B3)
- [79] 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
- [80] Wint, S.M.E., “An Overview of Risk”, RSA Risk Commission, ca. 2006
- [81] 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
- [82] Artzner, P., J. Eber, D. Heath, “Coherent Measures of Risk”, Mathematical Finance, Vol. 9, No. 3 (1999), p. 203-228
- [83] Frittelli, M., E.R. Gianin, “Putting Order in Risk Measures”, Journal of Banking and Finance 26 (2002), p. 1473-1486
- [84] Cox, L.A., “Why Risk is Not Variance: An Expository Note”, Risk Analysis, Vol 28 (2008), p. 925-928
- [85] Wikimedia Foundation, “Risk metric”, version 7 December 2014, http://en.wikipedia.org/wiki/Risk_metric
- [86] 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>
- [87] 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
- [88] B. Obama, “Remarks by the President in a Press Conference” from 19 December 2012, Press Office of the White House, December 2012 (published online)
- [89] WENRA, “Safety of New NPP Designs, Study by Reactor Harmonization Working Group RHWG”, March 2013
- [90] IAEA, OECD/NEA, “INES The International Nuclear and Radiological Event Scale User’s Manual, 2008 Edition”, Vienna, amended version March 2013
- [91] INSAG, Basic Safety Principles for Nuclear Power Plants; 75-INSAG-3 Rev. 1 - INSAG-12; 1999
- [92] Western European Nuclear Regulators Association (WENRA), “WENRA Safety Reference Levels for Existing Reactors”, September 2014
- [93] 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
- [94] M. Borysiewicz, K. Kowal, S. Potempski, 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
- [95] Mustajoki J, Hamalainen RP. Web-HIPRE: Global decision support by value tree and AHP analysis. INFOR 2000;38(3):208-220.
- [96] Berg HP. Quantitative safety goals and criteria as a basis for decision making. Reliability: Theory & Applications 2010;17(2):62-78.

- [97] International Atomic Energy Agency. Safety margins of operating reactors. Analysis of uncertainties and implications for decision making. IAEA-TECDOC-1332, Vienna: IAEA; 2003.
- [98] Office for Nuclear Regulation, Probabilistic Safety Analysis, NS-TAST-GD-030 Revision 4, June 2013
- [99] Wikimedia Foundation, Expected Utility Hypothesis , last accessed 14 June 2016, http://en.wikipedia.org/wiki/Expected_utility_hypothesis
- [100] 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>
- [101] 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>
- [102] Office for Nuclear Regulation, Safety Assessment Principles for Nuclear Facilities, 2014 Edition Revision 0, November 2014
- [103] 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
- [104] OECD Nuclear Energy Agency, “Use and Development of Probabilistic Safety Analysis”, NEA/CSNI/R(2012)11, December 2012
- [105] Vitazkova, J.: Methodology of Common Risk Target Assessment and Quantification for Severe Accidents of Nuclear Power Plants based on INES Scale. Thesis, Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Nuclear and Physical Engineering, Bratislava May 2014.
- [106] “ASAMPSA_E guidance for level 2 PSA -Volume 3. Verification and improvement of SAM strategies with L2 PSA. Technical report ASAMPSA_E/WP40/D40.7/2017-39 volume 3. Reference IRSN PSN/RES/SAG/2017-00001
- [107] E. Raimond, The “Extended PSA” concept: a current challenge for the PSA community - an opportunity for enhancing the NPPs safety? Example of 10 lessons from the ASAMPSA_E project. Presentation at PSAM13 conference, Oct 2016, Seoul, Korea.
- [108] US-NRC, NUREG 1855 rev 1- Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making - final report. March 2017.
- [109] IAEA, Draft TECDOC, 2015, Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events

11 LIST OF TABLES

Table 1.	Distribution of recommendations in D30.2 [2] from the Fukushima Dai-ichi accident.....	16
Table 2.	US-NRC probabilistic criteria [33].....	34
Table 3.	Summary of numerical criteria for CDF [104]	35
Table 4.	Summary of numerical criteria for L(E)RF [104].....	36

12 LIST OF FIGURES

Fig. 1	Screening approach to internal events	21
Fig. 2	Extension of screening approach to hazard scenarios.....	21
Fig. 3	Numerical criteria defined for Core Damage [33]	33
Fig. 4	Numerical criteria defined for large release. (Definition and timing of “large release” varies) [33]	34
Fig. 5	Selected Influencing Inputs to a Decision Maker	57
Fig. 6	Key elements of integrated RIDM approach from INSAG-25 [19], p. 6.....	58
Fig. 7	Simplified value tree diagram developed to support decision-making on nuclear safety [94].....	60
Fig. 8	Roles in RIDM [69], p. 8.....	61
Fig. 9	Hierarchy of Objectives in the Design Process [69], p. 34	62
Fig. 10	Performance objectives and performance measures [69], p. 40.....	62
Fig. 11	Performance measures and performance commitments in RIDM [69], p. 76	63
Fig. 12	Steps for the PSA assessment of DiD and details [6]	67
Fig. 13	Example of Event Tree organized following the structure of the DiD [6]	70
Fig. 14	Example of the possible use of INES-Based safety targets for prioritization of SAM actions	72

APPENDIX 1 - CURRENT UNDERSTANDING OF RIDM APPROACHES

Following ASAMPSA_E report [4], the following limitations on any decision making problem can be pointed out: “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 [75]. 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 [45], [48], [69], [70], [75], [77], [20]. 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 [80]. For the purpose of the ASAMPSA_E project, work on the ethical or legal or theoretical foundations of decision making [40], [72], [73], [74], [75] is clearly out of scope, as is a discussion on cultural influences.”

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 makers. In the end, the decision makers have to decide which aspects of risk and thus which risk measures are relevant for each alternative. This is illustrated in Fig. 5. Therefore, the recommendations in this report have to be understood as options for decision makers. 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.

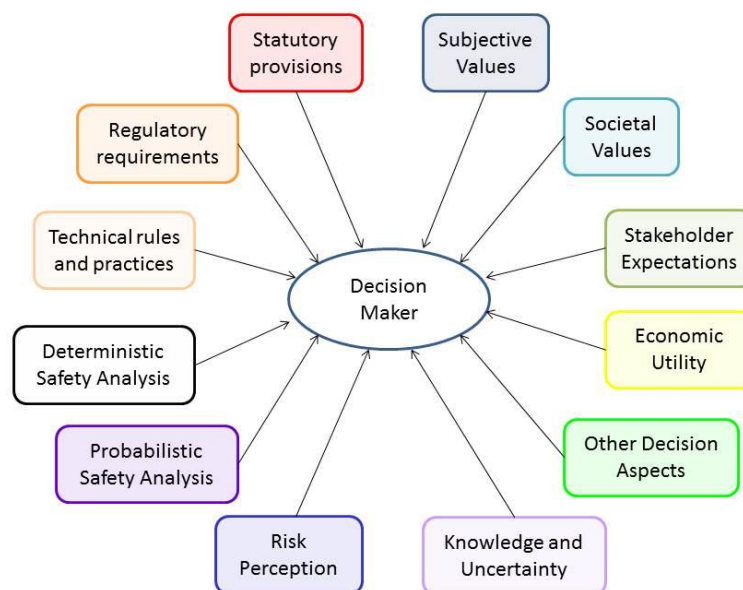


Fig. 5 Selected Influencing Inputs to a Decision Maker

APPENDIX 2 - INSAG-25 (IAEA)

The title of INSAG-25 is “A Framework for an Integrated Risk Informed Decision Making Process” [19]. The basic approach to risk-informed decision making (RIDM) is well described in INSAG-25. INSAG-25 provides a framework to achieve a balance between deterministic approaches, probabilistic analyses and other factors in order to support an integrated decision making process that serves in an optimal fashion to ensure nuclear reactor safety. While the details of IRIDM methods may change with better understanding of the subject, the framework presented in INSAG-25 (published in 2011) is expected to apply for the foreseeable future. Presently, IAEA is in the process of preparing a technical document (“TECDOC”) which aims at providing further details and examples related to IRIDM in line with INSAG-25. It is expected that this TECDOC will be available at the end of 2017.

Fig. 6 illustrates the integrated RIDM approach as defined in INSAG-25. The report identifies key elements of the IRIDM process, the integration of these elements, and the IRIDM process management. The reader is encouraged to directly make himself familiar with this fundamental document.

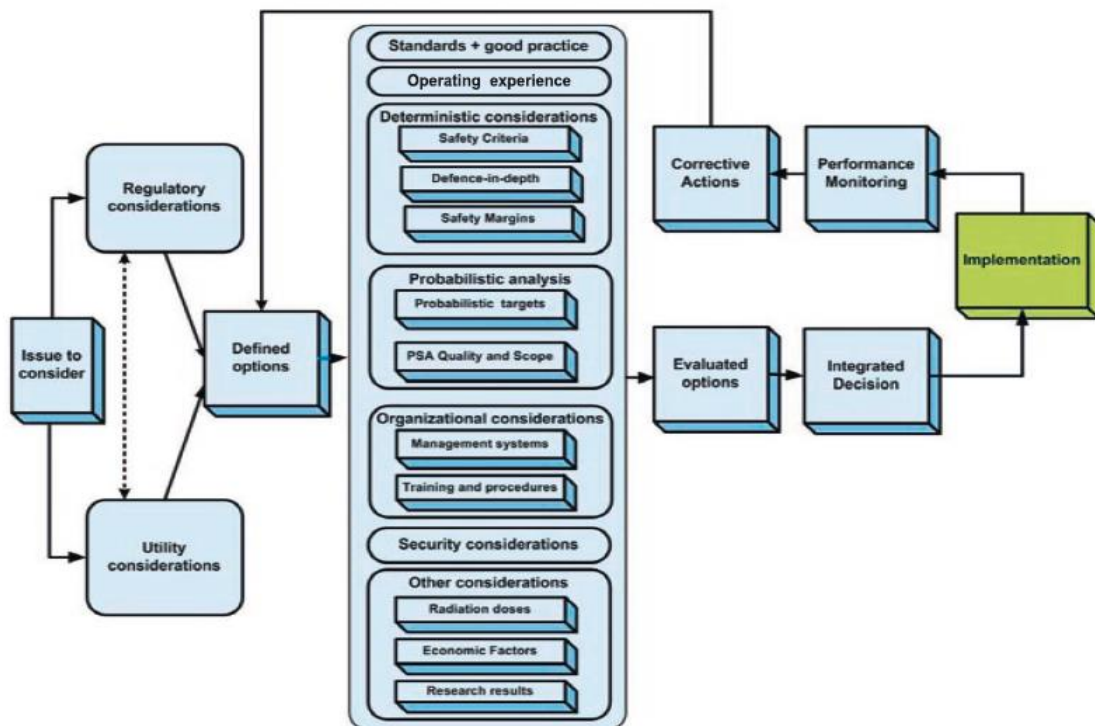


Fig. 6 Key elements of integrated RIDM approach from INSAG-25 [19], p. 6

A.2.1 EXTENSIONS OF RIDM APPROACHES

A.2.1.1 PRACTICAL APPROACH TO THE IMPLEMENTATION OF INTEGRATED RIDM PROCESS

In this section a short description of possible practical approach for the implementation of IRIDM process is given based on paper [94]. This should be understood as an example and not as a common practice.

In order to select optimal options from possible decision strategies, in IAEA guidelines it is proposed to calculate the score S 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 [94].

Implementation of VTA consists of the following steps [95]:

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. 7. 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 a facilitated workshop, in which a 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 [94], [95]. 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.

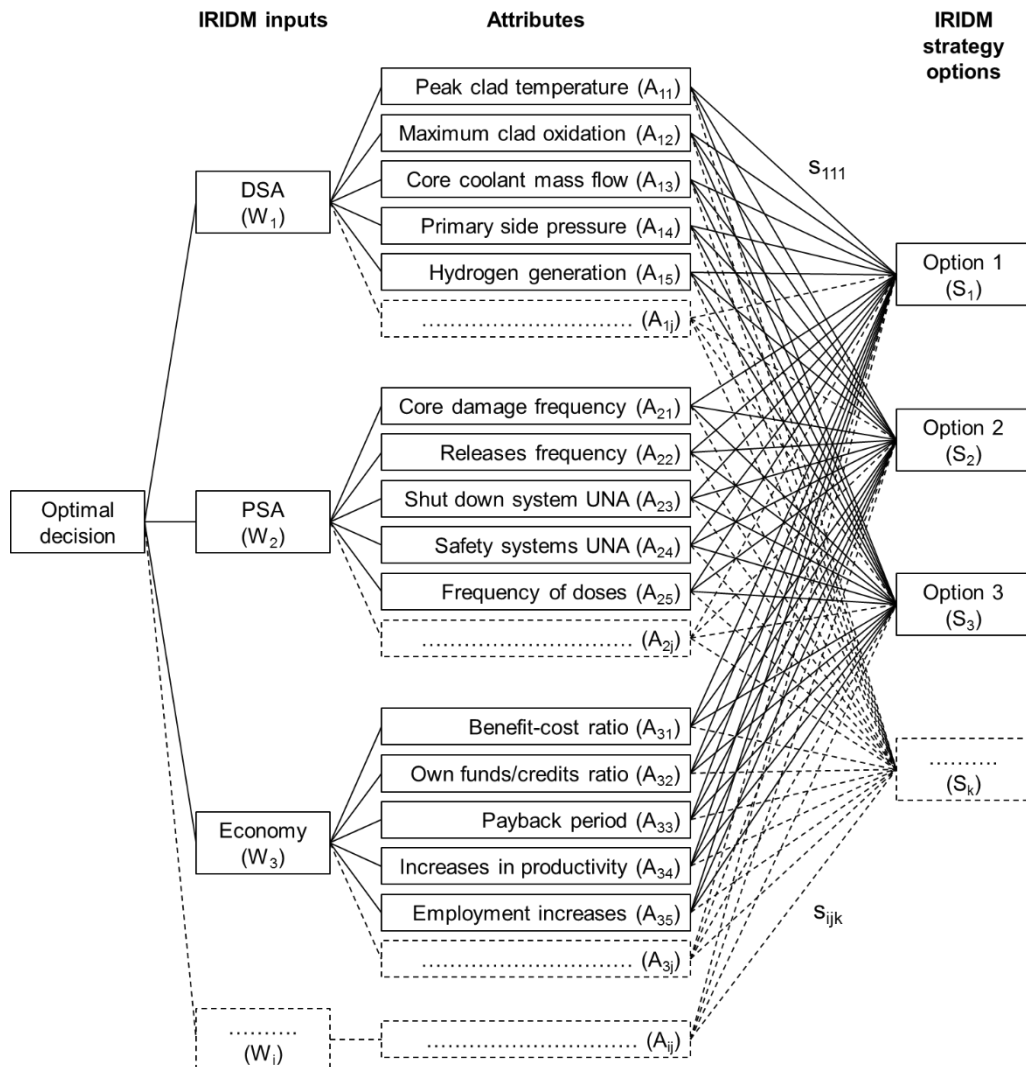


Fig. 7 Simplified value tree diagram developed to support decision-making on nuclear safety [94].

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 [33]. 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).

A.2.1.2 SOME INSIGHTS FROM NASA'S RIDM HANDBOOK

The Risk Informed Decision Making Handbook by NASA [69] 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 [69] clearly describes role and responsibilities in the RIDM process (during design), cf. Fig. 8. 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 maker 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.

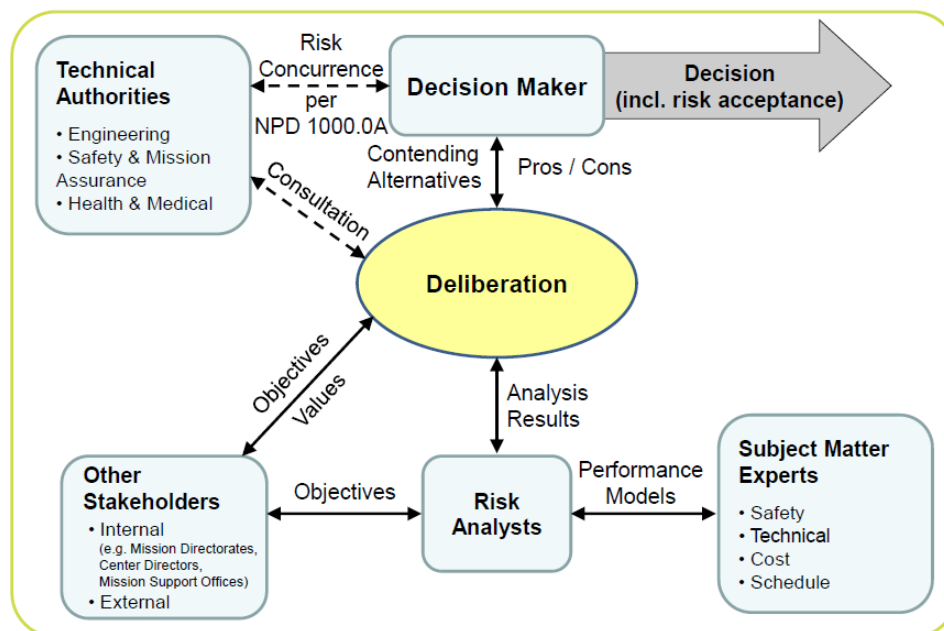


Fig. 8 Roles in RIDM [69], p. 8

For the design, NASA's RIDM Handbook [69] specifically mentions that a hierarchy of (design) objectives should be developed, cf. Fig. 9. 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. 10.

With regard to performance measures, these include e.g. that 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.

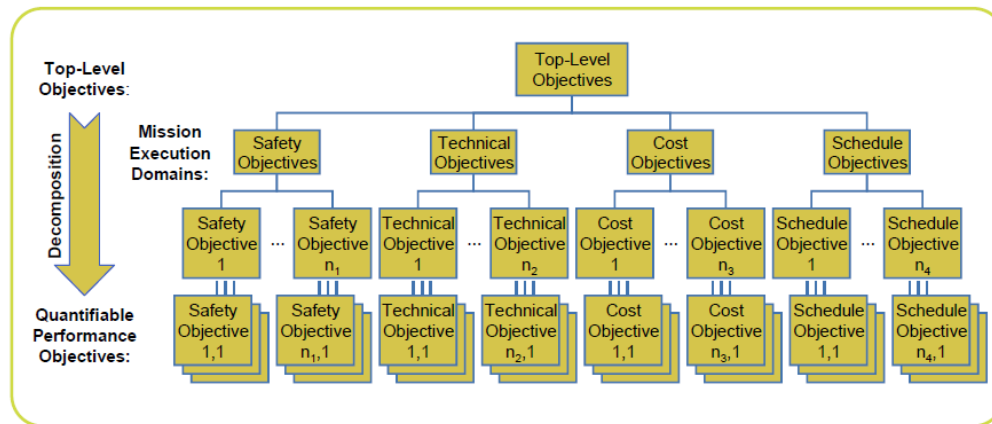


Fig. 9 Hierarchy of Objectives in the Design Process [69], p. 34

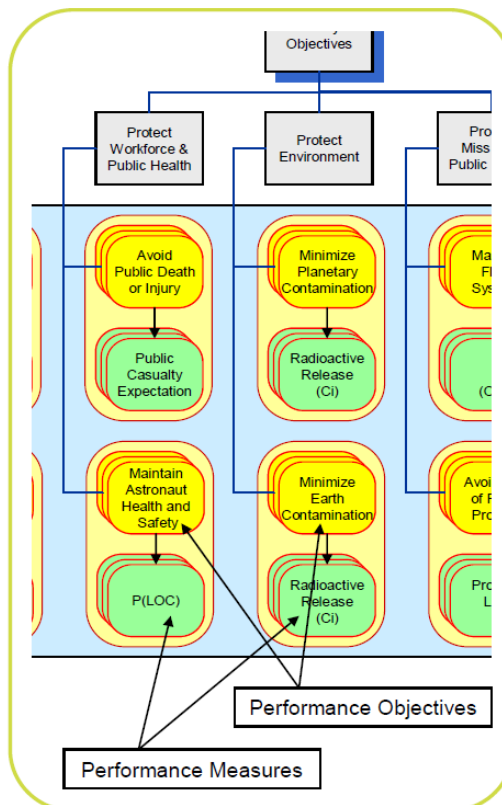


Fig. 10 Performance objectives and performance measures [69], p. 40

Importantly, each performance commitment corresponds to an accepted level of risk (cf. Fig. 11) 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 using a risk normalization procedure [69] 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 NPP⁴.

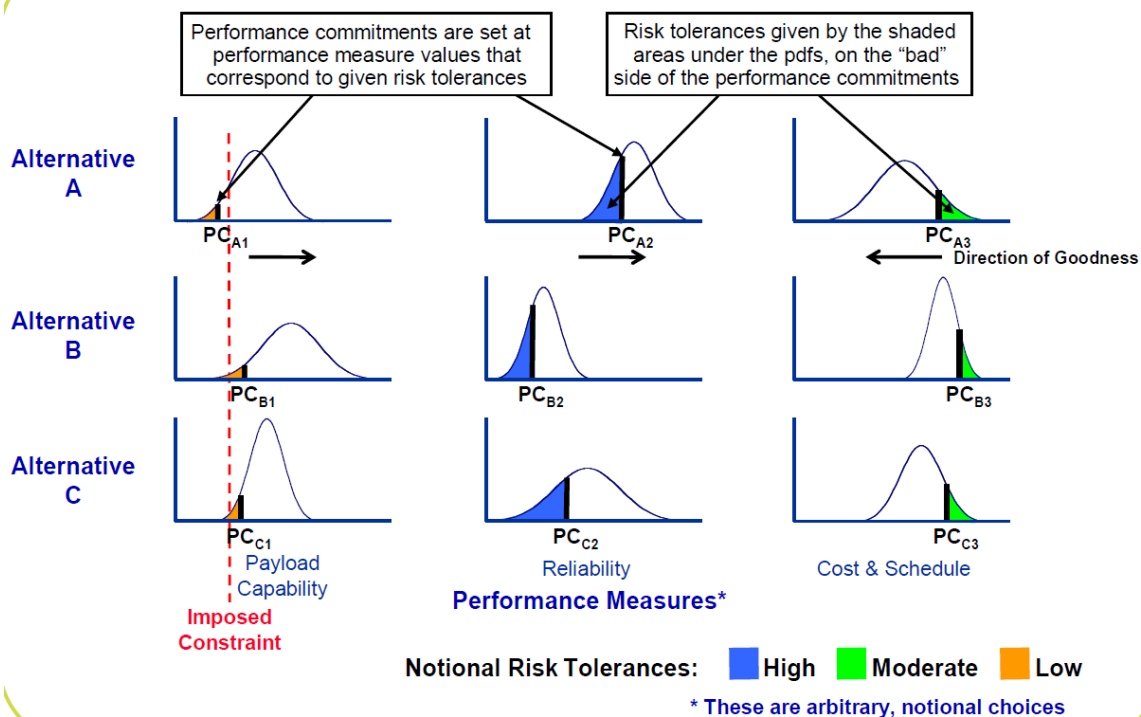


Fig. 11 Performance measures and performance commitments in RIDM [69], p. 76

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. NASA's RIDM Handbook [69] clearly explains that all these aspects of the decision (termed performance measures and related objectives or commitments) are uncertain and contribute (to

⁴ 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.

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.

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 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." [69], 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.

APPENDIX 3 - VULNERABILITY OF NPPS ACCORDING TO RECENT IAEA TECDOC

IAEA has developed a draft TECDOC on assessment of vulnerabilities of operating nuclear power plants to extreme external events [108]. The TECDOC is still under development and not released publicly, however it contains several sections of interest and discussions. This section provides a short summary of IAEA TECDOC. The TECDOC is focused on identifying what can go wrong in an existing installation when external events exceed the design basis, while looking at the lesson learned from the Fukushima Dai-ichi accident. The TECDOC stressed to perform assessments to review the response of the installation “as-is” against extreme external events and identifying the “weak links” i.e. “vulnerabilities”. The purpose of the methodology presented in the IAEA TECDOC is as follows:

- *Identify the plant “weak links” for the applicable extreme external events, that is, the structures, systems and components (SSCs) more vulnerable to external events exceeding the plant design basis;*
- *Determine the severity of the external event below which there is a high confidence that the “weak links” will not fail;*
- *Explore the plant response when those “weak links” fail and estimate the time frame until reaching fuel damage, together with the SSCs governing the time frame.*

This methodology is intended to be used for existing nuclear power plants in their “as-is” condition i.e. an installation refers to the present state and actual conditions of the facility, considering the “as-built”, “as-operated” and “as-maintained” state of SSCs.

The methodology covers the impact of all types of external events, both natural and human induced, except for willful human induced hazards (i.e. not accidental), such as military action or industrial sabotage. The methodology does not assess the accident management.

A general workflow is proposed, which starts from a comprehensive list of potential external hazards. By using a given set of screening criteria and conservative bounding analyses, the list is screened in order to eliminate from the assessment those hazards that do not need to be analyzed further. The screening criteria and bounding analyses are similar to those used in other contexts related with design or safety assessment referring to WENRA, IAEA and US NRC guidelines. The low frequency of occurrence cannot be used to screen - out a hazard.

For each of the applicable external hazards, the next step is to identify the SSCs required to maintain the fundamental safety functions in case of an event derived from the hazard. The “success path” approach and the “event tree - fault tree” approach is in current practice for assessment of beyond design basis external events.

The next step of the methodology is based on deterministic analysis in which assessment assumes failure of the weak links and looks into the plant response to those failures, taking into account the likely conditions of the site after the extreme event (e.g. site devastation, access routes cut-off) and considering auxiliary or movable equipment included in the plant procedures that might remain available.

The methodology will then identify the vulnerabilities against the applicable extreme external events. However, unless the results of the corresponding probabilistic hazard assessments are available, the methodology will not be able to provide any indication about the actual risk posed for the installation. It is expected that the easy fixes of weak links will be implemented without further considerations. But, as mentioned above, the decision about whether a major fix has to be implemented should normally be based on the comparison between the actual risk and the safety goals established at each Member State.

When the results of probabilistic hazard assessments are available (hazard curves), the plant level capacity obtained for each applicable hazard could be used to obtain a point estimate for the annual frequency of the hazard causing safety significant damage. For each hazard, the approach involves the computation of a plant-level fragility curve from the high confidence plant-level capacity and the convolution of this fragility curve with the mean hazard curve. This approach has already been followed by regulators in some Member States to obtain quick risk estimates.

The TECDOC discussed the methodology for five specific hazards: earthquake, high winds, flood, aircraft impact and explosion/hazardous releases those has been considered in the ASAMPSA_E hazard specific topical reports. The consideration of combination of hazards is stressed based on the credibility for the site and associated common physical phenomenon. Examples of earthquake combined with other hazards are given, however it is not discussed how to selected combination of hazards, what are the co-relation between them and how this combination could impact the NPPs. ASAMPSA_E project proposed a hazard correlation chart with a detailed list of possible combination of ASAMPSA_E selected hazards, which has been elaborated in ASAMPSA_E topical hazard reports. Similarly there is no guidance in IAEA TECDOC on how to handle the screening during the combination of hazards. ASAMPSA_E report on screening provides a systematic framework on screening approach for both individual and combined hazards.

IAEA TECDOC is useful for assessment of plant capacity using the deterministic and semi-probabilistic approaches. It provides interesting insights to obtain risk estimates, namely, the hazard assessment, the computation of a plant-level fragility curve, and the convolution of hazard and fragility.

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

“... 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 [...].”

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.”

In [6], 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. Based on these consideration, event trees can be derived along the lines of DiD. Fig. 13 illustrates this concept.

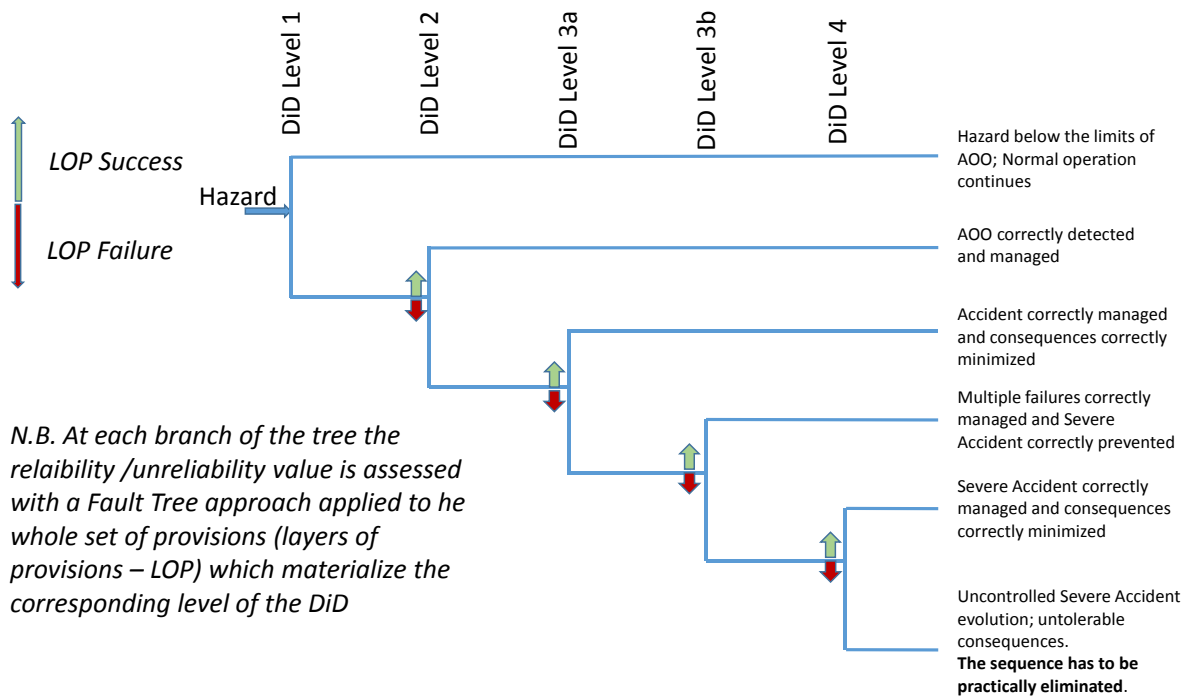


Fig. 13 Example of Event Tree organized following the structure of the DiD [6]

APPENDIX 5 - EXAMPLE FOR THE “CRT” APPLICATION

This section provides an example of application of the concept common risk target (CRT) introduced in section 6.3.2.

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 (the “CRT”) had been applied from the onset, a clearer response had been given. This is illustrated in Fig. 14. 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.

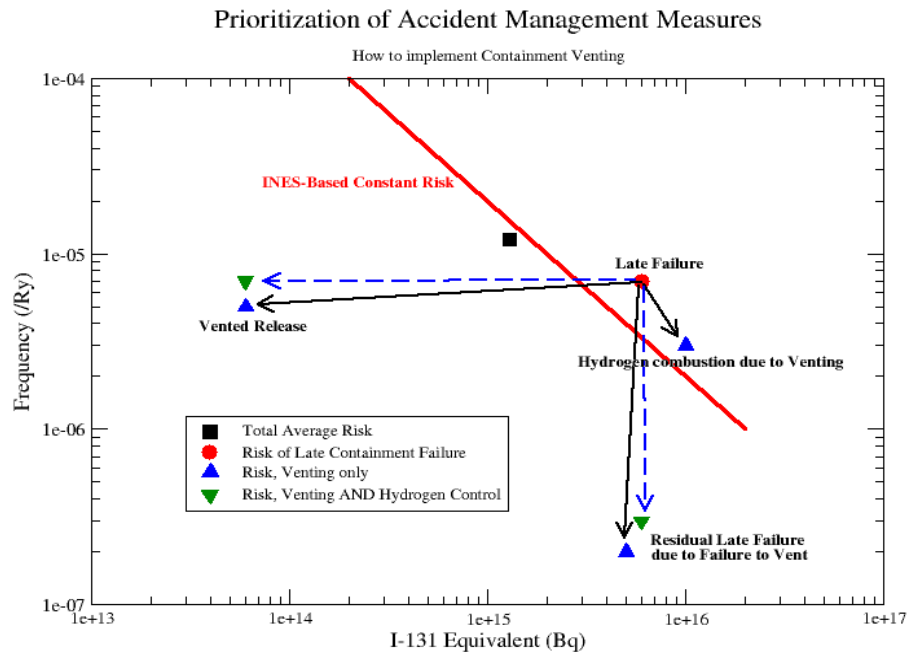


Fig. 14 Example of the possible use of INES-Based safety targets for prioritization of SAM actions