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

"NUCLEAR FISSION "
Safety of Existing Nuclear Installations

Contract 605001

**Summary report of already existing guidance on the
implementation of External Hazards in extended Level 1 PSA**

Reference ASAMPSA_E
Technical report ASAMPSA_E / WP22 / D22.1 / 2015-11
Reference IRSN PSN/RES/SAG/ 2015-00235




J. Klug (LRC), M. Kumar (LRC), J. Prochaska (VUJE), P. Brac (EDF), D. Vasseur (EDF),
H. Brinkman (NRG), S. Kahia (NRG), M. Nitoi (INR), M. Apostol (INR), G. Georgescu
(IRSN), A. Volkanovski (JSI), J. Mustoe (AMEC), R. Alzbutas (LEI), S. La Rovere (NIER)

Period covered: from 01/07/2013 to 30/11/2014	Actual submission date:	
Start date of ASAMPSA_E: 01/07/2013	Duration: 36 months	
WP No: 22	Lead topical coordinator : Joakim Klug	His organization name : Lloyd's Register Consulting

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

ASAMPSA_E Quality Assurance page

Partners responsible of the document : LRC, VUJE, EDF, NRG, INR, IRSN	
Nature of document	Technical report
Reference(s)	Technical report ASAMPSA_E/ WP22 / D22.1 / 2014-05 Rapport IRSN-PSN-RES/ SAG/2015-00235
Title	Summary report of already existing guidance on the implementation of External Hazards in extended Level 1 PSA
Author(s)	J. Klug (LRC), M. Kumar (LRC), J. Prochaska (VUJE), P. Brac (EDF), D. Vasseur (EDF), H. Brinkman (NRG), S. Kahia (NRG), M. Nitoi (INR), M. Apostol (INR), G. Georgescu (IRSN), A. Volkanovski (JSI), J. Mustoe (AMEC), R. Alzbutas (LEI), S. La Rovere (NIER)
Delivery date	August 2015
Topical area	Level 1 PSA, Extended PSA, external hazards, correlation
For Journal & Conf. papers	No
<p>Summary :</p> <p>This document is a summary of already existing guidances on the implementation of external hazards in extended level 1 PSA. It is a deliverable of the ASAMPSA_E project, in the framework of the work package WP22 : 'How to introduce hazards in L1 PSA and all possibilities of events combinations'. This workpackage shall promote exchanges and identify some good practices on the implementation of external events in an existing (internal events) L1 PSA (event trees), having as a perspective the development of extended PSA.</p> <p>The four following topics are associated to the workpackage WP22 :</p> <ol style="list-style-type: none"> 1) Impact of external events on the SSCs modelled in L1 PSA event trees, 2) Impact of external events on Human Reliability Assessment modelling in L1 PSA, 3) Modelling site impact in L1 PSA event trees, 4) Link between external initiating events of PSA and NPP design basis conditions. 	

Visa grid			
	Main author(s) :	Verification	Approval (Coordinator)
Name (s)	J. Klug, M. Kumar	WP22 partners	E. Raimond
Date	26-08-2015	Remarks (by e-mails) have been taken into account.	26-08-2015
Signature			

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
1	2014-12-15	J. Klug (LRC), M. Kumar (LRC), J. Prochaska (VUJE), P. Brac (EDF), D. Vasseur (EDF), H. Brinkman (NRG), S. Kahia (NRG), M. Nitoi (INR), M. Apostol (INR), G. Georgescu (IRSN), A. Volkanovski (JSI), J. Mustoe (AMEC), R. Alzbutas (LEI), S. La Rovere (NIER)		Initial version for approval before delivery by the project.
2	2015-07-17	E. Raimond	All	Editorial modifications for delivery.
3	2015-08-25	M. Kumar, E. Raimond	Details	Editorial modifications

LIST OF DIFFUSION

European Commission (scientific officer)

Name	First name	Organization
Passalacqua	Roberto	EC

ASAMPSA_E Project management group (PMG)

Name	First name	Organization	
Raimond	Emmanuel	IRSN	Project coordinator
Guigueno	Yves	IRSN	WP10 coordinator
Decker	Kurt	Vienna University	WP21 coordinator
Klug	Joakim	LRC	WP22 coordinator
Wielenberg	Andreas	GRS	WP30 coordinator
Loeffler	Horst	GRS	WP40 coordinator

REPRESENTATIVES OF ASAMPSA_E PARTNERS

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

Name	First name	Organization
Karlsson	Anders	FKA
Ljungbjörk	Julia	FKA
Pihl	Joel	FKA
Loeffler	Horst	GRS
Mildenberger	Oliver	GRS
Sperbeck	Silvio	GRS
Tuerschmann	Michael	GRS
Wielenberg	Andreas	GRS
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Serrano	Cesar	IEC
Apostol	Minodora	INR
Nitoi	Mirela	INR
Groudev	Pavlin	INRNE
Stefanova	Antoaneta	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

Name	First name	Organization
Rebour	Vincent	IRSN
Sotti	Oona	IRSN
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Matuzas	Vaidas	LEI
Rimkevicius	Sigitas	LEI
Häggström	Anna	LRC
Klug	Joakim	LRC
Knochenhauer	Michael	LRC
Kumar	Manorma	LRC
Olsson	Anders	LRC
Borysiewicz	Mieczyslaw	NCBJ
Kowal	Karol	NCBJ
Potemski	Slawomir	NCBJ
La Rovere	Stephano	NIER
Vestrucci	Paolo	NIER
Brinkman	Hans (Johannes L.)	NRG
Kahia	Sinda	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Morandi	Sonia	RSE

Name	First name	Organization
Dybach	Oleksiy	SSTC
Gorpinchenko	Oleg	SSTC
Claus	Etienne	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Grondal	Corentin	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Oury	Laurence	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	TUS
	Kaleychev	TUS
Hladky	Milan	UJV
Holy	Jaroslav	UJV
Hustak	Stanislav	UJV
Jaros	Milan	UJV
Kolar	Ladislav	UJV
Kubicek	Jan	UJV
Mlady	Ondrej	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

EXECUTIVE SUMMARY

The report provides a summary of already existing guidance on the implementation of external hazards in extended level 1 PSA. It summarized the lessons learnt from existing standards, existing gaps and possibility for future development within the workpackage WP22 ‘How to introduce hazards in L1 PSA and all possibilities of events combinations’.

The report is focused on the four following areas, for several hazards:

- 1) Impact on the SSCs modelled in L1 PSA event trees
- 2) Impact on Human Reliability Assessment modelling in L1 PSA
- 3) Site impact modelling in L1 PSA event trees
- 4) Link between external initiating events of PSA and NPP design basis conditions.

During the review of existing guidance, it appeared that many of the references form a suitable basis to introduce external hazards in L1 PSA including event combination. Available guidelines provide usable recommendations to evaluate failure probabilities of SSCs depending on the influence of single hazard or events combination. The most detailed guidelines are devoted to the seismic events and fires. Even if these guidelines deal only with single event impact, they can be also used for combined events purpose to evaluate particular effects induced by analyzed external hazards. Guidelines provide general systematic framework how to determine the scope of SSCs for extended PSA and failure modes (develop an extended list of components). In general available guidelines provide detailed framework for analysis of seismic event. The other external hazards are not always covered so deeply. This is probably caused by specific site nature of these hazards like external floods, fires etc.

In case of HRA, more detailed information and HRA models are available for seismic events or fire events. For the other external hazards, the literature with regard to HRA is not well developed. The PSA for external hazards should take account the potential for human response to be affected by the external event. More realistic Human Reliability models could be developed for the periods during and after an external event, including the implementation of emergency plans. In general, the reliability of operational measures could be explored, including monitoring and alerting actions. Also, there may be a need for data on operator response (Human Reliability models) in the case of an external event, possibly available from training and evaluation of personnel on simulators.

The general practice of performing safety assessment for multiple reactor units on the site is to analyze one reactor at a time and not considering several important multi-unit dependencies and interactions. The CDF for the site rather than the unit is necessary to be considered. Many recent standards are applicable to plant level which is defined as a nuclear power facility, which may refer to a single-unit or multi-unit site. Many aspects highlighted by these standards are directly, or with a minimum of adaptation, applicable to the modeling of events affecting multi-unit sites. Regarding risk metrics for a site PSA: existing standards and documents give some high level requirements. It would be interesting to come to a common proposal of risk metrics for a site PSA. Methodological documents which propose acceptable methods to deal with the risk metrics for a site PSA are not available and it would be useful to develop them.

The majority of the countries assessed use the 10^{-4} p.a. Annual Exceedance Probability (AEP) as the design basis hazard level. If some ‘cliff edge’ effects can be expected, a lower frequency has been specified to take this into account. Using a lower frequency with a reduced confidence level moves the assessment to a ‘best estimate’ rather than ‘conservative design basis’ type of analysis. If one frequency is to be used, this should be the conservatively assessed hazard level that corresponds to a 10^{-4} p.a. AEP. ‘Conservatively assessed’ is generally understood to correspond to the 84th percentile confidence level, i.e. one standard deviation. Where cliff edge effects may occur (e.g. external flooding) a lower frequency should be considered. It is noted that frequencies of 10^{-5} and 10^{-6} p.a. have been used for this hazard. The frequency level for design extension conditions should also be defined. A value of below the design basis level to 10^{-7} p.a. or 10^{-8} p.a. (depending on the overall risk target) should be considered. Finally the approach needs to take into account whether the frequency and hazard levels are to be used for design basis purposes (i.e. with a conservative approach) or for design extension and PSA purposes (i.e. best estimate).

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
3	AMEC NNC Limited	AMEC NNC	United-Kingdom
5	Lloyd's Register Consulting	LRC	Sweden
10	Nuclear Research and consultancy Group	NRG	Netherlands
12	Electricité de France	EDF	France
13	Lietuvos energetikos institutas (Lithuanian Energy Institute)	LEI	Lithuania
19	VUJE	VUJE	Slovakia
20	NIER Ingegneria	NIER	Italy
24	Jožef Stefan Institute	JSI	Slovenia
26	Regia Autonoma Pentru Activitati Nucleare Droberta Tr. Severin RA Suc	INR	Romania

CONTENT

MODIFICATIONS OF THE DOCUMENT	1
LIST OF DIFFUSION	1
EXECUTIVE SUMMARY	6
ASAMPSA_E PARTNERS	8
CONTENT	9
GLOSSARY	11
1 INTRODUCTION.....	13
2 OBJECTIVES AND SCOPE	14
3 STRUCTURE	16
4 METHODOLOGY	16
5 WORK ACTIVITIES SUMMARIES	16
5.1 WA1 – IMPACT ON THE SSC'S MODELED IN L1 PSA EVENT TREES	16
5.1.1 SSC FAILURE PROBABILITY ASSESSMENT DEPENDING ON THE INFLUENCES OF PARTICULAR HAZARDS.....	17
5.1.2 CONSISTENCY BETWEEN ASSUMPTIONS USED IN EXISTING PSA AND EXTENDED PSA COVERING EXTERNAL HAZARDS	20
5.1.3 MODELING IMPACT OF A COMBINATION OF EVENTS	24
5.1.4 IMPORTANCE AND SENSITIVITY ANALYSIS	27
5.2 WA2 – IMPACT ON HUMAN RELIABILITY ASSESSMENT MODELLING IN L1 PSA.....	29
5.2.1 ASSESSMENT OF THE HUMAN FACTOR DEPENDING ON THE NATURE OF THE EXTERNAL EVENTS	29
5.3 WA3 – SITE IMPACT MODELLING IN L1 PSA EVENT TREES.....	32
5.3.1 INITIATING EVENTS.....	33
5.3.2 IMPACT ON THE PSA MODEL.....	34
5.3.3 STATUS OF MULTI-UNIT PSA MODELING	36
5.4 WA4 – LINK BETWEEN EXTERNAL INITIATING EVENTS OF PSA AND NPP DESIGN BASIS CONDITIONS....	38
5.4.1 INTRODUCTION	38
5.4.2 HISTORICAL BACKGROUND	38
5.4.3 APPLICATION TO CURRENT PLANTS.....	39
5.4.4 NEW REACTOR DESIGNS	41
5.4.5 SAFETY BASED DESIGN	42
5.5 DOCUMENTS REVIEW	45

6 CONCLUSIONS.....	49
6.1 CONCLUSION OF WA1 (external hazards on SSC modelling in L1 PSA).....	49
6.2 CONCLUSION OF WA2 (HUMAN RISK ASSESSMENT).....	50
6.3 CONCLUSIONS OF WA3 (MULTI-UNITS IMPACTS)	50
6.4 CONCLUSIONS OF WA4 (LINK WITH DESIGN BASIS)	51
7 LIST OF REFERENCES	52
8 BIBLIOGRAPHY	55
9 LIST OF TABLES	57
10 LIST OF FIGURES.....	57
11 APPENDIX.....	58
11.1 APPENDIX 1 – DOCUMENTS REVIEW RESULTS	58
11.2 APPENDIX 2 - MULTI UNIT ASSESSMENT.....	109
11.2.1 INTRODUCTION	109
11.2.2 POTENTIAL LIMITS OF A UNIT MODEL.....	110
11.2.3 RISK ASSESSMENT FOR THE SITE	111
11.2.4 REFERENCE.....	112

GLOSSARY

As discussed in Uppsala End User Meeting (May 2014), ASAMPSA_E project glossary and its definition will be introduced later in this project. The below glossary is tentative and can be changed later in Final version.

AEP	Annual Exceedance Probability
ARP	Alarm Response Procedure
CCF	Common Cause Failure
CDF	Core Damage Frequency
DPD	Discrete Probability Distributions
DSG	Design Safety Guide
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
EPZ	Emergency Planning Zones
ETL	Event Tree Linking
FDF	Fuel Damage Frequency
FTL	Fault Tree Linking
HCLPF	High Confidence of Low Probability of Failure
HEP	Human Error Probability
HFE	Human Failure Events
HRA	Human Reliability Analysis
IPEEE	Individual Plant Examination of External Events
ISRS	In Structure Response Spectra
LERF	Large Early Release Frequency
LHS	Latin Hypercube Sampling
LOCA	Loss of Coolant Accidents
LOOP	Loss of Off-Site Power
MCS	Monte Carlo Simulation
NDRC	National Defence Research Committee
PDF	Probability Density Functions
POS	Plant Operational State
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSHA	Probabilistic Seismic Hazard Analysis
PSR	Periodic Safety Review
RLE	Review Level Earthquake
NDC	NPH Design Category
NPH	Natural Phenomena Hazards

NPP	Nuclear Power Plant
SAM	Severe Accident Management
SAP	Safety Assessment Principles
SAR	Safety Analysis Report
SBO	Station Black Out
SMA	Seismic Margin Assessment
SPAR	Standardized Plant Analysis Risk
SPRA	Seismic Probabilistic Risk Assessment
SSC	Structure System and Component
SSI	Soil Structure Interaction
THERP	Technique for Human Error Rate Prediction
WP	Work Package

1 INTRODUCTION

An **extended PSA** (probabilistic safety assessment) applies to a site of one or several Nuclear Power Plants (NPPs) with different types of reactors 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.

An *extended PSA* includes an *extended Level 1 (L1) PSA*, which identifies and calculates scenarios of fuel damage (and their frequencies) and an *extended Level 2 (L2) PSA* which calculates scenarios of radioactive release (frequencies, kinetics and amplitude of release). It could include an *extended Level 3 (L3) PSA* which calculates the risk outside the site (health, economy and environment). Important aspect of an *extended PSA* is also the *quality of the interfaces between the levels in the chain L1-L2-L3, which is also true for traditional PSA*.

An *extended PSA* should cover (for example):

- The risk contribution from both reactors and spent fuel pools;
- The risk contribution from
 - internal initiating events,
 - internal hazards (internal flooding, internal fire, etc.),
 - single and correlated external hazards (earthquake, external flooding, external fire, extreme weather conditions or phenomena, oil spills, industrial accident, explosion, etc.),
 - human factors in- and out-side of the NPP, and
 - possible combinations of the previous events, factors and consequences, including correlations (especially if induced by potential consequences of external hazards).

The Fukushima nuclear accident in Japan resulted from two correlated extreme external events (for instance it was caused by a violent earthquake followed by a major tsunami that has devastated the site and resulted in severe damages). The consequences (flooding in particular) went beyond what was considered in the initial NPP design. Such situations can be identified using PSA methodology that complements the deterministic approach. Prior to Fukushima accident, the performance of a L1 - L2 PSA concluded this event as a "low probability event" which can lead to extreme consequences outside of the plant (however analyses performed after the event concluded that this event was not "a low probability event"). The industry (system suppliers and utilities) or the Safety Authorities may take appropriate decisions to reinforce the defence-in-depth of the plant and the relevant emergency planning.

In case of existing seismic PSA, it is judged that the reason for severe consequences is not so often the direct seismic impact on the plant with catastrophic force. In more often cases, a distant impact disturbs the external grid, and leads to a long term cutoff from external power. In seismic PSA, normally, it is conservatively assumed that off-site grid will not be available (24 hours+). This results in increased importance of on-site power sources. Therefore, plant internal emergency power becomes crucial for an extended period, and its failure becomes more risk dominant than the direct seismic impact on the plant. The integral seismic impact is considered in seismic PSA for example seismic failure of electrical panels or elements of safety electrical systems. The seismic failure (in

general) of components/systems is dominant contributor to CDF increase. The Seismically induced Station Black Out (SSBO) created from »normal« (full power) SBO Event tree can be modified to consider available systems/functions.

The project ASAMPSA_E, which was preceded by the project ASAMPSA2¹, aims at identifying good practices for the identification of such situations with the help of Level 1 and 2 PSA and for the definition of appropriate criteria for decision making in the European context. It offers a new framework to discuss, at a technical level, how extended PSA can be developed efficiently and be used to verify if the robustness of NPPs in their environment is sufficient. It will allow exchanges on the feasibility of "extended PSAs" to quantify risks induced by NPP sites (multi-unit reactors and spent fuel pools, modelling impact of internal initiating events, internal and external hazards on equipment, and human recovery actions).

2 OBJECTIVES AND SCOPE

The objective and scope of the present document is to provide a summary of already existing guidance on the implementation of external hazards in level 1 PSA and moreover its implication in extended level 1 PSA in the next project deliverables. This document is a deliverable of work package 22 (WP22) - 'How to introduce hazards in L1 PSA and all possibilities of events combinations' - which aims to update the list of the already introduced external hazards in the existing guidance, to promote exchanges and to identify good practices on the implementation of external events in L1 PSA, having as a perspective the development of extended PSA.

Further, the objective of WP22 activities is to discuss good practices for the implementation of modelling for relevant external hazards and the possible combinations between them and internal events starting from an existing (internal events) L1 PSA. Furthermore in the ASAMPSA_E meeting in July 2013, it has been decided that only natural external hazards should be addressed.

The work description for WP22 divides the work into four activities:

1) **WA1 - Impact on the SSCs modelled in L1 PSA event trees**

The following topics are covered in this work activity:

- Practices to assess the conditional failure probabilities of Structure System and Components (SSCs) depending on the initial event (hazard or combination of hazards).
- How to make and assure consistency between the previous assumptions of an existing L1 PSA (assumptions for (new) external hazards) and the possible combinations between them?
- How to integrate into model combination of events induced² by external hazard?
- What are the available approaches allowing to obtain relevant results with limited resources?
- In general, what can be learnt from existing standards and what is missing and what should be with priority developed?

¹ The experience from ASAMPSA2 is described in the ASAMPSA_E deliverable D40.1.

² Induced events are understood as events that are initiated by impact of external hazards, e.g. seismic event -> collapses of internal external structures can initiate floods, fires etc., strong wind -> tidal waves, grid failures, etc.

Note: a significant part of this topic will concern seismic and flooding PSA, which is defined in scope of ASAMPSA_E project (however the scope of ASAMPSA_E is not limited to these two hazards).

2) WA2 - Impact on Human Reliability Assessment modelling in L1 PSA

The following topics are covered in this work activity:

- How to assess the human factor depending on the nature of the external events? (see also site impact below),
- In general, what can be learned from existing standards and what is missing and what should be developed with priority?

3) WA3 - Site impact modelling in L1 PSA event trees

The following topics are covered in this work activity:

- How to model in L1 PSA, a multi-units site (in relation with the different combinations of operating states of the different reactors, the human actions and the management of all sources of radioactivity, the impact of external hazards on the different sources of radioactivity on site and associated SSCs, the impact of external hazards on behaviour of accident mitigating systems such as the containment system, for the accident management)?
- Consideration of the impact on level 1 end states and the interface towards level 2 PSA following the external event (some exchange with WP40 is foreseen) and perhaps the interface towards level 3 PSA.

4) WA4 - Link between external initiating events of PSA and NPP design basis conditions (only IE frequency)

The following topics are covered in this work activity:

- The objective is to compare the rules/methods applied for defining the NPPs design basis conditions with the rules/methods used for assessing PSA initiating events. Different implementations will be discussed depending on the effects of external hazards (beyond or below the design basis conditions) and possible combinations, including between external and internal hazards. It will be discussed to what extent external PSA initiating events should be considered in the design basis conditions. This part of the project includes a strong linkage between PSA and defence-in-depth, which is redundant with WP 30 (D30.3 and D30.4).

The work will include few technical meetings with the ASAMPSA_E partners (if possible with WP21), exchanges on existing practices (feasibility of extended L1 PSA, with modelling of correlated rare events), bibliography (key references and synthesis), constitution of small groups in charge of drafting recommendations on each specific issue.

In the post-Fukushima context, it is expected that many other initiatives will be organized at an international level. In addition, the respective results in WP30 on Lessons of Fukushima for PSA will be taken into consideration. The WP21 and WP22 partners will try to contribute to these initiatives and make the link with the ASAMPSA_E project.

3 STRUCTURE

The introduction and objectives of this project and report are covered in Sections 1 and 2. The structure of this report is based on the four work activities discussed in Section 2. The methodology is explained in Section 4, while document summaries with the four work activities are discussed in Section 5. The conclusion of document summaries is covered in Section 6. Section 7 includes a list of documents with references to the four work activities.

4 METHODOLOGY

The main methodology used in the report is based on selection and screening of a list of reference documents, given in Section 7 with respect to each work activity. The list is a compilation of already existing published guidance on the implementation of external hazards in L1 PSA. The summary of documents and its applicability to each work activity is covered in Section 5. For each work activity, one partner is assigned as responsible for the document summary preparations and coordinating the efforts of the group of partners. In cases where guidance documents are related to one or more work activities, the contributing partners reviewed the sections or paragraphs specific to their work activity, and added the reviews of their sections to the summary at the end.

The list of documents in Sections 5 and 7 is based on the most relevant publicly available PSA guidance, regarding the work activities (a first list has been provided by ETSON PSA group). However, some general PSA guidances, standards and research papers are also included. The list is modified from the initially proposed list based on partners' review and comments. The writing partners were invited to analyse the relevance and significance of the references. Based on their experience, the writing and commenting partners have added references to the list and/or propose other modifications to the WP lead organisation.

5 WORK ACTIVITIES SUMMARIES

5.1 WA1 - IMPACT ON THE SSC'S MODELED IN L1 PSA EVENT TREES

(Contributed by VUJE and supported by EDF, Section 5.1.4 contributed by NIER)

The WA1 and its referenced documents cover the followings:

- Practices to assess the (conditional) failure probabilities of SSC depending on the influences of hazards or combination of hazards ;
- Assurance of consistency between the assumptions used in existing L1 PSA (mainly L1 PSA for internal events which serves as basis for further extension of PSA scope) and the assumptions for extended PSA covering external hazards ;

- Modeling of impact of the combination of events (e.g. the combination of external events or events induced by a particular hazard).

The covering of above mentioned topics is based on available guidelines that are briefly discussed in the “APPENDIX 1 - DOCUMENTS REVIEW RESULTS Documents Review” of this report. Consequently, relevant information from reviewed documents serve as input for specific sections dealing with above introduced topics.

5.1.1 SSC FAILURE PROBABILITY ASSESSMENT DEPENDING ON THE INFLUENCES OF PARTICULAR HAZARDS³

The external hazards can influence directly (or indirectly) the operability of the SSCs. This chapter deals with practices to assess the failure probabilities of SSC depending on the influence of hazards. The external hazards cover a large spectrum of phenomena. Each phenomenon has its own specific damage mechanism and requires a specific approach to assess the SSCs failure probability.

In general the PSA analysis of impact of external hazards should use a multi stages approach to evaluate the impact of the hazard effect on SSCs, e.g. qualitative and quantitative screening⁴ followed by the detailed analysis. Further details of such multi stages approach are briefly introduced in Section 5.1.2.1. This part deals only with approaches for final assessment of SSCs failure probabilities used to provide data to quantify the PSA model, for instance, external hazards like earthquake, floods, fires and missiles.

5.1.1.1 EARTHQUAKE⁵

The probability of component failure is derived in the form of so called fragility curve, based on approaches published in [9], [10] etc. The component fragilities are usually estimated by using information of the plant design basis and responses calculated at the design-analysis stage or as part of the seismic qualification of the plant.

The basic input data are A_m , B_R and B_U which are respectively, the median ground acceleration capacity, the logarithmic standard deviation of randomness in capacity and the logarithmic standard deviation of the uncertainty in the median capacity.

The calculation of the fragility curve, i.e. the conditional probability of failure f_0 with perfect knowledge of the failure mode and parameters describing the ground acceleration capacity, i.e. only the random variability B_R is considered, which is performed using below mathematical equation:

³ Chapter 10 of NUREG/CR-2300 [5] discusses the wind related fragility assessment in detail. Fragility analysis for other hazards could be completed in the same way as for earthquake or wind.

⁴ The screening on component level, for example, there is only one simple criterion perfectly qualified component, i.e. high resistance can be screened out.

⁵ ‘Seismicity refers to the geographic and historical distribution of earthquakes’ by U.S. Geological Survey (USGS) glossary.

$$f_o = \Phi \left[\frac{\ln \left(\frac{a}{A_m} \right)}{\beta_R} \right]$$

Where:

Φ - the cumulative standard normal or Gaussian distribution;

a - earthquake ground motion (peak ground acceleration : PGA^6);

A_m - median fragility (median ground acceleration capacity).

In case, the modeling or state of knowledge uncertainty is included, the fragility at a specific acceleration becomes a random variable (uncertain). At each acceleration (PGA) value a , the fragility f can be represented by a subjective probability density function as follows:

$$f' = \Phi \left[\frac{\ln \left(\frac{a}{A_m} \right) + \beta_U \Phi^{-1}(Q)}{\beta_R} \right]$$

Where:

Φ - the cumulative standard normal or Gaussian distribution;

Φ^{-1} - inverse function of the Φ ;

a - earthquake ground motion (pga);

A_m - median fragility (median ground acceleration capacity).

$Q = P[f < f' | a]$; i.e., the subjective probability (confidence) that the conditional probability of failure, f , is less than f' for a peak ground acceleration a .

A key parameter of the fragility is the so-called High Confidence of Low Probability of Failure (HCLPF) value. It is defined as the value of the PGA for which there is a high confidence (95%) that the probability of failure does not exceed 5% (i.e. it is low) and has the following form,

$$HCLPF = A_m \exp(-1.65(\beta_R + \beta_U))$$

An alternative way of obtaining the fragility curve is to first estimate the HCLPF value directly, via the so-called Conservative Deterministic Failure Margin (CDFM) method and then to derive the entire curve by assigning generic variability parameters. This approach is denoted as hybrid approach and is described in [34].

⁶ Peak Ground Acceleration

Soil liquefaction - Liquefaction of soil and unconsolidated fine-grained sediment is caused by ground shaking during an earthquake. The phenomenon results from the expulsion of pore water and leads to an extreme reduction of shear strength of the soil. In such cases, soil has very little strength and behaves more like a liquid than a solid unable to carry loads. This behavior causes base failure at the foundation of buildings and infrastructure. Down-slope flow of liquefied soil (referred to as lateral spreading) may additionally lead to destruction of underground infrastructure (e.g, cables, pipes).

5.1.1.2 FLOOD

The floods as such can envelope many specific damage mechanisms as wave ramp and impact forces, erosion and sliding, ponding, hydrostatic loading and overturning, leakage, blockage of cooling water intakes etc. The major impact of flooding is simply submergence of the equipment, resulting in its failure. If the equipment is "flooding qualified" then this should be taken into account.

For fragility analysis of the SSCs of a nuclear power plant related to the wave ramp, impact forces and hydrostatic loading an approach similar to that used for the fragility to earthquakes can be applied [4]. The input parameters for calculation are provided by plant basic design or as a result of specific analytical work. Moreover, chapter 11.2 of [5] contains standard discussion regarding median capacity etc. This concept is generally used in fragility analysis in many industrial branches. However; we have none further details and ideas how to obtain B_R and B_U for specific flood case. This statement is associated to one conclusion, see last paragraph "In general available guidelines provide detailed framework for analysis of seismic event. The other external hazards are not always covered so deeply. This is probably caused by specific site nature of these hazards like external floods, fires etc."

Based on ASAMPSA_E partner's experience, the assessment of SSCs failures related to the long term flooding effects like erosion, sliding etc. is always site dependent, which should be based on the results of specific analytical work. By the time of writing this report, the detail of such guidance or reference documents are not identified and the next deliverable D22.2-3 of this project shall explore this topic.

5.1.1.3 EXTERNAL FIRES

The evaluation of direct impacts of fires use simplified two-state approach, i.e. all components in affected compartment will be considered as damaged or intact. Another option is usage of some standard method as for internal fire analysis, e.g. [37], which enables exact addressing scope of damages. However analysis of external fires should take into account the side effects of external fires like impact on external grid, habitability of control room, induced internal fires etc.

5.1.1.4 MISSILES

The evaluation of missiles direct impact from the same topic as of floods and fires, i.e. approach used for internal hazard analysis is used. If a potential missile has sufficient kinetic energy (BRL formula etc.) then the problem will be reduced on geometric probability and consequently the probability of target hitting is assessed. Side effect of several external hazards can consist in a generation of missiles. Typical hazards capable of missiles generation are strong wind and explosions.

The damages of structure walls could result hairline cracks, penetration, front face spall, back face scabbing and perforation. Impact trajectory and impact velocity is calculated by using complex codes. An alternative is usage of simplified formulas from [89]. Impact of missile can be evaluated by using modified NDRC formula [90] or numerical simulation (programs such as LS-DYNA, ABAQUS can be used).

However sources [88], [89] and [90] deal with deterministic analyses. Quoted references are intended as guidelines to determine and demonstrate design basis for wind-borne missiles. They provide rationale for determination of scope of considered wind-born missiles as well as design recommendations but deal neither with assessment of probability of missile generation nor with assessment that missile hits sensitive target.

In actually analysis of missiles generated by explosion should be covered within explosion analysis. Such analysis brings the same problems as analysis of wind-born missiles.

In general it is difficult to predict number of generated missiles and this part of analysis will be probably based on expert judgment. Probability of affecting sensitivity target can be obtained by using geometric probability, i.e. likelihood of impact on particular area will be uniformly distributed. Probability of target damage will be based on scope of damage evaluated by appropriate empirical formula like NDRC one's.

5.1.1.5 SUMMARY OF APPROACHES TO OBTAIN RELEVANT RESULTS BY USING LIMITED RESOURCES

Finally if assessment of SSCs failure probabilities can be supported by data from design basis, relevant results can be obtained even if limited resources are available. Existing guidelines provide good background to perform such assessments. The relevant guidelines are briefly discussed in APPENDIX 1 - DOCUMENTS REVIEW RESULTS.

5.1.2 CONSISTENCY BETWEEN ASSUMPTIONS USED IN EXISTING PSA AND EXTENDED PSA COVERING EXTERNAL HAZARDS

Nowadays PSA are usually developed as an integral model covering the whole spectrum of plant operational states (POSS) which combines L1 PSA and L2 PSA (and L3 in some countries). If the multidisciplinary nature of PSA is taking into account then an extended PSA forms a complex challenge and requires ensuring consistency across all assumptions used by involved scientific and PSA teams.

The available L1 PSA model for internal events is usually a basic step to perform external event analysis. It is difficult to build an internal events model that foresees all modelling/details needed for external hazards. It means that the used model shall respect the basic scope stated in regulatory guidelines, for instance, in [1] and [5] (i.e. definition of POSSs, determination of initiating events and scope of systems that are used to mitigate or to cope with consequences of considered events) to the extent required by PSA quality standards like [7] and [8]. If a certain

hazard can not be modelled within the scope of available PSA then the L1 PSA for internal events should be expanded or specific probabilistic analyses dealing with particular hazard must be developed.

The extension of the PSA model depends on the nature of considered external hazards. Specific aspects that can affect consistency between assumptions used in the existing PSA for internal events and extended PSA covering external hazards and also possible combinations between them are briefly discussed in the following text. These aspects are:

- Scope of SSCs
- Failure modes induced by external hazards and side effects including internal hazards as consequences, e.g. induced initiating events
- Walkdowns
- Human Reliability Analysis⁷ (HRA)
- Quantification / modeling tools
- Internal hazard analysis on its own or as consequence of an external event.

In general, existing guidelines provide, apart from seismic event, overall framework to achieve consistent results and these frameworks should consider site conditions. Reference [9] can serve as a starting point for such work. The determination of extended list of SSCs should evolve from the list of SSCs considered for PSA internal events in such a way to cover all structures which are housing safety relevant components in the internal event PSA. However, identification of the credible failure modes is largely based on the analyst's experience and judgment. It is also based on walkdowns (covered in Section 5.1.2.3) which is a crucial stage for the identification of failure modes and internal hazard analysis. Improperly determined scope of SSCs and their failure modes can lead to the inconsistent assumptions and the biased PSA results.

5.1.2.1 SCOPE OF SSC'S

The initial list of SSCs which is based on the list of components for L1 PSA should be expanded to include all SSCs that are required to cope with a specific external event or combination of events induced by respective external event. This process should also take into account effects of potential collapses of civil structures and their internal parts on safety equipment. Determination of the scope of SSCs depends on nature of considered external hazard. Examples of such extension for seismic event are given in [9] *Table II - Important vulnerabilities to earthquakes (List taken from the Oconee PRA study [14])* and partially in [1]. Extension of the list of SSCs in case of flood and high wind is discussed in [9]. For a flooding analysis, it is necessary to identify the (floor) level that SSCs are placed on. For a river barge collision, nearby vulnerable equipment such as the water intake structure must be identified.

⁷ The specific aspect of HRA is covered by Section 5.2.

If the used approach is based on the existing model for internal events then consistency is maintained “semi-automatically” because extended PSA works basically with the same set of components as PSA for internal events and takes in mind the same safety functions (criticality, heat removal etc.). A necessary condition to achieve consistent results is to respect system and component boundary across all stages of the analysis, i.e. the list of SSCs for external hazards should respect division of plant SSCs or their parts by the same manner as it was done in PSA for internal events.

5.1.2.2 FAILURE MODES

This part of work runs interactively with the previous one, i.e. determination of the scope of SSCs and can use indirect way to determine scope of SSCs and failure modes. The starting point is an identification of the initiating events that can be induced by the considered hazard and consequently the relevant SSCs affected by such events.

The extended list of relevant SSCs should be complemented by all realistic failure modes that can influence operability of SSCs ensuring safety functions as result of the hazards. A general guideline for such an analysis that should consider duration of effects, indirect effects and dependencies, physical environment and load combination is given in [9]. To determine the additional failure amongst others one should consider dynamic loads (vibration, overpressure, impulse and impact), over flooding, dynamic effects of the waves, slope instability and short term erosion etc.

Furthermore, there is a need for building industrial PSA models which could be proportionated to the safety issues and fit for purpose, while not necessarily providing an exhaustive list of all the systems, components and related failure modes. When building the PSA model and deciding which systems/components/failures modes have to be modeled in the PSA, an exhaustive assessment has to be made beforehand. Then, only the relevant systems/components/failures modes have to be modeled in the PSA model itself. It means that some systems/components could be discarded (i.e. not explicitly modeled) if considered not relevant enough. It also means that aggregation modeling can be performed, at the failure mode level if needed. For instance when dealing with diversion pathways in the frame of a seismic PSA, each diversion pathway, its systems/components and related failure modes can be explicitly modeled or some aggregation can be performed to provide a “global” model of a system and its diversion pathways. In the latter case, failure modes of the “global” system will have reliability parameters built on the aggregation of all the individual components.

A difficult aspect of determination of the scope SSCs and their failure modes is formed by spatial interactions, e.g. fire and flood spreading, impact of collapsed SSCs etc. This problem, i.e. addressing all spatial interactions can be extremely complex and must respect specific site conditions. All known standards can cover this aspect only generally to provide some systematic framework, however application details are the responsibility of the PSA development team (see walkdowns).

5.1.2.3 WALKDOWNS

The walkdowns as such, or familiarization, are a standard part of any PSA which should be performed in the case of internal and external event analysis, where appropriate e.g. [1]. The walkdowns form an essential tool to verify spatial dependencies among SSCs as well as to verify assumptions adopted during determination of the scope of SSCs and their failure modes that was based on design documentation and to identify the vulnerabilities against hazards.

5.1.2.4 HUMAN RELIABILITY ANALYSIS

Human reliability analysis provides the assessment of human error probabilities for actions performed by plant staff as a part of (emergency) response on particular initiating events (post-accident analysis) or assessments related to normal operation (pre-accident analysis). In general it is expected that staff post-accident response can be affected by some negative factors in the case of external hazards. The occurrence of such negative factors depends on the context of the particular hazard. The consistency of assumptions for internal events and external hazards should be based on respective results of human reliability analysis for internal events. It means that assessment of human error probabilities for external hazards should follow basic assumptions from PSA for internal events that will be tailored on external hazard conditions. Another important point is consideration of multi unit impacts, i.e. management difficulties, sharing of human resources, human reliability analyses relying on intervention of technical support center (safety engineers, emergency and maintenance specialists etc.). For all HRA topics, further details are covered in Section 5.2.

5.1.2.5 QUANTIFICATION TOOLS

Important aspects of used logic models (resp. software tools) are related to their capability to reflect convolution of the hazard curves and fragilities including combination of events as well as consideration of event success probabilities (positive branches in event trees).

First aspect, convolution and fragility are briefly discussed in Section 5.1.3. Importance of second aspect, considering positive (success) branches, increases in the cases when event tree consequence evaluation involves many positive branches. Simplified treatment of complements can lead to the overestimation of the conditional probability of fuel damage or large early release.

5.1.2.6 INDUCED INTERNAL HAZARD ANALYSIS

In order to keep the consistency of the work evaluation of impacts of induced fires, floods and missiles on components within external hazard analysis, such analysis should use the same approaches and assumptions as of internal hazard analysis.

The approaches should lead to a good consistency between PSA for internal events and extended PSA, as well as consistency between different specialized teams involved in the work. They should be based on well-developed PSA for internal events and supported by specific deterministic analyses for any particular hazards. In general analysis of events induced by external hazards, e.g. floods, fires etc., should use when the internal hazard PSA is available, the same method and assumptions that were used in analysis of corresponding internal hazards. Example of such approach for seismic event is represented by [3].

5.1.3 MODELING IMPACT OF A COMBINATION OF EVENTS

The study of hazard combinations is emphasized in the majority of documents dealing with external hazards. This emphasizing takes into account the fact that some hazards can evoke a spectrum of events like induced fires, floods, deterioration control room habitability etc. Consequently considered hazards together with induced events can lead to the safety systems operability degradation, unintentional actuations of fire suppression systems etc.

The quantification of the external hazard sequence model may require integration of the hazard curve or hazard frequency and SSC fragility curves⁸ along with the random SSC failure modes, according to a boolean representation in which the plant response on the hazard occurrence that could lead to a fuel damage or a large early release.

The composition of such complex model strongly depends on the capability of used software. Basically this task can be accomplished by using Fault Tree Linking (FTL) model or Event Tree Linking (ETL) model where the first approach is more frequently used.

The both approaches use event trees and fault trees to model accident sequences, but differ in the way dependencies are considered and then in the sequences considered level of details. Whilst in FTL a relatively small number of function events (shared across the whole model) is used with a some customization (e.g. house event⁹) to deal with the different contexts for the same function, in ETL, a relatively large number of function events¹⁰ is used to split function events in such manner to avoid their dependency.

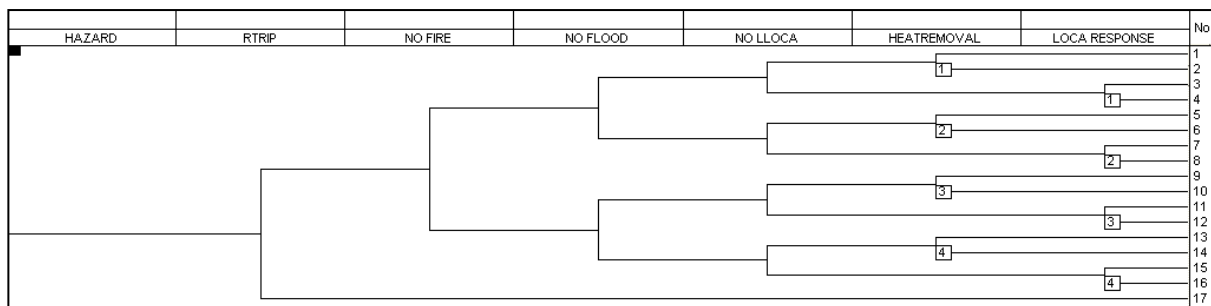
A typical approach uses event trees to outline basic scenarios of plant response in a particular hazard. The approach outlined in Figure 1 is based on information from [6], chapter 3.3.1.

⁸ Also, this depends on the approach used in the modelling e.g. fragility curves are not a necessity but could be one of the many possibilities.

⁹ House event : flags or switches (events having the logical value TRUE or FALSE) used in FTLs logic to modify the FT structure as a function of the accident sequence context

¹⁰ Function events : top events (headings) of the PSA event trees

FIGURE 1 - PLANT RESPONSE ON PARTICULAR HAZARD USING EVENT TREE



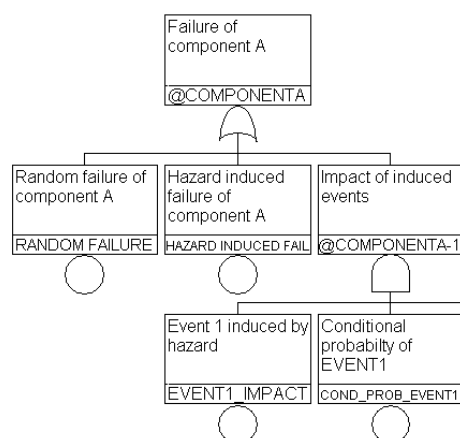
In a more general framework, analyst can start using event sequence diagrams to model the different accident scenarios and may decide which level of details can be used for event trees regarding any of these approaches. It can be said that with minimal effort, it is possible to generate event trees from event sequence diagrams using computer programs [32]. Moreover, for transparency purposes and in order to break complexity, it is possible to adopt modularity (modular PSA [33]) and split the model with modules considering each external event as a specific variant.

In the example of figure 1, event tree describes scenario which requires reactor trip (RTRIP) as first step in response on particular hazards. Consequently this tree evaluates combinations of fire, flood and LOCA induced by analyzed hazard. If a particular hazard is analyzed then specific event trees are usually developed for limited number of intervals of the relevant hazard curve, typically 4-6 intervals¹¹. Branching of event trees is directed by conditional probabilities that the induced event is triggered by effects of analyzed hazard.

The failure of systems used to mitigate consequence of hazard is modeled by fault trees. In these fault trees, the failure of a given component combines impact of random failure modes for internal events together with hazard induced failure modes by using OR gates.

¹¹ The main basis of this example is based on the currently used approaches that do not use specific software to incorporate convolution of hazard curve and fragilities, i.e. probably one manageable approach for classic PSA.

FIGURE 2 AN EXAMPLE OF COMBINATIONS OF COMPONENT RANDOM FAILURE MODES WITH INDUCED FAILURE MODES



This approach enables to incorporate an impact of combinations of events induced by analyzed hazard, as event tree evaluates only one top event, then an effect of such induced events can be modeled indirectly. For example as the impact of induced event on the component operability, i.e. it is used a conditional probability (COND_PROB_EVENT1) that secondary event induced by analyzed hazard (EVENT1) put out of order particular SSCs (COMPONENT).

The occurrence of the external hazard (which shall be a single basic event repeated in different parts of the FT-ET model), as well as of its induced events, introduces correlations at “Failure of component” level, while random failures are generally assumed as independent (typically in L1 PSA software using boolean algebra). One implication is that if the extended PSA includes an Importance and/or sensitivity analysis, the measures used to rank components should consider interactions among them. “Traditional” measures as Birnbaum, RAW, RRW, Fussell-Vesely are not adequate. Different Importance and Sensitivity analysis approaches are proposed in some scientific papers and discussed in Section 5.1.4.

Assigned probability of failures (failure modes) induced by a hazard is based on approaches discussed in Section 5.1.1. The SSCs failure probability assessment depends on the influences of particular hazards. However there is no closed and universal solution how to assign, in the PSA model, the conditional probabilities for induced events. For example pre-computation of conditional LOCA frequencies after an earthquake can be based on available seismic data by the same way as in [7] (i.e. conditional frequencies for particular LOCAs are derived from fragility analysis of relevant pipes) or this frequency can be evaluated directly by fault tree. Similar approach as for LOCA can be used for induced floods having internal water sources, e.g. large tanks.

Both fault tree and event tree development strongly depends on the used software, e.g. if software allows usage of specific logical switches (like so called “house events” mentioned above etc.) then it is possible to develop generic fault trees that are suitable to model a plant response on the large spectrum of hazards.

In addition considering further initiating events induced by particular hazard can lead to the infinitive number of possible combinations that can potentially take place. For example there can be several induced fires in different compartments that can occur in the same time or subsequently. This fact emphasizes importance of screening process to determine manageable set of representative scenarios which has also impact on traceability of work.

In general available guidelines provide detailed framework for analysis of seismic events, e.g. [10], [11] that enable to obtain relevant results. The other external hazards are not covered so deeply what is probably caused by specific site nature of these hazards like external floods, fires etc. Basically analysis of those hazards can be based on general framework for external event published in [1] and very similar technics can be used regarding event trees as described in this part.

5.1.4 IMPORTANCE AND SENSITIVITY ANALYSIS

One of the principal activities within a risk-informed regulatory process is the ranking of structures, systems and components (SSCs) with respect to their risk and/or safety-significance [I]¹².

Risk metrics in probabilistic safety assessment (PSA) of nuclear power plants (e.g. core damage frequency, large early release frequency) can be written as function of the probability of occurrence of the basic events¹³ (PSA model at basic event level) or as function of the fundamental parameters¹⁴ (PSA model at parameter level).

Different techniques, based on the use of importance measures have been proposed for ranking SSCs. Importance measures traditionally used include [I], [II], [III], [IV]:

- the “Birnbaum measure”, which is the probability that the system is in a “critical” status for the component (i.e. the system is working / failed only if the component is working / failed); it only depends on the structure of the model (i.e. it does not depend on the component unreliability).
- the “Criticality importance measure”, which is the (conditional) probability that the system fails because of the failure of the component;
- the “Risk Reduction Worth”, which measures the “worth” of the component in reducing the risk level, by considering the maximum decrease achievable when the component is always working.
- the “Risk Achievement Worth”, which measures the “worth” of the component in achieving the risk level, by considering the maximum increase achievable when the component is always failed; typically, it is used as a safety-significance measure;

¹² Conceptually, risk-significance is related to the role that the SSC plays in the measures of risk; safety-significance is related to its role in the prevention of the occurrence of an undesired end state.

¹³ A particular SSC may be represented in the logic model by several basic events. These different basic events can represent different modes of failure or unavailability of the SSC [I].

¹⁴ Typically, the basic events of the model are the failures of components; by assuming exponential distributions for their failure times, the fundamental parameters are the failure rates of components.

- the “Fussell-Vesely” measure, which is the probability (at a given time) that at least one “minimal cut set” that contains the component is failed (i.e. all components in the minimal cut set are failed), given that the system is failed (at that time); typically, it is used as a risk-importance measure.

Originally, importance measures were defined for individual basic events [I]. The uncertainty in the probabilities of the basic events, due to the uncertainty in the fundamental parameters, makes it difficult to determine a robust ranking of SSCs; however, consideration of uncertainty should be integrated decision making process [I].

Therefore, a general framework should be adopted for the development of an Importance and sensitivity analysis, as allowed by some approaches recently proposed in the scientific literature. The Importance and Sensitivity analysis aims at quantifying the contribution of the input variables to the model output (Importance analysis) and to the related uncertainty (Sensitivity analysis). They allow the ranking of the input variables and give information about the “direction” of the model output change due to the “one at time”¹⁵ and simultaneous changes of the input variables, the key-drivers of the change and the structure of the model.

Different techniques developed for sensitivity analysis can be classified into two main branches, depending on the problem setting [X]:

- Global analysis, which is focused on the uncertainty on the model output with reference to the entire range of values of all the input variables;
- Local analysis, which is focused on the uncertainty on the model output with reference to some values of the input variables.

From the above point of view, the importance measures belong to the family of local sensitivity indicators [II]. As proved by the comparison between the application to PSA model of importance measures and of global sensitivity analysis techniques, elements that are important to the risk (as revealed by importance measures) are also important contributors to the model uncertainty (as revealed by global sensitivity analysis) [III].

The aforementioned “traditional” measures are “local” ones. They deal with a point value of the model output and input variables (basic events or parameters). They cannot be used for finite changes of the input variables or, in this case, they do not include the contributions of non-linear terms (i.e. interactions among input variables, whose effects are manifested for their simultaneous changes and are not taken into account by the superimposition of the effect due to the one at time change of variables). Moreover, they are not “additive”: the measure for a group of input variables cannot be computed as the sum of the measures estimated for each single variable but requires new evaluations of the model. Furthermore, some measures (e.g. RAW) cannot be used to compute importance of parameters.

The approaches recently proposed for Importance and sensitivity analysis refer to two different representations of the model output, which are briefly introduced in the following:

- Taylor series representation [IV], [V], [VI];
- High Dimensional Model Representation (HDMR) [VII], [VIII], [IX], [X].

Methods for the uncertainty propagation and for the computation of the sensitivity indices include the solution of multi-dimensional integrals by sampling-based methods (MonteCarlo or quasi-MonteCarlo, Latin Hypercube Sampling) and the application of the Fourier transform on a space filling curve in the input space [IX], [XII]. The Fouri-

¹⁵ One variable changes while the remaining ones are fixed to their values.

er amplitude sensitivity test (FAST) is more efficient than methods based on MonteCarlo integration. However it is usually limited to the computation of the “main effect” and “total effect”.¹⁶ Sampling-based methods require the computation of the model output for different sets of values of the input variables, which are sampled from the probability distributions that describe their uncertainty. Without looking at computational cost, a brute force approach could be applied in order to compute all indices specified in the variance decomposition of the model output. An efficient and parsimonious procedure can be adopted for the computation of the Main and Global Sensitivity indices [XIII].

5.2 WA2 - IMPACT ON HUMAN RELIABILITY ASSESSMENT MODELLING IN L1 PSA

(Contributed by NRG and supported by INR)

5.2.1 ASSESSMENT OF THE HUMAN FACTOR DEPENDING ON THE NATURE OF THE EXTERNAL EVENTS

The objective of this chapter is to analyze internationally available documents and to identify the aspects related to the assessment of the human factor depending on the nature of the external events in the PSA. All the documents listed in APPENDIX 1 - DOCUMENTS REVIEW RESULTS were reviewed. However, in this section only those documents containing useful information on this subject are referenced.

5.2.1.1 GENERAL RECOMMENDATIONS TO ASSESS THE HUMAN FACTOR FOLLOWING AN EXTERNAL EVENT

Several documents (references [1], [5], [7], [9], [13], [24], [38], [39] and [40]) recognize that the effects generated by external hazards could be of considerably great importance to safety and that they could have the potential to adversely impact plant personnel (e.g. the possibility of implementing emergency procedures could be affected, access by the operators could be impaired) and present general recommendations to revise and adjust the probabilities of human errors or recovery actions modeled in the Level 1 PSA for internal initiating events to account for the impact of external events on operator’s performance. The treatment of human actions after an external initiator is an important analytical issue [9]. It includes consideration of two contributions: the success of operators to follow related emergency procedures [28], as the success of improvised recovery actions for human and equipment failures, in opposition with inadvertent and erroneous actions with potential to exacerbate the situation [5]. Compared to accident scenarios caused by internal initiating events, the operators stress levels and conditions in the plant may differ considerably after an external initiating event. Among the aspects of human interactions that must be taken into account in hazard analysis, the following are specified in reference [5]: warning time, if any, to shut-down the plant; the conflicts between hazard mitigation and plant operation; the effects of stress.

¹⁶ The relationship between FAST and Sobol sensitivity indices was revealed in the general framework of HDMR decomposition; an extended FAST method able to calculate sensitivity indices referring to “total effects” was developed [XI].

Some general recommendations are given in the PSA related literature such as in reference [7] where it is mentioned that the reasoning for increasing or not the human error probabilities should be presented and the basis for the error rates used should be justified. It should be verified that the HRA adequately accounts for the additional influences caused by external event, that human failure events adopted from an Internal Events PRA have been modified as appropriate to reflect external hazard effects and that new human failure events are included to account for specific hazard related actions that are consistent with plant procedures that were not covered by the Internal Events PRA.

Setting-up specific operational procedures for operator action following an accident caused by an external human induced event is also recommended [13].

It is recommended in several documents ([1], [7] and [24]) to organize comprehensive and structured plant walkdowns as a starting point of the human reliability analysis for external events PSA. Indeed, plant walkdowns are an efficient way to gather specific information such as on access issues and on buildings and system locations. This understanding is crucial to the development of correct human reliability models. But walkdowns can only be performed at the operating plants. This process is not relevant for plants at design stage. In the following subsections, only seismic events and fire events are developed in more in detail. Indeed, internationally available documents mainly focus on these two external events. Detailed information on the assessment of the human factor following other external events is missing. In some documents (as in reference [7]), it is only specified that the requirements related to seismic or fire events may be applicable to other external events.

5.2.1.1.1 SEISMIC EVENTS

In general, more details on the way to assess the human factor in case of seismic events are available in the literature. Thus, references [1], [7] and [24] specifically address the impact of seismic events on human reliability analysis.

The following seismically induced effects on the operators' performance shaping factors are identified [1]:

- Availability of pathways to specific SSCs after a seismic event;
- Increased stress levels;
- Failures of indication or false indication;
- Failure of communication systems;
- Scenarios with consequential fire and flood;
- Other applicable factors impacting the operators' behavior.

In addition, references [7] and [24] highlight the issues raised by the specificities of human reliability analysis for seismic PSAs. Recovery actions that cannot be performed due to the impact of seismic events of certain magnitude should be removed from the Level 1 PSA model or probabilities of failure whilst performing the action should be increased. All post-initiator human errors that could occur in response to the initiating event as modelled in the Level 1 PSA for internal initiating events should be revised and adjusted for the specific seismic conditions [1].

In many seismic PSAs, the human-error probabilities are increased for some post-earthquake actions compared to the probabilities assigned in analogous internal events initiated sequence (some actions are even considered as certainly failed in such conditions). It is considered that strong ground motions can adversely affect human performance, due to stress, physical impacts, inability to access required control stations, etc. Indeed, during and after a strong-motion earthquake, it seems likely that for instance the ability of control-room operators to perform their assigned tasks without error should be substantially degraded because of high levels of stress and confusion. This issue has been examined but the basis for determining the increases in probability versus ground motion level is not well developed in the seismic-PSA literature. This aspect can represent an important source of uncertainty in the numerical results of a seismic PSA.

Several different seismic human reliability analysis (HRA) models to account more effectively for possible high operator stress have been proposed and are in use (of course, this factor has reduced importance to the extent that most new nuclear power plants have designs that do not require operator intervention for the first half-hour or more after a design base earthquake. Unfortunately, because good benchmarking between methods in the frame of seismic PSA was not yet performed, there is no way today to sort out with confidence which of the several models of degraded post-earthquake operator performance is the best to be used.

5.2.1.1.2 INDUCED INTERNAL FIRE

Reference [39] focuses on human reliability analysis in case of internal fire events. It provides a detailed methodology and guidance to perform a fire HRA and thus to assess the impact of fire events on human reliability analysis. The methods to be used for internal fire events induced by the external hazards may be similar. Several important aspects are presented hereafter:

- Identification of operator actions and definition of human errors;
- Qualitative analysis;
- Quantification with three different successive approaches;
 - Screening

The screening methodology assigns quantitative screening values to the Human Failure Events (HFEs) modelled in the fire PSA by addressing the unique conditions that can influence crew performance during fires, ensuring that the time available to perform the necessary action is appropriately considered and ensuring that potential dependencies among HFs modelled in a given accident sequence are addressed. The Human Error Probabilities (HEPs) assigned in this manner are conservative.

- Scoping fire HRA

Scoping methodology allows assignment of a single overall failure probability value to represent the failure of reaching safe state using alternate means (including MCR abandonment) if certain minimal criteria are met. The scoping analysis uses decision-tree logic, as well as descriptive text, to be guided to the appropriate HEP value. The scoping quantification process requires a more detailed analysis of the fire PSA scenarios and the associated fire context and a good understanding of several factors likely to influence the behaviour of the operators in the fire scenario.

- Detailed HRA

For those cases in which the scoping approach cannot be used or a more detailed and possibly less conservative analysis is desired, a detailed analysis using either EPRI detailed HRA methodology approach or ATHEANA HRA method can be performed.

- Recovery actions analysis;
- Dependency analysis;
- Uncertainty analysis.

It is specified that the main difference for a fire HRA is to consider the impact of the fire on the ability to perform recovery actions associated with specific fire scenarios [39].

Certain aspects of fire HRA, especially in the area of quantification, continue to evolve and likely will see additional developments.

5.3 WA3 - SITE IMPACT MODELLING IN L1 PSA EVENT TREES

(Contributed by IRSN and supported by JSI)

The objective of this section is to analyse the internationally available documents and to identify the aspects related to the site impact modeling in the PSA. All the documents listed in Section 7 were reviewed. However, in this section only those documents containing useful information on this subject are referenced and detailed document review summaries are provided in APPENDIX 1 - DOCUMENTS REVIEW RESULTS.

The subject of the site impact on the PSA modeling, considering the initiating events affecting the site, is not new. Some of the existing international guidelines and other available documents already mention this issue. However, after the accident of Fukushima the treatment of the site as a whole becomes a more common requirement. For example, the WENRA position paper on Periodic Safety Reviews (PSRs) taking into account the lessons learnt from the TEPCO Fukushima Dai-ichi NPP accident [41] states that, *"in the safety assessment, specific considerations are needed for multi-unit sites and to address long term measures, as well as to cover all areas with significant amounts of radioactive material at the site. On multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analyzed. Hazards that may affect several units need to be identified and included in the analysis. It would be preferable to carry out the site specific studies for all units at the plant site at the same time, taking into account the possible interactions among different*

units. Even if some PSR studies were applicable to several similar NPPs, site specific aspects should be reviewed separately in PSRs."

Also the recent WENRA document [57] states that *"Where applicable, all reactors and spent fuel storages on the site have to be taken into account. Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity shall be covered."*

As the use of updated PSA is part of the PSR in many countries, the generalization of the WENRA concept could lead to extension of the scope and objectives of actual PSAs including the treatment of site impact aspects in the effective modeling of the initiators and of the accident sequences in the PSA.

In most of the current PSAs developed for a given installation (reactor, spent fuel pool...), there is an implicit assumption that the other site installations (reactor units or other site radioactive sources) are adequately protected and, hence, do not participate in any of the accident modeling or in the calculated releases [42]. This is the consequence of the practice of performing safety assessments for one reactor at a time and not considering multi-unit dependencies and interactions in both deterministic and probabilistic safety assessments [43]. To gain an accurate view of the site's risk profile, the CDF for the site rather than the unit is necessary to be considered. There are two basic approaches to create a multi-unit PSA [42]. One method is to develop an entirely new multi-unit PSA, and the other is to integrate existing single-unit PSAs, adequately addressing the dependencies (SSCs, humans, phenomena...) between the different site installations. Currently there has only been one published multi-unit PSA performed on Seabrook Station in the mid-1980's [44].

The NRC is continuing to investigate the impacts of multi-unit and multi-module events to risk, as evidenced by the Level 3 PRA Project [45]. In draft Standard Review Plan section 19.0, the NRC has stated that it will review risk from accidents that could affect multiple modules [46].

5.3.1 INITIATING EVENTS

Several documents, for example [1], [7], [8], [40], [48] and [56] mention that initiating events, affecting more than one unit at the same time, should be identified. These initiating events can be produced by:

- External events (for instance seismic, high wind, flooding), leading mainly to the loss of off-site power (LOOP) or/and loss of service water. In fact, severe weather-related and grid-related LOOP events are more likely to affect two or more units at a site,
- Internal hazards:
 - in case of fire events, there is a potential for spreading of a fire from one unit to a fire compartment of another unit. Also, there is a possibility of fires in common areas, e.g. swing diesels (diesels shared between units), and switchyards;
 - in case of internal flooding, possible propagation paths can lead to impact on multiple units in the same time,
- Failures of shared systems like instrument air, Alternate Current (AC) or Direct Current (DC) bus, etc.

In addition, events can arise in one of the units and lead to an initiating event in another unit. For example, for a Level 1 PSA for internal hazards, an initiating event in the unit being analyzed could be caused by a strike from a missile generated by disintegration of a turbine in an adjacent unit.

For multiple reactor sites, the risk of the site will increase as units are added. The probabilistically defined design bases can be used in these contexts to allow the design basis to vary whilst keeping the overall risk within tolerable or acceptable limits [49].

5.3.2 IMPACT ON THE PSA MODEL

Multiple units may provide both significant benefits - by virtue of the sharing of equipment and personnel - and significant challenges if all units require accident mitigation simultaneously [53] and [83]. There may be substantial plant capability that exists within the plant to use AC, DC, or fluid systems via cross-ties. These cross-ties may or may not be proceduralized and the subject of training exercises. Their use in the PSA should be represented by a realistic assessment of their likelihood of use [15] and [55].

Several documents [8], [47] state that the systems that are shared between units in multi-unit plants should be identified. In addition the manner in which the sharing is performed and the impact of these shared systems when the units experience a common initiating event should be assessed. This includes operator actions as required and specified by plant procedures or operating practices.

The WENRA report on new reactor designs [40] state that for the multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analysed. Hazards that may affect several units need to be identified and included in the analysis.

It is difficult to identify and adequately treat dependencies that exist between systems at multi-unit sites, particularly

- (i) sites with highly convoluted support system dependencies (systems and subsystems shared by different units),
- (ii) human action dependencies in deciding how to deploy equipment and personnel to support all plants on the site, and
- (iii) the possibility of accidents involving two or more reactors.

The standards [7], [10], [16] and [82] are applicable to plants which are defined as a nuclear power facility, which may refer to a single-unit or multi-unit site. It has to be noted that many aspects highlighted by these standards are directly, or with a minimum of adaptation, applicable to the modeling of events affecting multi-unit sites. Also, the handbook [48] mentioned aspects related to the treatment of multi-unit events. Some of the modeling aspects mentioned in these documents are:

- Multi-unit sites with shared systems, including the multi-unit site initiators, may impact the PSA model;

- For multi-unit sites with shared systems, it is important not to subsume multi-unit initiating events if they impact the mitigation capability;
- Failures to start/run, unavailability for test and maintenance (including when the unaffected plant is in shut-down), and any operator action such as manual cross-tie from the unaffected unit should be modeled appropriately;

It has to be noted that most of the existing PSAs already account for shared equipment and systems, as well as cross-tie capability as allowed by design and procedures. If multi-unit considerations are taken into account in the PSA, and if a shared asset only has the capacity to support one plant at a time, then a shared availability factor should be incorporated into the system fault tree that reflects the probability that the other plant will not need the asset in order to meet minimal functional success criteria. The shared availability factor should include the human error probabilities of implementation actions, and hardware failure probabilities. Constructing an aid such as a table or matrix showing all possible combinations of available equipment may be useful (e.g., EDGs, alternative AC power, and service water pumps). It is necessary to review relevant system fault trees where operator action to cross-tie units is credited and to ensure the reasonableness of actual plant and operator response to an event (e.g., time available for operator response vs. feasibility of recovery actions under changing environmental conditions).

- The existing human error analyses may extensively change in case of multi-unit site initiators, for example if the model considers the plant procedures dealing with shared diesel response to loss of off-site power initiators for a multi-unit site. For example, it may be necessary to modify the values of performing shaping factors to take into account the external hazard impact while using the actual human reliability analysis methodology.
- Inter-system common cause failures should be considered for components in systems that are shared between different plants [8]. In case of multi-unit site initiators, it is necessary to review common cause component groups and probabilities.
- The credited recovery action may be also, reviewed. For example, the recovery actions are less probable in a multi-unit LOOP than in a single-unit LOOP.
- In the frame of seismic PSA, for multiple unit sites, the recovery assessment must consider the fact that all units are affected by the ground motion placing additional demands on the resources available for recovery [10].

In the treatment of the internal hazards, the modeling may change if multi-unit aspects are considered. For example, for internal flooding affecting multi-unit sites with shared systems or structures:

- multi-unit areas should be included,
- any potential sources with multi-unit or cross-unit impacts should be included,
- multi-unit scenarios should be considered,
- multi-unit impacts on SSCs and plant initiating events caused by internal flood scenario groups should be included.

The risk metrics that are being employed - such as CDF and LERF - are being developed either for one representative reactor unit or for each reactor independently. Multi-unit reactor accident consequences are currently being ignored and there is no consideration that the frequency of core damage per site year will be increased due to contributions from each reactor at the site [83]. Consequently, for multi-unit or multi-modular plants, in the event sequence progression and end state definition the number of reactor units involved in the release of radioactive

material should be included. It would be interesting to come to a common proposal of risk metrics for a site PSA. Moreover, methodological documents which propose acceptable methods to deal with the risk metrics for a site PSA are not available and it would be interesting to develop them.

The impact of modelling of the site aspects on the definition of Level 1 PSA accident sequences end states as well as the interface with the Level 2 is partly covered by the existing guidelines. It can be also an interesting subject for further development in the frame of ASAMPSA_E (in cooperation with WP40).

It has to be noted that for modular, non-LWR reactors all the aspects presented in this paragraph are applicable [16] even for initiators which affect one unit (composed of multi modules) [16].

5.3.3 STATUS OF MULTI-UNIT PSA MODELING

In the frame of the OCDE-NEA-CSNI-WG-Risk Task on PSA of other external events than earthquake [21], a survey was performed. One of the aspects was the modeling of the impact of external hazards on multi-unit sites. The summary of the survey results is:

- In Canada, common mode impacts that may affect more than one unit are fully addressed in internal events PSA models and will be addressed in any future EE studies.
- In Finland, no special analyses have been carried out for multi-unit sites. However, some interconnections between units have been modeled.
- In France, the external events included in the internal events PSA done by IRSN (i.e., loss of heat sink and loss of external power) consider the impact on multi-unit sites. Some of the advantages and the disadvantages of the multi-unit sites are modeled (plant dependency on some equipment and resources sharing, but also the possibility of mutual help).
- In Germany there are no special considerations for analyzing multi-unit sites.
- In Japan, in the internal PSA event "cross-tie of electric power supplies" among units at the multi-unit site is taken into account, because the cross-tie is realized as one of the accident management measures. There are many research activities regarding simultaneous failure in seismic PSA.
- In Korea there is no special consideration for analyzing multi-unit sites. Only a research program was performed for multi-unit loss of off-site power induced by typhoon. A research program for multi-unit site effects is being prepared.
- In Slovakia, units of multi-unit sites are modeled as independent entities where none credit for support of neighboring units is paid in the case of events that can impact the whole site, e.g. total loss of all off-site power supplies to multi-units is considered in case of seismic event.
- In Switzerland, the support from systems of the other unit (located on the same site) is accounted for in the model. It shall be considered that these systems may not be available due to the external initiating event.
- In Chinese Taipei, there is no special consideration for analyzing multi-unit sites.
- In USA, the risk is evaluated on a per unit basis. Whether the risk for the entire site should be evaluated is an NRC Commission policy issue that has not yet been addressed. Further, most recent studies have not addressed the potential for a single external hazard to cause concurrent accidents at multiple units. However, in

the ASME/ANS standard, while the risk (e.g., CDF from external effects) is calculated on a per unit basis, the effects of one unit on the shared systems at multi-unit sites have to be addressed.

- In Czech Republic, the PSA model for Dukovany NPP is an integrated model, which comprises all initiating events (IEs) for all POSes in the same project. Moreover, models for the odd and even unit are developed in one project as well. They are cross-connected via models of shared equipment for the twin unit. The equipment unavailabilities in the neighbour unit can be, therefore, taken into account. However, the risk is calculated and evaluated separately on per unit basis.

In the UK the ONR Safety Assessment Principles (SAPs) [50] specifies for multi-facility sites:

- When considering the radiological hazards and risks posed by a nuclear site, all the facilities, services and activities on it need to be considered. In most cases, the SAPs are considered in relation to single facilities and so the control of risks is also generally considered on a facility basis. However, there is a need to consider the totality of control of risks from a site (see R2P21 paragraph 136). Two different situations arise: where all the facilities and services are under the control of a single licensee, covered by a single nuclear site licence, and where some of the facilities and services are on neighbouring sites, under the control of different dutyholders. Many of the issues are similar.
- Sites that have multiple facilities often produce a set of individual safety cases for each facility. Shared services are also generally dealt with by separate cases. The division of the site in this way requires the definition of boundaries and interfaces between facilities, facilities and services, and services. It also requires an appropriate combination of the individual analyses to develop the site safety case. This is necessary to account for the interactions and interdependencies between facilities and services.
- Determining whether risks have been controlled and reduced ALARP therefore requires an overall consideration of the site and, in determining if good practices have been met, all risks need to be assessed. On a complex site there will be many different radiological hazards and risks that, in determining the necessary safety measures for the site, may need to be balanced in demonstrating that the overall risks are ALARP.
- In considering the risks from a site, and whether they are ALARP, consideration on a site-wide basis will be needed for certain internal or external hazards that have the potential to affect all the facilities and services on the site.
- Where a site has been considered for analysis purposes as comprising several facilities, a specific consideration of overall site risks should be carried out, unless it can be shown that there are no common shared services or interactions between the facilities, between facilities and shared services and between shared services.
- Where neighbouring sites, which may be under the control of different dutyholders, share common systems or have the potential for interactions, there should be co-operation between them in developing safety cases. Formal mechanisms should be established and demonstrated to be working to regulators. All relevant dutyholders should be able to demonstrate that they are undertaking liaison and acting upon agreed decisions with site owners and all external stakeholders.

Where there are multiple sites in close proximity, a dose constraint should be applied to each site to ensure that the overall dose to a person off the site is below the relevant dose limit. The IRR Guidance¹⁰ advises constraining the dose to members of the public from each source to less than 0.3 mSv pa. HSE's view is that a single source

should be interpreted as a site under a single dutyholder's control, in that it is an entity for which radiation protection can be optimised as a whole.

5.4 WA4 - LINK BETWEEN EXTERNAL INITIATING EVENTS OF PSA AND NPP DESIGN BASIS CONDITIONS

(Contributed by AMEC and supported by LEI)

5.4.1 INTRODUCTION

External hazards have traditionally been defined deterministically, and the design basis hazard magnitude has been based on historical hazard levels. In some instances an additional margin based on judgement was added to provide a conservative value and to account for uncertainties.

When risk based assessments were being developed for plant faults it became necessary to define the hazard risks in a probabilistic manner as well.

5.4.2 HISTORICAL BACKGROUND

The seismic hazard was the first hazard to be assessed probabilistically, and the initial studies were carried out in the 1970s. This coincided with the development of a risk based approach to plant faults, e.g. WASH-1400 in 1975 [58].

The first attempts to combine the deterministic hazards approach with probabilistic considerations were being carried out at about the same time in the UK. In 1982 the (then) Central Electricity Generating Board (CEGB), published a Design Safety Guide (DSG) for the proposed new generation of PWRs. This document defined a probabilistic approach to the seismic and wind hazards, as well as to other design aspects [84]. A similar guide was published in 1985 for the AGRs [85].

The CEGB DSG specified a conservatively assessed design basis level for a site with a cumulative probability of exceedance less than, or equal to 10^{-4} per annum. It was also judged that the probability of failing to shut down and cool the reactor would be no greater than 10^{-3} per demand. Failure was defined as causing a dose to a member of the public greater than 100 mSv.

The design basis frequency of 10^{-4} p.a. was chosen for a number of reasons. The overall probabilistic aim was to demonstrate that the risk to a member of the public from the nuclear power plant was less than 10^{-6} p.a. In order to achieve this aim it was judged that any one significant contributor should be no more than 10% of this target. Combining the 10^{-4} p.a. seismic initiating frequency with a failure probability of 10^{-3} p.d. gave a frequency for a large release (i.e. greater than 100 mSv) of 10^{-7} p.a. This meant that achieving this seismic risk would allow the

overall target risk for the plant to be met (assuming that the contribution from other hazards and plant faults also met the frequency targets).

Conservatively specifying the design basis level also meant that there would be no ‘cliff edge’ at lower seismic frequencies and higher accelerations than the design basis level.

In addition, it was considered that specifying seismic hazard levels at frequencies below 10^{-4} p.a. were increasingly unpredictable and difficult to justify.

For the Sizewell B design the design level for all design basis natural external hazards was taken to be the 10^{-4} p.a. Annual Exceedance Probability (AEP)¹⁷. It was demonstrated during the licensing process that the overall probabilistic risk target for hazards was met [59].

In the UK conservatively specifying the design basis levels for natural hazards at the 10^{-4} p.a. AEP has withstood the test of time. This has become the licensing expectation [50], and there is currently no movement to change or redefine the hazard levels derived at this frequency.

5.4.3 APPLICATION TO CURRENT PLANTS

A review of current literature (listed below) has shown that the 10^{-4} p.a. AEP is the predominant frequency for defining the design basis level of natural external hazards. However, in some countries a lower frequency is now defined (with an increased degree of conservatism), and in particular for the external flooding hazard a lower design basis frequency has been used. In addition, for some countries with low seismicity the 10^{-4} p.a. AEP hazard level is less than the minimum 0.1g acceleration recommended by the IAEA. Where this is the case, in general the deterministic value (i.e. 0.1g) has been used.

The most useful recent source for identifying the design basis frequency used in defining hazard levels in the EU are the stress tests carried out following the Fukushima Dai-ichi Tsunami event. These reports all date from the end of 2011 and a number of updates are available. The following table summarises the positions in 2011. Where the country stress test did not give probabilistically defined hazard levels no entry has been made.

¹⁷ ‘Return period’ is also used for natural hazards which is the inverse of ‘Annual Exceedance Probability’ (AEP).

TABLE 1 - THE DESIGN BASIS FREQUENCY USED IN DEFINING HAZARD LEVELS IN THE EU

Country	Design Hazard Frequency (p.a.)	Hazards Considered
Belgium [60]	10^{-4} 10^{-4} $\sim 6 \times 10^{-7}$	Earthquake External flooding Tornado (wind speed defined deterministically)
Bulgaria [61]	10^{-2} 10^{-4} 10^{-4} 10^{-4}	Design Earthquake (OBE) Maximum Calculated Earthquake (SSE) Wind External flooding. Assessment at 10^{-5} - 10^{-7} p.a.
Czech Republic [62]	10^{-4}	Earthquake External flooding Wind Snow Temperature
Finland [63]	10^{-5} 10^{-5} 10^{-7}	Earthquake External events (general). Much longer for events with “cliff edge” type consequences Design extension for external events
France [64]	10^{-2} 2×10^{-3}	Seismic Maximum Historically Probable Earthquake (10^{-3}) Design basis on Safe Shutdown Earthquake (SSE) $I(SSE) = I(MHPE) + 1$ Lightning (Category 2 incident) Oil slick off the Normandy coast
Germany [65]	10^{-5} 10^{-4} 10^{-4} 2×10^{-2}	Earthquake, median value (new KTA 2201.1) Earthquake using 84% ground motion parameters (historical). External site flooding Wind
Hungary [66]	10^{-4}	Every external natural hazard, assessment to 10^{-7} Listed are: Flooding, Wind, Precipitation, Snow, Maximum temperature, Minimum temperature, Low cooling water level
Netherlands [67]	3×10^{-5} 10^{-6}	Earthquake (deterministically defined at VI½ MMI) Flooding
Romania [68]	10^{-3} 10^{-3} 10^{-4} 10^{-5}	Earthquake Wind (for assessment purposes) Low river level External flooding (high river level)
Slovakia [69]	10^{-4}	Earthquake Precipitation/ flooding Extreme temperatures Wind
Sweden [70]	10^{-5} 10^{-7} 10^{-4} - 10^{-6} 10^{-4} - 10^{-6}	Earthquake Consequence limiting systems Flooding Natural phenomena
Ukraine [71]	10^{-2} 10^{-4}	Design Earthquake (OBE) Maximum Calculated Earthquake (SSE)
United Kingdom [72]	10^{-4}	All natural external hazards, conservatively assessed Note ‘conservatively assessed’ is generally understood to correspond to the 84th percentile, i.e. one standard deviation. It is however recognised that data may not always be available to carry out a suitable statistical analysis

The majority of the countries assessed use the 10^{-4} p.a. AEP as the design basis hazard level. However, some countries assess some or all hazards at a lower AEP, and this reflects developments since the 10^{-4} p.a. frequency was first defined in the late 1970s. In particular, where there are ‘cliff edge’ effects a lower frequency has been specified to take this into account. In addition, using a lower frequency with a reduced confidence level moves the assessment to a ‘best estimate’ rather than ‘conservative design basis’ type of analysis.

Recently, WENRA [57] states that the *“Design basis events shall be defined based on the site specific hazard assessment. The exceedance frequencies of design basis events shall be low enough to ensure a high degree of protection with respect to natural hazards. A common target value of frequency, not higher than 10^{-4} per annum, shall be used for each design basis event. Where it is not possible to calculate these probabilities with an acceptable degree of certainty, an event shall be chosen and justified to reach an equivalent level of safety.”*

Design extension conditions (DEC) are increasingly used. Application of probabilistic techniques approach will allow the overall risks from new plant to be minimised.

The WENRA report [57] states that *“the selection process for DEC A shall start by considering those events and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage. It shall cover:*

- *Events occurring during the defined operational states of the plant;*
- *Events resulting from internal or external hazards;*
- *Common cause failures.*

Where applicable, all reactors and spent fuel storages on the site have to be taken into account. Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity shall be covered.”

5.4.4 NEW REACTOR DESIGNS

The position with respect to new reactors is similar to the above, and any differences reflect the national approach rather than any change in the overall philosophy. The IAEA TECDOC-1487 [14], which addresses advanced nuclear plant design options, notes the following:

- Earthquake consideration is almost uniform among the presented NPPs, with an exceedance probability of 10^{-4} /year. The design basis is in general quite high (0.5 g PGA)¹⁸. There is a disagreement on the vertical component of an earthquake to be used in the design: sometimes it is 0.75 of the horizontal, sometimes it is not mentioned;

¹⁸ The pga values given in the table 1 are for specific sites. The pga values given in TECHDOC 1487 are non site specific, and are therefore specified to encompass all potential sites.

- Flood design is usually accomplished by placing the plant grade above flood elevation. Flood elevation is typically based on a probability of exceedance, which ranges between 10^{-3} /year to 10^{-6} /year. A reasonable probability of exceedance consistent with other design basis external events might be 10^{-4} /year probability of exceedance, recognizing the need to avoid cliff edge effects;
- As a result of varying national experience with wind loads, there does not appear to be any consensus with respect to wind load design with probabilities of exceedance, which range from 10^{-2} /year for straight wind to 10^{-7} /year for tropical cyclones (tornadoes). A reasonable compromise may be a 10^{-4} /year probability of exceedance from all wind sources in the range of 50 m/sec for a 3 second gust.
- Precipitation (rain, snow or ice) loads appear to be based on national norms. Where such norms exist, they are usually given as numerical values taken from national maps. These maps are typically based on a probability of exceedance level of 2×10^{-2} /year. Once these precipitation loads are determined for design purposes, they are typically multiplied by load factors, which range between 1.5 and 2.0. As a result, the actual probability of exceedance of such precipitation loads, when explicitly considered in design, is between 2×10^{-3} /year and 10^{-3} /year probability of exceedance.

The possibility for beyond design basis events receives more and more emphasis in siting procedures for advanced NPPs; however, there is no common stance on the probability of exceedance to be associated with such scenarios: sometimes it is 10^{-7} /year; sometimes it is 10^{-4} /year; and sometimes it is deterministic.

It should be noted that for some new standardized reactors the above earthquake design values are non-site specific, and are therefore specified to envelope all potential sites. Most sites will have a lower PGA.

5.4.5 SAFETY BASED DESIGN

The design basis for any plant and site is deeply related to the effects of any postulated external events and the limitation of the plant capability to cope with accidents i.e. perform safety functions [14]. In the Safety-by-Design^{TM19} approach, the Probabilistic Safety/Risk Assessment (PRA) plays a key role therefore a Preliminary PRA can be developed along with the design. For the design and pre-licensing process of NPP the external events analysis may include both qualitative evaluation and quantitative assessment. In general, applying the quantitative assessment, bounding site characteristics can be used in order to minimize potential future restrictions on plant siting and risk zoning [74], [79].

The key idea of the Safety-by-DesignTM concept is to physically eliminate the possibility of occurrence or to reduce consequences of accidents, rather than focusing only on the mitigation phase. The most evident implication of this design approach is the choice of an integral reactor configuration, where for instance the integral reactor vessel (e.g. containing internal steam generators and reactor coolant pumps), the consequential absence of large primary

¹⁹ This is a term used by Westinghouse for the study referred to.

pipes, the recently introduced internal control rod drive mechanism and a secondary side designed for full primary pressure to the secondary isolation valves have possibility either eliminate major design basis events such as Large Break LOCA or significantly reduce the consequences of them. This unprecedented application of the PRA techniques in the initial design phase of the reactor and the deep impact that this is having in the development of the project has been described in already published papers [77], [78] and [80].

The Safety-by-Design™ approach, used by the designers of NPP to eliminate the possibility of occurrence of certain severe accidents caused by internal events, is being extended to the external events. The focus can be on the balance of plant (BOP) that has not been analyzed as extensively or explicitly as NPP accidents caused by internal events. However, since extreme external events have one of the largest contributions to the degradation of the defence in depth barriers, the external events represent a major challenge to the designer in order to define design basis parameters and criteria (e.g. for meteorological variables [52]) as well as to determine siting parameters and to reduce the total risk.

It has been observed that the PRA methodologies to deal with Emergency Planning Zones (EPZ) and external events have not reached the same level of maturity as for internal events [73]. In general, the EPZs are defined as well as plant site and arrangement structures are designed to minimize the potential for natural and manmade hazards external to the plant from affecting the plant safety related functions, which can affect nearby population and environment. This may include consideration of extreme winds, fires, flooding, aircraft crash, seismic activity, etc. Thus the design basis for plant and site is deeply related to the effects of any postulated external events and the limitation of the plant capability to cope with accidents i.e. perform safety functions.

While for the “older” plants accidents initiated by internal events were typically dominant, PRAs for existing and advanced plants, with improved design of safety systems, have shown that external events may now account for a significant fraction of the total public risk due to specific plant vulnerabilities. Moreover, evaluation of external events can be used to determine if there are any unforeseen vulnerabilities in the design that can be eliminated by design during the still evolving design phase of the reactor.

Accident prevention is the main driving force for advanced reactor designs. Several design innovations are currently aimed towards bringing down conditional core damage frequencies to an extent that makes the plant less vulnerable to accident scenarios related to internal events, extreme external events and even malevolent events such as terrorist attacks.

In general, even taking into consideration the expected large diversities in the design features of advanced reactors, siting and emergency requirements, as well as risk zoning criteria for advanced reactors appear to need some modifications, with respect to the conventional approach developed for older reactors. Recent efforts to get benefits from adopting a complete risk-informed, performance-based regulatory process and licensing of new NPP (e.g. [81]) is a clear indication that advanced reactor designs are credited to be safer and a certain degree of recognition for the effort in increasing the safety level can be accomplished.

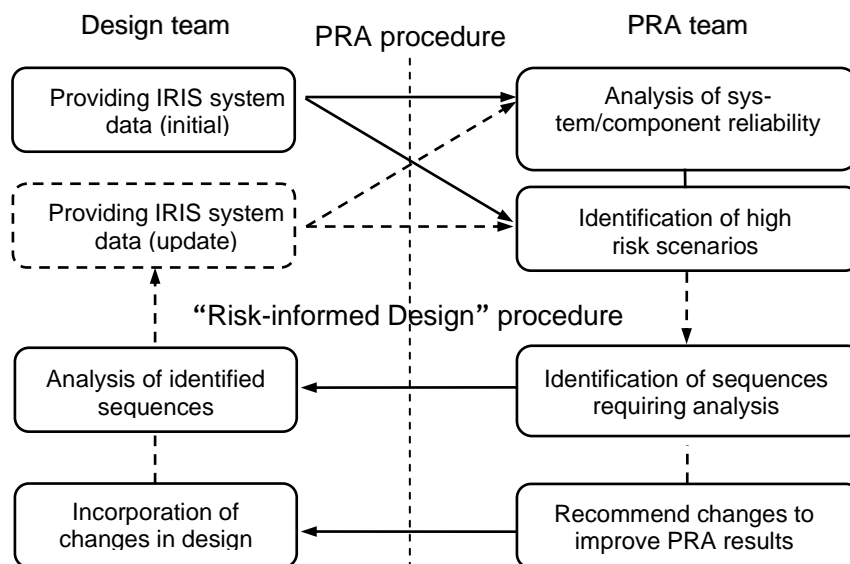
The success of the Safety-by-Design™ approach [78], i.e. PRA-guided design is due to the effective interactions between the Design team and the PRA team (see Figure 3). The main task of the PRA team is to identify high risk events and sequences.

The Design team provides information concerning the plant and site design. It updates component/system description and design data. PRA team identifies assumptions concerning plant and site design requirements. The Design team then reviews assumptions concerning plant and site design requirements.

A preliminary evaluation of internal and external events can be performed in the Preliminary PRA, to determine if there were any unforeseen vulnerabilities in the plant design that could be eliminated by design during the still evolving design phase of the plant.

Being still in a design development/refinement phase, the PRA may be kept constantly updated with the evolution of the design; moreover, all the assumptions, required to have a reasonably complete PRA model capable of providing quantitative insights as well as qualitative considerations, might be accurately tracked down and the uncertainties connected with such assumptions might be assessed.

FIGURE 3 DESIGN TEAM AND THE PRA TEAM INTERACTION PROCEDURE



The same method can be extended also to any low frequency extreme events and severe accidents. In comparison to events dominant in other plant PRA, the plant designed using Safety-by-Design™ approach is expected to be significantly less vulnerable to some external events. In general, the plant arrangement structures can be designed to minimize the potential for natural and manmade hazards external to the plant from affecting the plant safety related functions. The external events PRA insights are expected to help taking full advantage of the potential safety oriented features of the plant design, which will imply probabilistic consideration of extreme winds, fires,

flooding, aircraft crash, seismic activity, etc. In addition, it can be shown that estimation of risk measures is related to the site size and can be the input for emergency zone planning. In external events PRA (e.g. [76]), the focus currently can be set on the plant BOP, that has not been analyzed as extensively or explicitly as accidents caused by internal events.

Within this framework the information gathered from the PRA (both internal and external events) can be also used to provide a basis for the redefinition of the EPZ defining criteria [74]. The proposed approach consists of coupling the PRA results with deterministic dose evaluations associated to each relevant PRA sequence considered, and thus achieving a technically sound bases for the definition of a plant specific EPZ. In this approach the two basic components of risk (i.e. probability of occurrence and consequences of a given accident) are therefore explicitly combined. The EPZ radius then can be defined as the distance from the plant such that the probability of exceeding the dose limit triggering the actuation of emergency procedure is equal to a specified threshold value. To identify this threshold value, detailed analysis of existing installations can be performed to infer the risk and economic factors associated with the current EPZ definition [74].

It must be noticed that the use of existing regulations and installations as the basis for this redefinition may not in any way impact the high degree of conservatism inherent in current regulations. Moreover, the remapping process makes this methodology partially independent from the uncertainties still affecting probabilistic techniques. Notwithstanding these considerations, it is still expected that applying this methodology to advanced plant designs with improved safety features will allow significant reductions in the emergency planning requirements, and specifically the size of the EPZ. In particular, in the case of plant designed using Safety-by-Design™ approach it is expected that this will allow a dramatic reduction in the EPZ requirement, while still maintaining a level of protection to the public fully consistent with existing regulations.

5.5 DOCUMENTS REVIEW

(Contributed by all WA leads and ASAMPSA_E partners)

The APPENDIX 1 - DOCUMENTS REVIEW RESULTS briefly discusses publically available guidelines and their applicability for the development of extended L1 PSAs. The following table summarizes the documents which have been considered.

TABLE 2 LIST OF REVIEWED DOCUMENTS

	Reference	WA1	WA2	WA3	WA4	Remarks
1	IAEA SSG-3	x	x	x		General
2	IAEA NS-G-2.13	x				Seismic
3	IAEA - A Methodology to Assess the Safety Vulnerabilities of Nuclear Power Plants against Site Specific Extreme Natural Hazards, 2011	x				Extreme Natural Hazards /weather, Seismic, Flood

	Reference	WA1	WA2	WA3	WA4	Remarks
4	NUREG/CR-2300, Volume 2 PRA	x	x			General
5	NUREG/CR-4840	x				Earthquake, Fire, Flood
6	ASME/ANS RA-Sa-2009	x	x	x		Seismic, High winds, External Floods
7	IAEA-TECDOC-1511	x	x	x		General
8	IAEA 50-P-7	x	x			Earthquake, High winds, Flood, Man-induced events
9	EPRI 1002989	x	x	x		Seismic
10	IAEA-TECDOC-724	x				Seismic
11	IAEA SSG-21	x				Volcanic Hazard
12	IAEA NS-G-3.1	x	x			Human Induced Events
13	IAEA TECDOC-1487	x	x		x	General Seismic
14	EPRI-1009652	x		x		General Risk Informed
15	ASME NON-LWR (DRAFT)	x		x		General Int. Flooding Seismic
16	ASN - RFS 2002-1		x			General
17	CNSC S-295	x	x			General
18	WENRA Issue O	x	x			All External Events
19	NEA/CSNI/R(2009)1	x				Seismic
20	NEA/CSNI/R(2009)4	x		x		Non-Seismic Hazard
21	NEA/CSNI/R(2011)6	x				Seismic
22	NEA/CSNI/R(2010)10/Part2		x			General SAM Measures L1-L2 interface
23	NEA/CSNI/R(97)22	x	x			Seismic
24	NEA/CSNI/R(2007)17	x	x			Seismic
25	NEA/CSNI/R(2011)8	x				Missiles
26	ENSI-A05/e	x				General
27	SKI, Report 02:27	x	x			Non-Seismic External Events
28	Department of Energy "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities, January 2002, Superseding DOE-STD-1020-2002, 2013"	x				All Natural Hazards
29	10CFR 50.54(f)	x				All External Events
30	EUR 2001 "Volume 2 Generic Nuclear Island Requirements. 2.1 Safety requirements. 2.17 PSA Methodology. Revision D"	x	x			General
31	O. Nusbaumer, and A. Rauzy, In Journal of Risk and Reliability. Professional Engineering Publishing. Vol. 227, Num. 3, pp 315-326, June, 2013.	x				FT-ET Linking
32	M. Hibti, T. Friedlhuber & A. Rauzy, Automated Generation of Event Trees from Event Sequence/Functional Block Diagrams and Optimisation Issues, PSAM Tokyo, 2013	x				ET
33	EPRI TR-103959	x				Seismic
34	EPRI-1002988	x				Seismic
35	EPRI-1019200	x				Seismic
36	NUREG 6850, EPRI/NRC-RES	x				Fire
37	IAEA Safety Series No. 50-P-10		x			HRA
38	EPRI 1019196 - NUREG-1921		x			Fire/HRA
39	WENRA RHWG, Safety of New NPP Designs - March 2013		x			General
40	WENRA "Position paper on Periodic Safety Re-views (PSRs)", March 2013			x		General

	Reference	WA1	WA2	WA3	WA4	Remarks
41	Fleming, Karl N. In Proceedings of the AMS International Topical Meeting on Probabilistic Safety Analysis, pp. 11-15. 2005.			x		Flooding Earthquake
42	Suzanne Schroer, Mohammad Modarres, An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment, Reliability Engineering & System Safety, Volume 117, September 2013, Pages 40-51, ISSN 0951-8320,			x		Not available publically
43	Pickard Lowe And Garrick Inc., "Seabrook Station Probabilistic Safety Assessment -Section 13.3 Risk of Two Unit Station", Prepared for Public Service Company of New Hampshire, PLG-0300, 1983			x		Not available publically
44	U.S. Nuclear Regulatory Commission. (2012). Full-Scope Site Level 3 Probabilistic Risk Assessment Project.			x		No summary
45	U.S. Nuclear Regulatory Commission. (2012). NUREG-0800, Chapter 19			x		No summary
46	NUREG/CR-6813			x		No summary
47	NRC Handbook "Risk Assessment of Operational Events - Revision 1.03", August 2009			x		General
48	IAEA-TECDOC-1341			x		General
49	HSE Safety Assessment Principles for Nuclear Facilities 2006 , Revision 1			x	x	General
50	IAEA NS-R-3			x		General
51	IAEA SSG-18			x	x	Meteorological and Hydrological Hazards
52	IAEA-TECDOC-1135			x		General Regulatory Review
53	NEA/CSNI/R(2004)20			x		Risk Monitors
54	Woo Sik Jung, Joon-Eon Yang, Jaejoo Ha - Korea Atomic Energy Research Institute			x		Multi-unit site
55	EPRI 1022997			x		General External Hazards
56	WENRA-RHWG, Guidance Document Issue T: Natural Hazards.			x		Natural Hazard
57	NUREG-75/014 (WASH-1400)				x	No summary
58	C Dawson, J Mustoe. The Sizewell 'B' PWR: Results of the Probabilistic Safety Assessment for Hazards. European Safety and Reliability Conference (ESREL '95), June 1995, Bournemouth.				x	No summary
59	Belgian EU Stress Test 2011				x	No summary
60	Bulgarian EU Stress Test 2011				x	No summary
61	Czech Republic EU Stress Test 2011				x	No summary
62	Finnish EU Stress Test 2011				x	No summary
63	French EU Stress Test 2011				x	No summary
64	German EU Stress Test 2011				x	No summary
65	Hungarian EU Stress Test 2011				x	No summary
66	Netherland EU Stress Test 2011				x	No summary
67	Romanian EU Stress Test 2011				x	No summary
68	Slovakian EU Stress Test 2011				x	No summary
69	Swedish EU Stress Test 2011				x	No summary
70	Ukrainian EU Stress Test 2011				x	No summary
71	ONR Technical Assessment Guide - External Hazards. T/AST/013 - Issue 4, July 2011				x	General
72	Alzbutas R., et al "External Events Analysis and Probabilistic Risk Assessment Application for IRIS Plant Design"				x	No summary
73	Alzbutas R., Maioli A. Risk zoning in relation to risk of external events (application to IRIS design)				x	No summary
74	Alzbutas R., Norvaiša E., Maioli A. Analysis of emergency planning zones in relation to probabilistic risk assessment and economic optimization for international reactor innovative and secure				x	No summary
75	ANSI/ANS-58.21-2003				x	No summary
76	Carelli M. D., Petrovic B., Ferroni P., "IRIS Safety-by-Design™ and Its Implications to Lessen Emergency Planning Requirements,"				x	No summary
77	Carelli, M. D., et al., "The Design and Safety Features of the IRIS Reactor",				x	No summary

	Reference	WA1	WA2	WA3	WA4	Remarks
78	IAEA-TECDOC-1652.				x	No summary
79	Maioli, A., D. J. Finnicum, Y. Kumagai, "IRIS Simplified LERF Model,"				x	No summary
80	NEI 02-02, A Risk-Informed Performance-Based Regulatory Framework For Power Reactors, Washington, 2002.				x	No summary
81	ANSI/ANS-58.21-2007 "External-events PRA methodology", 2007. This standard was superseded by ASME/ANS RA-Sa-2009 [9]			x		Not available publically
82	NUREG/CR-6813			x		General Not available publically
83	CEGB Pressurised Water Reactor Design Safety Guidelines, April 1982. This document is now out of print.				x	Seismic and Wind Hazard Not available publically
84	CEGB Advanced Gas-cooled Reactor Design Safety Guidelines, August 1985. This document is now out of print.				x	Not available publically
85	NUREG/CR-1278		x			General HRA
86	NUREG/CR-4772		x			ASEP HRA
87	UCRL-CR-135687 S/C B505188	x				Wind-Borne Missile
88	NUREG/CR-7004	x				Hurricane-Borne Missile
89	I.A.Rahmant et al.: Review on Empirical Studies of Local Impact Effects of Hard Missile on Concrete Structures	x				Missiles

6 CONCLUSIONS

6.1 CONCLUSION OF WA1 (EXTERNAL HAZARDS IMPACT ON SSC MODELING IN L1 PSA)

WA1 was oriented on evaluation of impact of external hazards and combination of events on the SSCs modeled in L1 PSA event trees. The work was divided in three basic parts:

- Practices to assess the (conditional) failure probabilities of SSC depending on the influences of hazard or combination of events induced by particular hazards.
- Assurance of consistency between the assumptions used in existing L1 PSA and assumptions for extended PSA covering external hazards
- Modeling the impact of events combination in PSA

Practices to assess the (conditional) failure probabilities of SSC depending on the influences of combination of events induced by particular hazards are covered by Section 5.1.1. This chapter demonstrates that available guidelines provide usable recommendations to evaluate failure probabilities of SSCs depending on the influence of single hazard or events combination. The most detailed guidelines are devoted to the seismic events and fires. Even if these guidelines that are described in APPENDIX 1 - DOCUMENTS REVIEW RESULTS deal only with single event impact they can be also used for combined events purpose to evaluate particular effects induced by analyzed external hazards.

Consequently if assessment of SSCs failure probabilities can be supported by data for example from design basis, relevant inputs for PSA can be obtained. For beyond design external hazards, difficulties can be encountered to determine such failure probabilities and can be discussed in the ASAMPSA_E project.

Consistency between assumptions used in existing PSA and extended PSA covering combination of events induced by external hazards is discussed in Section 5.1.2. This part deals mainly with determination of scope of SSCs for extended PSA and failure modes. Many of quoted guidelines provide general systematic framework how to develop such extended list of components. Scope of considered failure modes obviously follows from nature of analyzed hazards like mechanical load, heat produced by fires etc.

Modeling of impact of events combination in PSA is presented in Section 5.1.3. This part provides a generic example of typical approach that uses standard PSA software to combine fault and event trees. It should be noted that particular approach will strongly depend on used software.

In general available guidelines provide detailed framework for analysis of seismic event. The other external hazards are not always covered so deeply. This is probably caused by specific site nature of these hazards like external floods, fires etc. Within ASAMPSA_E, examples of applications shall be discussed for seismic events and solutions for the other hazards.

6.2 CONCLUSION OF WA2 (HUMAN RISK ASSESSMENT)

Most of the available guidelines provide general recommendations and a framework to assess the human factor depending on the external event. More detailed information and HRA models are available for seismic events or induced internal fire events. For the other external hazards, the literature with regard to HRA is not well developed.

It may be concluded that the PSA for external hazards should take account the potential for human response to be affected by the external event. The grace time for operator intervention for mitigation of external event effects is an important factor that needs to be considered in analysis. The additional stresses that can increase the likelihood of human errors or inattention should be examined, compared to the likelihood assigned in the internal events HRA, when the same activities are undertaken in non-hazard accident sequences.

However, the basis for determining these increases is not well developed in the PSA literature. This is something important and missing in the existing documentation since whether or not increases in error probabilities are used, the basis for this decision about what error rates to use should be justified. During revision, it should be verified that the HRA adequately accounts for the additional influences caused by external event, that HFEs adopted from an Internal Events PRA have been modified as appropriate to reflect external hazard effects and new HFEs are included to account for specific hazard related actions that are consistent with plant procedures that were not covered by the Internal Events PRA.

6.3 CONCLUSIONS OF WA3 (MULTI-UNITS IMPACTS)

The general practice of performing safety assessment for multiple reactor units on the site is to analyze one reactor at a time and not considering several important multi-unit dependencies and interactions in both deterministic and probabilistic safety assessments.

In order to obtain the site's risk profile, the CDF for the site rather than the unit is necessary to be considered. Even there is not specific standard for the treatment in the PSA of the events affecting multi units (on a given site), many recent standards are applicable to plant level which is defined as a nuclear power facility, which may refer to a single-unit or multi-unit site. Many aspects highlighted by these standards are directly, or with a minimum of adaptation, applicable to the modeling of events affecting multi-unit sites. The existing PSA methods and tools are, in general, applicable for the PSA of multi-units events. The main issue of PSA for multi-unit sites is to ensure the analysis completeness mainly regarding the treatment of the aspects which are more specific for

such sites and events. The ASAMPSA_E guidelines may be focused on these aspects: ensure the completeness of the analysis and modeling (based on existing PSA modeling techniques) of specific aspects for PSA treating events affecting multi-units on one site and integration of obtained results on plant and site level.

Regarding the risk metrics for a site PSA the existing standards and documents give some high level requirements. It would be interesting to come to a common proposal of risk metrics for a site PSA. Moreover, methodological documents which propose acceptable methods to deal with the risk metrics for a site PSA are not available and it would be interesting to develop them.

Also the impact of the modelling of the site aspects on the definition of Level 1 PSA accident sequences End States as well as on the interface with the Level 2 can be an interesting subject for further development in the frame of ASAMPSA_E (in cooperation with WP40).

6.4 CONCLUSIONS OF WA4 (LINK WITH DESIGN BASIS)

If one frequency is to be used, this should be the conservatively assessed hazard level that corresponds to a 10^{-4} p.a. AEP. As noted in Section 5.4, 'conservatively assessed' is generally understood to correspond to the 84th percentile²⁰ confidence level, i.e. one standard deviation. It must however be recognised that data is not always be available to carry out a suitable statistical analysis. Where this is the case engineering judgement must be used.

Where cliff edge effects may occur (e.g. external flooding) a lower frequency should be considered. It is noted that frequencies of 10^{-5} and 10^{-6} p.a. have been used for this hazard.

The frequency level for design extension conditions should also be defined. A value below the design basis level, 10^{-7} p.a. or 10^{-8} p.a. (depending on the overall risk target), should be considered.

Defining the hazard at a given frequency is not in itself enough. There should also be a statement as to whether the hazard is conservatively assessed, and where this is the case the conservatism should be quantified (if practicable).

Finally the approach needs to take into account whether the frequency and hazard levels are to be used for design basis purposes (i.e. with a conservative approach) or for design extension and PSA purposes (i.e. best estimate). The data derived should be used appropriately.

²⁰ The 84th percentile is generally understood in the UK and was used in Germany. Therefore this confidence level is stated.

7 LIST OF REFERENCES

- [1] ASAMPSA_E - Grant Agreement N° 605001 - Description of work
- [2] IAEA Specific Safety Guide No.SSG-3 “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants”, 2010
- [3] IAEA Safety Guide NS-G-2.13 Evaluation of Seismic Safety for Existing Nuclear Installations, 2009
- [4] IAEA - A Methodology to Assess the Safety Vulnerabilities of Nuclear Power Plants against Site Specific Extreme Natural Hazards, 2011
- [5] NUREG/CR-2300, Volume 2 PRA Procedures Guide, 1983
- [6] NUREG/CR-4840 Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150, 1990
- [7] ASME/ANS RA-Sa-2009 Addenda to ASME/ANS RA-S-2008 Standard for Level 1 /Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, 2009
- [8] IAEA-TECDOC-1511 Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants
- [9] IAEA 50-P-7 Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants
- [10] EPRI 1002989 Seismic Probabilistic Risk Assessment Implementation Guide
- [11] IAEA-TECDOC-724 Probabilistic safety assessment for seismic events
- [12] IAEA Safety Standard Series No. SSG-21 “Volcanic Hazards in Site Evaluation for Nuclear Installations”
- [13] IAEA Safety Standard Series No. NS-G-3.1 “External Human Induced Events in Site Evaluation for Nuclear Power Plants”
- [14] IAEA TECDOC-1487 “Advanced nuclear plant design options to cope with external events”
- [15] EPRI-1009652 “Guideline for the Treatment of Uncertainty in Risk Informed Applications”
- [16] ASME NON-LWR (DRAFT) “Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications” (recommended by NRC but probably still in draft version)”
- [17] ASN - RFS 2002-1 “Development and utilisation of probabilistic safety assessments December 2002”
- [18] CNSC S-295 “Probabilistic Safety Assessment (PSA) for Nuclear Power Plants”
- [19] WENRA Issue O “Reactor Safety Reference Levels, Issue O, Probabilistic Safety Analysis”
- [20] NEA/CSNI/R(2009)1 “PROCEEDINGS of the Workshop on Recent Findings and Developments in Probabilistic Seismic Hazards Analysis (PSHA) Methodologies and Applications - Lyon, France, 7-9 April 2008”
- [21] NEA/CSNI/R(2009)4 “Probabilistic safety analysis of other external events than earthquake”
- [22] NEA/CSNI/R(2011)6 “NEA/IAEA Workshop on “Soil Structure Interaction (SSI) Knowledge and Effect on Seismic Assessment of NPPs Structures and Components” - Workshop Proceedings, Ottawa, Canada, 6-8 October 2010”
- [23] NEA/CSNI/R(2010)10/Part2 “Implementation of Severe Accident Management Measures, ISAMM 2009”
- [24] NEA/CSNI/R(97)22 “State of the art report of the current status of methodologies for Seismic PSA”
- [25] NEA/CSNI/R(2007)17 “Differences approach between nuclear and conventional seismic standards with regard to hazard definition”
- [26] NEA/CSNI/R(2011)8 “Improving robustness assessment methodologies for structures impacted by missiles”
- [27] ENSI-A05/e “Probabilistic Safety Analysis (PSA): Quality and Scope, Guideline for Swiss Nuclear Installations”
- [28] SKI, Report 02:27 “Guidance for External Events Analysis”
- [29] Department of Energy “Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities, January 2002, Superseding DOE-STD-1020-2002, 2013”

- [30] 10CFR 50.54(f) (Generic Letter no. 88-20, Supplement 4) "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, USA, 1991"
- [31] EUR 2001 "Volume 2 Generic Nuclear Island Requirements. 2.1 Safety requirements. 2.17 PSA Methodology. Revision D"
- [32] O. Nusbaumer, and A. Rauzy, *Fault Tree Linking versus Event Tree Linking Approaches: a Reasoned Comparison*. In *Journal of Risk and Reliability*. Professional Engineering Publishing. Vol. 227, Num. 3, pp 315-326, June, 2013.
- [33] M. Hibti, T. Friedlhuber & A. Rauzy, *Automated Generation of Event Trees from Event Sequence/Functional Block Diagrams and Optimisation Issues*, PSAM Tokyo, 2013
- [34] EPRI TR-103959 "Methodology for Developing Seismic Fragilities", June 1994
- [35] EPRI-1002988 "Seismic Fragility Application Guide", December 2002
- [36] EPRI-1019200 "Seismic Fragility Applications Guide Update", December 2009
- [37] NUREG 6850, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.
- [38] IAEA Safety Series No. 50-P-10 "Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants"
- [39] EPRI 1019196 - NUREG-1921 "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines"
- [40] WENRA Reactor Harmonization Working Group RHWG, *Safety of New NPP Designs* - March 2013
- [41] WENRA "Position paper on Periodic Safety Re-views (PSRs) taking into account the lessons learnt from the TEPCO Fukushima Dai-ichi NPP accident", March 2013.
- [42] Fleming, Karl N. "On The Issue of Integrated Risk-A PRA Practitioners Perspective." In *Proceedings of the AMS International Topical Meeting on Probabilistic Safety Analysis*, pp. 11-15. 2005.
- [43] Suzanne Schroer, Mohammad Modarres, *An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment*, *Reliability Engineering & System Safety*, Volume 117, September 2013, Pages 40-51, ISSN 0951-8320, <http://dx.doi.org/10.1016/j.res.2013.03.005>.
- [44] Pickard Lowe And Garrick Inc., "Seabrook Station Probabilistic Safety Assessment -Section 13.3 Risk of Two Unit Station", Prepared for Public Service Company of New Hampshire, PLG-0300, 1983
- [45] U.S. Nuclear Regulatory Commission. (2012). *Full-Scope Site Level 3 Probabilistic Risk Assessment Project*. Washington, D.C.
- [46] U.S. Nuclear Regulatory Commission. (2012). *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition-Severe Accidents: Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors (NUREG-0800, Chapter 19)*. Washington, D.C.
- [47] NUREG/CR-6813 "Issues and Recommendations for Advancement of PRA Technology In Risk-Informed Decision Making", April 2003
- [48] NRC Handbook "Risk Assessment of Operational Events - Revision 1.03", August 2009
- [49] IAEA-TECDOC-1341, *Extreme External Events in the Design and Assessment of Nuclear Power Plants*, Vienna, 2003
- [50] HSE *Safety Assessment Principles for Nuclear Facilities 2006 Edition*, Revision 1
- [51] IAEA Safety Requirements No. NS-R-3, *Site Evaluation for Nuclear Installations*, 2003
- [52] IAEA SSG-18, *Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations*, 2011
- [53] IAEA-TECDOC-1135 *Regulatory Review of Probabilistic Safety Assessment (PSA) Level 1*, 2000

- [54] NEA/CSNI/R(2004)20, Risk Monitors: The State of the Art in their Development and Use at Nuclear Power Plants - 2004
- [55] Woo Sik Jung, Joon-Eon Yang, Jaejoo Ha - Korea Atomic Energy Research Institute, A new method to evaluate alternate AC power source effects in multi-unit nuclear power plants
- [56] EPRI 1022997 Identification of External Hazards for Analysis in Probabilistic Risk Assessment. Technical Update, December 2011.
- [57] WENRA-RHWG, Safety Reference Levels for Existing Reactors Update in relation to lessons learned from TEPCO Fukushima Dai-ichi accident. 30 May 2014.
- [58] Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants [NUREG-75/014 (WASH-1400)], October 1975
- [59] C Dawson, J Mustoe. The Sizewell 'B' PWR: Results of the Probabilistic Safety Assessment for Hazards. European Safety and Reliability Conference (ESREL '95), June 1995, Bournemouth.
- [60] Belgian EU Stress Test 2011
- [61] Bulgarian EU Stress Test 2011
- [62] Czech Republic EU Stress Test 2011
- [63] Finnish EU Stress Test 2011
- [64] French EU Stress Test 2011
- [65] German EU Stress Test 2011
- [66] Hungarian EU Stress Test 2011
- [67] Netherland EU Stress Test 2011
- [68] Romanian EU Stress Test 2011
- [69] Slovakian EU Stress Test 2011
- [70] Swedish EU Stress Test 2011
- [71] Ukrainian EU Stress Test 2011
- [72] ONR Technical Assessment Guide - External Hazards. T/AST/013 - Issue 4, July 2011
- [73] Alzbutas R., Augutis J., Maioli A., Finnicum D.J., Carelli, M. D., Petrovic B., Kling C.L., Kumagai Y., "External Events Analysis and Probabilistic Risk Assessment Application for IRIS Plant Design" 13th International Conference on Nuclear Engineering (ICONE-13), Beijing, China, Atomic Energy Press, CD: 8 pp., May 16-20, 2005.
- [74] Alzbutas R., Maioli A. Risk zoning in relation to risk of external events (application to IRIS design) // International journal of risk assessment and management. ISSN 1466-8297.2008. Vol 8, No. 1/2, p. 104-122.
- [75] Alzbutas R., Norvaiša E., Maioli A. Analysis of emergency planning zones in relation to probabilistic risk assessment and economic optimization for international reactor innovative and secure // Nuclear power plants / Ed. Soon Heung Chang. Rijeka, Croatia : InTech, 2012. ISBN 978-953-51-04087, p. 1-18.
- [76] ANSI/ANS-58.21-2003 External-Events PRA Methodology, American Nuclear Society, March 3, 2003.

- [77] Carelli M. D., Petrovic B., Ferroni P., "IRIS Safety-by-Design™ and Its Implications to Lessen Emergency Planning Requirements," 13th International Conference on Nuclear Engineering (ICONE-13), Beijing, China, May 16-20, 2005.
- [78] Carelli, M. D., et al., "The Design and Safety Features of the IRIS Reactor", Nuclear Engineering and Design, Vol. 230, 151-167, 2004.
- [79] IAEA-TECDOC-1652. Small reactors without on-site refuelling: neutronic characteristics, emergency planning and development scenarios // Vienna: International Atomic Energy Agency, 2010.
- [80] Maioli, A., D. J. Finnicum, Y. Kumagai, "IRIS Simplified LERF Model," Proc. of ANES 2004 Conf., Miami, FL, October 3-6, 2004.
- [81] NEI 02-02, A Risk-Informed Performance-Based Regulatory Framework For Power Reactors, Washington, 2002.
- [82] ANSI/ANS-58.21-2007 "External-events PRA methodology", 2007. This standard was superseded by ASME/ANS RA-Sa-2009 [9]
- [83] NUREG/CR-6813 - K. Fleming Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making, 2003
- [84] CEGB Pressurised Water Reactor Design Safety Guidelines, April 1982. This document is now out of print.
- [85] CEGB Advanced Gas-cooled Reactor Design Safety Guidelines, August 1985. This document is now out of print.
- [86] NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, August 1983
- [87] NUREG/CR-4772, Accident Sequence Evaluation Program, Human Reliability Analysis Procedure, February 1987
- [88] James R. McDonald, Ph.D., P.E.: Rationale for Wind-Borne Missile Criteria for DOE Facilities, UCRL-CR-135687 S/C B505188 Lawrence Livermore National laboratory, September 1999
- [89] NUREG/CR-7004 Technical Basis for Regulatory Guidance on Design-Basis Hurricane-Borne Missile Speeds for Nuclear Power Plants
- [90] I.A.Rahmant et al.: Review on Empirical Studies of Local Impact Effects of Hard Missile on Concrete Structures, International Journal of Sustainable Construction Engineering & Technology.

8 BIBLIOGRAPHY

Theses references are not publically available and no separate summary included.

- I. M.C. Cheok, G.W. Parry, R.R. Sherry, "Use of importance measures in risk informed regulatory applications", Reliab Eng Syst Safety, 60 (1998) 213-226.
- II. E. Borgonovo, "Differential, criticality and Birnbaum importance measures: an application to basic vent, groups and SCCs in event trees and binary decision diagrams", Reliab Eng Syst Safety, 92 (2007) 1458-1467.
- III. E. Borgonovo, G.E. Apostolakis, S. Tarantola, A. Saltelli, "Comparison of global sensitivity analysis techniques and importance measure in PSA", Reliability Engineering and System Safety (2003) 175-185.

- IV. E. Borgonovo, G.E. Apostolakis, "A new importance measure for risk-informed decision making", *Reliab Eng Syst Safety*, 72 (2001) 193-212.
- V. E. Borgonovo, 2010, "The reliability importance of components and prime implicants in coherent and non-coherent system including total-order interactions", *European Journal of Operational Research* 204 (2010) 485-495.
- VI. X.Gao, L. Cui. J Li, "Analysis for Joint importance of components in a coherent system", *Reliab Eng Syst Safety*, 182 (2007) 282-299.
- VII. H. Rabitz, O.F. Alis, "General foundations of high-dimensional model representations", *Journal of Mathematical Chemistry* 25 (1999), 197-233.
- VIII. E. Borgonovo, 2010, "Sensitivity analysis with finite changes: An application to modified EOQ models", *European Journal of Operational Research* 200 (2010) 127-138.
- IX. I.M. Sobol, "Global Sensitivity indices for nonlinear mathematical models and their MonteCarlo estimates", *Mathematics and Computers In Simulation* 55 (2001) 271-280.
- X. T. Homma, A. Saltelli, "Importance measures in global sensitivity analysis of nonlinear models", *Reliab Eng Syst Safety*, 52 (1996) 1-17.
- XI. Saltelli A., S. Tarantola and K.P.S. Chan (1999). A quantitative model-independent method for global sensitivity analysis of model output. *Technometrics*, 41, 39-56.
- XII. J.C. Helton, J.D. Johnson, C.J. Sallaberry, C.B. Storlie, "Survey of sampling-based methods for uncertainty and sensitivity analysis", *Reliab Eng Syst Safety* 91 (2006) 1175-1209.
- XIII. A. Saltelli, "Making Best use of model valuation to compute sensitivity indices", *Computer Physic Communication*, 145 (2002) 280-297.

9 LIST OF TABLES

TABLE 1 THE DESIGN BASIS FREQUENCY USED IN DEFINING HAZARD LEVELS IN THE EU

TABLE 2 LIST OF REVIEWED DOCUMENTS

TABLE 3 RISK METRIC AND THEIR MEAN VALUE

TABLE 4 INITIATING EVENT AND CDF FOR MULTI UNIT

TABLE 5 CATEGORY AND INITIATING EVENTS

10 LIST OF FIGURES

FIGURE 1 PLANT RESPONSE ON PARTICULAR HAZARD USING EVENT TREE

FIGURE 2 AN EXAMPLE OF COMBINATIONS OF COMPONENT RANDOM FAILURE MODES WITH INDUCED FAILURE MODES

FIGURE 3 DESIGN TEAM AND THE PRA TEAM INTERACTION PROCEDURE

FIGURE 4 FREQUENCY OF EXCEEDANCE OF DAMANGE

FIGURE 5 DISTRIBUTION OF THE CONSEQUENCES OF RELEASE

11 APPENDIX

11.1 APPENDIX 1 - DOCUMENTS REVIEW RESULTS

[2] IAEA Specific Safety Guide No.SSG-3 “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, 2010”

This reference is applicable to WA1, WA2 and WA3.

Summary relevant to WA1

Concerning the scope of Level 1 PSA this Safety Guide includes all operational conditions of the plant (i.e. full power, low power and shutdown) and all potential initiating events and potential hazards, including external hazards, both natural (e.g. earthquake, high winds, external floods) and of human-induced (e.g. airplane crash, accidents at nearby industrial facilities).

Section 8 of the Guide provides specific recommendations for selected external hazards (seismic hazards, high winds, external floods, human-induced hazards) that cannot be screened out in many cases. This section in general considers impact of external hazards on SSCs and provides some aspects of bounding analysis, parametrization, detail analysis of external hazards, fragility analysis for SSCs and integration of external hazards in the Level 1 PSA model.

According to IAEA SSG-3, the following screening criteria are typically applied (individually or in combination) to screen out a hazard (or to its subcategories):

- that will not lead to an initiating event; this criterion is generally applied when the hazard cannot occur close enough to the plant to affect it;
- that will be slow to develop and it can be demonstrated that there will be sufficient time to eliminate the source of the threat or to provide an adequate response;
- that is included within the definition of another hazard;
- that has a significantly lower mean frequency of occurrence than other hazards with similar uncertainties and will not result in worse consequences.

Summary relevant to WA2

This document provides a general guidance for developing a Level 1 PSA and consequently provides guidance for carrying-out Human Reliability Analysis and External Hazards Analysis. The information relevant from WA 2 point of view is summarized below.

External Hazards have often the potential to adversely impact plant personnel and this guideline presents a general recommendation to revise and adjust the probabilities of human errors or recovery actions modeled in the Level 1 PSA for internal initiating events to account for the impact of external events on operators' performance shaping factors. To determine, conservatively, the possible impact of a given external hazard on operator actions or recovery actions, it is recommended to organize comprehensive plant walk-down during which the plant buildings, locations and systems are examined.

More details are given on the way to assess the human factor in case of seismic event. Thus, it is mentioned that human errors should already be appropriately integrated into the Level 1 PSA and that a thorough check and associated adjustment should be performed in relation to recovery actions and probabilities of human errors. Recovery actions that cannot be performed due to the impact of seismic events of certain magnitude should be removed from the Level 1 PSA model or probabilities of failure whilst performing the action should be increased. All post-initiator human errors that could occur in response to the initiating event as modeled in the Level 1 PSA for internal initiating events should be revised and adjusted for the specific seismic conditions. As a minimum, the following seismically induced effects on the operators' performance shaping factors should be taken into account:

- Availability of pathways to specific SSCs after a seismic event;
- Increased stress levels;
- Failures of indication or false indication;
- Failure of communication systems;
- Scenarios with consequential fire and flood;
- Other applicable factors impacting the operators' behavior.

Regarding high winds, external flooding and other natural hazards, it is specified again that human errors that are not related to this specific external hazard should be considered and that the probabilities of human errors should be adjusted to account for wind effects on performance shaping factors (in particular the accessibility of the equipment as far as external flooding is concerned).

Summary relevant to WA3

Document SSG3 gives high level recommendations according to the same technical elements as TECDOC 1511. However, its relatively recent publication (2010) ensures current best practices are effectively taken into account. In addition, this guide covers the shutdown states.

In this guide, only the obligations relating to internal hazards contain elements that include multi-unit aspects:

- **Fire**
The scenarios for fire propagating from one unit to another must be considered. The possibility of fire starting in the areas containing shared systems must be postulated.
- **Flooding**
When identifying potential sources of flooding, systems shared between several units must be taken into consideration. Likewise, the possibility of the flood propagating from one unit to another must be analysed.

[3] IAEA Safety Guide NS-G-2.13 “Evaluation of Seismic Safety for Existing Nuclear Installations, 2009”

This safety guide is only applicable to WA1.

This Safety Guide provides recommendations in relation to the seismic safety evaluation of existing nuclear installations. Such an evaluation may be prompted by a seismic hazard perceived to be greater than that originally established in the design basis, by new regulatory requirements, by new findings on the seismic vulnerability of SSCs, or by the need to demonstrate performance for beyond design basis earthquake conditions, in line and consistent with internationally recognized good practices.

The objective of guideline is to understand the true state of the SSCs in terms of their required safety function and their seismic capacity and, as a result, to assess the seismic safety margin of the installation.

Although peak ground acceleration is a parameter that is widely used to scale the seismic input, it is a known technical finding that the ability of seismic ground motions to cause damage to SSCs that behave in a ductile manner is not well correlated with the level of peak ground acceleration. It is recognized that other parameters such as velocity, displacement, duration of strong motion, spectral acceleration, power spectral density and cumulative absolute velocity should play a significant role in a judicious evaluation of the effects of seismic ground motions on SSCs.

An initial step of any programme for seismic safety evaluation should be to establish the seismic hazard with regard to which the seismic safety of the existing installation will be evaluated. In this regard, the seismic hazard specific to the site should be assessed in relation to three main elements:

- (a) Evaluation of the geological stability of the site, with two main objectives:
 - To verify the absence of any capable fault that could produce differential ground displacement phenomena underneath or in the close vicinity of buildings and structures important to safety.
 - To verify the absence of permanent ground displacement phenomena (i.e. liquefaction, slope instability, subsidence or collapse, etc.).
- (b) Determination of the severity of the seismic ground motion at the site, that is, assessment of the vibratory ground motion parameters, taking into consideration the full scope of the seismotectonic effects at the four scales of investigation.
- (c) Evaluation of other concomitant phenomena such as earthquake induced river flooding due to dam failure, coastal flooding due to tsunami, and landslides.

After finishing of seismic safety evaluation typical documentation of the results should be a report documenting the following:

- (a) Methodology and assumptions of the assessment;
- (b) Selection of the review level earthquake (for the SMA), or of seismic hazard curves and uniform hazard spectra (for the SPSA);

- (c) Composition and credentials of the team;
- (d) Verification of the geological stability at the site;
- (e) Success path(s) selected, justification or reasoning for the selection, HCLPF of path and controlling components (for the SMA);
- (f) Summary of system models and the modifications introduced to the internal event models for the SPSA;
- (g) Table of selected SSC items with screening (if any), failure modes, seismic demand, HCLPF values (for the SMA) and fragility functions (for the SPSA) tabulated;
- (h) For the SPSA, results of quantification of the sequence analysis, including core damage frequency, dominant core damage sequences, large early release frequency or containment failure frequency, and dominant sequences for failures of the confinement function;
- (i) Summary of seismic failure functions for front-line and support systems modeled, including identification of critical components, if any, for the SPSA;
- (j) Walkdown report summarizing findings and system wide observations, if any;
- (k) Operator actions required and the evaluation of their likely success;
- (l) Containment and containment system HCLPFs or fragility functions (if required);
- (m) Treatment of non-seismic failures, relay chatter, dependences and seismic induced fire and flood;
- (n) Peer review reports.

[4] IAEA - “A Methodology to Assess the Safety Vulnerabilities of Nuclear Power Plants against Site Specific Extreme Natural Hazards, 2011”

This reference is only used in WA1.

This document includes requirements and methodologies to assess the seismic and flooding hazard, characterization and identification of the SSCs that are needed to maintain the plant safety functions under the different scenarios considered, the process of safety margin assessment using deterministic and probabilistic approaches. It also includes the actions and measures that need to be implemented to address scenarios that incorporate severe accident management during station blackout and loss of the ultimate heat sink with the goal to retain or regain control of at least the plant fundamental safety functions: reactivity control, residual heat removal and containment/confinement functions till the reestablishment of emergency power source and alternative heat sink.

Appendix III of the document describes seismic margin assessment methodology in general sense (SMA methodology - seismic margin assessment and S-PSA methodology - seismic PSA).

The Seismic Margin Assessment (SMA) is comprised of many steps:

- (a) Selection of the RLE;
- (b) Selection of the assessment team;
- (c) Plant familiarization and data collection;
- (d) Selection of success path(s);
- (e) Determination of seismic response ISRS of structures for input to capacity calculation;

- (f) Systems walkdown to review preliminary success path(s), select success path(s) and SSCs;
- (g) Seismic capability walkdown;
- (h) HCLPF calculations (SSCs and plant);
- (i) Peer Review; Enhancements; and
- (j) Documentation.

The key elements of a Seismic PSA can be identified as:

- a) Seismic Hazard Analysis: To develop frequencies of occurrence of different levels of ground motion (e.g., peak ground or spectral acceleration) at the site;
- b) Data collection and plant familiarization
- c) Structural Response Analysis including SSI or Equipment Structure Interaction when appropriate (this could be part of Seismic Fragility Evaluation)
- d) Seismic Fragility Evaluation: to estimate the conditional probability of failure of important structures and equipment whose failure may lead to unacceptable damage to the plant, including screening process; plant walkdown is an important activity in conducting this task;
- e) Systems/Accident Sequence Analysis: starts with development of S-PSA database and development of the logic models of the various combinations of structural and equipment failures (including HRA and seismic induced flood, fire, internal explosion, high energy line breaks), for seismic events that could initiate and propagate a seismic core damage sequence;
- f) Risk Quantification: assembly of the results of the seismic hazard, fragility, and systems analyses to estimate the frequencies of core damage and plant damage states, including sensitivity analysis development of S-PSA insights and risk reduction evaluation.
- g) Peer review Requirements
- h) Documentation Requirements

[5] **NUREG/CR-2300, "Volume 2 PRA Procedures Guide, 1983"**

This reference is used in WA1 and WA2.

Summary relevant to WA1 and general

The main objective of the PRA Procedures Guide is to provide general assistance in the performance of probabilistic risk assessments for nuclear power plants; therefore the document is structured in several chapters describing the principal methods used in PRA.

Chapters 10 and 11 are concerned with the topics needed to make the preceding efforts a full risk assessment: analyses of external events. Chapter 10 describes how external events are selected for detailed evaluation in a PRA, discusses the methods used to evaluate their hazards, and explains how the assessment of external events is integrated with the analysis of internal events in evaluating the total plant risks. With this, Chapter 10 of NUREG/CR-2300 discusses the wind related fragility assessment in detail. Fragility analysis for other hazards could be completed in the same way as for earthquake or wind.

The basic elements of the analysis of risk from an external event are:

- (1) hazard analysis,
- (2) plant-system and structure response analysis,
- (3) evaluation of component fragility and vulnerability,
- (4) plant-system and sequence analysis, and
- (5) consequence analysis.

The objective of Chapter 11 is to illustrate the application of procedure mentioned in Chapter 10 to three specific external events: earthquakes, fires, and floods including fragility analysis. The results of this analysis will be used as input in defining initiating events, in developing system event trees and fault trees, in quantifying the accident sequences, and in modifying the containment event trees and consequence models to reflect the unique features of appropriate event.

According to NUREG/CR-2300, uncertainty in the analysis of external events (i.e. estimation of risk for accidents caused by external events), which tends to be greater than uncertainty for internal events, arises from the lack of data and analytical models and concerns:

- the frequency of occurrence of the hazard intensity;
- the characterization of the phenomenon (e.g. line source or point source for seismic events, path width and length models for a tornado, available sources of missiles for a tornado, and models for explosive-vapor cloud transport);
- the characterization of the transmission of effects from the source to the site (e.g. overpressure, missiles, and ground acceleration);
- the component-fragility evaluation (due to an insufficient understanding of the properties and failure modes of structural materials, errors in the calculated response due to approximations and use of generic data and engineering judgment).

It should be noted that this document has broad scope covering almost all of the tasks that are performed within PSA and presented general methods and recommendations are reflected in many latest guidelines.

Summary relevant to WA2

HRA constitutes the subject of a dedicated chapter, with the purpose to provide a procedure for estimating the probabilities of human errors (HEP) in the operation of nuclear power plants. It is highlighted that the basic components of a human-reliability analysis are the task analysis and the Technique for Human Error Rate Prediction (THERP). NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, is specified as a reference source for presenting the HRA. Although an important aspect of a HRA is the qualitative assessment of the sources of human errors, this document treats in detail only the quantitative evaluations. The intended acts of sabotage are not considered. The general framework of HRA is presented, by specifying the four phases (familiarization, qualitative assessment, quantitative assessment, incorporation) with their activities. Each activity is defined, described and illustrated by an example. The chapter presents also alternative methods for HRA (Oconee PSA, Operator Action Tree - OAT, Accident Initiation and Progression Analysis - AIPA) with their advantages and disadvantages.

Another chapter of the document is focused on external event analysis. It is specified that the external event analysis should address the influence of design and construction errors, as the human errors due to operator actions or inactions. It is specifically mentioned that operator action in mitigating an accident may not be effective under extreme stress conditions (e.g., beams and walls cracking and collapsing in the control room under a large earthquake or a major fire in the control room). Still, commission operator errors (e.g., turning off a wrong valve) under extreme stress were not included in the past studies. In case of earthquakes, it has been shown that potential for design error would greatly influence the frequency of system failure.

The detection of hazard effects often requires a human response. As with other initiating events, separate event trees may be constructed for induced hazards, because the operator, rather than automatic actions, may be responsible for shutting down the plant in response to a hazard occurrence. Human intervention plays an important role in the accident, with the two opposite contributions: first, the operators may extinguish the fire, mitigate the flooding effects and manually operate the equipment, they may make repairs and replacement on equipment as well; adversely, they may be misled by fire-caused faulty information and may actually exacerbate the situation. Among the aspects of human interactions that must be taken into account in hazard analysis, the following are specified: warning time effects, if any, to shut-down the plant; the conflicts between hazard mitigation and plant operation; the effects of stress.

[6] NUREG/CR-4840 “Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150, 1990”

This guide is only used in WA1.

This report presents methods which can be used to perform the assessment of risk due to external events at nuclear power plants. Presented methods were used to perform the external events risk assessments for the Surry and Peach Bottom nuclear power plants as part of the NRC-sponsored NUREG-1150 risk assessments.

Presented methods apply to the full range of hazards such as earthquakes, fires, floods, etc. which are collectively known as external events. They also include the most up-to-date data bases on equipment seismic fragilities, fire occurrence frequencies and fire damageability thresholds. After the screening analysis of all applicable site specific hazards has been performed, the general steps in the CDF analysis of each remaining external event are:

- a. Determine the hazard non-exceedance frequency.
- b. Model plant and systems.
- c. Solve fault trees with screening techniques to determine no negligible accident sequences and cut sets.
- d. Determine responses, fragilities, and correlation for each basic event in the (non-negligible) cut sets.
- e. Evaluate mean values and uncertainty distributions for all accident sequence and core damage frequencies.
- f. Perform sensitivity studies on contributors to CDF and to uncertainty.

This report is focused mainly on the fire and seismic procedures.

[7] ASME/ANS RA-Sa-2009 “Addenda to ASME/ANS RA-S-2008 Standard for Level 1 /Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, 2009”

This standard is used in WA1, WA2 and WA3.

Summary relevant to WA1 and general

This Standard establishes requirements for a Level 1 PRA of internal and external hazards for all plant operating modes (low power and shutdown modes will be included at a future date). Parts 5 to 10 of this PRA Standard provides dedicated information to external hazards; however the specific requirements for the following external hazards are discussed in much detail:

- (a) Seismic Events (Part 5)
- (b) High Winds (Part 7)
- (c) External Floods (Part 8)

Nonmandatory Appendix 5-A contains a short introduction and review of the seismic-PRA methodology.

This standard sets out the obligations to be complied with to develop a Level-1 PSA and LERF for internal events (including fire and flooding) and external hazards. This standard defines three categories of PSA model which correspond to three levels of quality. High level requirements and supporting requirements are associated with each category for every technical element that constitutes a PSA.

The document provides specific requirements for the internal events, internal and external floods, internal fires, seismic events and high winds groups. The requirements of each group specified above contain a short description of each technical PRA element included in the hazard PRA process. A set of objectives and High Level Requirements is provided for each PRA Element. The High Level Requirements set forth the minimum requirements for a technically acceptable baseline PRA, independent of an application and for each high level requirement, a set of Supporting Requirements is provided.

In addition to providing technical requirements for detailed PRA of these hazards, this Standard provides requirements for screening and conservative analyses of external hazards. Technical requirements for seismic margin analysis are provided, with discussion of the elements of seismic margin assessment methodology. A list of external hazards requiring consideration, with applicable screening criteria, and remarks, adapted from NUREG/CR-2300, is included.

Summary relevant to WA2

The information relevant from WA 2 point of view is summarized below.

In Part 5 of the document, a list of requirements for seismic PSA is given among which some of them are related to HRA:

- In the human reliability analysis aspect, additional post-earthquake stresses that can increase the likelihood of human errors or inattention, compared to the likelihood assigned in the internal-events HRA when the same activities are undertaken in non-earthquake accident sequences should be examined. Whether or not increases in error probabilities are used, the basis for this decision about what error rates to use should be justified.
- In many seismic PSAs, the human-error probabilities are increased for some post-earthquake actions, compared to the probabilities assigned in analogous internal events initiated sequence. The rationale is usually that strong seismic motions can adversely affect human performance shortly after a very large earthquake. However, the basis for determining these increases is not well developed in the seismic-PSA literature, and several different seismic human reliability analysis (HRA) models are in use. (Of course, this factor has reduced importance to the extent that most modern nuclear power plants have designs that do not require operator intervention for the first half-hour or more after a postulated earthquake. But, errors of commission must still be accounted for). This aspect can represent an important source of uncertainty in the numerical results of a seismic PSA. The corresponding technical requirements for internal events PSA should be consulted in performing the HRA aspect of a seismic PSA.
- The possibility that a large earthquake can cause damage that blocks personnel access to safety equipment or controls, thereby inhibiting operator actions that might otherwise be credited should be examined. This information is most effectively gathered during the walkdown, which must be structured to search for access issues. Coordination with the human reliability analysis aspect of the PSA is important. If access problems are identified, the systems model needs to be modified so as to assign the weaker seismic fragility of the failure causing the access problem to each presumably stronger SSC, or a combination thereof to which access is thereby impaired. In making these evaluations, it may be assumed that portable lighting is available and that breathing devices are available for confined spaces, if in fact the plant configuration includes them.

The document also mentions that all seismic-PSA analyses are characterized by large numerical uncertainties not only in the seismic hazard aspect but also in the seismic-fragility and systems-analysis aspects as well. Also one of the analysis areas where uncertainties arisen in seismic PSA are different from those encountered in internal-events PSA is the human reliability-analysis.

Parts 7, 8 and 9 of the document are dealing with high winds events, external flood events and other external events respectively. The requirements related to HRA are the same for all these events categories:

- The PSA systems models should reflect external hazard-caused failures as well as other unavailabilities and human errors that give rise to significant accident sequences or significant accident progression sequences.
- In the human reliability aspect of the external hazard PSA systems analysis work, the corresponding requirements for internal events PSA should be satisfied, except where they are not applicable or where it includes additional requirements. A defined basis to support the claimed non-applicability of any exceptions should be developed. When the requirements for internal events PSA are used, the same Capability Category should be used in this analysis for consistency.
- In the human reliability analysis (HRA) aspect, additional stresses that can increase the likelihood of human errors or inattention, compared to the likelihood assigned in the internal events HRA when the same activities are undertaken in non-external hazard accident sequences should be examined. Whether or not increases in error probabilities are used, the basis for this decision about what error rates to use should be justified. The human-error probabilities may be increased for some external hazard actions, compared to the probabilities

assigned in analogous internal events-initiated sequences. The corresponding technical requirements of internal events PSA should be consulted in performing the HRA aspect of an external hazard PSA.

- The possibility that the external hazard can cause damage or plant conditions that preclude personnel access to safety equipment or controls, thereby inhibiting operator actions that might otherwise be credited should be examined. This information is most effectively gathered during the walkdown, which must be structured to search for access issues. Coordination with the human reliability analysis aspect of the PSA is important. In making these evaluations, it may be assumed that portable lighting is available and that breathing devices are available, if in fact the plant configuration includes them.

This Standard establishes requirements for Level 1 PRA of internal and external hazards for normal operating modes (without low power and shutdown modes) and requirements for a limited Level 2 PRA, sufficient to evaluate large early release frequency (LERF). Accidents resulting from intended human-induced security threats (e.g. sabotage) are excluded.

For HRA, high level requirements include pre-initiator and post-initiator HRA. HRA supporting requirements are specified for the following: identification of specific routine activities that may impact the availability of equipment, screening of activities, definition of appropriate human failure event, assessment of the probabilities of the pre-initiator human failure events, systematic review of the relevant procedures to identify the set of operator responses required for each of the accident sequences (definition of post-initiator human failures, assessment of the probabilities of the post-initiator modelling recovery actions), documentation.

For all human failure events in the internal hazard scenarios, the following should be considered:

- additional workload and stress;
- cue availability;
- effect of hazard on mitigation, required response, timing and recovery activities (accessibility restrictions, possibility of physical harm);
- hazard specific job aids and training (procedures, training exercises).

The hazard PRA plant response model shall include hazard-induced initiating events, both hazard-induced and random failures of equipment, hazard-specific as well as non-hazard-related human failures associated with safe shutdown, accident progression events (e.g., containment failure modes), and the supporting probability data.

A summary comparison between EPRI FIVE, the Fire PRA Implementation Guide, the EPRI/NRCRES Fire PRA Methodology for Nuclear Power Facilities, and the FPSDP on the way they are approaching the technical tasks is given, emphasizing the key differences (with insights as to the strengths and weaknesses related to Post-fire operator manual actions) of these methods.

It is stated that seismically induced fires and floods should be addressed as described in NUREG-1407. Considering that strong seismic motions can adversely affect human performance shortly after a very large earthquake, in many seismic PRA, the human-error probabilities are increased for some post-earthquake actions, compared to the probabilities assigned in analogous internal-events-initiated sequences. However, since the basis for determining these increases is not well developed, and several different seismic HRA models are in use, this aspect can represent an important source of uncertainty in the numerical results of a seismic PRA.

It may be concluded that in the HRA aspect of external hazard analysis, additional stresses that can increase the likelihood of human errors or inattention should be examined, compared to the likelihood assigned in the internal events HRA, when the same activities are undertaken in non-hazard accident sequences. The human-error probabilities may be increased for some external hazard actions, compared to the probabilities assigned in analogous internal events-initiated sequences. Whether or not increases in error probabilities are used, the basis for this decision about what error rates to use should be justified. During revision, it should be verified that the HRA adequately accounts for the additional influences caused by external event, that HFEs adopted from an Internal Events PRA have been modified as appropriate to reflect external hazard effects and new HFEs are included to account for specific hazard related actions that are consistent with plant procedures that were not covered by the Internal Events PRA.

Summary relevant to WA3

The obligations of this standard that address the multi-unit issue are summarized below:

Initiating Events

For sites with several units, include the initiating events that can affect all the units (for example: loss of offsite power or loss of water intake). "Multi-unit" initiating events should be distinguished according to their potential impact on the mitigation systems.

Data

The establishment of data relating to the unavailability of components must include the cases of components shared between two units, especially when the STE differ according to the state of the two units. Accurate modelling of this type of situation generally leads to an allocation of unavailability data to take account of this dependency.

Internal flooding

When developing an internal flooding PSA, multi-unit aspects are only to be taken into account in cases where systems are shared. In these cases, we must:

- Identify the areas shared by the different units where internal flooding may lead to unacceptable consequences for the units;
- Identify potential sources of internal flooding likely to have an impact on the units simultaneously or in cascade;
- Take account of multi-unit flood propagation scenarios;
- Take account of the impact of a scenario involving internal flooding on shared SSCs or on the occurrence of a multi-unit initiating event.

Earthquake

The aim of an earthquake PSA is to obtain a risk profile relating to the earthquake for a unit, using data specific to the unit and site. Several earthquake PSAs have demonstrated that the assessments and lessons learned from them were quite specific to a unit and varied from one unit to another, even for two units on the same site assumed to

be identical. However, we must consider the multiple impacts and the dependencies linked to a large earthquake, especially on safeguard systems.

Strong winds and external flooding

We must consider the multiple impacts and the dependencies linked to strong winds or external flooding, especially on safeguard systems.

[8] IAEA-TECDOC-1511 “Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants”

This document is used in WA1, WA2 and WA3.

Summary relevant to WA1 and general

The scope of this document is restricted to Level 1 PSA, developed for internal events, at power operation. Internal fires and floods, external hazards (natural and man-induced hazards), Level 2 PSA, and PSA for shutdown and low power operation modes are not addressed. ‘PSA quality’ for a specific purpose refers to the technical adequacy of the methods, level of detail and data used to develop the PSA model. The report provides a mapping of PSA features, necessary to support specific applications. General attributes are formulated for a ‘base case PSA’ (used to assess the overall plant safety level) and where appropriate, special attributes (generally providing enhanced capabilities) are provided for specific PSA applications. The appendices comprise risk metric definition and PSA applications list. For each PSA application, a brief description of the purpose of the application, along with the information on PSA results and metrics that can be used in the decision making process is provided.

The publication takes into consideration the advanced worldwide experience in the area of PSA quality assessment and verification and in particular the ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications. This guide has similar intention as [7]. However the external hazards like earthquakes, tornadoes, and other natural and man-induced hazards are not included in the scope of this publication.

TECDOC-1511 only covers Level-1 PSA for internal events at power and based on obligations featured in the ASME standard, corresponding to capability category II, which is that required for the majority of PSA applications. The structure of the PSA technical elements covered by the TECDOC borrows from that of the ASME standard, namely:

- IE: Initiating Events Analysis
- AS: Accident Sequence Analysis
- SC: Success Criteria Formulation and Supporting Analysis
- SY: Systems Analysis
- HR: Human Reliability Analysis
- DA: Data Analysis

- QU: Quantification

However a "Dependent Failures analysis" (DF) element has been added and the quantification part is explicitly divided into two sub-parts:

- Model Integration & Core Damage Frequency Quantification (MQ)
- Results Analysis and Interpretation (RI).

It is therefore no surprise that the same type of obligations is found in the ASME standard.

Summary relevant to WA2

Concerning the PSA element HRA, its objective, the main tasks, and the description of general and special attributes for these tasks are presented. As important HRA topics the following are specified:

- identification of the specific human activities whose impact should be included in the analysis;
- representation of the impact of success or failure to correctly perform those activities in the accident sequence models (e.g. event trees) and the supporting system reliability models (e.g. fault trees);
- estimation of the probabilities of the HFE representing the contribution of the operators failure to correctly perform the required actions as specific modes of unavailability of the component, system or function affected.

The main tasks of HRA are grouped in Pre-initiating event HRA (comprising the following: Identification of Routine Activities, Screening of Activities, Definition of Pre-initiator Human Failure Events, Assessment of Probabilities of Pre-initiator Human Failure Events) and Post-initiating event HRA (which comprises Identification of Post-Initiator Operator Responses, Definition of Post-initiator Human Failure Events, Assessment of Probabilities of Post-initiator Human Failure Events, Recovery Actions).

The method used to assess HEP addresses failure in cognition (detection, situation assessment and response planning) as well as failures in execution. It is stated that particular attention should be paid to activities that can simultaneously disable multiple trains of a system. The model used to assess the HEP addresses the following PSF on a scenario and plant-specific basis:

- type (classroom or simulator) and frequency of training on the response;
- quality of the written procedures and administrative controls;
- availability of necessary instrumentation;
- degree of clarity of the indications for alerting the operators about the necessity of action;
- timing issues - timing of cues relative to accident progression, time required to perform the response and the time available to complete the response;
- complexity of the tasks to be performed;
- nature of the human-machine interface.

When the response requires actions outside the control room, the following factors should be taken into account in addition to the above:

- environmental factors (e.g. heat, radiation, humidity);
- accessibility of equipment to be manipulated;

- need for special tools;
- time to reach physically the place if not permanently occupied;
- communication issues between MCR and local personnel.

The degree of dependence between HFE appearing in the same accident sequence or cutset should be assessed, considering as factors affecting the degree of dependence the following:

- use of common cues;
- responses called for in the same procedure;
- closeness in time of cues or required actions;
- increased stress caused by failure of the first response.

A conditional probability of the second, third, etc. event, given failure of the first, second, etc. should be evaluated and the assumption of independence between HFE should be justified.

Recovery actions are credited only if:

- a procedure is available and operator training has been provided for the action OR it is considered to be a skill-of-the-craft action AND
- cues (e.g. an annunciator) alert the operators about the necessity for action OR the procedure directs the operator to check the status of the component AND
- feasibility of the action is confirmed.

The potential for dependency between recovery actions and any other HFE in the accident sequence cutset should also be assessed.

Summary relevant to WA3

The summary relevant to WA3 is discussed below:

Initiating Events

Events likely to affect several units on the same site must be identified. These events can occur on several units at once or be prompted by an event occurring on a given unit and affecting another unit.

Success Criterion

For multi-unit sites, systems shared between several units and the manner in which this sharing is managed should an initiating event occur on the site are identified. This includes the operator actions required and specified in the unit's operational procedures.

Systems Analysis

Common cause failures that can affect the systems shared by different units and the possibilities of mutual backup must be taken into account in the analysis.

Data

When analysing the unavailability of shared systems, the STE, which can depend on the state of the two units, must be taken into account.

[9] IAEA 50-P-7 “Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants”

This document is used in WA1 and WA2.

Summary relevant to WA1 and General

This Safety Practice provides guidance on conducting a PSA for external hazards in nuclear power plants and presents the general treatment of external hazards, with application to four specific types of hazard (earthquakes, high winds, floods and man induced events). The methodology itself is general and can be applied successfully to other types of hazard. Emphasis is placed on the procedural steps of the PSA rather than on the details of corresponding methods. The document provides information on the inclusion of external hazards in PSA Level 1 or Level 2, as well as comments about the way external hazards should be considered for a Level 3 PSA.

The standard PSA approach towards external hazards involves two steps: hazard analysis and plant response analysis. Hazard analysis includes the identification of possible types of external hazards, to which a plant is exposed and the determination of the frequencies of those hazards that are considered important. It is performed through seven tasks:

- selection of initiating events,
- parameter definition for each initiator,
- approximate screening by impact,
- detailed screening by frequency,
- detailed parameterization of each initiator,
- hazard analysis (frequency versus size) and
- sensitivity analysis.

The plant response analysis (identification of vulnerable features, generalized load analysis, failure mode analysis, fragility analysis, sequence and system analysis, plant damage state evaluation) covers the analysis of the full spectrum of possible undesirable plant responses, including analysis of the probability of a core degradation or core melt accident and analysis of containment integrity.

It has been noted that this publication is no longer valid; however this document is quoted due to good analytical framework.

Summary relevant to WA2

It is stated that a key issue in systems analysis is represented by the combination of failures caused by an external initiator with unrelated failures caused by internal plant faults or human errors.

Another important analytical issue is represented by the treatment of human actions after an external initiator. This includes consideration of the success or failure of operators to follow related emergency procedures, of inadvertent and erroneous actions with a potential for aggravating the situation and of the success of improvised recovery actions and repairs. Compared to accident scenarios caused by internal initiating events, the operators stress levels and conditions in the plant may differ considerably after an external initiating event.

[10] EPRI 1002989 “Seismic Probabilistic Risk Assessment Implementation Guide”

This document is used in WA1, WA2 and WA3.

Summary relevant to WA1

The report provides implementation guidance for performing Seismic Probabilistic Risk Assessment (SPRA). This report contains detailed guidance on each phase of the SPRA process (seismic hazard analysis, plant systems/sequence analysis, fragility evaluation and seismic risk quantification), addressing important concepts such as screening criteria and correlation. The similarities and differences between the internal events PRA and the SPRA are presented. The objective of SPRA, its basic steps, together with the possible outputs, is specified. For each step, sources of information, along with guidance for treatment of uncertainties are presented.

The guidance provided in this report is consistent with a Level 1+ analysis (it includes guidance for the quantification of sequence frequencies that lead to core damage and guidance for assessing LERF). Level 2 beyond LERF has not been included, as the guidance for the additional scope required in a Level 3 assessment. Guidance for Level 2 assessment of containment phenomenology is not described. It is considered (to the extent that this can be verified to be true), that Level 2 analysis for seismic events can be reduced to looking for failures in active containment systems and then using the conditional probabilities for LERF that apply to the resulting core damage sequences.

The report provides also examples of the methods and results. There are presented four basic approaches (Diablo Canyon, McGuire, San Onofre, Kewaunee) used for SPRA logic model development, together with a summary description of each SPRA methodology and the way in which it addresses the 3 key elements (Systems Analysis; Hazard Analysis; Fragility Evaluation).

The systems analysis effort is to model the combinations of structural and equipment failures that could initiate and propagate a seismic core damage sequence. The systems analysis element includes the development of the event trees for accident sequence modeling, and of the logic models for each of the individual event tree top events. Both seismic induced failures and random failures must be considered in the logic.

The seismic hazard analysis effort is to develop frequencies of occurrence of different levels of earthquake ground motion (e.g. peak ground acceleration) at the site. This includes the determination of the seismic initiating event occurrence frequencies. Frequencies must be estimated over the entire range of possible seismic magnitudes. A

single parameter (usually the peak ground acceleration at the site) is chosen to characterize this seismic motion throughout the SPRA.

The third major element of the SPRA is fragility evaluation. The seismic fragility evaluation is to estimate the conditional probabilities of failure of important structures and equipment; i.e. those which are the most limiting systems, structures, and components of the plant. They are developed using plant design information and realistic response analysis. A plant walkdown is an important part of this effort.

Summary relevant to WA2

Concerning HRA, it is specified that the recovery of safety functions by plant staff can be inhibited following an earthquake by any of several types of causes. In many SPRA, the human error probabilities are increased for some post-earthquake actions, compared to the probabilities assigned in internal-events-initiated sequences (it is considered that strong ground motions can adversely affect human performance, due to stress, physical impacts, inability to access required control stations, etc.). However, the basis for determining the increases in probability versus ground motion level is not well developed, this aspect representing an important source of uncertainty in the numerical results of SPRA. For multiple unit sites, the recovery assessment must consider the fact that both units are affected by the ground motion placing additional demands on the resources available for recovery.

The corresponding technical requirements for post-initiator human errors, in the ASME standard (ASME, 2002) should be consulted in performing the HRA aspect of a SPRA.

Summary relevant to WA3

This implementation guide is written to address the needs of the utilities with an appreciation of different elements of the seismic PSA. This document states that for multiple unit sites, the recovery assessment must consider the fact that both units are affected by the ground motion placing additional demands on the resources available for recovery.

[11] IAEA-TECDOC-724 "Probabilistic safety assessment for seismic events"

This document is used in WA1 only.

The purpose of this document is to provide information and some measure of guidance and insight to those who are considering starting a seismic PSA. It tries to give an overall picture of the seismic PSA and attempts to bridge the gap between an internal event PSA and a seismic PSA. This report is not intended to be an extensive manual or handbook but tries to help the reader by providing some references for further information on current practices and insights obtained by conducting seismic PSAs.

This document covers mainly the frequency of occurrence of ground motion, the seismic accident sequence initiators, the fragility analysis of safety related items, the capability of systems to mitigate accidents from seismic events and the integration of these aspects which might lead to core damage.

[12] IAEA Safety Standard Series No. SSG-21 “Volcanic Hazards in Site Evaluation for Nuclear Installations”

This document is used in WA1 only.

The objective of this Safety Guide is to provide recommendations and guidance on the assessment of volcanic hazards at a nuclear installation site, so as to enable the identification and comprehensive characterization of all potentially hazardous phenomena that may be associated with future volcanic events. These volcanic phenomena may affect the suitability of the selected site and some of them may determine corresponding design basis parameters for the installation.

This Safety Guide is very specific and is not intended to deal with response analysis and capacity evaluation of volcanic hazards at the nuclear installation (i.e. plant design aspects, capacity or fragility calculations of systems, structures and components).

[13] IAEA Safety Standard Series No. NS-G-3.1 “External Human Induced Events in Site Evaluation for Nuclear Power Plants”

This document is referenced in WA1 and WA2.

Summary relevant to WA1

The purpose of the present Safety Guide is to provide recommendations and guidance for the examination of the region considered for site evaluation for a plant in order to identify hazardous phenomena associated with human induced events initiated by sources external to the plant. In some cases it also presents preliminary guidance for deriving values of relevant parameters for the design basis.

In this sense, the Safety Guide concentrates on the definition of hazards for the site and on the general identification of major effects on the plant as a whole, according to the reference probabilistic or deterministic criteria, which are to be used in a design or in a design assessment framework. This document brings only identification of effects and associated parameters due to external human induced events (Table I., II. and III.).

Summary relevant to WA2

This document focuses on external human induced events and provides recommendations and guidance for carrying-out a site evaluation for a plant in order to identify potential human induced events initiated by sources external to the plant.

Regarding the impact of external human induced events on Human Reliability Assessment, it is simply mentioned that the effects generated by external human induced events could be of considerably great importance to safety and that they could affect both the plant's facilities and items essential for safety such as the possibility of implementing emergency procedures (access by the operator could be impaired). It is also recommended to set up specific operational procedures for operator action following an accident caused by an external human induced event. But this document does not give specific insights on how to assess the human factor following an external human induced event.

[14] IAEA TECDOC-1487 "Advanced nuclear plant design options to cope with external events"

This document is referenced in WA1, WA2 and WA4.

Summary relevant to WA1 and General

The objective of this document is to present the state-of-the-art in design features and approaches for the protection of NPPs with evolutionary and innovative reactors from external event impacts, as well as to assist the designers of advanced NPPs in the definition of a consistent strategy of design and siting evaluation in relation to extreme external events. The main objectives of this report are the following:

- (1) Through direct cooperation with the designers of advanced NPPs, to define, collate and present the state-of-the-art in design features and approaches used to protect plants from external event impacts, making a focus on NPPs with evolutionary and, when possible, innovative designs;
- (2) Reflecting best practices achieved in Member States, to provide a technical and information background to assist designers of advanced NPPs in defining a consistent strategy regarding selected design and site evaluation issues in relation to extreme external events;
- (3) To bring to the attention of designers of advanced NPPs the recently updated IAEA safety guides and other publications on issues of plant protection from external event impacts; to collect comments on their applicability to NPPs with evolutionary and innovative reactors; to identify safety and technological issues and proposals for their resolution; and to outline future challenges and potential contribution of the IAEA.

The report was prepared on the basis of responses to the questionnaires which were sent to Member States. Annex I presents an extended summary of the methodology for seismic PSAs of NPP, which has been established as US national standard on external event PSA. The key elements of a seismic PSA identified by this work are in compliance with information given in above mentioned guidelines as [1], [3] and [10] etc.

Summary relevant to WA2

The information relevant from WA 2 point of view are summarized below.

This document presents the results of a technical meeting on the definition of plant safety design options to cope with external events and of the analysis of a questionnaire targeted at the advanced, both evolutionary and

innovative, NPP designs. The objective of the questionnaire was to collect experiences in relation to the hazard evaluation. This document mentions thereby several trends of PSA technique improvement which appeared to be urgent from the questionnaire analysis and one of them concerns the Human Reliability Analysis. It is mentioned that more realistic Human Reliability models could be developed for the periods during and after an external event, including the implementation of emergency plans. In general, the reliability of operational measures could be explored, including monitoring and alerting actions. Also, one of the conclusion and recommendation derived from the technical meeting is that there may be a need for data on operator response (Human Reliability models) in the case of an external event, possibly available from training and evaluation of personnel on simulators.

Also, this document mentions repeatedly that one of the important considerations in the treatment of external hazards is the possibility of disruption of external sources of electricity, cooling water, other essential supplies and of prompt operator action following an external event. It is recalled that several passive systems enable prolonged grace period to the operator during which the reactor is maintained in a safe state without any operator intervention. So one of the design options recommended in this document is to implement passive systems, independent from external sources of energy and human interaction, since they may play a significant role to reduce the conditional probabilities of occurrence of severe accidents scenarios following extreme external events and they enable to reduce the need for prompt operator actions to prevent significant fuel failure and fission product release.

This document highlights the fact that the advanced reactors are more and more designed in such a way that no operator intervention is required in the short term following an external hazard. Indeed, no operator action can be required immediately after onset of an external event if the design includes passive systems managing all required safety functions.

The implementation of passive systems in the design to cope with external events and to avoid operator interventions which could be jeopardized following such events is a design option that is often mentioned in the document and which leads to the reduction of required operator actions following an external hazard and consequently to a Human Reliability Analysis with a reduced and limited scope for external events PSA. This document is not discussed the way to model human error in PSA in the frame of an external event.

[15] EPRI-1009652 “Guideline for the Treatment of Uncertainty in Risk Informed Applications”

This document is referenced in WA1 and WA3.

Summary relevant to WA1

This report provides the technical basis for a process to characterize the uncertainty distribution for risk metrics derived from probabilistic risk assessments (PRAs). The intent is to provide a pragmatic process for uncertainty characterization that is to be used in risk-informed applications and decision making. It is considered an industry best practice, and it uses state-of-the-art technology information. This document forms good framework to perform systematic uncertainty analysis.

Summary relevant to WA3

This guideline provides a process for uncertainty characterization that is to be used in risk-informed applications and decision making. This document provides description of the identified sources of modelling uncertainty and those related to the multi-unit sites are:

Multi-unit impacts, Multi-unit events: Multiple units may provide both significant benefits - by virtue of the sharing of equipment and personnel - and significant challenges if all units require accident mitigation simultaneously.

Multi-unit credit/impact, Multi-unit interactions: There may be substantial plant capability that exists within the plant to use AC, DC, or fluid systems via cross-ties. These cross-ties may or may not be proceduralized and the subject of training exercises. Their use in the PRA should represent a realistic assessment of their likelihood of use.

[16] ASME NON-LWR (DRAFT) “Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications” (recommended by NRC but probably still in draft version)”

This document is referenced in WA1 and WA3.

Summary relevant to WA1

This Standard sets forth the requirements for probabilistic risk assessments (PRAs) used to support risk informed decisions for advanced non-light water reactor nuclear power plants and prescribes a method for applying these requirements for specific applications. Intention of this draft is similar as in case of [7].

Summary relevant to WA3

This standard presents the requirements associated with the development of full scope PSAs for advanced non-LWR nuclear power plants. The obligations contained in this standard are "neutral" with regard to the different technologies postulated within the framework of the Gen IV programme. Amongst these new technologies, this standard notes in particular the modular high temperature CO₂ gas cooled reactors which are particularly concerned by the multi-unit issue. In the same way as the standard relating to light water reactors, high level requirements and supporting requirements are associated with three categories or levels of quality of PSA for every technical element of which it is composed. The obligations of this standard that address the multi-unit issue are summarized below:

Initiating Events

For sites with several units or modular reactors, include the initiating events that can affect all the units or modules (for example: loss of offsite power or loss of water intake). Identify the specific combinations affected by a given initiating event.

Accident Sequence Analysis

For sites with several units or modular reactors, include the number of units or modules concerned by the release of radioactive material in the definition of the accident scenario and final state.

Systems Analysis

Identify the shared mitigation systems and the manner in which this sharing is managed in the occurrence of an initiating event affecting at least two units or modules.

Incorporate the effects of sharing systems on the success criteria to be taken into account.

Data

The establishment of data relating to the unavailability of components must include the cases of components shared between two units, especially when the STE differ according to the state of the two units. Accurate modelling of this type of situation generally leads to an allocation of unavailability data to take account of this dependency.

Internal flooding

When developing an internal flooding PSA, multi-unit aspects are only to be taken into account in cases where systems are shared. In these cases, we must:

- Identify the areas shared by the different units where internal flooding may lead to unacceptable consequences for the units;
- Identify potential sources of internal flooding likely to have an impact on the units simultaneously or in cascade;
- Take account of scenarios involving multi-unit propagation of flooding, specifying the number of units or modules concerned by the release of radioactive material in the definition of the accident scenario and final state.

Earthquake

The aim of an earthquake PSA is to obtain a risk profile relating to the earthquake for a unit, using data specific to the unit and site. Several earthquake PSAs have demonstrated that the assessments and lessons learned from them were quite specific to a unit and varied from one unit to another, even for two units on the same site assumed to be identical. However, we must consider the multiple impacts and the dependencies linked to a large earthquake, especially on safeguard systems.

Other External Hazards

We must consider the multiple impacts and the dependencies linked to other external hazards, especially on safeguard systems.

[17] ASN - RFS 2002-1 “Development and utilisation of probabilistic safety assessments December 2002”

This document is referenced in WA2 only.

Summary relevant to WA2

The objective of this document is to present a methodology to perform a Level 1 PSA and for its applications. This document provides general information on how to perform a PSA but there is no specific or detailed information on how to address external hazards and on how to assess the human factor depending on the external event considered. At present, it is noted that this document is not publically available.

[18] CNSC S-295 “Probabilistic Safety Assessment (PSA) for Nuclear Power Plants”

This document is referenced in WA1 and WA2.

General summary

The purpose of this Regulatory Standard, when corporated into a license to construct or operate a NPP or other legally enforceable instrument, is to assure that the licensee conducts a “PSA” in accordance with defined requirements. However; this document has only proclamative nature.

This document sets-out the requirements for PSA development, necessary to be conducted by a licensee who constructs or operates a NPP. The necessary activities that shall be carried out are specified and a glossary with usual terms for PSA studies is included. There are no specific requirements about conducting an external event PSA, or even more specific, references to human reliability analysis.

[19] WENRA Reactor Safety Reference Levels, Issue O “Probabilistic Safety Analysis (PSA)”

This document is referenced in WA1 and WA2.

General summary

WENRA countries develop a harmonized approach to reactor safety (18 safety issues). These issues are grouped in 5 safety area: Safety Management; Design; Operation; Safety Verification and Emergency Preparedness. One of the 18 safety issues deals with safety requirements in the area of probabilistic requirements - issue O: Probabilistic Safety Analysis (PSA). Content of document is formed by general requirements including parts related to external hazards. WENRA does not deal with specific analysis of external hazards.

In the issue *Design Basis Envelope for Existing Reactors*, from the *Design* safety area, a reference level included into *Set of design basis events* category, provides the types of natural and man-made external events that shall be taken into account in the design of the plant, according to site specific conditions. These external events (as minimum) are the following:

- extreme wind loading;

- extreme outside temperatures;
- extreme rainfall, snow conditions and site flooding - extreme cooling water temperatures and icing;
- earthquake;
- airplane crash;
- other nearby transportation, industrial activities and site area conditions which can cause fires, explosions or other threats to the safety of the nuclear power plant.

Combination of events represents another reference level in the above issue. It is stated that credible combinations of individual events, including internal and external hazards, that could lead to anticipated operational occurrences or design basis accident conditions, shall be considered in the design.

Probabilistic Safety Assessment (PSA) is included in *Safety Verification* area, together with *Contents and updating of Safety Analysis Report (SAR)* and *Periodic Safety Review (PSR)* issues. The reference levels for PSA issues have been included into 4 main categories: scope and content of PSA, quality of PSA, use of PSA and demands and conditions on the use of PSA. An important reference level from the *Scope and content of PSA* category refers to the development of specific PSA Level 1 and Level 2 for each plant design, including all modes of operation and all relevant initiating events (including internal fire and flooding). It is highlighted that the severe weather conditions and seismic events shall be addressed.

Summary relevant to WA1

According to the WENRA Safety Reference Levels, (natural) external hazards identified as potentially affecting the site can be screened out on the basis of being incapable of posing a physical threat or being extremely unlikely with a high degree of confidence. The screening process shall be based on conservative assumptions. The arguments in support of the screening process shall be justified. The assessment of all natural hazards that have not been screened out shall be performed using deterministic and, as far as the current state of science and technology permits, probabilistic elements. The assessment shall produce a relationship between the hazards severity (e.g. magnitude and duration) and exceedances frequency and the maximum credible hazard severity, if practicable. It shall be based on all relevant site and regional data, including beyond recorded and historical data. Special consideration shall be given to hazards that change with time. The methods and assumptions used shall be justified. Uncertainties on the results of the assessments shall be evaluated. Design extension conditions could result from natural events exceeding the design basis events or from events leading to conditions not included in the design basis accidents. This could include other natural hazards, internal hazards or human induced hazards.

Summary relevant to WA2

Concerning the HRA, the reference level from the *Scope and content of PSA* category, refers to performing HRA, taking into account the factors which can influence the performance of the operators in all plant states.

[20] NEA/CSNI/R(2009)1 “PROCEEDINGS of the Workshop on Recent Findings and Developments in Probabilistic Seismic Hazards Analysis (PSHA) Methodologies and Applications - Lyon, France, 7-9 April 2008”

This document is referenced in WA1 only.

Summary relevant to WA1

This document is a summary report from the “Workshop on Recent Findings and Developments in Probabilistic Seismic Hazards Analysis (PSHA) Methodologies and Applications”. The report is a huge document that consists of particular participant contributions and brings their experiences in PSHA.

In this document, there is provided summarization of best practices for seismic hazards analyses in particular countries including used methodology, input data, construction of seismicity model, seismic hazard maps, conclusions, recommendations etc.

[21] NEA/CSNI/R(2009)4 “Probabilistic safety analysis of other external events than earthquake”

This document is referenced in WA1 and WA3.

General summary

The objective of the document was to review the methods for risk analysis of off-site external events other than earthquake as well as the results and the insights developed in these analyses in order to present a basis for advances in the area. The main means to collect information was a questionnaire distributed to the regulatory authorities or their technical support organizations in the NEA countries.

In conclusion there was presented that: International and some national standards/guides on external events PSA are available. The approaches used to treat external hazards in PSA are similar in all the countries and the questionnaire responses did not identify general deficiencies in these methods. This reference does not bring any new information about used references.

[22] NEA/CSNI/R(2011)6 “NEA/IAEA Workshop on “Soil Structure Interaction (SSI) Knowledge and Effect on Seismic Assessment of NPPs Structures and Components” - Workshop Proceedings, Ottawa, Canada, 6-8 October 2010”

This document is referenced in WA1 only

Summary relevant to WA1

This report documents the proceedings from the "Workshop on Soil Structure Interaction (SSI) Knowledge and Effect on the Seismic Assessment of NPPS Structures and Components". In the workshop the input was provided by professionals involved with all elements of the Nuclear Power Plant (NPP) seismic analysis and design chain: seismologists, soil-structure interaction specialists, civil, structural and mechanical engineers.

The objective of this workshop was to review and disseminate recent findings and issues in SSI knowledge and effect on the seismic assessment of NPP Structures and Component (non linear behavior of soil/backfill material, cracking of concrete, embedment effect, partial separation of foundation and soil, SSI analysis of pile foundations, interaction of heavy adjacent structures on SSI analysis, etc.).

Orientation of this document devoted mainly to specific areas dealing with soil behavior and issues of the civil engineering.

[23] NEA/CSNI/R(2010)10/Part2 "Implementation of Severe Accident Management Measures, ISAMM 2009"

This document is referenced in WA2 only

Summary relevant to WA2 and General

The document represents the OECD ISAMM Workshop Proceedings, workshop held in Switzerland, on October 2009. The document is composed by power point presentations, grouped into an opening and introduction, 8 work sessions and a panel discussion. 41 papers on 6 main topics were presented. The objective of the ISAMM 2009 workshop was to put balanced emphasis on both severe accident consequence analysis and risk assessment aspects, such as:

- the current status and insights related to Severe Accident Management (SAM);
- issues of modelling SAM in PSA;
- code analysis supporting SAM development;
- decision-making tools, training, risk targets, and SAM entrance;
- design modifications for implementation of SAM;
- physical phenomena affecting SAM.

Below are summarized some presentations that make references either to external events or human factors.

Presentation from IRSN, Some international efforts to progress in the harmonization of L2 PSA development and their implication

The major role of PSA Level 1 and Level 2 analyses is outlined, these analyses being used to demonstrate that the probability of occurrence of a severe accident is low enough and that, if such an accident occurs, all reasonable provisions are taken to limit the consequences. The activities within the European Framework Programmes (SARNET - Severe Accident Research NETwork of Excellence and ASAMPSA2 - Advanced Safety Assessment Methodology: Level 2 PSA) were presented, focusing on ASAMPSA2 activity. An important aspect is represented by the best-practice guideline that includes all issues related to Level 2 PSA development and applications. Aspects

regarding Level 1-Level 2 PSA interface and Human Reliability Assessment, are included into the second part (Technical recommendations) of the guideline.

Presentation from Switzerland, Accident Management and Risk Evaluation of Shutdown Modes at Beznau NPP

The contributions from system and human errors to CDF in shutdown conditions are specified, highlighting that human errors are the dominating contributors.

Presentation from Switzerland, Overview of the Modelling of Severe Accident Management in the Swiss PSAs

This presentation outlines that HRA-type analysis is important in modelling the actions and measures supported by SAMG in Level 2 PSA. Some elements relevant for HRA modelling are specified (non-prescriptive nature of the guidance, strategy selection, option selection for a specific SAM measure, factors affecting potential dependence of SAM actions on previous HFEs). Also the specific challenges are mentioned, as being:

- Uncertainties in assessing plant state and expected accident progression;
- In-situation strategy selection (informative, non-prescriptive guidance);
- Dependence factors;
- Option selection, given a SAM measure has been selected;
- Timing of decisions.

Presentation from Switzerland, Insights from a full-scope Level 1/Level 2 all operational modes PRA with respect to the efficacy of Severe Accident Management actions

In this presentation, the scope of Goesgen PSA and main results were outlined. The Goesgen Level 1/ Level 2 PSA study was performed for all operational modes. The external hazards (explicit model) taken into consideration were: airplane crash; earthquakes; external floods; loss of service water intakes. Implicit models (via "shutdown scenarios" or manual scrams) consisted of the following: Wind and Tornado; Forest fire; Hail; Extreme snow loads; Climate change; Transportation and industry accidents; Turbine missiles.

For Level1 PSA, the CDF is dominated by external events. For Level 2 PSA at power operation, 96% of LERF come from external events (seismic events and aircraft crashes) also. Results obtained for Shutdown operational modes, Fuel Damage Frequency (FDF) and Releases, were presented (fire is the largest contributor to FDF, FDF > CDF).

Presentation from EDF, Extended use of MERMOS to assess Human Failures Events in Level 2 PSA

MERMOS methodology is presented, together with the application frame (choice of methods to take into account project constraints & specific objectives, HRA team organization, etc.). The main steps of MERMOS methodology are the following: Task analysis, Data analysis, Qualitative analysis, Quantification and the final result is a HEP. The Performance Shape Factors (PSF) are not considered in the analysis.

A MERMOS simplified approach can be used for pre-initiator, post-initiator, crisis organization, and fire screening. The detailed MERMOS approach can be used for post-initiator HFE (Level 1, Level 2, fire, precursor analysis), crisis organization and fire. Aspects about crisis organization, on-site emergency response plan tasks and how to take

into account crisis organization are also presented. An assessment of HFE by Severe accident experts including examples of MERMOS scenarios is given.

Presentation from Korea Institute of Nuclear Safety, Human and Organizational Aspects of SAM, their importance vs. technical issues

The framework of SAMG and SAMG structure is included. An illustrative example of possible results of Decision Making, using two opposite choices (Risk aversion attitude and Risk taking attitude) is given.

[24] NEA/CSNI/R(97)22 “State of the art report of the current status of methodologies for Seismic PSA”

This document is referenced in WA1 and WA2.

Summary relevant to WA1 and General

This report is a review of the methodology for conducting a seismic-PSA at nuclear power station. The objective of this report is to provide a review of the state-of-the-art of the various sub-methodologies (hazard, response and systems methodologies) that comprise the overall seismic-PSA methodology for addressing the safety of nuclear power stations, plus an overview of the whole methodological picture. The objective of this review is as follows:

- To provide an up-to-date review of the state-of-the-art of the various sub-methodologies that comprise the overall seismic-PSA methodology for addressing the safety of nuclear power stations, plus an overview of the whole methodological picture.
- Output of the report is formed by brief summary part which evaluates particular steps of standard methodology for seismic PSA. General conclusion states matureness of used method and noted problems related to the uncertainties.

Summary relevant to WA2

The information relevant from WA 2 point of view is summarized below.

The documents mention that one of the most important sub-methodologies of a seismic PSA is the walkdown methodology. One of the major reasons for the walkdown is the opportunity to understand how the operating crew has been trained to carry out its tasks, especially during emergencies. This understanding is crucial to the development of correct system and human reliability models.

In the frame of the evaluation of the systems analysis methodology, the document addresses the specificities of human reliability analysis for seismic PSAs. During and after a strong-motion earthquake, it seems likely that the ability of control-room operators to perform their assigned tasks without error should be substantially degraded, because of high levels of stress and confusion. This issue has been examined and several models to account more effectively for possible high operator stress have been proposed and are in the literature. Unfortunately, because good data are lacking, there is no way today to sort out with confidence which of the several models of degraded post-earthquake operator performance is best.

However, at least for U.S. nuclear power plants, this issue does not have as much effect on the results of seismic PSAs as might be thought at first, principally because the assumption is commonly made that based on plant operating instructions no credit is allowed for operator control actions during the early minutes, often for as long as a half-hour, after a large earthquake. This assumption is justified by the existence in U.S. plants of automatic equipment that usually does not require any operator intervention in the first half-hour or so. By that time, things should have settled down, so that the normal (non-seismic) PSA methodology for analyzing operator errors should apply. If this is true of other plants in other countries, then the same argument would apply.

The document concludes that, based on this, the operator-response aspect of the seismic-PSA methodology, while not as strongly based on knowledge as would ultimately be desirable, is reasonably mature, and is as robust as the approach for operator error analysis used in internal initiators PSA studies.

[25] NEA/CSNI/R(2007)17 “Differences approach between nuclear and conventional seismic standards with regard to hazard definition”

This document is referenced in WA1 and WA2.

General summary

This report compares the nuclear seismic hazards and design standards with similar standards for conventional facilities. It is aimed at safety philosophy, approach regarding the seismic hazard definition and the design and methods of analysis.

The document aimed to identify the differences between nuclear and non-nuclear conventional standards and their potential significance related to seismic hazards and design methods. The following topics were analysed:

- The safety philosophy behind the seismic nuclear and conventional standards;
- The differences in approach regarding the seismic hazard definition;
- The difference in approach regarding the design and the methods of analysis.

Brief description of the conventional and the nuclear approaches in some NEA member countries (Belgium, Canada, Czech Republic, Germany, Japan, South Korea, Spain, and USA) is given. Based on the differences in approaches on safety objective, hazard definition and methodologies, it is concluded that there are no gaps between nuclear standards dedicated to seismic hazards determination and design and similar conventional standards. The document contains no specific reference to human reliability analysis.

[26] NEA/CSNI/R(2011)8 “Improving robustness assessment methodologies for structures impacted by missiles”

This document is referenced in WA1 only.

Summary relevant to WA1

This report documents the results and conclusions of the Integrity and Ageing of Components and Structures Working Group (WGIAGE)' activity called IRIS_2010 "Improving Robustness assessment of structures Impacted by missiles". The objective of the activity was to conduct a benchmark study as a means of validating the evaluation techniques used in the assessment of the integrity of structures impacted by missiles. This reference forms very detailed document as regards the impact of missiles on selected structures, however its results are not applicable to the purpose of WA1 task.

[27] ENSI-A05/e “Probabilistic Safety Analysis (PSA): Quality and Scope, Guideline for Swiss Nuclear Installations”

This document is referenced in WA1 only.

Summary relevant to WA1

The guideline ENSI-A05 defines the quality and scope requirements regarding the plant-specific level 1 and level 2 Probabilistic Safety Analysis (PSA) for both internal and external events and covering all operating modes of the nuclear power plants. In addition, this guideline establishes the PSA requirements for other nuclear installations. External hazards are covered by 4.6 Chapter where appropriate requirements are specified. This document is written in general sense as regards PSA study and does not present detailed methodologies.

[28] SKI, Report 02:27 “Guidance for External Events Analysis”, February 2003

This document is referenced in WA1 and WA2.

Summary relevant to WA1 and General

This documents aims at creating a common framework for analysis of external events as part of Probabilistic Safety Assessment study for a nuclear power plant. The guidance does not cover seismic events or events originating from acts of sabotage or terrorism.

The main elements presented are as follows:

- The procedure for the identification of a complete set of potential single external events is described, using a categorization of external events in accordance to main group, cause of event (air based, ground based, water based) and relevant deviations. An additional classification of events into natural and man-made external events is made.
- A procedure for the identification of a complete set of potential combined external events is given, together with the used selection criteria (definition of events; different safety functions affected; degree of impact on plant safety functions; single external events criteria).

- The main screening criteria are presented and their use is described with some examples. A relevancy screening should be performed, to obtain a list of site relevant external events. Afterwards, to obtain a list of potential plant relevant external events, an impact screening should be performed (when the maximal strength imaginable at the site will not even have a minor effects on the plant structures cooling, electrical transmission or on the plant operation, the event should be eliminated). The deterministic screening eliminates such plant relevant external events, either single or combined, which do not cause any initiating event modeled in PSA and loss of safety systems needed after the initiating event. The aim of probabilistic screening is to evaluate which events represent an acceptable risk.
- An introduction to some deterministic analysis methods that use analysis experience data for external event, and data sources discussion is given.
- The information needed on plant response to the external events remaining after the impact screening is defined and a work procedure for performing a plant response analysis is given.
- The modeling and quantification of external events using an internal events PSA model is described, as well as how a PSA model can be used in order to estimate the importance of a specific external event.

Summary relevant to WA2

Concerning human activities, it is stated that if they are performed within the relevant surroundings, they may impact the plant via man-made external events. The natural environment may impact the plant itself directly or by affecting man-made activities, the site or other plants on the site.

The plant response information regarding an external event consists of relevant design characteristics, concerning plant characteristics, and protective or mitigating human interactions. The analysis must decide what kind of impact the external events will have on the plant, and how the plant is protected against the impact. The protection may include both structural characteristics, characteristics of active or passive safety functions and protective or mitigating human actions, as defined in safety and operating procedures.

[29] Department of Energy “Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities, January 2002, Superseding DOE-STD-1020-2002, 2013”

This document is referenced in WA1 only.

Summary relevant to WA1

This Standard provides criteria and guidance for the analysis and design of facility structures, systems, and components (SSCs) that are necessary to implement the requirements of DOE, Facility Safety, and to ensure that the SSCs will be able to effectively perform their intended safety functions under the effects of Natural Phenomena Hazards (NPHs), such as: earthquakes, extreme winds (inclusive of tornado, hurricane, and extreme straight line winds), floods, lightning, precipitation (inclusive of snow, rain, and ice), and volcanic eruptions.

The NPH analysis and design process involves the following steps:

Step 1: Sitting new facilities to avoid active geologic faults, areas of instability subject to landslides, and areas of likely soil liquefaction. Special attention shall be given to sites potentially subject to flooding from upstream dams or reservoirs, including seismically induced failures.

Step 2: Establishing the performance requirements for SSCs in terms of parameters that define failure of their safety functions (e.g., flood water level relative to the location of a SSC that is vulnerable to inundation, the state of SSC deformation under various NPH loads, limit states under seismic loads, etc.), that can be determined from the NPH Design Category (NDC) which is based upon the consequences of SSC failure when subjected to NPH events.

Step 3: Calculating NPH demands on SSCs resulting from NPH events in terms of parameters that define failure of their safety functions.

Step 4: Designing (or, for existing facilities, design evaluation) SSCs to ensure their ability to maintain required functionality when subjected to demands of NPH events.

This document does not deal with methodology and analysis process of external hazards. It is aimed as a definition of requirements on natural phenomena hazard design category.

[30] 10CFR 50.54(f) (Generic Letter no. 88-20, Supplement 4) "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, USA, 1991"

This document is referenced in WA1 only.

General summary

This Generic letter states general scope of examination of external initiating events (i.e. high winds / tornadoes, transportation accidents, external floods and earthquakes) and identifies approaches requested for the purpose. The letter is oriented to severe accident, i.e. Level 2 PSA.

[31] EUR 2001 "Volume 2 Generic Nuclear Island Requirements. 2.1 Safety requirements. 2.17 PSA Methodology. Revision D"

This document is referenced in WA1 and WA2.

General summary

The objective of this document is to specify an approach that will result in a comprehensive, high quality and credible PSA. The section 6 of Chapter 2.17 deals with External Hazards. General requirements regarding External Hazards PSA are presented but there is no information on how to assess the human factor depending on the external event. The intention and scope of document is similar with [19].

[32] O. Nusbaumer, and A. Rauzy, *Fault Tree Linking versus Event Tree Linking Approaches: a Reasoned Comparison*. In *Journal of Risk and Reliability*. Professional Engineering Publishing. Vol. 227, Num. 3, pp 315-326, June, 2013.

This document is referenced in WA1 only.

This paper compares Fault tree linking and Event tree linking approach of PSA. This article aims to give ground and to complement this assertion by comparing the two approaches from a mathematical and algorithmical perspective.

This paper is focused mainly on the mathematical background of both methods and it is not useful for the purpose of the report.

[33] M. Hibti, T. Friedlhuber & A. Rauzy, *Automated Generation of Event Trees from Event Sequence/Functional Block Diagrams and Optimisation Issues*, PSAM Tokyo, 2013.

This document is referenced in WA1 only.

General summary

This presentation deals with how to generate event trees so that they would be easy to read and understand, practical for applications, easily to update and maintain, etc. This document is aimed at very specific technical matters and it is not useful for the purpose of the report.

[34] EPRI TR-103959 “Methodology for Developing Seismic Fragilities”, June 1994

This document is referenced in WA1 only.

General summary

This report presents a methodology for performing fragility analysis for use in seismic PSA. It describes basic variables that influence the fragility curves for structures and equipment. It gives the procedure for actually calculating a fragility curve. It provides strategies that will minimize the fragility analysis effort; because it is impractical to perform a fragility analysis for every structure and component. These strategies involve screening of elements out of the system model. And finally it presents example fragility analyses for a variety of typical structure and equipment elements in nuclear power plant.

[35] EPRI-1002988 “Seismic Fragility Application Guide”, December 2002

This document is referenced in WA1 only.

General summary

This report provides an implementation guide for deriving seismic fragilities together with representative example fragility calculations. It provides methodology, procedures, and an array of example problems that encompass

most situations what fragility analysts will encounter with. The information in this document is intended to envelop most cases for development of seismic fragility for Capability Categories 1 through 3. It focuses on applicability of methodology to the requirements in the Standard and provides additions and enhancements to the existing methodology where applicable.

[36] EPRI-1019200 “Seismic Fragility Applications Guide Update”, December 2009.

This document is referenced in WA1 only.

General summary

This update of selected seismic fragilities methods provides utilities with in-depth guidance for performing fragility analysis for a seismic probabilistic risk assessment (SPRA). These cost-effective and practical procedures for fragility evaluations can be used in performing a SPRA in support of Risk Informed/Performance Based applications. It provides utilities with state-of-the-art guidance on seismic fragility analysis methods in support of regulatory and non-regulatory applications.

[37] NUREG 6850, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities.

This document is referenced in WA1 only.

General summary

This guideline provides complete methodology for analysis of internal fires including several application examples.

[38] IAEA Safety Series No. 50-P-10 “Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants”

This document is referenced in WA2 only.

General summary

This document presents a practical approach for incorporating HRA into PSA. It describes the steps needed and the documentation that should be provided to support the PSA. It also describes a framework for analyzing those human actions which could affect safety and for relating such human influences to specific parts of a PSA. But this document does not address the specificities of external events PSA and their impact on the HRA.

[39] EPRI 1019196 - NUREG-1921 “EPRI/NRC-RES Fire Human Reliability Analysis Guidelines”

This document is referenced in WA2 only.

Summary relevant to WA2

This document provides a methodology and guidance for estimating Human Error Probabilities (HEPs) for human failure events under fire generated conditions, building upon existing HRA methods. This process includes identification and definition of post-fire human failure events, qualitative analysis, quantification, recovery,

dependency and uncertainty analyses. This document provides three approaches to quantification: screening, scoping and detailed HRA. Regarding screening, specific guidance is given for scenarios with long time windows. Scoping is a new approach to quantification developed specifically to support the iterative nature of Fire PSA quantification. Scoping is intended to provide less conservative HEPs than screening but requires fewer resources than a detailed HRA. For detailed HRA quantification, guidance has been developed on how to apply existing methods to assess post-fire HEPs.

First the report delineates the objectives and the scope as well as provides the background information on the tasks conducted in developing the fire HRA methodology and guidelines. It then provides an overview of the guidance provided in the report. It is intended to show various steps in conducting fire HRA and how these steps may fit into a fire PSA. Following this overview, the document describes in detail the methodology for each step of the process to conduct a fire HRA.

Step 1: identification of operator actions and definition of human errors

The identification of operator actions and definition of human errors is the first step of a fire HRA. The objectives are to identify operator actions and associated instrumentation that are necessary for successful mitigation of fire scenarios and to define the HFEs at the appropriate level of detail. As in the internal events HRA, operator actions are primarily identified by accident sequence and procedure review. Identification of post-initiators for fire HRA is primarily concerned with three types of procedures: emergency operating procedures (EOPs), alarm response procedures (ARPs) and fire procedures. The following types of post-initiator human errors are to be considered:

- Existing Internal Events Human Failure Events (HFEs) that is to say the actions from the internal events PSA;
- Fire Response HFEs - including Main Control Room Abandonment HFEs (which are considered as a special subset of the fire response HFEs);
- HFEs corresponding to undesired response to spurious actuation or spurious instrumentation.

Once the operator actions have been identified and the HFE defined, the feasibility of the operator actions should be determined. In order to determine the feasibility of the operator actions, the following information should be addressed qualitatively and early in the HRA task to avoid unnecessary analysis:

- What are the critical operator tasks required for success?
- Is the location where the action is accomplished accessible given the fire?
- Is there sufficient time to complete the action?
- Is there enough staff available to complete the action?
- Has the fire impacted equipment such that required critical tasks cannot be performed?

Consideration of the above should allow the HR analyst to make a preliminary qualitative assessment about feasibility. The feasibility step is not unique in the identification and definition stage but this process is iterative as more information is known about the HFE, the feasibility could be re-assessed.

Step 2: qualitative analysis

All HRA methods require a qualitative analysis prior to quantification. Whether this analysis is embedded in the identification and definition step or is considered explicitly. For fire HRA, the qualitative analysis involves defining the HFE narrative (accident sequence, timing information, availability of cues, physical environment...) in the

context of the fire PSA and developing an understanding of Performance Shaping Factors (PSF) (cues and indications, timing, procedures and training, complexity, workload, pressure and stress, human machine interface, environment, special equipment, special fitness needs, crew communication, staffing and dynamics) and other qualitative attributes contributing to quantification of HFEs in the context of the fire PSA. Actually, many if not all of the fire impact on the HRA comes through the influence on PSFs. Depending on the quantification approach that is applied (screening, scoping or detailed analysis), the level of detail required for a given HFE differs but all quantification approaches need qualitative analysis as input.

Step 3: quantification

This report describes three different approaches to quantify the HFEs identified in the fire PSA models. For each HFE required quantification, the options for quantification are the following:

- Screening HRA
- A new scoping fire HRA quantification method developed in detail in this report
- Two detailed HRA quantification approaches modified for application in fire PSAs.

Screening HRA

The screening methodology assigns quantitative screening values to the HFEs modelled in the fire PSA by addressing the unique conditions that can influence crew performance during fires, ensuring that the time available to perform the necessary action is appropriately considered and ensuring that potential dependencies among HFs modelled in a given accident sequence are addressed. To determine appropriate HEPs, a given HFE must be matched to a set of criteria. For a particular HFE, if an appropriate set of criteria cannot be identified or met, no screening value should be used (i.e. a 1.0 failure probability should be assigned). The HEPs assigned in this manner are conservative and may be not acceptable as a final HEP for a given HFE, that is to say a more realistic HEP is needed. In addition since the screening approach assigns a screening value of 1.0 for MCR abandonment or alternative shutdown actions, a possible next step is the scoping methodology which allows assignment of a single overall failure probability value to represent the failure of reaching safe shutdown using alternate means (including MCR abandonment) if certain minimal criteria are met.

Scoping fire HRA

The scoping fire HRA approach could be more adequate to quantify HFEs if a less conservative analysis than the screening HRA is required. It is a simplified quantification approach that has been developed specifically for this report. In order to use the scoping approach, first the feasibility of the action must be demonstrated and the minimum criteria relative to several PSFs need to be met. Then, the scoping analysis uses decision-tree logic, as well as descriptive text, to be guided to the appropriate HEP value. The scoping quantification process requires a more detailed analysis of the fire PSA scenarios and the associated fire context and a good understanding of several factors likely to influence the behaviour of the operators in the fire scenario. Given such an analysis, it is expected that the flowcharts provided and for which guidance is given in this report, can be used to perform quantification for many of the HFEs being modelled. However, some actions may not be able to meet some of the criteria and may result in an HEP of 1.0. Furthermore, the HEPs developed using this method may be conservative compared to that which could be developed using one of the two detailed HRA approaches mentioned below.

Detailed HRA

Some actions may not be able to meet some of the criteria in the scoping fire HRA approach for any of a number of reasons and result in an HEP of 1.0. Furthermore, the HEPs developed using this approach may be fairly conservative compared to that which could be developed using one of the two detailed HRA approaches described in this report. For those cases in which the scoping approach cannot be used or a more detailed and possibly less conservative analysis is desired, a detailed analysis using either EPRI detailed HRA methodology approach or ATHEANA HRA method can be performed. At present time the method selected for detailed quantification should be based on considerations such as plant-specific scenario information, fire context/impact and general suitability (for non-fire conditions).

Step 4: recovery actions analysis

New recovery actions are needed for development and evaluation of realistic fire PSA models at different stages of development. For fire HRA, recovery actions are modelled in the PSA the same way as in the internal events HRA. The main difference for a fire HRA is to consider the impact of the fire on the ability to perform recovery actions associated with specific fire scenarios. Guidance is given in this report on how recovery action can be modelled in the post-initiator fire HRA. And the requirements that should be met before applying recovery actions with an HEP less than 1.0 are also provided. The types of recovery actions considered are those that were not added to the fault trees and event trees as part of the planned plant response. Instead, they are actions that are added at the sequence or cutset level to re-align the affected system or to provide an alternate system such that success of these actions would have prevented core damage and/or large early release. Another recovery action that is considered in the fire PSA involves modelling the fire brigade and their actions to extinguish the fire. This type of recovery action is treated in the fire modelling task via statistical models derived from fire suppression event data. Because the impact is on the fire itself, it is not addressed as an HRA modelling issue. Instead a fire scenario with suppression considered is defined to include its impact on the electrical instruments, controls and power cables to define the input conditions for the HRA models that impact the Core Damage Frequency PSA model.

Step 5: dependency analysis

The analysis of dependent HFEs is important because risk metrics such as core damage frequency can be significantly underestimated in cutsets or sequences containing multiple HEPs. A review of the cutsets for dependencies could show some combinations in which there are both screening and scoping HEPs. The screening HEPs by definition are considered conservative and adjusting these HEPs even more may either increase the HEPs to 1.0 or make them overly and unrealistically conservative. Thus, the screening HEPs will not usually need to be further adjusted to account for dependencies as long as the combination of HFEs is shown to be feasible, that is to say, there is enough time to complete all the actions and enough crew members are available to complete all the actions. But scoping HEPs (and detailed HRA HEPs) can be treated using the approach described in the report, but the criteria for the scoping HEPs must still be met. That is, if credit for the action is taken, the adjustments in the HEPs should still reflect that the actions are feasible and there is an adequate time margin given the dependent effects.

Step 6: uncertainty analysis

It is mentioned in this report that for fire PSA, uncertainties are addressed in the same manner as for internal events HRA. Thus, the HRA should characterize the uncertainty in the estimates of the HEPs consistently with the

quantification approach and provide mean values for use in quantification. In Fire modelling and HRA, by identifying the areas of uncertainty and focusing on those aspects of uncertainty that can be reduced, the associated decision-making processes could be improved.

The guidance in this report represents the state of the art in fire HRA practice. Certain aspects of HRA, especially in the area of quantification, continue to evolve and likely will see additional developments.

[40] WENRA Reactor Harmonization Working Group RHWG, Safety of New NPP Designs - March 2013

This document is referenced in WA2 only.

Summary relevant to WA2

This report sets out the common positions established by the Reactor Harmonization Working Group (RHWG) of WENRA on the selected key safety issues. The report discusses also some considerations based on the major lessons from the Fukushima Dai-ichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions.

All the selected external hazards for analysis should be characterized in terms of their severity and/or magnitude and duration. The characterization of the external hazard will depend on the type of analysis that is to be carried out and shall be conservative for the general design basis analysis and could be realistic/best estimate for rare and severe external hazards analysis and PSA. It should be noted that for external hazards PSA, a range of frequencies and associated hazard parameters is often required. For some external hazards:

- the ability to forecast the magnitude and timing of the event, and the speed at which the event develops may be relevant and should be considered;
- several parameters could be relevant to characterize severity and/or magnitude.

In choosing the multiple failure events to be addressed in the design, the event frequency, the grace time for necessary human actions, the margins to cliff-edge effects, and the radiological or environmental consequences of the event are important factors that should be considered.

PSA for external hazards should include consideration of building and structural reliability as well as system and component fragilities and should take account of the potential for human response to be affected by the external event.

[41] WENRA "Position paper on Periodic Safety Re-views (PSRs) taking into account the lessons learnt from the TEPCO Fukushima Dai-ichi NPP accident", March 2013

This document is referenced in WA3 only.

Summary relevant to WA3

The document based on the study by WENRA Reactor Harmonization Working Group and position paper on periodic safety reviews taking into account the lessons learnt from the TEPCO Fukushima Dai-ichi NPP accident. This docu-

ment discussed the consideration needed for multi-unit sites in PSRs. It stated that on multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analysed.

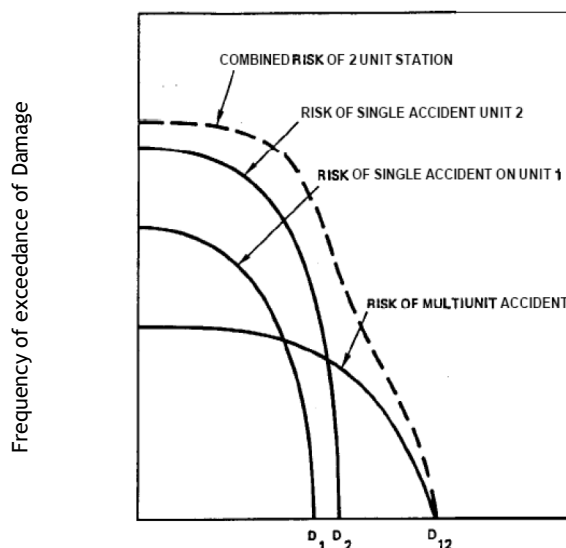
[42] On The Issue of Integrated Risk - A PRA Practitioner's Perspective

This document is referenced in WA3 only.

Summary relevant to WA3

This article presented at the 2005 PSA congress in San Francisco discusses the issue of integrated risk in relation to the initial PSA at Seabrook which was a Level-3 PSA of internal (including fire and flooding) and external events (flooding and earthquake) at power, including multi-unit aspects. Even though there are already many sites in the United States with several units in operation, the necessity of calculating an "integral" risk on a site has until now not been considered a priority by the NRC, as the majority of operators have been licensed based on an assessment of the risk per unit. With the probable future arrival of modular reactors, the NRC now appears more concerned by this issue and has sought to define the safety goals to be applied to these future reactors, with the difficulty linked to an apparent ambiguity on the level of application of the safety objectives defined at society level (QHO). Are they applicable at site level or at single unit level? One way of presenting the integral risk on a site is given in the figure 4 below:

FIGURE 4 FREQUENCY OF EXCEEDANCE OF DAMAGE



In the case presented, both units are considered to be different, which was not the case at Seabrook where both units were identical and actually shared very little equipment. In spite of this relative independence of the two units, the risk associated with multi-unit impacts has proven to be fairly significant. The results obtained are presented in the following table 3:

TABLE 3 RISK METRIC AND THEIR MEAN VALUE

Risk Metric	Mean Value
Single Reactor Unit CDF	2.3×10^{-4} /reactor-year
Two Unit Station CDF	
- Core damage to one reactor	4.0×10^{-4} /station-year
- Core damage to both reactors	3.2×10^{-5} /station-year
- Total	4.3×10^{-4} /station-year

When we look at the integral result (station PSA), we obtain a risk which is less than twice that calculated on a single unit. We note that the risk is expressed as /station-year, which is an appropriate unit for such a risk. The assessment of the frequency of the initiating events must therefore also be expressed in this unit. The distribution of the multi-unit risk by initiating event is given in the following table 4:

TABLE 4 INITIATING EVENT AND CDF FOR MULTI UNIT

Initiating Event	Frequency of Core Damage on multi - units (Events/station-year)
Seismic Events	2.8×10^{-5}
Loss of Offsite Power	2.8×10^{-6}
Truck Crash into Transmission Lines	1.0×10^{-7}
External Flooding	1.6×10^{-6}
Total	3.2×10^{-5}

The proportion of the multi-unit risk at Seabrook is significant as the risk linked to a single unit is dominated by initiating events likely to affect both units, such as loss of offsite power. If the risk for a unit had been dominated by circuit breaks, for example, the proportion relating to the multi-unit risk would have been lower.

In terms of modelling, the main lessons learned from this analysis are as follows:

- The elements linked to the design and operation of the units with the greatest impact (positive or negative) on the multi-unit risk are:
 - The existence of a few shared systems and primarily the offsite power and tunnels carrying the service water.
 - The redundant equipment and teams at site level intended to help one or other unit in the event of a problem.

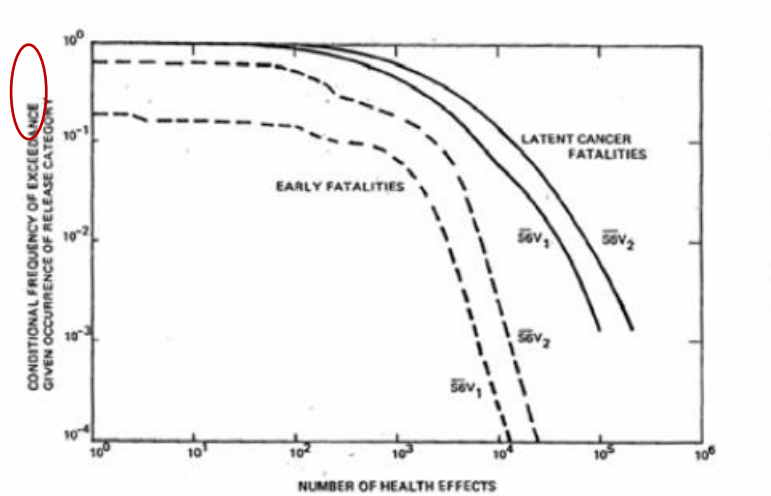
- The physical proximity of the two units, separated by approximately 150m, increasing their shared sensitivity to external hazards such as flooding and earthquakes.
- The existence of potential CCFs on equipment identical to the two units due to design or maintenance errors.
- Initiating events can be categorized according to their potential impact on the units. The categories obtained for Seabrook are presented in the following table 5:

TABLE 5 CATEGORY AND INITIATING EVENTS

Category	Initiating Events
Events Impacting Both Units	Loss of Offsite Power Seismic Events Tornado and Wind External Flooding Truck Crash in Switchyard
Events Impacting Both Units under certain conditions	Loss of Condenser Vacuum Loss of Service Water Turbine Missile
Events impacting each unit independently	Loss of Coolant General Transients Loss of Component Cooling Loss of one DC bus Internal fires Internal floods Aircraft crashes

- One important point of the modelling concerns the inclusion of potential inter-unit CCFs. With regards to earthquakes, the usual but very conservative hypothesis of total dependency of the failures of all the equipment at a given level, associated with the same fragility curve, has been used. For losses of offsite power, one CCF possible on all the site's auxiliary diesel generators has been postulated. The analysis of feedback has allowed the modelling to be separated into one CCF group of order 2 for each unit and one CCF group of order 4 on the site. It has also allowed the variables to use to be refined.
- The following figure 5 gives the distribution of the consequences of releases in terms of early fatalities and cancer fatalities for a given release category (corresponding to the failure to isolate small penetrations during a total loss of offsite power). In these curves, index 1 corresponds to the calculations for a single unit while index 2 is allocated to data relating to the multi-unit scenarios.

FIGURE 5 DISTRIBUTION OF THE CONSEQUENCES OF RELEASE



It is interesting to note that the probability of having at least one early fatality is multiplied by approximately 5 when considering the multi-unit risk. This effect does not exist for cancer fatalities. The non-linearity observed for early fatalities is due to the existence of a dose threshold.

[48] Risk Assessment of Operational Events - Handbook - Volume 1 - Internal Events Revision 1.03 - August 2009

This document is referenced in WA3 only.

The primary aim of the Risk Assessment of Operational Events Handbook (sometimes referred to as the RASP Handbook) is to document the methods the NRC analysts can use to obtain greater consistency when analysing the risks associated with operational events or safety issues on US units.

The second aim is to provide SPAR (Standardized Plant Analysis Risk) model developers with a guide that ensures these models will be developed to represent the actual state of the units (as-built, as-operated) with the level required to support the analyses.

This document is divided into three volumes:

- Volume 1 - Internal Events
- Volume 2 - External Events
- Volume 3 - Review of SPAR models

Volume 1 contains considerations relating to the multi-unit aspects summarized below.

General

Multiple units on the same site are often connected to be able to mutually benefit from each other's support systems. Thus, if we consider that the connection itself cannot be the source of failures, having four pumps for the service water system shared by two units is better than having two isolated pumps per unit. Modelling this situa-

tion requires the manner in which the sharing is managed to be addressed, especially in the event of the failure of at least one of the pumps, which can become complex.

Even if two units are not physically connected, the risks associated with them can be correlated due to the existence of identical equipment on both units potentially concerned by common cause failures.

Shared systems

Typically, the shared systems, or those that can be shared at site level, are:

- The HV or LV switchboards through possible interconnections
 - The equipment used for the emergency power supply, such as for example:
 - Auxiliary diesel generators
 - SBO Diesels
 - Gas turbines
 - Hydroelectric generators
- Compressed air supply
- CCS/ESWS systems
- Auxiliary feedwater system
- Chemical and volume control system

Multi-unit initiating events

Typically, the initiating events that can affect the site as a whole are:

- Loss of offsite power
- Loss of service water
- Loss of compressed air (for a shared system)
- External hazards (including earthquake, strong winds and external flooding)

Consideration of shared systems

Overall, SPAR models, and more especially fault trees, already take account of shared systems and equipment and the possibilities of mutual backup of the units given the existing physical connections and associated procedures.

If the shared system is sized to operate one unit at a time, the fault tree for this system included in the PSA for unit A must be adapted to reflect the probability that twin unit B is not using the system. This modification can be achieved through a shared availability factor. This factor must take account of the frequency of a potential multi-unit initiating event, the probability of human error and the probability of the associated equipment failures.

Twin unit configuration

For the analysis of a given unit, it is important to take account of the other unit's possible different states. In particular, any maintenance operations in hand on the other unit's shared equipment must be considered and included in the success criterion associated with the system concerned and in any change in probability relating to the inter-unit CCF groups.

Modelling initiating events that only affect one unit

For events that affect one unit at a time (such as the loss of feedwater, SGTR, spurious lift of a pressurizer valve, primary and secondary circuit breaks, for example), we consider that:

- It is reasonable to assume that the other unit is not affected by an initiating event at the same time;
- Shared equipment and interconnections can be fully assessed; it is nonetheless necessary to correctly model equipment failures and unavailability, taking account of the state of the twin unit; likewise, the interconnection operator actions must be carefully assessed.

Modelling initiating events that affect the site

In this case, care will be taken to:

- Assess the impact of the initiating event on all units.
- Not assess the shared equipment for both units at the same time; it is recommended an overall analysis of both units be performed (even if developing one model per unit).
- Take account of the STE and in particular the only authorized interconnections and sharing.
- Take account of the procedures and in particular the existence of any priority of one unit over another with regard to the shared equipment.
- Take account of an appropriate initiating event frequency (only take account of events that affect both units).
- Take into account the probability of success of the restoration actions. The success of these is less likely in the case of a multi-unit event.
- Check that operator actions to implement the interconnections are realistic (time available, feasibility given the conditions induced by the initiating event) and possibly modify the failure probability of these actions in accordance with the PAHR method used;
- Take account of the CCF groups and the associated variables.

It is recommended a grid be constructed to indicate all possible equipment combinations.

[49] IAEA-TECDOC-1341, Extreme External Events in the Design and Assessment of Nuclear Power Plants, Vienna, 2003

This document is referenced in WA3 only.

This publication provides a technical background to regulators, plant owners and designers in the definition of a consistent strategy in selected safety issues on site evaluation, design and operation in relation to extreme external events.

This document recommends, in case of multiunit sites, co-ordination of the scram logic among the different units. For multiunit sites in case of events able to induce common cause failures, the required shutdown time has to be multiplied for the number of units.

The risk from a single reactor site can vary depending upon the power state or shutdown mode of the reactor. For multiple reactor sites, the risk from the site will increase as units are added. Document states that the probabilistically defined design bases can be used in these contexts to allow the design basis to vary whilst keeping the overall risk within tolerable or acceptable limits.

[50] ONR Safety Assessment Principles (SAPs), 2006 Edition, Revision 1 (2008)

This document is referenced in WA3 and WA4.

General summary

This document gives the current Safety Assessment Principles for use by the ONR inspectors. It is not prescriptive, but gives guidance for the assessments that need to be carried out. It gives the overall probabilistic requirements expected of the nuclear plant (not just nuclear power plants) and gives guidance on the topics that need to be addressed in a safety case, including external hazards. This specifies the general design basis requirement for external hazards as natural hazards that conservatively have a predicted frequency of being exceeded of more than 1 in 10 000 years.

The SAPs are currently being updated and are expected to be re-issued in 2014.

[51] IAEA Safety Requirements No. NS-R-3, Site Evaluation for Nuclear Installations, 2003

This document is referenced in WA3 only.

This guide establishes requirements and provides criteria for ensuring safety in site evaluation for nuclear installations.

Section 2 provides the general safety criteria for site related evaluation of external natural and human induced hazards to the nuclear installation. Section 3 establishes specific requirements for their characterization. Section 4 establishes specific requirements for site related evaluation of the effects of the installation on the regional environment, the atmosphere, the hydrosphere and biosphere, and the population. Section 5 establishes the requirements for continuous monitoring of natural and human induced hazards throughout the lifetime of the installation. Section 6 establishes requirements for a quality assurance programme for site evaluation.

The scope of this publication encompasses site related factors and site - installation interaction factors relating to plant operational states and accident conditions, including those that could lead to emergency measures, and natural and human induced events **external to the installation** that are important to safety.

The phrase 'external to the installation' includes more than the external zone. In addition to the area immediately surrounding the site, the site area itself may contain objects that pose a hazard to the installation, such as an oil storage tank for diesel generators or another reactor on a multiunit site.

[52] IAEA SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, 2011

This document is referenced in WA3 and WA4.

General summary

This guide supplements and provides recommendations on meeting the requirements for nuclear installations with regard to the assessment of meteorological and hydrological hazards.

The potential for common cause effects and damage across the site is an important consideration when analysing possible implications for a site, including for the incorporation of new, upgraded or appropriately located safety related systems. These considerations are more important when a multiunit or multi-installation site is under consideration, and in particular if structures, systems and components important to safety are shared between units.

[53] Regulatory Review of Probabilistic Safety Assessment (PSA) Level 1 - IAEA-TECDOC-1135

This document is referenced in WA3 only.

This document, intended more for the safety authorities, is the result of cooperation between the IAEA and OECD to produce a guide enabling them to review PSA models to ensure their quality before they are used in regulatory decision-making processes. The obligations relating to the multi-unit aspects are summarized below:

On a multi-unit site, some systems important for safety can be shared by the units or there may be mutual backup through interconnections. In such cases, reviewers must ensure that the initiating events likely to affect several units have indeed been taken into account and that the shared systems are correctly modelled (they must not be considered to be fully available for a given unit). Any missiles that may be generated by the disintegration of a turbine on a given unit could also generate an initiating event by affecting a vulnerable component on the neighbouring unit. This type of initiating event must be studied and its elimination must be based on a detailed analysis. Finally, the possibility of having an initiating event common to both units due to a problem with the shared systems or possible interconnections must be studied.

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

This document is referenced in WA3 only.

This report from 2004, established jointly by the IAEA and OECD WGRISK, presents a state of the art of the development and use of risk monitors in nuclear power plants in member countries. The questionnaires used to gather the information used related to the following three points:

- The development and use of risk monitors
- The associated software tools
- The prospects for use in a regulatory framework.

Of the characteristics desired for a risk monitor, the report mentions the fact that a risk monitor used on dual units should be based on a single model, extended to take account of the shared equipment and systems, to ensure consistency between the two units. Thus, when for example one of the shared pieces of equipment is used by one unit, the risk associated with the configurations for the other unit will take account of this unavailability. This of course implies use of the risk monitor on the network.

[55] A new method to evaluate alternate AC power source effects in multi-unit nuclear power plants

This document is referenced in WA3 only.

In this paper new approach for evaluation of a station blackout (SBO) event frequency of a multi-unit nuclear power plant that has a shared alternate AC (AAC) power source is presented. The approach accommodates the complex inter-unit behavior of the shared AAC power source under multi-unit loss of offsite power conditions. The SBO frequency at a target unit of probabilistic safety assessment could be underestimated if the inter-unit dependency of the shared AAC power source is not properly modeled.

The approach is illustrated for two cases, 2 units and 4 units at a single site, and generalized for a multi-unit site. Furthermore, the SBO frequency of the first unit of the 2-unit site is quantified. Obtained results show that the effect of the inter-unit behavior of the shared AAC power source on the SBO frequency is not negligible depending on the CCF characteristics among AC power sources.

[56] EPRI 1022997 Identification of External Hazards for Analysis in Probabilistic Risk Assessment. Technical Update, December 2011.

This document is referenced in WA3 only.

This document reports on the assessment of current practices related to the identification of external events (hazards) that can potentially affect the safety of nuclear power plants and provides recommendations on the screening criteria used to perform this identification process. The identification process is intended for use by individual plants, and the identified external events are appropriate candidates for evaluation using probabilistic risk assessment (PRA). One of the outcomes of an external event PRA is the determination and quantification of plant safety vulnerabilities resulting from the external event. The population of potential external events is assembled in this report. The identification process then applies screening approaches that eliminate from consideration events whose impact cannot initiate an event sequence that could lead to core damage (qualitative) and those whose frequency of occurrence is low enough that the resulting core damage frequency would be very low (quantitative). This report addresses all external events except for seismic: historically, seismic events have been con-

cluded to be, on a generic basis, an appropriate candidate for PRA study. In addition, internal fires and internal floods occurring in nuclear power plants - which have sometimes been considered part of external events analyses in the past - are not included in the scope of external events in this report nor are intentional, non-accidental events. Current practice assessed in this report includes both U.S. and international practice.

[57] WENRA-RHWG, Guidance Document Issue T: Natural Hazards. Guideline for the WENRA-RHWG Safety Reference Levels for Natural Hazards introduced as lesson learned from TEPCO Fukushima Dai-Ichi accident. Draft, February 2014

This document is referenced in WA3 only.

The purpose of this Guidance is to provide an improved understanding of the intent of the Safety Reference Levels of Issue T, to contribute to a consistent interpretation and to permit insights into the consideration which have led to their formulation. In addition, some background information is provided for easy reference. Appendix 1 to this document provides an initial listing of those Natural Hazards which should be considered as potentially affecting a facility.

[72] ONR Technical Assessment Guide - External Hazards. T/AST/013 - Issue 4, July 2011

This document is referenced in WA4 only.

This document follows on from the SAPs and gives an interpretation of the relevant SAPs with respect to external hazards. It also provides more detailed guidance on the assessment of the design approach and frequency requirements for external hazards. It gives a comprehensive, but not necessarily exhaustive list of hazards that should be considered. References to other ONR Technical Assessment Guides are given as well as to external documents such as IAEA Guides and Western European Nuclear Regulators Association (WENRA) Reference Levels.

This document is currently being revised to reflect the update of the SAPs described above.

[82] ANSI/ANS-58.21-2007 "External-events PRA methodology", 2007.

This document is referenced in WA4 only.

This standard was superseded by ASME/ANS RA-Sa-2009 [10]

[83] Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making - NUREG/CR-6813 - K. Fleming

This document is referenced in WA4 only.

This NUREG was compiled by K. Fleming at the request of the NRC's Advisory Committee on Reactor Safeguards to serve as input data for preparing the General Rules relating to the technical appropriateness of PSAs for their use in risk-informed applications.

From the point of view of the consideration of multi-unit aspects, the conclusions of this NUREG are as follows:

Some initiating events (for example, loss of offsite power) can have an impact on several units at once and this is not generally modelled at the moment. Likewise, inter-unit dependencies are not sufficiently addressed. This is especially the case when there are strong dependencies via the shared systems' support systems. The tendency in current PSAs is to too easily assess the shared systems and possible interconnections, without taking account of the possible negative interactions (occurrence of an initiating event, CCF, dependency between the decisions made at site level, during deployment of shared equipment and human resources, etc.).

The risk metrics currently used are the CDF and LERF defined as frequencies per unit and per year. These metrics are representative of the risk associated with the unit taken in isolation. They are poorly suited to representing an integral risk at site level, taking account of both the contribution of all of the site's units taken individually and that of the multi-unit scenarios.

[84] CEGB Pressurised Water Reactor Design Safety Guidelines, April 1982.

This document is referenced in WA4 only.

In 1982 the (then) Central Electricity Generating Board (CEGB), published a Design Safety Guide (DSG) for the proposed new generation of PWRs. This document defined a probabilistic approach to the seismic and wind hazards, as well as to other design aspects. It consists of a short safety statement followed by 20 Annexes that deal with all aspects of reactor design. One of the Annexes addresses external hazards. The overriding requirement in the external hazard Annex is to ensure that following any specified (design basis) external hazard the failure to shut down and cool the reactor will be no greater than 10^{-3} per demand where failure is defined as the causation of (public) doses greater than 100 mSv. It then goes on to list the anticipated design basis hazards and specifies the seismic hazard as having a cumulative probability of exceedance less than, or equal to 10^{-4} per annum. This document is now out of print and has been superseded by updated requirements.

[85] CEGB Advanced Gas-cooled Reactor Design Safety Guidelines, August 1985.

This document is referenced in WA4 only.

This document is now out of print.

[86] NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, August 1983

This document is referenced in WA2 only.

The objective of this document is to provide methods, models and estimated Human Error Probabilities (HEPs) to enable qualified analysts to make quantitative or qualitative assessments of occurrences of human errors in Nuclear Power Plants (NPPs) that affect the availability or operational reliability of engineered safety features and components. This document provides much of the modeling and information necessary for the performance of human reliability analysis (HRA) as a part of Probabilistic Risk Assessment (PRA) of NPPs. But this document puts the emphasis on internal initiating events (LOCAs and transients) even if it is mentioned that the models can be applied to other abnormal events displayed in the control room. Thus, operator response to external initiating events is not specifically addressed in this guideline.

[87] NUREG/CR-4772, Accident Sequence Evaluation Program, Human Reliability Analysis Procedure, February 1987

This document is referenced in WA2 only.

This document presents a simplified version of the procedure for HRA presented in [86]. The objective of this HRA procedure called “ASEP HRA Procedure” is to enable PSA analysts with minimal support from experts in HRA to make estimates of Human Error Probabilities (HEPs) which are sufficiently accurate for many PSAs. This document presents four different procedures, two for pre-accident errors (procedures for a screening HRA and a nominal HRA) and two for post-accident errors (procedures for a screening HRA and a nominal HRA). A screening HRA involves the use of conservative estimates of human behaviour (i.e., higher HEPs and longer response times than one expects to be the case). A nominal HRA involves the use of the analyst’s best estimates of HEPs and response times. This document aims to be used for HRAs in PSAs in general. It presents procedures to assess the human factor independently of the abnormal event analysed. As mentioned in the document, the specific abnormal events to be analysed in HRAs should be designated by PRA analysts. This document does not address the specificities of external events PSA and their impact on HRA.

[88] James R. McDonald, Ph.D., P.E.: Rationale for Wind-Borne Missile Criteria for DOE Facilities, UCRL-CR-135687 S/C B505188 Lawrence Livermore National laboratory, September 1999

This document is referenced in WA1 only.

This document is intended as guidelines to determine and demonstrate design basis for wind-borne missiles. They provide rationale for determination of scope of considered wind-born missiles as well as design recommendations including evaluation of missile parameters as well as missile impact velocity.

[89] NUREG/CR-7004 Technical Basis for Regulatory Guidance on Design-Basis Hurricane-Borne Missile Speeds for Nuclear Power Plants

This document is referenced in WA1 only.

This document is intended as guidelines to determine and demonstrate design basis for wind-borne missiles. They provide rationale for determination of scope of considered wind-born missiles as well as design recommendations including evaluation of missile parameters as well as missile impact velocity.

[90] I.A.Rahmant et al.: Review on Empirical Studies of Local Impact Effects of Hard Missile on Concrete Structures, International Journal of Sustainable Construction Engineering & Technology.

This document is referenced in WA1 only.

This document brings overview of empirical formulas used to evaluate dynamic response of concrete structures after impact of missiles, especially impact of missiles that can be classified as “hard body”.

11.2 APPENDIX 2 - MULTI UNIT ASSESSMENT

(Proposed by EDF R&D)

11.2.1 INTRODUCTION

Most nuclear generation sites worldwide have more than one reactor in operation. In the perspective of PSA scope extension to multiple units site risk assessment, it should be taken into account when assessing the risk related to these installations, in particular, when assessing the consequences in terms of impacts on the health of the population and on the environment. Generally speaking, mainly models relating to a single unit have been developed to date. Therefore, the purpose of the work handled by EDF R&D was to propose solutions or methodological options, depending on the situation, in order to switch from a risk assessment for the unit to a risk assessment for the site.

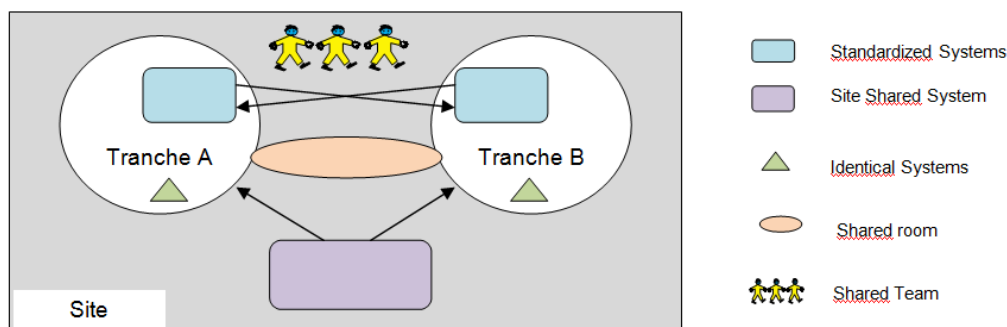
Only the case of a site with two units has been dealt with here²¹. A review of existing PSA standards and documents (see bibliography below) showed that the specificity of a site PSA was to deal with the dependencies existing between the units on the site. These dependencies may come from various sources:

- Both units are on the same site and are therefore subject to the same environmental constraints, in particular in terms of external hazards.
- Systems may exist that are shared by both units. These common systems may be of three types:
 - identical systems present on each unit but dedicated to one unit;
 - systems that are shared on a site level;
 - standardized systems present on each unit but useable by the other unit thanks to cross connecting devices.
- Common or inter-connecting rooms may exist between the two units.
- Resources that are common in terms of operating and maintenance teams may exist.

The following diagram gives a representation of such a site

²¹ To take into account more than 2 units on a site, it would be necessary to make some adjustments on the proposed approach. It could be documented in an update of the present document.

FIGURE A1 REPRESENTATION OF A SITE WITH TWO UNITS WITH ITS DEPENDENCIES



11.2.2 POTENTIAL LIMITS OF A UNIT MODEL

A unit model is often developed by assuming that there is only one unit on the site considered. This case can therefore be summarized as follows:

The initiating events emerge and/or are applied to a single unit and the consequences are therefore assessed for this unit only. The frequency of the initiating events (internal events and internal and external hazards) is expressed as /unit.year, as is the associated risk. Any systems shared on the "site" level and all human resources, are credited entirely for this unit. Any backup of one unit by a twin unit may be evaluated based on the assumption that it is systematically available.

The question that can be asked is the following: should the risk associated to the unit model simply be multiplied by 2 to obtain the risk for a site with two units?

Strictly speaking, the answer is no. Indeed, a unit model, as previously described, can overestimate the risk by not correctly taking into account the standardization of certain systems. Conversely, it underestimates the risk by:

- fully crediting the site shared systems for the unit studied,
- not taking into account any sharing of human resources on the site in the event of accident scenarios,
- forgetting initiating events generated in a unit and that propagate to the other unit,
- not taking into account any impact of the presence of two units on the frequency of certain initiating events.

It is difficult to actually foresee the impact of these opposite effects on the overall risk. The case of the Seabrook PSA²² shows a risk of core meltdown at the site level that is slightly lower than twice the risk at the unit level. But can this be generalized? Probably not. Thus, the limits of a unit PSA model, as previously defined, need to be exceeded in order to correctly assess the risk for the site. These limits in fact relate to three aspects of the PSA model:

1. Initiating events

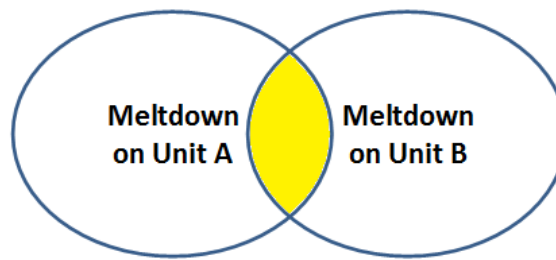
²² Seabrook Station Probabilistic Safety Assessment R Summary reports & Volumes 1 to 6 December 1983

2. Modeling of common systems (and related data)
3. Consideration of the human factor (Human Errors Probabilities - HEPs)

11.2.3 RISK ASSESSMENT FOR THE SITE

When a site with two units A and B is considered, as described in paragraph 5.3, the risk may be represented in the following way:

FIGURE A2 REPRESENTATION OF THE CORE MELTDOWN RISK FOR A SITE WITH TWO UNITS



This representation shows that some scenarios only concern unit A (respectively B) with no impact on unit B (respectively A) and that conversely, some scenarios have an impact on both units at the same time.

The calculation for the core meltdown risk for the site is therefore expressed by:

$$P(\text{meltdown}_{\text{site}}) = P(\text{meltdown}_A \cup \text{meltdown}_B) \\ = P(\text{meltdown}_A) + P(\text{meltdown}_B) - P(\text{meltdown}_A \cap \text{meltdown}_B)$$

To model this risk, it should therefore be possible to correctly identify and treat:

1. The initiating events that may only affect one unit at a time. These events will be called type I initiating events throughout the rest of the document.
2. The initiating events that have the potential to affect one or both units at the same time. These events will be called type II initiating events throughout the rest of the document.

Furthermore, the accident scenarios produced by these initiating events may require the use of the 3 types of common systems, as defined in paragraph 5.3. Therefore, the dependencies produced through use of these systems should be modeled correctly. Given the above-defined 2 types of initiating events and 3 types of common systems, 6 standard scenarios can be defined.

Finally, the management of shared resources in terms of operating and maintenance teams needs to be taken into account specifically in a multi-unit PSA.

In the work performed by EDF R&D, the distribution of events by type of initiating event (I or II) is discussed based on their origin (internal events, internal hazards, external hazards), the types of common systems are presented in more detail, a modeling of the 6 standard scenarios is proposed (taking into account specific CCF modeling, suc-

cess criteria depending on the operating modes of the units and on the performance of systems) and finally, a specific methodology is proposed for the assessment of HEPs.

11.2.4 REFERENCE

- [1] Safety Assessment for the Adoption of a Twin Reactor Design for HPC - CN376-700-00002 issue 2
- [2] Strategy to assess the impact of twin reactor site on the PSA - HPC-NNBOSL-U0-000-RES-000073 05/09/2012
- [3] Standard ASME (ASME/ANS RA-Sa-2009)
- [4] STANDARD FOR PROBABILISTIC RISK ASSESSMENT FOR ADVANCED NON-LWR NUCLEAR POWER PLANTS - draft
- [5] Risk Assessment of Operational Events - Handbook - Volume 1 - Internal Events Revision 1.03 - August 2009- US-NRC
- [6] Regulatory review of probabilistic safety assessment (PSA) Level 1 - IAEA-TECDOC-1135
- [7] Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making - NU-REG/CR-6813
- [8] Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants - IAEA-TECDOC-1511 - juillet 2006
- [9] Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants - IAEA SSG 3
- [10] Risk Monitors : The State of the Art in their Development and Use at Nuclear Power Plants - NEA/CSNI/R(2004)20
- [11] A new method to evaluate alternate AC power source effects in multi-unit nuclear power plants - RESS référence 82 (2003) 165-172
- [12] On The Issue of Integrated Risk - A PRA Practitioners Perspective - Proceedings du PSA05 San Francisco
- [13] Options for Proceeding with Future Level 3 Probabilistic Risk Assessment Activities - SECY-11-0089 - July 7, 2011