

"NUCLEAR FISSION"

Safety of Existing Nuclear Installations

Contract 605001

Lessons of the Fukushima Dai-ichi accident for PSA

Reference ASAMPSA_E



Technical report ASAMPSA_E /WP30/D30.2/2017-32

Reference IRSN PSN-RES/SAG/2017-00021

M. Kumar (LR), J. Klug (LR), R. Alzbutas (LEI), L. Burgazzi (ENEA),
M. Farcasiu (RATEN ICN), I. Ivanov (TUS), D. Bogdanov (TUS),
K. Hashimoto (JANSI), K. Hirata (JANSI), S. La Rovere (NIER), M. Nitoi
(RATEN ICN), O. Sevbo (SSTC), J. Vitazkova (CCA), S. Hustak (UJV),
A. Wielenberg (GRS), E. Raimond (IRSN)

Period covered: from 01/07/2013 to 19/12/2016		Actual submission date: 31/12/2016
Start date of ASAMPSA_E: 01/07/2013		Duration: 42 months
WP No: 30	Lead topical coordinator : Manorma Kumar	Her organization name : Lloyd's Register, Sweden

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

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

ASAMPSA_E Quality Assurance page

Partners responsible of the document : LR, GRS, IRSN	
Nature of document	Technical report
Reference(s)	Technical report ASAMPSA_E/ /WP30/D30.2/2017-32 Report IRSN-PSN-RES/ SAG/2017-00021
Title	Lessons of the Fukushima Dai-ichi accident for PSA
Author(s)	M. Kumar (LR), J. Klug (LR), R. Alzbutas (LEI), L. Burgazzi (ENEA), M. Farcasiu (RATEN ICN), I. Ivanov (TUS), D. Bogdanov (TUS), K. Hashimoto (JANSI), K. Hirata (JANSI), S. La Rovere (NIER), M. Nitoi (RATEN ICN), O. Sevbo (SSTC), J. Vitazkova (CCA), S. Hustak(UJV), A. Wielenberg (GRS), E. Raimond (IRSN)
Delivery date	31 December 2016
Topical area	PSA Level 1, PSA Level 2, Hazards PSA, RIDM, Fukushima Dai-ichi
For Journal & Conf. papers	No
<p>Summary: The objective of this document is to identify some lessons learned from the Fukushima Dai-ichi accident for PSA. Based on the public information on the causes that have led to major radioactive release during the Fukushima Dai-ichi accident (initiating events, material and human response), the authors, ASAMPSA_E WP30 members have performed a review to examine the gaps/insufficiencies/incompleteness in the existing Level 1 and Level 2 PSAs. This is the aim of this report which is one of WP30 deliverables i.e. D30.2. The consideration of external initiating events for the different levels of defense-in-depth is one of the focal points in this review. Recommendations in the way of developing the different elements of PSAs have been proposed by the authors and were completed later during the ASAMPSA_E project. Moreover, first recommendations on the use of PSA information in decision making have been included as well.</p>	

Visa grid			
	Main author(s) :	Verification	Approval (Coordinator)
Name (s)	M. Kumar et.al.	H. Löffler	E. Raimond
Date	2016-12-19	2016-12-19	2017-01-25

MODIFICATIONS OF THE DOCUMENT

Version	Date	Authors	Pages or paragraphs modified	Description or comments
1	2014-12-19	M. Kumar (LR), J. Klug (LR), R. Alzbutas (LEI), L. Burgazzi (ENEA), M. Farcasiu (RATEN ICN), I. Ivanov (TUS), H. Kazuta (JANSI), S. La Rovere (NIER), M. Nitoi (RATEN ICN), O. Sevbo (SSTC), J. Vitazkova (CCA), S. Hustak (UJV), A. Wielenberg (GRS)	All	First version
2	2014-12-29	-	All	Review by E. Raimond (IRSN) before delivery by the project
3	2015-01-14	LRC, GRS	All	Incorporated comments and updated report to next version
4	2015-01-22	LRC, GRS	none	Final version with document reference numbers
5	2016-11-16	M. Kumar (LR)	All	Final end user workshop comments, EDF, JANSI, JSI, LEI, NIER, Forsmark comments incorporated
6	2016-12-19	M. Kumar (LR)	All	Technical report editing and incorporated comments received from GRS, JSI, AMEC and TUS.
7	2017-01-25	E. Raimond (IRSN)	Few	Approval reading

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	LR	WP22 coordinator until 2015-10-31
Kumar	Manorma	LR	WP22 coordinator from 2015-11-01
Wielenberg	Andreas	GRS	WP30 coordinator until 2016-03-31
Löffler	Horst	GRS	WP40 coordinator WP30 coordinator from 2016-04-01

REPRESENTATIVES OF ASAMPSA_E PARTNERS

Last 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
Sauvage	Estelle	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

Last name	First name	Organization
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

Last name	First name	Organization
Hultqvist	Göran	FKA
Karlsson	Anders	FKA
Ljungbjörk	Julia	FKA
Pihl	Joel	FKA
Loeffler	Horst	GRS
Hage	Michael	GRS
Sperbeck	Silvio	GRS
Wielenberg	Andreas	GRS
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC
Serrano	Cesar	IEC
Apostol	Minodora	RATEN ICN
Farcasiu	Mita	RATEN ICN
Nitoi	Mirela	RATEN ICN
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
Rebour	Vincent	IRSN
Scotti	Oona	IRSN
Prošek	Andrej	JSI

Last name	First name	Organization
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Matuzas	Vaidas	LEI
Rimkevicius	Sigitas	LEI
Häggström	Anna	LR
Klug	Joakim	LR
Kumar	Manorma	LR
Olsson	Anders	LR
Borysiewicz	Mieczyslaw	NCBJ
Kowal	Karol	NCBJ
Potemski	Slawomir	NCBJ
La Rovere	Stephano	NIER
Vestrucci	Paolo	NIER
Brinkman	Hans	NRG
Kahia	Sinda	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Morandi	Sonia	RSE
Dybach	Oleksiy	SSTC
Gorpinchenko	Oleg	SSTC
Claus	Etienne	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Grondal	Corentin	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Oury	Laurence	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	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

Last name	First name	Organization
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 Fukushima Dai-ichi nuclear accident in Japan resulted from the combination of two correlated extreme external events (earthquake and tsunami). 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 for beyond design accidents. If the performance of a Level 1 and Level 2 PSA concludes that such a low probability event can lead to extreme consequences, the industry (system suppliers and utilities) or the Safety Authorities may take appropriate measures to reinforce the defence-in-depth of the plant.

In this report, the implications from the Fukushima Dai-ichi accident for PSA Level 1 and Level 2 and to decision making using PSA results have been investigated by the ASAMPSA_E project. Since the scope of PSA in Japan in general as well as for the Fukushima Dai-ichi units did not extend to the relevant scenarios, direct lessons to be learned on these issues are limited. Therefore, the authors have used their experience on the current status of PSA Level 1 and Level 2 models worldwide and in Europe as well as the insights gained from the ASAMPSA_E questionnaire [119] for identifying further gaps of PSA methodologies and for derived related conclusions and recommendations.

Some main lessons learned on PSA Level 1 and Level 2 as well as decision making using PSA results is briefly summarized in this report. The complete summary of this report is provided in section 6, which includes a numbered list of the conclusions and recommendations.

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

Risk-informed decision making should consider the risk profile of the plants based on sets of PSA risk measures/metrics for Level 1 and Level 2, which are understood and presented as uncertainty distributions. These should be accompanied with sensitivity analyses demonstrating the influence of different important sources of uncertainty. Risk-informed decision making should consider always potential long-term consequences of accidental

releases. Moreover, the decision making should take into account uncertainty assessments on safety margins, particularly those to known or suspected cliff-edge effects.

In summary, the Fukushima Dai-ichi accident justifies the basic assumption of the ASAMPSA_E project of extending the scope of PSA to include all operating modes, all events and hazards, and all relevant potential sources like e.g. the spent fuel pool. It has to be acknowledged that extended PSA models, which cover all the scenarios and events recommended above, will require a lot of work on the development of efficient PSA methods, generation of (plant-specific) data, further research on such diverse areas as structural analysis, site screening, human reliability, geosciences, severe accident phenomena identification, and on the improvement of PSA models themselves. In this sense, the PSA community is facing a series of complex and difficult problems. The ASAMPSA_E project tackled the aforementioned issues during the project.

ASAMPSA_E PARTNERS

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

1	Institute for Radiological Protection and Nuclear Safety	IRSN	France
2	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gmbH	GRS	Germany
3	AMEC NNC Limited	AMEC NNC	United-Kingdom
5	Lloyd's Register Consulting	LR	Sweden
6	Nuclear Research Institute Rez pl	UJV	Czech
8	Cazzoli Consulting	CCA	Switzerland
9	Italian National Agency for New Technologies, Energy and the Sustainable Economic Development	ENEA	Italy
13	Lietuvos energetikos institutas (Lithuanian Energy Institute)	LEI	Lithuania
15	Forsmark kraftgrupp AB	FKA	Sweden
18	State Scientific and Technical Center for Nuclear and Radiation Safety	SSTC	Ukraine
20	NIER Ingegneria	NIER	Italy
26	Regia Autonoma Tehnologii pentru Energia Nucleara Institutul de Cercetari Nucleare	RATEN ICN	Roumania
27	Technical University of Sofia - Research and Development Sector	TUS	Bulgaria
30	Tokyo Electric Power Company	TEPCO	Japan
31	Japan Nuclear Safety Institute	JANSI	Japan

CONTENT

Modifications of the Document.....	3
List of Diffusion.....	4
Executive Summary	7
ASAMPSA_E Partners	9
Content.....	10
Glossary	12
1 Introduction	14
1.1 Context.....	14
1.2 Objectives	16
2 Fukushima Dai-ichi Accident from a PSA Point of View.....	16
2.1 Major Safety Gaps Learned from the Accident	16
2.2 Changes in Japanese Regulatory Requirements After the Accident	17
2.3 Lessons Learned.....	21
2.3.1 The Accident and its Causes	22
2.3.2 Utilization of PSA in Japanese Context	23
2.3.3 Defense in Depth (DiD).....	25
2.3.4 Initiating Events.....	26
2.3.5 Risk Criteria	26
3 PSA Level 1 Issues in Light of the Fukushima Dai-ichi Accident	27
3.1 Initiating Events and Low Probability/High Impact Events.....	28
3.1.1 Hazards Identification for PSA	29
3.1.2 Correlation of Hazards	33
3.1.3 External Hazards Screening	35
3.1.4 External Hazards Assessment	36
3.1.5 External Hazards and Initiating Events	39
3.2 Systems Reliability and Conditional Unavailability for the DiD Levels	41
3.2.1 Systems Reliability.....	41
3.2.2 Modelling and Assessment Issues	44
3.3 Emergency Operating Procedures and Event Specific Boundary Conditions	46
3.4 Human Reliability Assessment and Event Specific Boundary Conditions	47
3.5 Lessons Learned for PSA Level 1	50
3.5.1 Initiating Events.....	50
3.5.2 Systems Reliability.....	51
3.5.3 Emergency Operatinng Procedures and SAMG	51
3.5.4 Human Reliability Assessment	52
4 Review of Existing PSA Level 2 on Gaps and Insufficiencies	53

4.1 Initiating Events and Combination of Rare Events	53
4.2 Measures and Systems Reliability and Conditional Unavailability for the DiD Levels.....	56
4.2.1 Measures and Systems Reliability.....	57
4.2.2 Modelling and Assessment Issues	60
4.3 Severe Accident Management Procedures/Guidelines and Event Specific Boundary Conditions	63
4.4 Human Reliability Assessment and Event Specific Boundary Conditions	65
4.5 Lessons Learned for Level 2 PSA.....	67
4.5.1 Initiating Events and Combination of Rare Events	67
4.5.2 Systems Reliability and conditional UNAVAILABILITY for the DiD Levels.....	68
4.5.3 Severe Accident Management Procedures/Guidelines and Event Specific Boundary Conditions	69
4.5.4 Human Reliability Assessment and Event Specific Boundary Conditions	69
5 Use of PSA Results in Decision Making	70
6 Summary	77
6.1 Main Conclusions.....	77
6.2 List of Conclusions and Recommendations	81
7 References	90
8 Appendix 1 - Lessons Learned (Examples).....	96
8.1 Bulgaria-I.....	96
8.2 Bulgaria-II	99
8.3 Germany	101
8.4 Italy.....	103
8.5 Sweden	105
8.6 Lithuania	111

GLOSSARY

AB	Accumulator Battery
AC	Alternating Current
AESJ	Atomic Energy Society of Japan
AM	Accident Management
APET	Accident Progression Event Tree
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ASUNE	Act on the Safe Use of Nuclear Energy
ATHEANA	A Technique for Human Error ANALysis
BNRA	Bulgarian Nuclear Regulatory Agency
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CFF	Containment Failure Frequency
CDF	Core Damage Frequency
DBA	Design Basis Accident
DC	Direct Current
DiD	Defence in Depth
EDG	Emergency Diesel Generator
ENSREG	The European Nuclear Safety Regulators Group
EOC	Errors of Commission
EOP	Emergency Operating Procedures
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HPCI	High Pressure Coolant Injection
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
ICS	Isolation Condenser System
IRRS	Integrated Regulatory Review Service
I&C	Instrumentation and Control
LOOP	Loss Of Off-site Power
NAIIC	National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission
NARA	Nuclear Action Reliability Assessment
NIED	National Research Institute for Earth Science and Disaster Prevention
NISA	Nuclear and Industrial Safety Agency

NPP	Nuclear Power Plant
NRA	Nuclear Regulation Authority
NSC	Nuclear Safety Commission
LERF	Large Early Release Frequency
LRF	Large Release Frequency
PCV	Primary Containment Vessel
PDS	Plant Damage State
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PSHA	Probabilistic Seismic Hazard Analysis
PSR	Periodic Safety Review
RCIC	Reactor Core Isolation Cooling
RIDM	Risk Informed Decision Making
SCRAM	System for Control Rod Actuation Mechanisms
SAMG	Severe Accident Mitigation Guidelines
SBO	Station Blackout
SFP	Spent Fuel Pool
SLIM	Success Likelihood Index Method
SPAR-H	Standardized Plant Analysis Risk - Human reliability analysis
SSC	System Structure Component
SSM	Swedish Radiation Safety Authority
THERP	Technique for Human Error Rate Prediction
WENRA	Western European Nuclear Regulator Association
WP	Work Package

1 INTRODUCTION

"Lack of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes, until self-preservation strikes its jarring gong—these are the features which constitute the endless repetition of history." Winston Churchill, 1935

1.1 CONTEXT

The Fukushima Dai-ichi nuclear accident in Japan resulted from the combination of two correlated extreme external events (earthquake and tsunami). 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 for beyond design accidents. If the performance of a Level 1 and Level 2 PSA concludes that such a low probability event can lead to extreme consequences, the industry (system suppliers and utilities) or the Safety Authorities may take appropriate decisions to reinforce the defence-in-depth of the plant, if possible.

The project ASAMPSA_E aims at describing good practices for the identification of such situations with the help of Level 1 and Level 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” able to quantify risks induced by NPPs site taking into account the following challenging aspects: multi-units site, risk associated to spent fuel pools and coupling with reactors, and the modelling of the impact of internal initiating events, and internal and external hazards on equipment and human recovery actions. The ASAMPSA_E project has paid a particular attention to the risks induced by the possible natural extreme external events and their combinations. In the post-Fukushima Dai-ichi context, the respective results in WP30 on Lessons of Fukushima Dai-ichi for PSA have been taken into consideration.

The accident at Fukushima Dai-ichi has shown that extreme external events, with a magnitude exceeding the NPP design, can strike an NPP and make impossible to control the plant. In the history of nuclear industry, some high amplitude external events above the plant design conditions have already occurred in some countries but without off-site consequences. These events have been investigated to reinforce the NPPs and the safety rules. (See for example [1] for accidents before the Fukushima Dai-ichi event).

Additional post-Fukushima Dai-ichi accident activities are as below:

- a) What should be harmonized for PSA after the Fukushima Dai-ichi accident?

It is recognized today that the Fukushima Dai-ichi site protections against a realistically estimated tsunami were not sufficient.

This fact can be considered as an insufficiency in the definition of the deterministic design basis conditions of Fukushima Dai-ichi NPPs and an implicit underestimation of the residual risk; the PSA approach (if correctly implemented in complement of the deterministic design, i.e. with an enlarged scope concerning the covered hazards), could have led to identify this weakness and to evaluate the residual risk which was excessively high and led to a decision of site reinforcement (e.g. different positioning of the emergency Diesel generators (DGs)).

For all industrial or natural disasters, it seems very easy to conclude that reinforcements were needed **after** the accident. But **before** the accident, the fact that such disaster can happen is always “virtual” (or based on simulations) and can be:

- associated to a low frequency of occurrence,
- associated to high level of uncertainties that does not allow for supporting a decision,
- fully unidentified.

Decision-making process based on risk induced by rare events is difficult and associated to societal acceptance of risks. It is also recognized that many disasters associated to facilities were predicted but:

- either have not been considered as frequent enough to justify reinforcement,
- or the decision-making “process” (rarely a single stakeholder) has delayed the decision to implement the needed reinforcements.

The PSA methodology is, in theory, able to combine all components of risks (frequencies, consequences) but needs to be credible. Its relevance depends on the quality of PSA’s content which covers an extremely large scope:

- definition, characterization and frequency of initiating events (internal events, external and internal hazards) and their combinations, including identification of “risk” sources and plant operating modes to consider,
- modelling of the accident sequences and of the NPP response (human and equipment) with, for instance a fault trees /event tree approach,
- assessment of accident consequences for each accident sequences,
- presentation and summary of the results and their interpretation as input for the decision-making process.

Each step needs to be appropriately performed to obtain a final relevant risk assessment. For European countries, it seems that harmonization of practices or technical exchanges will be particularly fruitful for all the steps mentioned above but with a high focus on external hazards or in general high impacts events. For example:

- What should be the “human reliability assessment” (HRA) model in the case of a major earthquake or flooding?
- How to consider the containment efficiency after an earthquake in the assessment of accident consequences?

b) Link with the stress test effort conducted in countries and at European level

The Fukushima Dai-ichi accident has lead EC and National Safety Authorities to request a public review, “stress tests” [2] of all European NPPs, with the objective to assess the robustness of NPPs and to identify potential possibilities of reinforcements where needed.

This review, organized by ENSREG, based on deterministic approach, examined European NPPs resilience against events like earthquake or flooding, and the response in case of partial or total loss of the ultimate heat sink and/or loss of electrical power supply.

The review concluded that the level of robustness of the concerned plants is sufficient but for many plants, safety reinforcements have been defined or accelerated to face the possibility of beyond design events. The reinforcements include:

- protective measures (against flooding, earthquake),
- additional equipment (mobile equipment, hardened stationary equipment) able to control the NPP in case of beyond design events,
- protective structures (reinforced local crisis centers, secondary control room, protective building for mobile equipment),
- severe accident management provisions, in particular for hydrogen management and containment venting,
- new organizational arrangements (procedures for multi-units accidents, external interventions teams able to secure a damaged site).

Action plans to implement these measures are now discussed in all European countries.

1.2 OBJECTIVES

The objective of the present document is to identify lessons learned and prepare a report on the lesson learned from the Fukushima Dai-ichi accident that have an impact on PSA methodology and results. Based on the available public information (initiating events, material and human response), the authors have performed a review on existing L1 and L2 PSAs in order to examine the gaps/insufficiencies/incompleteness in this regard. The consideration of external initiating events and their impact on the different Levels of the defence-in-depth is one of the focal points in this endeavour. As a synthesis, recommendations for developing the different components of PSAs are proposed. Moreover, first recommendations on the use of PSA information in decision making are given as well.

2 FUKUSHIMA DAI-ICHI ACCIDENT FROM A PSA POINT OF VIEW

2.1 MAJOR SAFETY GAPS LEARNED FROM THE ACCIDENT

Prior to the Fukushima Dai-ichi accident major safety regulation problems have been found, including weakness in safety assessment and use of PSA. Major safety regulation problems prior the accident were [3]:

- Regulatory requirements did not cover 'severe accidents'. Countermeasures against severe accidents including external events were left purely to the discretion of operators. (National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission (NAIIC)).
- No legal framework was in place to retroactively apply new requirements to existing nuclear power plants, which hindered continuous safety improvements (NAIIC).

- Japanese regulators made little effort to either introduce the latest foreign technology or improve safety procedures dealing with uncertain risks (NAIIC).
- ***Comprehensive risk assessment covering not only earthquakes and tsunamis but also fires, volcanic eruptions, and landslides that may trigger accidents had not been conducted.*** (Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company).
- An integrated legal system is preferable to avoid confusion caused by multiple laws and the involvement of multiple government agencies (NAIIC).

Specifically regarding the situation for PSA and the related regulatory framework, the following observations can be made:

Before the Fukushima-Dai-ichi accident, Japanese electric utilities had conducted internal event PSA on a voluntary basis. The PSA models were produced and updated within the framework of the PSR (Periodic Safety Review), which was conducted every ten years as requested by the regulator. PSA analyses were performed up to “Level 1.5”, i.e. the extension of a PSA Level 1 from core damage until potential containment failure, whereas source term analysis is not performed. The PSA Level 1 model covered internal events during power operation and the shutdown state. The PSA considered human errors including the related HRA.

After 1995 Kobe earthquake, the document “Regulatory standards for reviewing seismic design of nuclear power reactor facilities” was revised by Nuclear Safety Commission of Japan in September 2006. The revised Japanese standard refers to seismic PSA. However, seismic PSA was not officially adopted in this standard as the method was considered to be “not matured” enough. Instead, the standard emphasises the “residual risk” caused by the impact of an earthquake, which might exceed the design basis level, and recommends related probabilistic seismic hazard analysis (PSHA). In answer to that regulatory recommendation, Japanese utilities conducted updated seismic hazard analyses at their plant sites and compared the results with the design basis earthquake ground motion and in addition determined the annual frequency of exceedance for beyond design basis ground motion due to earthquake. More detailed seismic PSA had been under development by some utilities, but these were mostly considered to be in an experimental and trial stage prior to the accident. Other external hazard PSA was out of scope in Japan.

The following standards for PSA were issued by Atomic Energy Society of Japan before 2011:

- Standard for PSA during power operation (Level 1 PSA),
- Standard for PSA during power operation (Level 2 PSA),
- Standard for PSA during power operation (Level 3 PSA),
- Seismic PSA implementation standard.

2.2 CHANGES IN JAPANESE REGULATORY REQUIREMENTS AFTER THE ACCIDENT

One of the centrepiece actions taken in Japan post-Fukushima to improve its nuclear safety management and regulation is the creation of a new nuclear regulatory body, the Nuclear Regulation Authority (NRA) [6]. Following its inauguration on September 19, 2012, the NRA carried out a complete review of safety guidelines and regulatory

requirements with the aim of formulating a set of new regulations to protect people and the environment. On July 8, 2013, the new regulatory requirements for commercial power reactors got into force [3], [6].

After Fukushima Dai-ichi accident, the following new regulatory requirements for commercial nuclear power reactors have been enforced [3]:

- Based on a concept of “Defence-in-Depth”, essential importance is placed on the third and fourth layers of defence and the prevention of simultaneous loss of all safety functions due to common causes.
- Previous assumptions on the impact of earthquakes, tsunamis and other external events such as volcanic eruptions, tornadoes and forest fires are re-evaluated, and countermeasures for nuclear safety against these external events are decided to be enhanced.
- Countermeasures have been taken against the internal fires and internal flooding, and to enhance the reliability of on-site and off-site power sources to deal with the possibility of station blackout (SBOs).
- In addition to the above described enhancement of countermeasures established for design basis, countermeasures for severe accident, containment vessel damage and release of radioactive materials, enhancement measures for water injection into spent fuel pools, countermeasures against malicious airplane crash, and installation of emergency response building have been also required.
- “Safety Culture” should be fostered among operators, other industry sectors and the NRA.
- New safety regulation emphasizing on major accidents requires nuclear operators to conduct periodic and comprehensive safety reviews and share the results with the regulator and public to ensure continuous safety improvement.
- Introduce a “back-fitting” system authorizing enforcement of the latest regulatory requirements on already licensed facilities.
- Integrate power plant safety regulations contained in the Electricity Business Act (periodic inspections) into the Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors (the Reactor Regulation Act).

Figures 1 to 3 show the comparison between prior and post Fukushima Dai-ichi accident Japanese regulatory requirements including new regulatory policies and requirements [3].

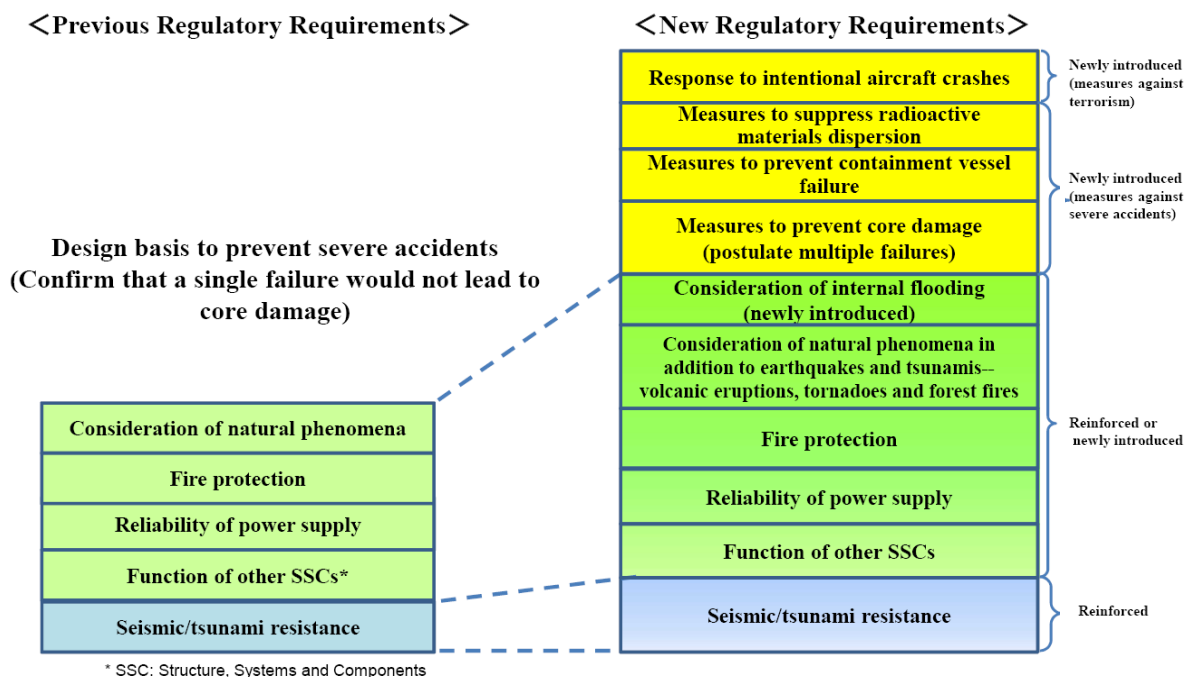


Fig. 1 Comparison between Previous and New Japanese Regulatory Requirements [3]

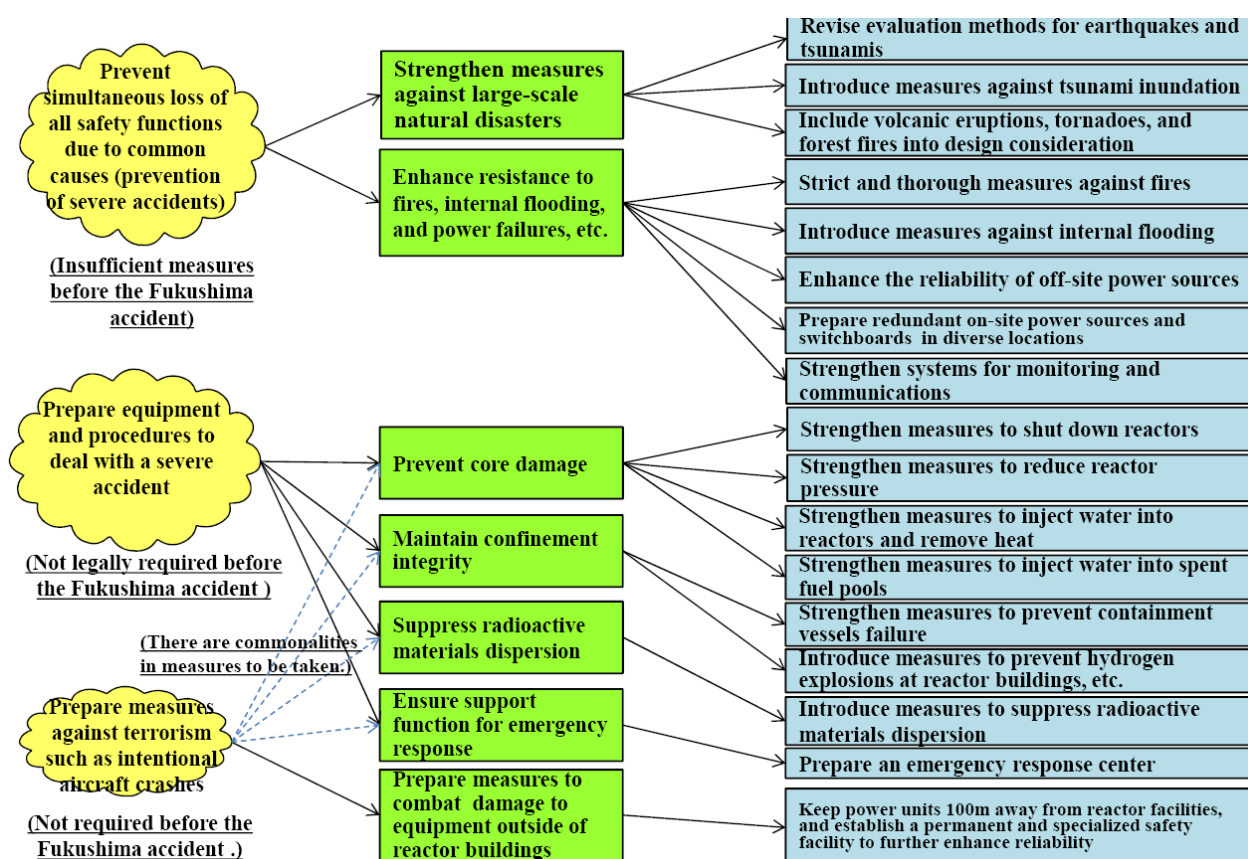


Fig. 2 New Japanese Regulatory Policies and Major requirements [3]

	Pre-existing Regulatory Requirements	New Regulatory Requirements
Off-site power	Two circuits (independence was not required)	Two circuits (independence is required)
On-site AC power source	Two permanently installed units (emergency diesel generators)	In addition to those set forth in the left column, another permanently installed unit and two more mobile units , and storage of fuel for seven days
On-site DC power source	One permanently installed system with a capacity for 30 minutes	Increase of the capacity of the system set forth in the left column to 24 hours duration and addition of one mobile system and one permanently installed system, both with 24 hours duration

*Additionally, require that switchboards and other equipment will not lose their operational capabilities because of common causes

Fig. 3 Comparison between the pre-existing and New Regulatory Requirements for power sources [3]

Specifically related to PSA for Japanese NPP, the situation is as follows.

The Japanese Nuclear Regulation Authority (NRA) has promulgated the regulation titled “New regulatory requirements for commercial nuclear reactors” in June 2013. Thereby, licensees are required to evaluate the effectiveness of severe accident measures for accident sequence groups as designated by the regulator NRA. In addition, licensees are required to perform PSA Level 1 for internal and external events for their individual plant in order to investigate if there are any other important accident sequence groups.

Licensees are also required to evaluate effectiveness of preventive measures against containment failure in case of a severe accident for those containment vessel failure modes designated by NRA. In addition, licensees are required to perform PSAs “Level 1.5” for internal and external events for their individual plant in order to investigate if there are any other important failure modes.

In compliance to this new regulatory requirement after Fukushima Dai-ichi accident, utilities are carrying out or extending plant-specific PSA in preparation for the restart of NPPs.

The scope of these PSA model covers:

- Internal events PRA (Level 1)
 - Operating state
 - Shutdown
- Seismic PRA (Level 1)
- Tsunami PRA (Level 1)
- Internal events PRA “Level 1.5”
 - Operating state

In addition, NRA has issued the guide “Implementation guide regarding safety enhancement for commercial NPPs” in November 2013. With regard to PSA, the guide strongly recommends performing/updating PSA models every five years. As first stage and in response to the shutdown of Japanese NPPs after the Fukushima Dai-ichi accident, the guide requires that PSA results shall be updated within 6 months after the first periodic inspection after restart of the NPP. Part of that first stage PSA shall be an internal events PSA Level 1 and Level 2 (or rather “Level 1.5”) for power operation and shutdown modes as well as seismic hazard and tsunami hazard PSA Level 1 and Level 2. Thereafter in the second stage, PSA models shall be extended to include internal hazards (flooding and fire), external hazards PSA other than seismic and tsunami, combined external hazards (e.g. seismic and tsunami). In addition, multi-unit issues and the risk from the spent fuel pool shall be assessed as well.

The following standards for PSA were issued by Atomic Energy Society of Japan after 2011:

- Seismic PRA¹ implementation standard (revised),
- Tsunami PRA implementation standard,
- Tsunami PRA implementation standard (considers combination of earthquake and tsunami, under revision during the preparation of this report),
- Internal flooding PRA implementation standard,
- Standard for PRA during power operation (Level 1 PRA, revised),
- Shutdown state PRA standard (Level 1),
- Internal fire PRA implementation standard.

Moreover, AESJ is preparing or planning additional PSA standards, e.g. on earthquake/tsunami induced internal flood, fire, Level 3 seismic/tsunami PRA, etc.

2.3 LESSONS LEARNED

Based on the lessons learned from Fukushima Dai-ichi accident, laws in Japan were amended in June 2012, adding the environment in addition to the general public as major safety targets, expanding coverage to include severe accidents and introducing a provision that new requirements can be applied to the existing nuclear facilities also. Amendments shall be enforced within 10 months after the date on which the Nuclear Regulation Authority was established (by July 18th, 2013).

Atomic Energy Society of Japan (AESJ) summarized the technical lessons learned generally from the Fukushima Dai-ichi accident in English at their webpage [7]; these lessons are summarised below:

- 1) Emphasis on Defence-in-Depth
Prepare multi-layered protective measures and achieve specific objectives in each layer independent of other layers
- 2) Significantly enhance design basis and strengthen protective measures against natural phenomena which may lead to common cause failure.
Strict evaluation of earthquakes, tsunamis, volcanic eruptions, tornadoes and forest fires: countermeasures against tsunami inundation and due consideration to ensure diversity and independence

¹ AESJ has changed the designation of PSA to PRA after 2011.

- 3) Enhance countermeasures against events other than natural phenomena that may trigger common cause failures.

Strict and thorough measures for fire protection, countermeasures against internal flooding, reinforcement of power supply systems to prevent power failure

- 4) Performance-based requirements in regulatory requirements

Operators select concrete measures to comply with requirements and the characteristics of their facilities.

Japan Nuclear Safety Institute (JANSI) has drawn the lessons learned from the Fukushima Dai-ichi accident and from the major accident investigation reports, and has compiled a report on the principal activities for the purpose of supporting activities of utilities reflecting the lessons learned in their operations for improving safety [117].

Note: Name ‘Fukushima Dai-ichi’ is a site name and Fukushima is a prefecture name. Fukushima prefecture government generally claimed that do not use the wording like ‘Fukushima’ accident. It is preferred to use the site name of ‘Fukushima Dai-ichi’ instead of ‘Fukushima’.

Before discussing the lessons learned from Fukushima Dai-ichi accident in detail, below sections will briefly summarise the accident and its causes, reasons for happening, probability to occur and the consequences.

2.3.1 THE ACCIDENT AND ITS CAUSES

On 11th March 2011, Units 1, 2, and 3 at Fukushima Dai-ichi were in operation; Units 4, 5, and 6 were shut down for routine refuelling and maintenance activities; Unit 4 reactor fuel was offloaded to the spent fuel pool. As a result of the earthquake, all of the operating units appeared to experience a normal reactor trip; the three operating units automatically shut down, apparently inserting all control rods into the reactor. As a result of the earthquake, off-site power was lost to the entire facility; the emergency diesel generators started at all six units providing alternating current (AC) electrical power to critical systems at each unit. Approximately 45 minutes following the earthquake, the first tsunami wave inundated the site followed by multiple additional waves. It resulted in extensive damage to site facilities and a complete loss of AC electrical power at Units 1, 2, 3, 4 and 5; Unit 6 retained the function of one (air-cooled) diesel generator (then used to provide AC power for Units 5 and 6, maintaining their reactors and spent fuel pools in cooled conditions). Cooling was lost in the reactors of the Units 1, 2 and 3 and in the spent fuel pool of the Unit 4, resulting in damage to the nuclear fuel of Units 1, 2, and 3. Units 1, 3 and 4 also experienced hydrogen explosions, further damaging the facilities and the secondary containment structures.

As shown in Figure 4, the main causes of the accident were:

- Loss of safety functions

Off-site power was lost due to earthquake, but shutdown was successful and emergency diesel generator operated without any trouble, until tsunami came.

- The initial impact spread and the crisis eventually developed into a ‘severe accident.’

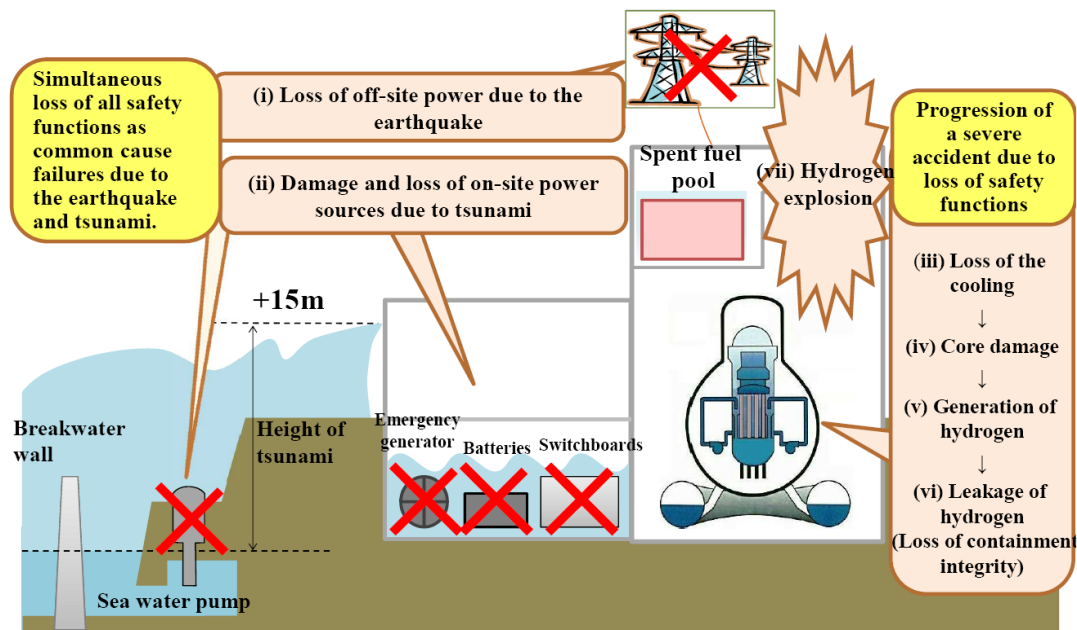


Fig. 4 Fukushima Dai-ichi accident [3]

The tsunami generated by the Great East Japan Earthquake caused the sequence of events and cascading accidents resulting in total station blackout at Fukushima Dai-ichi, loss of cooling, hydrogen explosions, and eventually radioactive dispersion into the air, deposition onto the land, and flow into the ocean.

The earthquake did cause the loss of offsite power initiating event as well as severely hampering recovery activities because of the damage to the local infrastructure. Current knowledge, gained by analysing the observations, monitoring records and visually checking on-site where possible, supports the conclusion that safety-related SSCs (including concrete structures) were likely not damaged by earthquake shaking [99], [116], [117].

It should be noted that in Level 2 PSA, seismic-induced diesel generator failure, leading to total station blackout, leading to failure of cooling systems is the most likely cause of nuclear accidents from an external event. While not directly contributing to “what went wrong”, it certainly contributed to an attitude of complacency and subsequent belief that the events which did occur were “unforeseeable” [10].

The long-term consequences of the accident at Fukushima Dai-ichi are continuing to unfold. Radiation readings have risen to 100 to 1,000 times the normal Level on the Pacific seabed as measured near Dai-ichi as late as May 10th [10], [99]. The persistence of radioactive deposition on the land and in the ocean; the ability of the evacuees to return to their homes; the economic viability of TEPCO; the shortfalls in electricity generation; these are some of the important consequences that should be remembered.

2.3.2 UTILIZATION OF PSA IN JAPANESE CONTEXT

Based on lessons learned from Fukushima Dai-ichi accident, NRA aims at adequate control of nuclear risks, by using PSA and safety goals [4]. NRA recognizes that the approaches in the former regulatory organizations, Nuclear Safety Commission (NSC) and Nuclear and Industrial Safety Agency (NISA), regarding the utilization of PSA remain

valid even after the TEPCO's Fukushima Dai-ichi accident. NRA also summarised the use of PSA in Japanese context [4]:

- Use of PSA and safety goals is essential,
- Limitation of PSA, incompleteness and uncertainty must be strictly recognized, and
- PSA should be used to revise the existing deterministic rules as much as possible.

Utilization of PSA and safety goals, however, had been stagnant in Japan in the past decade. NRA recently expressed its policy on the active use of PSA and safety goals.

NRA is contemplating PSA utilization; in revision or rationalization of regulation rules e.g. "Seismic Design Guideline", and in decision making for various regulatory issues e.g. adequacy of provisional countermeasures on a sump blockage problem. The approaches were described in NSC's "Interim report on the investigation and review on safety goals" and NISA documents provided for IRRS Mission to Japan.

NRA is developing design requirements for: measures against significant initiators, e.g., earthquake, tsunami, and airplane crash, and measures against severe accidents. In some areas, safety assessment methodologies are not mature enough to examine the adequacy of design and to define the adequate protection. As a matter of fact, it is presumed that all the PSA methodologies are still being imperfect [4]. NRA will, however, use PSA actively in the regulation taking into account the PSA limits.

According to Atomic Energy Society of Japan (AESJ/NSD) [4], in the Japanese context estimation of the frequency of rare external initiators is extremely difficult. A relationship between probabilistic consideration and regulation is shown in figure 5.

Historical records of some earthquakes, tsunamis, volcanism etc., are very limited [4]. Extrapolation is inevitable but it gives large uncertainties. Estimation of accident consequence is also very difficult. For example, past PSAs in Japan did not take account the following [4]:

- Hydrogen explosion in reactor building,
- Hydrogen transport from one unit to another, and
- Adverse effect of external initiators and severe accident phenomena on accident management operation.

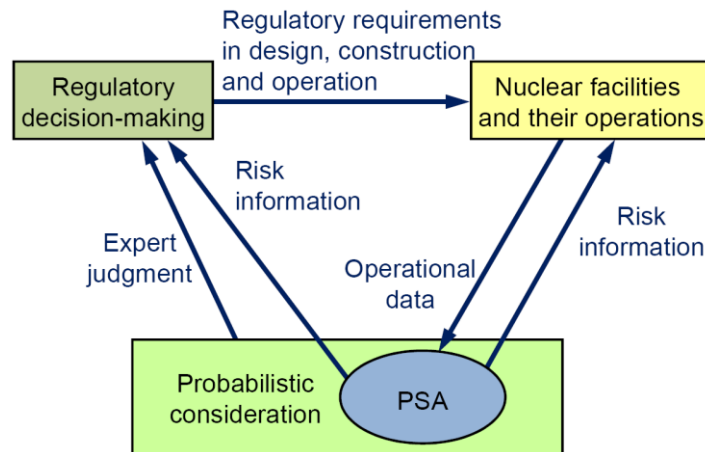


Fig. 5 Relationship between Probabilistic consideration and regulation [4]

Figure 6 shows the use of PSA in regulatory decision-making under uncertain conditions. Furthermore, it is required that PSAs must be carried out for various initiators.

In Japan, after Fukushima Dai-ichi accident, PSA is to be peer-reviewed by the third group and is to be opened for the public.

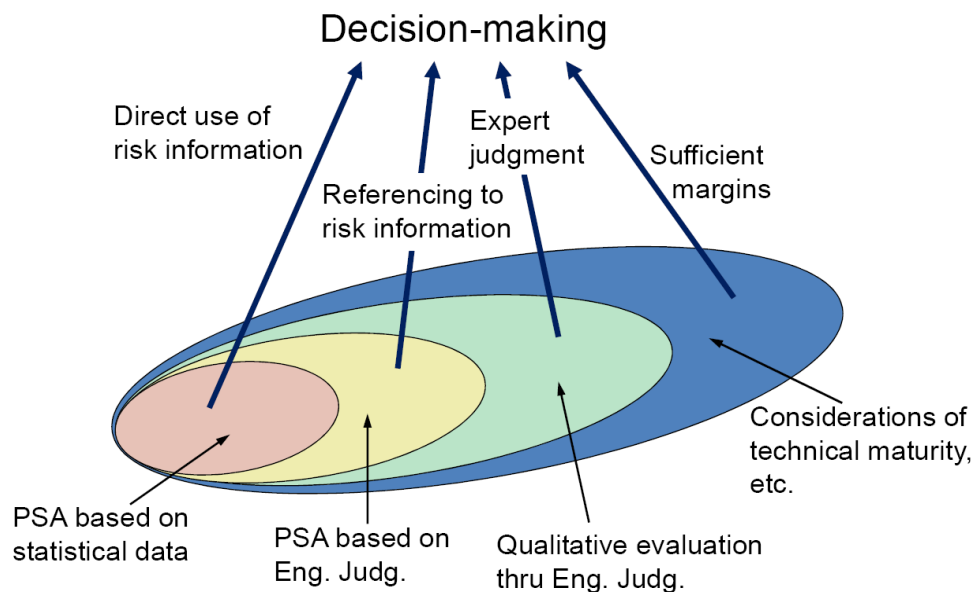


Fig. 6 Regulatory Decision-making under Uncertain Conditions [4]

2.3.3 DEFENSE IN DEPTH (DID)

Atomic Energy Society of Japan (AESJ) has performed a review of IAEA Safety Fundamentals (SF-1) taking into account the Fukushima Dai-ichi lessons learned. Also, AESJ is still pursuing discussions on DiD focusing on the basic concepts to be recognized, and DiD objectives that are recognized in IAEA Safety Report Series No. 46 considering the experience of Fukushima Dai-ichi accident. These discussions are not finished at this time. Reference [4]

briefly introduces another investigation of Fukushima Dai-ichi accident by AESJ. The investigations are still going on regarding the IAEA recommended DiD and the Japanese regulation.

2.3.4 INITIATING EVENTS

The NRA requires that plant risk evaluation includes a PSA as a reporting matter (not a licensing matter), for both internal and external hazards including earthquake and tsunami (More NRA documents are in the NRA webpage [8] in English).

Atomic Energy Society of Japan (AESJ) issued the guidelines for the selection of the risk evaluation method to be applied and external hazard correlation like earthquake and tsunami based on IAEA and ASME recommended methods. These activities are very similar to the work scope of WP20 in ASAMPSA_E.

2.3.5 RISK CRITERIA

Before the Fukushima Dai-ichi accident, Safety Goals to be implemented in Japan were discussed in one of the former regulatory bodies of Nuclear Safety Commission (NSC). Though results of these discussions were reported in the commission, Safety Goals were not implemented in the nuclear regulation. Current regulatory body of Nuclear Regulation Authority (NRA) refers to these Safety Goals of the former NSC and introduces additional criteria on the source term. NRA new Safety Goals are the followings:

- Core Damage Frequency: approximately 10^{-4} /year,
- Containment Failure Frequency: approximately 10^{-5} /year, and
- Discharge of 100 TBq CS-137: not exceeding 10^{-6} /year.

These Goals are applicable to all hazards including external hazard but not terrorist attack which is excluded. Since PSA is not a licensing matter but a reporting matter in the NRA regulation, there may still be some further discussions on how to use the Safety Goals.

Note: Brief discussions of risk criteria in Japan are shown in the last page of [3], and also on pages 5 and 6 of [4].

3 PSA LEVEL 1 ISSUES IN LIGHT OF THE FUKUSHIMA DAI-ICHI ACCIDENT

Section 2 has provided an overview over the Fukushima Dai-ichi accident contributed by JANSI. As there are quite a number of reports available or under preparation that summarize the events leading up to the accident, the development of the accident at the different phases, and the consequences of the accident and related mitigation measures, no repetition of this endeavour is merited (cf. e.g. [99], [102], [5], [7], [8], [9], [14], [15], [19], [22], [26], [70]). The same reports also give lessons learned from the accident on a number of fields - including the use of PSA. In this section, the methods and practice of Level 1 PSA are evaluated in light of the Level 1 PSA related issues highlighted by the Fukushima Dai-ichi accident.

In the following, the major issues related to Level 1 PSA are briefly repeated:

- The CDF and CFF for the Fukushima Dai-ichi plants were determined only for internal initiating events. The results obtained by TEPCO for the CDF of up to 10^{-7} per year were very low compared to other results for other BWR's, including those with more back fitting and/or newer designs.
- The low CDF reinforced the belief of Japanese decision makers that the plants were safe and severe accidents were excluded. Notably, the Japanese nuclear community communicated to the Japanese public that the risk of a severe accident could be ignored.
- There was an event at Fukushima Dai-ichi in 1993 where seawater from a corroded pipe leaked into the turbine building and flooded the emergency power supply. Based on this event (alone) a frequency of 10^{-3} per year for a scenario with a flooding of the below ground levels of the turbine hall and an extended SBO would have been merited. This investigation, however, was not performed in Japan. Also, the precursor event of the Le Blayais plant flooding in France in 1999 did not trigger sufficient probabilistic investigations.
- The frequency of beyond design seismic events as well as beyond design tsunamis was investigated by TEPCO (and the Japanese nuclear community). Some results showed that beyond design tsunamis, and particularly tsunamis with a run-up height exceeding the site level of 10 m could happen with an annual probability of at least 10^{-6} per year. These investigations, however, were seen as preliminary by TEPCO, as there was no agreement on the methods and data to be used. In addition, these results came with large uncertainty bands. For experts, a site flooded by a tsunami is related to a high conditional probability of core damage, especially in light of previous operating experience with flooding at the site.
- The probabilistic as well as deterministic assessment of SBO scenarios assumed a high probability of recovering AC power either via offsite power or via cross-connection to the adjacent unit(s) within 30 minutes. In fact, that chance was judged to be 95%. Therefore, extended SBO scenarios were not adequately modelled in the PSA. Potential common cause and/or consequential failures like flooding induced failures were not taken into account in that estimation.
- Similarly, other accident management actions like e.g. containment venting (mitigative prior to core damage) were evaluated as rather reliable. The failure probability assessed by TEPCO for Primary Containment Vessel

(PCV) venting is about 2×10^{-3} . That figures neglects the performance shaping factors typical for scenarios from e.g. catastrophic hazards.

- Multi-unit issues have been neglected in the unit-specific PSAs at the site. Particularly, common cause failures that would affect several units, as exemplified by the tsunami of March 2011, have not been considered in the PSAs.

As a general conclusion, no fundamental issues related to Level 1 PSA methods have been identified. There are however some evident areas where the methods and the practices of PSA need to be improved. In the following subsections, the authors have performed a review of existing Level 1 methods and practices in light of the aforementioned issues. Conclusions are drawn related to initiating events and low probability/high impact events, systems reliability, emergency operating procedures and event specific boundary conditions, and human reliability assessment.

3.1 INITIATING EVENTS AND LOW PROBABILITY/HIGH IMPACT EVENTS

This section analyses the identification of initiating events, particularly of low probability high impact events, for the purposes of PSA in light of the Fukushima Dai-ichi accident. The ASAMPSA_E project has investigated the issue of identifying initiating events for an extended PSA further within the report D30.3 “Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA” [118].

First, it has to be noted that the basic approach for identifying initiating events and particularly low probability/high impact events has a lot commonalities for deterministic as well as probabilistic analyses. In this respect, most of the following issues apply to probabilistic and deterministic assessments. Still, the section focuses on the impact on the identification of initiating events for an extended PSA. To this end, the lessons learned from the Fukushima Dai-ichi accident regarding initiating event determination for PSA are summarized and mirrored against current major regulatory requirements.

The Fukushima Dai-ichi accident obviously highlighted the identification of hazard scenarios (i.e. hazards and the combination of hazards) for safety assessments. During the event, a beyond design magnitude tsunami caused a flooding of the site and in particular safety related (lower) parts of the buildings introducing common cause failure mechanisms and producing permanent or long-term damage to the safety support systems (power supplies and ultimate heat sink), which hampered the fulfilment of the fundamental safety functions and an effective management of the resulting severe accidents [76]. The flooding of the plant site constitutes a good example of a cliff-edge² effect, as this led to the extended loss of all EDG for units 1 to 4, which in conjunction with the extended loss of all external power supply led to a severe accident SBO scenario. The following challenges are

²Cliff-edge effect is where a small change in a parameter leads to a disproportionate increase in consequences. [74].

identified in view of the Fukushima Dai-ichi accident, presenting new demands on the relevant scientific and engineering communities [73]:

- Characterization, screening and treatment of full spectrum of hazards;
- treatment of correlated hazards (e.g. earthquake-induced tsunamis and fires);
- treatment of multiple shocks (and associated component fragilities) and periods of elevated hazard;
- treatment of multiple damage mechanisms (e.g. a tsunami analysis should consider, in addition to inundation, such things as dynamic loads from water and debris, clogging from debris, water level drawdown effects, and soil erosion).

These issues are discussed in more detail in the following sections.

3.1.1 HAZARDS IDENTIFICATION FOR PSA

Improving hazard identification for PSA (as well as for deterministic analyses) is one of the main lessons learned from the accident in Fukushima Dai-ichi. However, it has to be noted that earthquake as well as tsunami hazard was evaluated by the licensee TEPCO [99]. With regard to the tsunami hazard identification, there were multiple issues.

- The tsunami hazard was underestimated (significantly) during the initial siting and design of the plant in the 1960s. This underestimation is partly due to the focus on the use of recent historical seismological data and the exclusion of more uncertain pre-historical and historical data by the Japanese civil engineering community [99]. Moreover, the scientific understanding of seismic and tsunami risk was not as far developed as it is today.
- With improved scientific understanding of seismic and tsunami risk in the Japanese scientific community, re-evaluations of the initial hazard analyses were performed by or on behalf of TEPCO. These, as already mentioned, showed significantly higher maximum probable floods. The preliminary studies by TEPCO between 2008 and 2010 actually showed maximum probable tsunami floods with a run-up height that could- under certain assumptions - flood the plant [96], [99]. Still, at design basis levels, the maximum probable flood calculated with methods approved by the Japanese regulator for tsunami flooding height calculations³ was always significantly below the site level.
- The scientific understanding of the maximum probable earthquake magnitude in the Fukushima region of the Japan Trench before 2011 was proven inadequate by the actual events. This contributed to an underestimation of tsunami flooding height.
- The possibility of multiple tsunamigenic sources being triggered simultaneously with wave interference leading locally to significantly larger tsunami flooding heights was not realized by the scientific community before 2011.

³The Japan Society of Civil Engineers began to create (in 1999) a unified methodology for the risk assessment of tsunami to NPPs. A first deterministic method was proposed in a report published in 2002, named “Tsunami Assessment Method for Nuclear Power Plants in Japan”. A probabilistic method was developed from 2003 to 2005 and a whole methodology for tsunami hazard analysis was developed from 2006 to 2008 but not published before March 2011. Still, the hazard identification approach was applied by TEPCO for newly received information on potential tsunamigenic sources.

- TEPCO actually installed an in-house task force within the company's Nuclear Power Division for more in-depth investigations of tsunami hazard. However, neither task force nor division proposed adequate actions to remediate the plant vulnerability to tsunami flooding [96].
- The estimated tsunami rate of occurrence for exceeding the relevant design basis (i.e. with a run-up height larger than the site level) of approximately 10^{-6} per year was significantly smaller than 10^{-4} per year as the reference value frequency for the design basis. In light of the very low CDF and LRF frequency below 10^{-6} per year determined by TEPCO for the plant, that scenario should have been flagged as potentially risk important, triggering further probabilistic assessment.

From the issues discussed above it is quite evident that the hazard identification itself actually did in principle work even for the tsunami risk at the Fukushima Dai-ichi site. Information available at least to TEPCO well before the 2011 earthquake would have merited at least a detailed probabilistic assessment of beyond design basis tsunamis with a run-up height sufficient for flooding the site. However, these assessments were postponed as were any decisions on corrective measures. This is, however due to factors which are independent of the hazard identification itself [99].

Surface fault and fault displacement were - and often still are - generally not included in the hazard identification or the PSA models, indeed (but cf. SSG-9 [23]). This is a problem since the fragility of SSCs (e.g. diesel generators, off-site power, steam generators, backup cooling pumps, pressurizer vessel, pipelines) is usually defined depending on the ground acceleration. Ground fault displacement can impact on the operability of SSC as well. Moreover, ground motion due to fault displacement can damage tsunami barriers and ground subsidence can make them ineffective against run-up heights lower than the design value. The effects of aftershocks in the time period after a major earthquake needed for putting the plant into a safe state are rarely considered in PSA and generally not addressed by seismic PSA standards (however, see the recent AESJ standard [77]).

With respect to current regulation on Level 1 PSA initiating event as well as deterministic hazard determination, it has to be acknowledged that recent regulatory requirements already call for an extensive investigation of internal and external hazards scenarios.

- WENRA Reference Levels for existing power plants from 2008 required a (deterministic) investigation of an external and internal hazards, "and their consequential events" [67], p. 11, for the design of the plant, gave a list of hazards for consideration and required to investigate all conditions "which reasonable can cause ... threats to the safety of the nuclear power plant" [67], p. 11. In addition, credible combinations particularly of hazards were required to be assessed, including with probabilistic methods.
The updated WENRA Safety Reference Levels for Existing Reactors from 2014 [97] have incorporated lessons learned for the Fukushima Dai-ichi accident. In the new issue T, specific requirements on the analysis of natural hazards are given. A systematic screening for all hazards, including combinations of hazards, shall be performed. Safety assessments should be done for design basis as well as design extension conditions. Assessments should be done with deterministic as well as probabilistic methods.
- IAEA SSG-3 [56] on Level 1 PSA calls for systematically analysing all hazards which could impact the plant on. The basic recommendations are in line with the updated WENRA Safety Reference Levels [97]. Moreover,

there are several IAEA guides on hazard analysis for NPP, which include hazard identification requirements ([56], [57], [58], [61], [62], [63] and [64]).

- The ASME/ANS PRA guide RA-S-2008 [98] as well as ASME/ANS RA-Sa-2009 [46] call for a systematic identification and screening of all potential hazards affecting the site. However, combinations are not addressed specifically.
- National regulations and guides, also from EU countries, required systematic hazard identification even before 2011.

In short, the authors find no major problems with current basic regulation and regulatory guidance regarding hazard identification.

From the authors experience and the results of the ASAMPSA_E questionnaire D10.2 [119] it is evident that the actual hazard identification for NPP (in Europe) has been somewhat limited before 2011. Often, the hazard identification from the original siting analysis had not been updated, even if frequency of exceedance curves were. Moreover, combinations and correlations of hazards have not been investigated systematically. And importantly, hazard identification was performed for determining the design basis of the plant. It was not used extensively for beyond design basis analysis. Probabilistic assessments, particularly detailed PSA models, were extended mostly only to seismic, fire and flooding; most hazards were screened out justified by low frequency of exceedance and an assumed sufficient resilience of the plant. This is, from the authors' point of view due to the following issues:

- Although hazard identification needs to be site-specific, there is a dearth of actual site specific data for rare events (with a "return period" well beyond 500 years). Generating such data is a costly endeavour, involving experts from multiple (geoscience) disciplines. The lower the frequency of exceedance (i.e. the higher the hazard intensity), the harder it is to determine such data. For some cases even if data is not available (records, informal "legends") a detailed geological study on the terrain and underground structure of the earth may reveal "hidden" specifics of the site that can impose critical impacts.
- Especially for low probability/high impact events, which are usually connected to a frequency of exceedance of below 10^{-5} per year, there are very large uncertainties associated with the results. There is no established method for a valid extrapolation of the limited amount of measurements, historic and pre-historic data to these very low frequencies. Expert judgements and simulation results can be important as well. Moreover, the results can largely depend on the extrapolation method chosen. Thus, it may be even hard to justify that events of such magnitude could reasonably happen at the site.
- Particularly for the combination of hazards, the knowledge about the actual (site-specific) correlations between different hazards or aspects of hazards, like e.g. how likely is a very severe flooding event with extremely high winds as well as debris levels in the service water intake jeopardizing the heat sink, is very limited. Therefore, these kinds of scenarios are difficult to assess.
- It is quite difficult to assess the impact of hazards with a large intensity/magnitude on the site and the plant in detail. In most cases, this will require detailed, time-consuming investigations and possibly complex simulations. These kinds of data and the respective methods are not easily available for the site or the plant. But if detailed information is not acquired, systematized and analysed, this may jeopardize the operation of the facility for the future. The economic losses to cope with NPP damages may be incomparable, more significant than those necessary for precise site screening.

- The design of nuclear power plants, particularly regarding hazards, usually includes significant safety margins. This can mislead to an inappropriate sense of safety in hazard analysts, if multiple failures and consequential failure due to hazard impact are not fully identified.

Finally, during the further progression of the accident at the Fukushima Dai-ichi reactors demonstrated that the inventory of fuel pools could be a significant contributor to the risk of accidental releases for long-term scenarios. Although none of the fuel pools on the Fukushima Dai-ichi site actually reached a state with an immediate risk for loss of fuel integrity [99], it has to be acknowledged that this risk can no longer be summarily excluded. From the author's experience and the answers to the ASAMPSA_E questionnaire [119] it is obvious, that hazard identification - especially for the purposes of PSA, did usually not include hazard identification for spent fuel in dry or wet storage on the site.

Conclusions

Based on the analysis above, the authors come to the following conclusions regarding hazard identification for an extended PSA.

- Hazard frequency assessment should take into account all events occurred in the immediate vicinity of the plant, in wider regions around the plant, and around the world **Erreur ! Source du renvoi introuvable.**;
- The frequency assessment should take account all correlation mechanisms **Erreur ! Source du renvoi introuvable.**;
- A necessary precondition for hazard identification for PSA is sufficient scientific knowledge about rare hazard scenarios with a potentially high impact. It has to be recognized that geosciences have not yet arrived at the level of understanding desirable for PSA assessment in a lot of cases but this cannot justify neglecting this area of risk. Obviously, further research in these fields and PSA experts on hazard assessment for nuclear facilities should establish strong links to geoscience researchers and integrate the best available scientific insights into their risk assessments.
- Since hazard identification needs to be site-specific, the original siting analyses have to be updated regularly for PSA purposes as well as for deterministic assessments. Site specific hazard identification has to be systematically extended to scenarios in the design extension conditions range (cf. WENRA Reference Levels [97]), especially for the purposes of an extended PSA.
- Hazard identification should be extended beyond the already established hazards like flooding or internal fire. All natural hazards that might affect the site shall be identified; a wide spectrum of rare events should be assessed (cf. WENRA Reference Levels [97]).
- There is a lack of accepted methods for extrapolating hazard intensity over frequency of exceedance curves in the range (frequencies smaller than approximately 10^{-4} per year) that can usually not be supported by actual data. There is on-going research in this area and PSA experts for nuclear facilities should be actively involved therein. It is noted that some methods like 'expert opinion elicitation techniques' are in use where probability of rare events occurrence is considered through the quantification of opinions of group of experts. Moreover, improved methods and better data are needed for limiting uncertainty bands for such extrapolated rare event frequencies.

- The lack of methods and/or data on hazard frequency should not be utilized to skip an assessment of the vulnerabilities of a plant to a hazard scenario, which is deemed physically plausible by experts. At least, the margins of the plant to severe accident scenarios and conditional core damage/large release probabilities should be estimated with a probabilistic approach. Use of expert judgement should be made as needed.
- More attention should be paid to worldwide operating experience in the nuclear industry as well as other industries regarding precursor hazard events and near misses. These insights should be systematically used in the site-specific hazard identification.
- Hazard identification should be made not only in regard to the risk to fuel in the core but extended also to the risk of spent fuel in dry or wet storage on the site.

3.1.2 CORRELATION OF HAZARDS

In the Fukushima Dai-ichi accident, seismic and tsunami (correlated) hazards manifested themselves through events (earthquake and external flooding) beyond the NPPs design basis. These dependent initiators caused the loss of the (off-site and on-site) power supply and of the ultimate heat sink, leading to core damage. In extension of the discussion in the previous section, the assessment by TEPCO on tsunami hazard did not adequately consider the correlation of the tsunami hazard with the simultaneous effect of a major earthquake, although Japanese experts were obviously aware that these events are correlated. Nonetheless, tsunami risk was evaluated by tsunami flood levels alone. Apparently, the combination of an extended loss of off-site power due to seismic impact with a long-term loss of the ultimate heat sink due to tsunami impact was not really addressed [99]. In fact, TEPCO apparently assumed a high probability for recovery of off-site power supply in its (internal events) PSA models. This assumption has apparently been (possibly implicitly) transferred also to most hazard scenarios, particularly the tsunami hazard [96], [99]. As a note: The modelling of safety systems recovery in internal events and hazards PSA can be a crucial issue regarding decision-making using PSA results. Optimistic assumptions for recovery in PSA could mask dominant risks.

Thus, the Fukushima Dai-ichi accident highlighted the need to properly address the correlation of hazards in the hazard identification and hazard screening process. Based on the authors' experiences and the insights from the ASAMPSA_E questionnaire [119], a systematic consideration of combinations and correlation of hazards is not systematically performed in PSAs.

In looking at recent international guidance for hazard identification and screening for PSA as well as deterministic analyses, the following observations can be made:

According to IAEA SSG-3, initiating events occurring at the plant may be the result of the impact of a single hazard or a combination of two or more hazards [56]. According to IAEA SSR 2/1 [55], where the results of engineering judgement, deterministic and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations shall be considered to be design basis accident or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Moreover, both the WENRA Reference Levels from 2008 [67] and 2014 [97] require a systematic investigation of credible combinations of hazards and combinations with other faults. The use of probabilistic assessment methods is mentioned [97].

According to the IAEA SSG-3 [56], initiating events occurring at the plant may be the result of the impact of a single hazard or a combination of two or more hazards. Furthermore, SSG-3 cautions that “combinations of hazards may have a significantly higher impact on plant safety than each individual hazard considered separately, and the frequency of occurrence of a combination of hazards may be comparable to that of the individual hazards, e.g. high level water and dam failure caused by storm precipitation. The process of identification of hazards should include all combinations of hazards that may be significant for risk.” [56], p. 60.

It has to be recognized that important international regulatory guidance raised the issue of combination of hazards (and other faults) on a conceptual level already well before 2011. The authors are, however, aware, that these basic requirements were - and still are - not fully reflected in national regulatory guidance. Moreover, the authors are aware that national guidance on performing PSA for NPP often does not address the issue of correlated hazards. In particular, there are no recommended methods in such guidance documents on how to actually perform a probabilistic investigation into correlated hazards. Simultaneously, there are no recommended methods for investigating the correlation between hazards and other faults (like internal initiating events). Finally, analyses of hazard scenario contributions to accidental release risks (PSA Level 2) were not required in most cases. Consequently, most current PSA assessments for NPP (in Europe) did not systematically consider all potentially relevant combinations of events.

From the authors’ point of view, this is mainly due to the following reasons:

- As already mentioned, there is a lack of scientific understanding of the correlation of hazards with other hazards and events. Moreover, there is also a lack of site specific data on which estimations for those correlations could be based.
- Correlated or simultaneous events were perceived as very unlikely. Thus, they have often been summarily (or implicitly) screened out as minor contributors for core damage, as the estimated probability of low frequency/high impact hazard scenarios (from e.g. correlated hazards) was often near or below screening limits.
- As analyses on the hazard contribution to accidental release were usually not required, screening based on accidental release frequencies was simply not done.

Conclusions

It appears that the importance of the risk associated to the correlation of hazards may have been underestimated by many PSA teams.

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

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

- hazards occurring at the same time and in the same conditions (e.g. winds and snow);
- hazards and other internal events occurring at the same time (e.g. if a hazard situation persists);
- external hazard inducing other external hazards (e.g. seismically induced tsunami)⁴;

⁴Combinations of natural and human-induced external hazards cannot be excluded a priori.

- external hazard inducing internal hazards (e.g. seismically induced internal fires);
- internal hazard inducing other internal hazards (e.g. internal floods induced by missiles).

Investigated correlation mechanisms should include at least the following **Erreur ! Source du renvoi introuvable.**:

- source correlated hazards (e.g. seismic and tsunami);
- phenomenologically correlated hazards (e.g. climatic events: strong winds and heavy rain, etc. ...);
- duration correlated hazards (e.g. hazards occurring during a long hot summer period);
- Induced hazards (see above).

Moreover, PSA experts should follow and encourage the scientific progress on hazards and hazards correlation. Probabilistic hazard assessments should be regularly updated with new information on (site-specific) correlations of hazards and other events.

3.1.3 EXTERNAL HAZARDS SCREENING

A screening process⁵ is generally established to focus on hazards that are risk significant. Screening criteria should ensure that none of the significant risk contributors are omitted.

With respect to the hazard assessment by TEPCO for the Fukushima Dai-ichi plant, it needs to be recognized that the (beyond design) tsunami hazard was effectively screened out from further probabilistic analysis due to its low perceived frequency of occurrence [99], [96]. However, if the low core damage frequency and accidental release values (PSA Level 1 and Level 2 results) reported by TEPCO for the Fukushima Dai-ichi units are taken into consideration, the frequency of exceedance estimation reported by TEPCO [99] could have merited further (probabilistic) analysis as significant contributor to both core damage and accidental release risk.

Based on the authors' experience and the results of the ASAMPSA_E questionnaire [119], most hazard scenarios are screened out for the majority of European plants based on frequency of exceedance or on estimated core damage frequency. Often, only selected external natural hazards like seismic and possibly flooding remain for detailed assessments. Even in light of the lessons learned from the Fukushima Dai-ichi accident this is not necessarily an indication of any deficiency in the screening process. There are some European plants for which hazard scenarios have been investigated in detail and for which those scenarios are identified as risk important or even risk dominant (albeit at relatively low core damage/release frequency figures). Still, in light of the Fukushima Dai-ichi accident, a closer look at hazards screening for PSA is justified.

Looking into the basic international guidance on hazards screening for the purpose of PSA, there are generic recommendations in e.g. SSG-3 [56]. The following screening criteria are typically applied (individually or in combination) to screen out a hazard (or to its subcategories) [56]:

- 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;

⁵A "screening" is a type of analysis aimed at eliminating from further consideration factors that are less significant for the aims of the analysis in order to concentrate on the more significant factors. This is typically achieved by considering pessimistic hypothetical scenarios [53].

- 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.

Moreover, SSG-3 provides guidance specifically on the screening of combined hazards and cautions against summarily screening out specific hazards prior to looking into the impact of hazard combinations [56], p. 63f. For the WENRA Reference Levels already in 2008, the combination of hazards was an issue for defining the design basis. There were no specific requirements on including combined hazards into the PSA, although the PSA should extend to hazards and should “provide confidence that there are no ‘cliff-edge effects’” [67], p. 34. The 2014 version of WENRA Reference Levels [97] emphasizes the PSA treatment of hazards, if practicable, and underscores the potential of hazard combinations. In addition, the importance of analysing hazards in the design extension range is highlighted.

Based on the authors’ experience, these general requirements have not yet fully been implemented into national regulatory guides and been substantiated with specific screening criteria. Consequently, a lot of PSA models still lack a systematic hazard screening, especially with consideration of design extension conditions induced by hazards leading to release scenarios. These open issues are mainly due to the following points.

- Prior to 2011, developing (detailed) hazard PSA up to severe accident scenarios was not commonly regarded as highly important in order to identify potential vulnerabilities of NPP. Consequently, hazard scenarios were screened out based on their small contribution to core damage frequency. Particularly, release frequencies were not used as additional screening metrics.
- The incomplete understanding of (site-specific) hazard frequencies and the correlation of hazards to other hazards and events (see above) impedes systematic screening.

Conclusions

In view of the Fukushima Dai-ichi accident, the screening of external hazards should take into account the following:

- The screening process should consider justifiable frequencies for the hazards of relatively high magnitude even if they have never been observed in the past in the plant vicinity. The impact of correlated hazards should be carefully considered.
- The set of screening criteria should ensure screening in low probability/high impact scenarios to the extent practicable.
- Screening criteria should include suitable risk metrics for covering accidental release risk like e.g. large release frequency or conditional containment failure probability.
- Screening should be done by combining fixed threshold values (e.g. for frequency of exceedance) with criteria relative to the risk level of the plant (e.g. using metrics like CDF, LRF, CFF, etc.).

With regard to hazard identification and quantification as well as correlations, the respective issues have already been described in the previous sections.

3.1.4 EXTERNAL HAZARDS ASSESSMENT

Uncertainty in the analysis of external events (i.e. estimation of risk for accidents caused by external events) tends to be greater than uncertainty for internal events. This uncertainty arises from the lack of data, analytical models, lack of scientific understanding and engineering experience of some of the phenomena and processes involved. It concerns [11]:

- 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-vapour 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).

This explains why hazard assessments for complex facilities such as NPP need significant effort and resources. In view of the (probabilistic) hazard for the Fukushima Dai-ichi units by TEPCO as well as the Japanese nuclear community the following points have to be noted.

- Design basis hazards were assessed deterministically for the units. Most experts agree with hindsight that the design basis assessment for the tsunami hazard was inadequate.
- Probabilistic assessment of external hazard risk was not performed for the Fukushima Dai-ichi units by TEPCO as it was not a regulatory requirement in Japan. Notably, a seismic back-check required by NISA in 2006 for all Japanese NPP was not yet finished [99].
- With hindsight, most experts assume that a probabilistic assessment of beyond design basis hazards, particularly of external flooding/tsunami hazard, would have clearly exposed existing plant vulnerabilities in the design extension region and would have served as justification for plant improvements⁶.

Based on the authors' experience and the results of the ASAMPSA_E questionnaire [119], detailed probabilistic investigations have been performed only for selected hazards at some NPP. This is for several reasons. For a number of sites, most (if not all) external hazards can be screened out from further consideration based on established screening criteria. Sometimes, external hazard PSA was not specifically required by the national regulator and not produced by the operator. (For example, they reached a consensus on the difficulty to perform such PSAs as no state-of-the-art methodology had been identified and in conclusion decided to neglect the risks that could appear from such situations.) Moreover, in most countries (detailed) probabilistic assessment of hazards was only required up to the core damage level (to the extent it was important to core damage risk). In addition, the analysis of slowly developing core damage scenarios was often aborted on the assumption that preventive mitigation measures would be able to reliably control such situations with sufficient time. In this case, the site

⁶TEPCO staff proposed related plant improvements (e.g. elevating emergency diesels) after design basis tsunami level re-evaluations. Consequently, the underlying plant vulnerabilities in the design extension range were not completely unknown. Unfortunately, no remedial actions were derived. [99]

impact of hazards was usually not investigated. Moreover, instead of following specific criteria for a controlled state, the time duration between the initiating event and the end of the analysis period (without apparent core damage) was specified for all systems and all accidents. Then, a time period of 24 hours was generally used [74]. This may be associated to optimistic views on equipment recovery possibilities.

With reference to the basic regulatory guidance on the international level and respective PSA guides, the following points can be highlighted. General and specific requirements for external hazards analysis are given in IAEA Safety Standard NS-R-3 [59] from 2003. Only minor changes (about the characterization of hazards) are introduced into the new draft revision [75]. The WENRA Safety Reference Levels from 2008 already require a systematic assessment of (natural) hazards. However, probabilistic assessment is only required for selected hazards [67], p. 33. In light of the Fukushima Dai-ichi accident, the WENRA Safety Reference Levels from 2014 requires the following. “For all natural hazards that have not been screened out, hazard assessments shall be performed using deterministic and, as far as practicable, probabilistic methods taking into account the current state of science and technology. This shall take into account all relevant available data, and produce a relationship between the hazards severity (e.g. magnitude and duration) and exceedance frequency, where practicable.” [97], p. 50 “Hazard assessment shall be based on all relevant site and regional data. Particular attention shall be given to extending the data available to include events beyond recorded and historical data. Special consideration shall be given to hazards whose severity changes during the expected lifetime of the plant. The methods and assumptions used shall be justified. Uncertainties affecting the results of the hazard assessments shall be evaluated.” [97], p. 51. Regarding the probabilistic assessment, “external hazards shall be included in the PSA for Level 1 and Level 2 as far as practicable, taking into account the current state of science and technology. If not practicable, other justified methodologies shall be used to evaluate the contribution of external hazards to the overall risk profile of the plant.” [97], p. 38

International guidance documents on Level 1 and Level 2 PSA likewise treated hazards PSA already before 2011. IAEA SSG-3 [56] contains basic recommendations on hazards identification, screening and performing (detailed) probabilistic hazards analysis. Moreover, SSG-4 recommends extending the probabilistic assessment of severe accidents to hazard scenarios. Both SSG-3 [56] and SSG-4 [57] emphasise to extend the analyses up to a point where a safely controlled state has been reached in order to catch potential cliff-edge effects. The basic recommendations are in line with e.g. [97].

Thus, there is no apparent gap in the basic regulatory requirements and recommendations on the international Level. As already mentioned, regulatory guidance and safety assessment practice in a number of countries did not entail probabilistic assessment of hazards, in particular with respect to Level 2 PSA. And, especially regarding hazard assessment in Level 2 PSA, this is currently still applicable.

Based on the authors’ experiences and ASAMPSA_E questionnaire [119] answers, operators’ not performing (detailed) hazards PSA is due to following issues:

- No respective requirements in national regulation.
- Current screening criteria (whether set by the regulator or defined by the licensee) in conjunction with hazard frequency estimations do not require more detailed assessments.
- Lack of (site-specific) data and large uncertainties in hazard frequency as well as impact on the plant are cited to doubt the validity of (specific) hazard PSA.
- Large amount of work for realistically determining the hazard impact on the plant and the essential safety functions because fragility of components

- Lack of models and tools for effectively performing (detailed) hazard PSAs for a number of specific hazards results in time-consuming and costly hazard PSA projects.
- Lack of expertise in the operator and regulatory organisations on state-of-the-art hazards assessment for specific hazards.
- The cost-effectiveness of (specific) probabilistic hazard assessments is questioned in light of existing large (deterministic) safety margins.

Conclusions

In view of the Fukushima Dai-ichi accident and in respect to probabilistic assessment of (external) hazards, the following issues should be considered in addition to the points stated in the sections above:

- Probabilistic hazard assessment should be systematically extended to support design extension and Level 2 PSA (significance for the risk of radioactive releases). Respective safety assessment practices should be established.
- Sufficiently detailed (probabilistic) hazard assessments are required to identify existing plant vulnerabilities particularly for low probability/high impact events.
- Detailed probabilistic assessment of hazards, which have not been screened out, should be performed up to a controlled safety state, which is defined by clear criteria for plant parameters and availability of essential safety functions. Challenges to such a controlled state should require additional, independent events in PSAs modelling.
- The community of hazard assessment and PSA experts should work towards establishing effective probabilistic hazard assessment approaches.
- Significant research effort is still needed for further improving the methods and tools needed for probabilistic hazard assessment, which requires long-term funding for public bodies and involvement of fundamental research institutions as well as end-users .

3.1.5 EXTERNAL HAZARDS AND INITIATING EVENTS

At the Fukushima Dai-ichi plant, the earthquake (first initiator) caused the automatic emergency shutdown (SCRAM) of the units in operation and the Loss of Off-site Power (LOOP) due to common cause failure of supply via the external power grid. The core was not damaged and recovery-prevention procedures could be adopted to prevent further damage.

After these initiating events (SCRAM and LOOP), the NPPs situation was (apparently) within the design basis accident envelope (although SSCs were exposed to beyond design seismic stresses). Then, the tsunami (second initiator) overcame the tsunami barriers producing an external flooding, introducing common cause failure between the electrical equipment (all nine water-cooled DGs and all but one of the air-cooled DGs) and leading to

a station blackout (SBO)⁷. The situation was aggravated by the loss of most switchboards and cabinets as well as large parts of the battery-secured DC power buses.

Station blackout is one of the most challenging accidents. For BWRs many safety systems required for core cooling, decay heat removal and containment heat removal depend on AC power and are not available during SBO⁸. During the further development of the accident it became apparent that restoring heat removal for the spent fuel in the respective pools was also important and consequently required respective resources and attention by operator staff. It is emphasized that nuclear power plants should be capable to survive in case of station blackout by utilising passive systems or diesel driven pumps or reliable steam driven pumps or some other electrically independent equipment's.

The Loss of Off-site Power (LOOP) is normally included in the Level 1 PSA, generally as an internal initiating event. Sequences of events starting from LOOP typically are important contributors to the core damage frequency. When these sequences evolve into the SBO scenario, it is one of the most important contributors. The Station Blackout (SBO) is often included in the PSA model as an initiating event with its own event tree. Then, event sequences from other initiating events leading to SBO conditions are jointly treated.

The loss of spent fuel pool cooling is usually investigated during low power and shutdown PSA as an internal event. The accidental risk for the spent fuel pool can be assessed with conventional PSA methods and tools. Some aspects on the scope of such an analysis are e.g. found in [51]. Fuel damage can be reached in case of e.g. extended SBO scenarios after a hazard impact. Extended SBO scenarios usually are major contributors to the risk of the plant from the spent fuel pool. However, internal events PSA models for the spent fuel pool or other relevant risk sources are often not available.

Probabilistic hazards analysis routinely maps the hazard impact on the plant to initiating events for an (internal) accident sequence model, which is usually already present in the PSA. This can be used for screening purposes as well as for detailed probabilistic assessment. Further consequences of the hazard impact (common cause failures) can then be considered by setting appropriate boundary conditions on the availability of required safety functions and accident management measures.

With respect to guidance on PSA on the international level, the approach of mapping hazard scenarios to existing initiating events (or defining new initiating events, if needed) is well described in e.g. SSG-3 [56]. Consideration of

⁷SBO is the complete loss of AC electric power to essential and non-essential switchgear buses in a nuclear power plant, i.e. the loss of offsite electric power system concurrent with turbine trip and unavailability on the onsite emergency ac power system (10 CFR 50.2).

⁸ The following safety systems can act in a BWR NPPs without the need for AC power:

- Isolation Condenser System (ICS), which is used in the Fukushima Dai-ichi Unit 1;
- Reactor Core Isolation Cooling (RCIC), which is used in the Fukushima Dai-ichi Units 2 and 3;
- High-Pressure Coolant Injection (HPCI), which is used in the Fukushima Dai-ichi Units 1, 2 and 3.

ICS aims at removing decay heat and conserving water inventory when the reactor becomes isolated from the turbine/condenser. RCIC has a steam-driven turbine-pump. It provides makeup water to the vessel, maintaining an adequate level. HPCI has a steam-driven turbine-pump and about seven times the capacity of RCIC. It can act as a backup for RCIC, providing water in isolation transients in which the main heat sink is lost and for small-break loss-of-coolant accidents.

hazard specific boundary conditions for that mapping is also routinely done and mentioned in basic guidance. No need for significant improvements in basic PSA guidance can be identified in that regard (a comparison of applications may be done in ASAMPSA_E). However, the accident highlighted the need for defining initiating events for risk sources other than the core (most importantly the spent fuel pool) and systematically mapping hazards to those initiating events for full power as well low power and shutdown operations. Based on the authors' experiences, in particular national regulation and PSA guidance would benefit from improvements in that regard.

Concerning the current state-of-the-art of hazard PSA with respect to initiating events, the following point can be made based on the authors' experience.

- Current PSA models do not systematically include screening and subsequent detailed assessments for initiating events for the spent fuel pool or during low power and shutdown states that are triggered by hazards.
- Additional correlated hazard events, which are likely to occur within the analysis time for the scenario, are not systematically considered in the selection of initiating events, nor in the respective events trees as further branches or additional boundary conditions.
- As long-term (hazard) scenarios are usually not considered systematically, additional independent frequent (hazard) events are not investigated as well in current hazard PSAs.

Conclusions

- Hazard PSAs need to be extended to risk sources other than the reactor core, in particular to a spent fuel pool. Respective initiating events have to be mapped to relevant hazard scenarios. Spent fuel pool and waste treatment facility related events should be considered in at-power PSAs as well.
- Hazard PSAs for other risk sources than the reactor core necessitate the development of PSA models on internal events for these sources. If such models are unavailable, the internal events PSA of a plant should be extended.
- The occurrence of further initiators during the time frame of the PSA analysis (specifically for correlated and long-term hazards) as well as the implementation of some recoveries should be considered.

3.2 SYSTEMS RELIABILITY AND CONDITIONAL UNAVAILABILITY FOR THE DID LEVELS

3.2.1 SYSTEMS RELIABILITY

System reliability is usually achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, and physical as well as functional separation and isolation. An important means for increasing DiD and robustness of plants is improving the plant's ability to withstand the loss of basic safety functions such as residual heat removal, and of correlated events such as the loss of power supply and the loss or degradation of critical instrumentation and control (I&C) systems. The reliability of safety functions is routinely assessed within a PSA (Level 1) for different initiating events and their specific boundary conditions. Indeed, one objective of PSA assessments is complementing deterministic assessments in identifying unacceptable vulnerabilities of safety systems.

With regard to the Fukushima Dai-ichi accident it first should be reiterated that neither the licensee nor the regulator actually performed a detailed probabilistic assessment of a beyond design tsunami (see above). While PSA experts agree that a detailed PSA would have exposed the related plant vulnerabilities and provided sound arguments for back fitting actions, information available from TEPCO [99] indicates that the basic vulnerabilities were at least partly known already from deterministic approaches. In any case, due to lack of modelling, no immediate lessons are evident for reliability assessment with PSA methods from the accidents.

However, the Fukushima Dai-ichi accident underscored the importance of common cause failures, particularly consequential failures after a beyond design impact, for the reliability of safety systems. Based on the authors' experience, systematic consideration of common cause failures and consequential failures is already a major issue in the PSA of NPP (and other multiple-redundancy technical systems) at least for internal events PSA. In addition, one major issue for detailed PSA events of hazards is the identification, quantification and modelling of consequential and common cause failures due to hazard impact. As evident from the answers to the ASAMPSA_E questionnaire [119], there is still a significant research effort needed for improving this part of probabilistic hazards assessment. In addition, PSA assessments are usually not used for assessing the reliability of safety systems within the scope of DiD assessments. This is partly due to the current structure of PSA models, which often are not suitable for such assessments (cf. e.g. [100], [101]), and partly due to the fact that complementary PSA assessments are mostly not required by regulators as part of DiD assessments.

In any case, the Fukushima Dai-ichi accident exposed some vulnerabilities of the plant design related to DiD, which are worth summarizing. The first plant vulnerability is related to the loss of electrical systems due to common cause failures induced by the tsunami. Importantly, the common cause failure affected redundant, diverse and physically separated systems more or less simultaneously. Moreover, systems and functions on all Levels of DiD were rendered unavailable leading to a failure of basic safety functions. Derived improvement measures relate to the electrical power generation and distribution systems within and outside the plant for maintaining critical safety functions (core cooling, containment integrity, spent fuel cooling and confinement of radioactivity) and for effectively monitoring them during prolonged loss of power events. Consequently, back fitting measures include optimizing DC battery loads and battery capacities and sustaining critically important power supply for extended periods of time, e.g. by protecting emergency diesels against hazard impact or by using mobile diesels as accident mitigation measures.

The second area of vulnerabilities relates to the loss of ultimate heat sink. Again, direct tsunami impact and consequential failures resulted in common cause failures affecting multiple redundancies, diverse and physically separated systems; systems and functions on all Levels of DiD were affected. Consequently, measures for ensuring core cooling and spent fuel pool cooling, the provision of alternate water sources for the reactor and for the spent fuel pool and for improving the availability of the electrical power supply [20] in case of a long-term loss of ultimate heat sink were derived.

Looking at the regulatory framework, the authors are aware of the increased importance of DiD assessments, specifically related to design extension conditions, in current regulatory positions. In reaction to the Fukushima Dai-ichi accident, WENRA has published updated Reference Levels for existing reactors [97] in September 2014. The updated requirements intend to strengthen DiD and underscore the importance of effective measures on the design extension conditions level (cf. also IAEA SSR 2/1 [55]). The use of probabilistic methods for assessing the

effectiveness of measures on the design extension level, e.g., is explicitly mentioned. However, the authors are not aware of current specific requirements regarding system reliability or criteria on systems independence verification (in a DiD sense) with PSA methodology by regulatory authorities. The need for the DiD assessment is obviously explicit within the IAEA requirements; cf. e.g. the GSR part 4:

“4.12. It shall be determined in the safety assessment whether adequate defence in depth has been provided, as appropriate, through a combination of several layers of protection (i.e. physical barriers, systems to protect the barriers, and administrative procedures) that would have to fail or to be bypassed before there could be any consequences for people or the environment”.

Requirement 13: Assessment of defence in depth, “It shall be determined in the assessment of defence in depth whether adequate provisions have been made at each of the Levels of defence in depth.....”

There is another area of concern which is underscored by the events at the Fukushima Dai-ichi plant. This is the consideration of detrimental actions for the reliability assessment of systems (and operating procedures). Human failure is known as one major root cause for severe accidents in the nuclear industry (Chernobyl, Three Mile Island) and in non-nuclear fields (chemical industry, aviation and transport, etc.). Within the Fukushima Dai-ichi context, the isolation of the ICS of unit 1 was identified with hindsight as probably detrimental despite being in accordance to the operation manual, because it rendered a safety function unavailable. One can point out that the procedures were wrong because the operator should not have the possibility to intervene on a passive system knowing that this intervention will allow losing the passive character. In a right design with passive systems, only “fail safe” actions should be possible.

This highlights the potential relevance of detrimental actions before an accidental state has been reached for the reliability assessment of systems. The issue is further discussed in also section 3.4.

Conclusions

In view of the Fukushima Dai-ichi accident and based on the analyses above, the following issues should be considered with regard to system reliability and PSA:

- Regulators should ensure that actions taken and resources relied upon at one level of DiD are independent from the other levels in order to minimize the potential for common-cause failures propagating from one level to another as occurred at the Fukushima Dai-ichi NPP [19], [8]. Specifically, assessment of these issues with PSA methods to the extent appropriate should be done.
- System reliability assessments with PSA methods should be extended to the design extension conditions regime. Similarly, DiD assessments for severe accident management measures, procedures, or systems should be performed using PSA methods as appropriate. Consequently, PSA Level 1 and Level 2 models should be considered for such assessments.
- Best practices for using PSA for DiD assessments need to be gathered. This issue is treated by the ASAMPSA_E project with the scope of a separate technical report [43]. In any case, there is still need for further research into how PSA models can be efficiently used to do DiD assessments. Moreover, related criteria need to be defined.
- Potentially relevant detrimental actions by operators before an accidental state has been reached, e.g. disabling safety systems or aggravating accidental consequences, should be systematically investigated.

Potentially relevant actions should be included in the systems reliability assessment and the fault tree/event tree modelling to the extent practicable.

3.2.2 MODELLING AND ASSESSMENT ISSUES

As in the previous section, it has to be acknowledged that due to the lack of detailed modelling for the Fukushima Dai-ichi plants, no direct lessons on PSA modelling can be drawn from the accident. However, the accident highlighted some issues relevant for PSA modelling. These are described in the following, based on the authors' experiences, the ASAMPSA_E questionnaire [119] results, and other sources.

- Adequately modelling hazard impact on plant components (common cause and/or consequential failure as well as component/structure specific fragilities) is still an open issue. There are some hazards like e.g. seismic, where quite sophisticated methods and procedures have already been applied for some sites, and there are hazards (or rather hazard impacts) like e.g. electromagnetic interference, for which detailed probabilistic modelling is only in the developmental phase. Thus, to a different degree for the hazards, there is still a lack of efficient modelling approaches as well as respective fragility/reliability data.
- Cliff-edge effects or threshold values, at which or by which the transient behaviour of the plant changes significantly (e.g. from a controlled state to a severe accident scenario) are recognized as highly important for the modelling of safety system effectiveness in event/fault trees. There is still a need for methods for efficiently identifying such critical values, particularly as part of screening procedures, for most hazards.
- For multi-unit sites, there can be interdependencies between the different units also on the systems and components level (e.g. via common support systems or even commonly used trains, or via common buildings and structures). These issues have been often not systematically considered in current PSAs or deemed not relevant.
- Reliability assessment of systems (rather safety functions) or components with established basic event models can be dependent on their assumed "mission time". This mission time applies, e.g., to the failure to operate (e.g. for emergency diesels during an extended loss of offsite power), to the number of system starts and shutdowns, and even to generating CCF data. In this respect, the widespread use in PSA Level 1 of 24 h as maximum mission time for all purposes is definitely a problem.
- In some PSA models, (manual) recovery actions or repair of faulty equipment of a certain time period are assumed. The recovery actions are quite difficult to model even for internal events as each component failure needs an appropriate assessment of recovery time and conditions. For external hazards conditions, the situation is even more complex. Firstly, the human reliability assessment methods for these operator actions are usually not really suitable for boundary conditions as seen during the Fukushima Dai-ichi accident. Consequently, these adverse boundary conditions are often not adequately reflected in the assessments of operator failures leading to optimistic results. Secondly, repair times and grace periods assumed for the PSA modelling might no longer be reasonable for boundary conditions as seen during the Fukushima Dai-ichi accident. This can have a significant impact on system reliability assessments. Here, there is a need for improved, more detailed investigations.

- Systems, which are not safety class systems, are often summarily excluded from PSA modelling, as they usually have no (adverse) impact on controlling an internal event. However, adverse effects due hazard impact can be transmitted from non-safety systems to safety systems. In addition, the potential effects from non-safety system can be dependent on the operating status of the plant. These are open issues for a lot of current PSAs, issues that must be addressed with adequate tools and notions.

With regard to the regulatory framework, the issues stated above are covered in a general sense by the recommendations given e.g. in SSG-3 or in ASME/ANS-RA-S-2009, and they are seen as well by national regulators. However, the authors are not aware of specific regulatory requirements or good practices for solving these issues.

Conclusion

Regarding system reliability PSA modelling and assessment, the authors arrive at the following recommendations in light of the lessons learned for the Fukushima Dai-ichi accident:

- PSA analysis times should be extended until a stable controlled state or an accidental stage has been reached. Success criteria for a controlled state in the long term after an event should be defined. Justified analysis times should form the basis for systems or component specific mission times in the fault tree modelling dependent on the scenario. This may necessitate changes to some PSA software tools.
- Common cause failures and consequential failures induced by hazards impact need to be systematically addressed considering site-specific conditions, particularly for detailed PSA assessments. As this task includes also spatial interactions (fire and flood spreading, impact of collapsed SSC), I&C interactions (faulty signals), and system interdependencies (e.g. supporting systems), it can be very complex. Moreover, erroneously established dependencies (e.g. due to faulty operator actions prior to or during the event scenario, should be considered in Level 1 PSAs, if relevant. Also, in addition to failed barriers or protective measures, degraded states should be included into detailed PSA assessments. Of particular importance are containment failure modes due to hazard impact, i.e. prior to accidental states. These should be systematically investigated in the PSA Level 1; respective pathways need to be described. On all these issues, new and improved methods as well as reliability/fragility estimations need to be developed.
- The dependencies of barrier effectiveness as well as safety systems effectiveness to non-safety class functions, which are in turn dependent on the plants operating status, should be investigated systematically. There is a need for new and improved methods as well as data.
- Similarly, failure and degradation mechanisms of qualified and non-qualified equipment for specific hazard impacts and their secondary effects need to be investigated in more detail. Dynamic loads (e.g. vibration, overpressure, etc.) should be considered as well. Consequently, respective failure modes and eventually basic events have to be defined. For this, probabilistic methods and application procedures have to be improved.
- The analysis period assumed for system reliability (as well as event progression) should not be artificially limited to 24 h. Instead, mission times should be chosen in a realistic way based on the time, the system performance is needed for controlling a scenario. Respective success criteria should be defined and justification should be provided, particularly on why a controlled state has been reached. The mission time should be used in basic event models and for quantification of e.g. certain common cause failures. Consistency with accident progression analysis should be maintained.
- For multi-unit sites, the interdependencies between the units, including dependencies on component or system level, should be included into the event tree/fault tree modelling. This includes dependencies

between the units due to existing connections between units (e.g. shared turbine building, cable trenches, ventilation ducts, spatial interactions between plant units compartments), which are usually neglected or underestimated for PSA purposes. Potentially relevant dependencies can arise due to failed isolation or erroneously open connections. On these issues, further developments are needed. In addition, appropriate conditional probabilities and/or event correlations have to be established for PSA modelling and quantification. This constitutes a significant challenge; methods and data for this task have to be developed.

- In system reliability modelling, a particular focus should be on common cause and consequential failure analysis. This has to include hazard impact (whether direct or indirect, by environmental conditions or as an area event, etc.).

3.3 EMERGENCY OPERATING PROCEDURES AND EVENT SPECIFIC BOUNDARY CONDITIONS

Accident management consists in taking a set of actions or applying existing measures during the evolution of a beyond design basis accident:

- (a) To prevent the escalation of the event into a severe accident;
- (b) To mitigate the consequences of a severe accident;
- (c) To achieve a long term safe stable state.

Consequently, accident management comprises preventive and mitigative domains. The former are subject to Level 1 PSA whereas the latter belong to Level 2 PSA and to the extent that those measures are external to the plant to Level 3 PSA. In this section, only preventive measures and procedures will be discussed. Mitigative measures as part of SAMG are treated in section 4.3.

For the Level 1 PSA, the preventive measures consist of Emergency Operating Procedures (EOPs), which are tailored to contain design basis level accidents and some beyond design basis scenarios (sometimes as part of SAMG) [97].

As EOPs are intended to cover accidents without core melting or some other damage, protection systems trigger most (or even all) safety functions foreseen for containing the event. Consequently, the primary role of the shift staff and particularly the control room personnel is monitoring the plant status and initiating measures for reaching a long-time controlled state (e.g. cold plant shutdown) after a certain grace period (for DBA analysis, usually 30 minutes is conservatively assumed). If EOP measures are not working as intended, the plant staff will either solve these problems (e.g. by manually starting systems, initiating and successful repairs, etc.) or they will lead to preventive accident measures. The latter usually require a more direct involvement of operators for their execution, e.g. for connecting or starting systems, and of course for initiating these measures in the first place. It should be noted that there is quite some flexibility for assigning a specific measures or procedure to EOPs or preventive Accident Management (AM), respectively. In the following, aspects relevant to PSA modelling will be discussed.

The Fukushima Dai-ichi accident has re-emphasized two important insights. First, the reliability assessment for EOP and AM rests on assumptions regarding the operability and accessibility of the respective equipment as well as the feasibility of measures. For internal events PSA,

- first - with the exception of parts directly affected by the initiating event and/or the accident progression - undisturbed situation is assumed. Consequently, operability and accessibility of systems and components is often of minor importance in these assessments as is the basic feasibility of measures. This situation may be altered drastically in the case of hazard impact or if an event affects a multi-unit site with one unit progressing to a severe accident, thereby affecting measures for other units. These aspects are evident from the Fukushima Dai-ichi accident.
- second, the reliability assessment for EOP as well as AM often utilizes human reliability assessment methods. While there are several more or less accepted methods for assessing operator actions during typical internal events scenarios it is less clear how this can be adequately treated under boundary conditions typical for severe hazard impact or severe accidents. This question will be discussed in more detail in sections 3.4 and 4.4.

With regard to the first issue, a review of current regulation shows that the operability and accessibility of equipment needs to be taken into account, cf. [97], p. 33ff. The guide IAEA SSG-3 in addition to the generic requirement for taking into account scenario-specific boundary conditions [56], p. 44, specifically recommends taking into account hazard specific boundary conditions in several instances ([56], p. 76, p. 86, p. 109f). Similar recommendation can be found in ASME/ANS-RA-Sa-2009 [46], p. 128, p. 184ff, p. 241, p. 279, and p. 294. However, some national regulatory guides on PSA do not treat this topic explicitly. Moreover, there is no commonly accepted specific methodology available for actually doing all these assessments.

Based on the authors' experience and the results of the ASAMPSA_E questionnaire [119], in (detailed) PSA assessments for hazards, EOPs and accident management measures are considered - if at all - without systematically investigating accessibility and operability issues or multi-unit dependencies.

Conclusions

- The probabilistic assessment of EOPs and preventive AM procedures/measures in PSA Level 1 should systematically consider accessibility and operability of equipment as well as feasibility of measures in case of hazard impacts. There is a need for more sophisticated methods and for better data on these issues.
- Similarly, Level 1 PSA for multi-unit sites should systematically consider the impact of a severe accident scenario in one unit on the accessibility and operability of equipment for other units. In addition, simultaneous availability of staff for performing actions needs to be taken into account. There is a need for more sophisticated methods and for better data on these issues.

3.4 HUMAN RELIABILITY ASSESSMENT AND EVENT SPECIFIC BOUNDARY CONDITIONS

Despite significant efforts and progress, Human Reliability Analysis (HRA) remains a challenging issue. There is a number of methods used for the identification and quantification of human errors, starting from traditional methods such as the Technique for Human Error Rate Prediction (THERP), Accident Sequence Evaluation Program

(ASEP), Success Likelihood Index Method (SLIM), Standardized Plant Analysis Risk - Human reliability analysis (SPAR-H), etc., which are still widely used by PSA practitioners. Other methods such as Method for Assessing the Completion of Operators Action for Safety (MERMOS), Human Error Assessment and Reduction Technique (HEART)/Nuclear Action Reliability Assessment (NARA), Crew Response Tree, etc. have also been developed and are used in particular countries. A discussion of the most common HRA methods is presented in e.g. [87], which identifies gaps or limitations that existed in the current HRA methods and which are still relevant for HRA methods available at the time of writing of this report. While several limitations may be covered in some methods, they are not adequately addressed in the remaining methods. In summary, the authors of [87] identified no method that could provide valid solutions for all limitations. All methods promote, although at varying degrees, working with a multi-disciplinary team for performing HRA so that none of the potentially important performance shaping factors (PSF) is missed and a clear understanding of the performance conditions can be obtained. Furthermore, a high level of knowledge and expertise of HRA and human factors on the part of the analyst is found to be required in the implementation of many methods. This necessary precondition is not sufficiently stressed in the descriptions and guides for several methods. Consequently, this issue should be emphasized in current guidance on HRA methods and their application, especially for those methods which claim that they can be easily implemented without such expertise or corresponding training. With these preliminary remarks, the aim of this section is to identify some gaps and insufficiencies in the application of HRA methods in light of the Fukushima Dai-ichi accident. In result of Fukushima case - it is important to study the human reliability in two directions:

- If the personnel successfully accomplishes the foreseen actions and procedures (for which has been trained and instructed) or fails;
- If the personnel succeeds to manage extreme situations which are not foreseen in the operational scenarios. Definitely such options are disputable, but the analysis of such case can indicate whether the operational procedures - normal operation and in particular emergency response are adequate.

After the Fukushima Dai-ichi accident, a number of HRA challenges (and, consequently gaps) have been identified. Regarding PSA Level 1, some of these challenges can be expressed as follows:

- HRA needs to include a more comprehensive and realistic assessment of the effect of hazards on human performance:
 - conditions where information /indications/ announcements (flying blind syndrome) are either not available or not reliable;
 - harsh environmental conditions on operator's performance and associated human errors;
- For multiple-unit sites, specific human reliability analysis of the actions and activities to be taken by shared staff, especially in light of work-load and availability of staff, during a scenarios affecting several units should be performed;
- Effects of long-term scenarios prior to core damage (including fatigue and stress) on operator's performance and associated human errors should be addressed better;
- Treatment of different or multiple decision makers, including external distractions is missing. The issue is related to the inclusion of different decision makers (i.e. in extension to a typical control room crew) who made potential errors in the prioritization of work or the initiation/omission/abortion of certain procedures

(possibly due to incorrect information regarding the system and plant status or input from external organizations).

- As discussed already in section 3.2.1, potentially relevant detrimental actions (e.g. erroneously shutting down a safety function) are often not included into PSA Level 1 models. Faulty decisions which aggravate a situation (human failure) are important root causes for severe accidents. They are more likely if operators are put into a situation which is outside of pre-planned procedures and required knowledge-based actions of, if information overload, faulty information and other stressors impair their performance. These situations are a current field of research for HRA, also outside of the nuclear field. Consequently, this is a gap of current PSA models and an area with a need for further research.

Furthermore, there is an additional potential HRA insufficiency which relates to the usual assessment (and modelling) approach with two distinct phases, a screening analysis and a detailed analysis. For the screening analysis, a simplified initial quantification of human error probabilities, i.e. a tentative over-estimation, is applied. Based on quantification results of affected sequences, key human actions (e.g., those with high importance contributions to risk) are identified and a detailed HRA and quantification of the risk-significant HEP is performed. These results are then used for the final PSA quantification and the interpretation of PSA results. Mechanistic application of this approach may lead to skewed results, where seemingly important contributors to risk from operator actions are routine and/or well-described staff actions for operating systems according to trained procedures. This typically happens if analysts have performed in-depth, best estimate assessments of initially risk-significant human actions while other routine actions were kept at a rough, conservative evaluation. The consequence might be that critical, complex actions are assigned smaller HEPs than routine actions. For example, some PSAs that used THERP /ASEP methods and a screening/detailed assessment approach reported that rather routine operator actions during long-term cooling in transients are the most risk-important operator actions in the model.

Looking at the general regulatory framework on human reliability assessment for the purpose of PSA, the following points can be made:

- The importance of operator actions and their consideration in PSA models is acknowledged in the relevant guides and regulations, like e.g. IEA SSG-3 [56] and ASME/ANS RA-S [46]. The importance of assessing human reliability assuming representative and appropriate boundary conditions is stressed, especially for hazard scenarios. In general, there are no specific requirements or recommended methods with regard to the issues and problems described above.
- Regulators usually do not specifically require the application of one of the aforementioned HRA methods. There are, however, explicit or implicit recommendations by some national regulators on specific methods. For example, the US NRC has contributed to the development of the SPAR-H method and uses SPAR-H for its own PSA.

In summary, current regulation on HRA for PSA is sufficiently generic to cover the issues identified from the Fukushima Dai-ichi accident, but it does neither explicitly require considering specific issues nor can provide specific help and guidance for performing assessments on these issues.

Conclusion

The above mentioned challenges are related to phenomena or situations for which current HRA methods do not appear to be sufficiently developed and/or qualified for supporting routine, efficient analyses. Although the current PSA methods and tools for HRA seem to be well matured for a number of aspects, they however need to be appropriately applied and improved as necessary. Aspects related to PSA Level 1 are listed below:

- Identification and treatment of “errors of commission” (EOC) (i.e. performance of inappropriate actions that may aggravate an accident scenario) involving intentional disabling of safety systems (e.g. intentional isolation of the Isolation Condenser system at Fukushima Dai-ichi as per operation manual). However, EOCs along with the associated contexts that would make such errors probable are not included in most PSA models except for quite obvious scenarios. There are HRA methods capable of treating some aspects of EOCs (e.g., ATHEANA), and such methods (or at least their key underlying concepts) should be useful when searching for cognitively challenging human failure events. These practices need to be improved.
- Assessment of the feasibility of recovery actions and delays in performing these actions (including accessibility and operability under accidental conditions; long time window needed to complete action). This aspect needs to be considered more systematically in PSA models and HRA methods and data need to be further improved in this regard; at minimum, all recovery actions modelled in a PSA should be precisely described, justified and their impacts on the PSA final results explained.
- Assessment of the effects of lack of or even misleading information (including loss of instrumentation and control equipment) and related uncertainties on decision making and operator actions. This aspect should be better included into PSA models. Particularly for knowledge-based decision making, development of practicable and qualified HRA methods is needed.
- Assessment of the variability in plant crew performance. This aspect needs to be accounted for in the uncertainties assigned to HEP, and there is a need for better data to that effect.
- Adequate treatment of cognitive between-person and within-person dependencies among sequential or parallel, operator actions due to weak knowledge about dependencies. There is still a strong need for the development of efficient, practicable methods on this aspect.
- Analysts need to find a balance in the application of initial (conservative) screening values and of (more realistic) values based on sophisticated HRA methods for the basic events for operator actions in the PSA model in order to prevent skewed or non-realistic results.
- HRA analysts should be sufficiently experienced, be informed about available assessment methods and should have access to expert level knowledge on plant behaviour, procedures, handling of components, etc. as appropriate for each assessment.

3.5 LESSONS LEARNED FOR PSA LEVEL 1

This section summarizes the main lessons learned on PSA Level 1 based on the conclusions in the previous sections (see above). Following the topical structure of this section, the main insights regarding the different topics are given below.

3.5.1 INITIATING EVENTS

The probably most important is that initiating events should be systematically determined for all operation modes and relevant sources of radionuclides, and should include all hazard impact with a special focus on low probability/high impact events, which can significantly challenge the safety concept of the plant and thus may give rise to cliff-edge effects. Specific to hazards, this includes the systematic extension of the PSA scope to beyond design basis hazard scenarios (at frequencies below $\sim 10^{-4}$ per year) as well as combinations of hazards events with other events, which includes correlated hazards as well as uncorrelated combinations with sufficient probability. It has been recognized that current methods as well as data used for determining frequency vs. likelihood characteristics or curves for a lot of hazards are limited in their validity and often fraught with high uncertainties. Methods for treating correlated (hazard) events - if available at all - are usually not mature or developed at sufficient level. Consequently, this is identified as a field for additional research; the PSA community should link-up with the geosciences community on this issue.

Further important lessons relate to the screening of initiating events, where screening criteria should be commensurate to overall PSA results and ensure that low probability/high impact events are not screened out. To that effect, a set of suitable risk metrics and threshold values (including CDF and LRF) should be defined. In order to screen and eventually model hazard impact for radionuclide sources out of the core, adequate internal events PSA models for these sources (e.g. in the spent fuel pool) are needed and have to be completed as appropriate.

3.5.2 SYSTEMS RELIABILITY

PSA assessments should not only be extended to all reasonable scenarios and relevant sources, but should also be used more systematically to complement assessments of Defence in Depth. Particularly, DiD measures dedicated to design extension conditions should be assessed by means of PSA with suitable Level 1 and Level 2 models. In addition, best practices for efficiently using PSA models and results for assessing DiD and the independence of safety features on different Levels of DiD need to be gathered and developed further.

During the development of accident sequence models for a PSA and for reliability assessments of systems, components, and operator actions best estimate boundary conditions should be used to the extent practicable. Specifically, analysis times for scenarios as well as mission times for safety functions should be extended until a defined stable or an accidental state has been reached as demonstrated with appropriate justification. This might require changes to current PSA models and eventually even to some current PSA software tools. PSA models should systematically consider dependencies between systems affecting safety function availability, including the effect of non-safety systems. This pertains particularly to multi-unit sites, for which relevant dependencies on the systems levels, e.g. via shared support systems or buildings, as well as dependencies on the accident sequence level, e.g. via the impact of a severe accident in one unit on measures or systems in another unit, have to be included into the PSA models. In addition, special attention should be given to common cause failure modelling, including design errors, hazard impact, operator errors, environmental conditions, and consequential failures of e.g. support systems unavailability, especially for safety related systems.

3.5.3 EMERGENCY OPERATING PROCEDURES AND SAMG

The probabilistic assessment of EOP and preventive AM procedure/measures in PSA Level 1 should systematically consider accessibility and operability of equipment as well as feasibility of measures in case of hazard impacts. Similarly, PSA Level 1 for multi-unit sites should systematically consider the impact of a severe accident scenario in one unit on the accessibility and operability of equipment for other units. In addition, simultaneous availability of staff for performing actions needs to be taken into account. There is need for more sophisticated methods and for better data on these issues.

3.5.4 HUMAN RELIABILITY ASSESSMENT

While there are a rather large number of HRA methods available, there are still areas for which commonly accepted methods are lacking or insufficient. Particularly, the authors have identified the assessment of knowledge-based actions like e.g. recovery action, of action in high-stress situation like e.g. operability under accidental conditions, and of potentially aggravation actions during and before the event as areas with a need for further improvement. In addition, the PSA model should be well balanced in its reliance of basic events with initial screening values and those based on more sophisticated assessments. Finally, HRA assessments for the purpose of a PSA should be performed and/or reviewed by analysts with sufficient experience and with expert level knowledge on all disciplines relevant for the analysed action and relevant installation of NPP.

The importance of recovery actions modelling on final PSA results has to be precisely explained in PSA final reports, especially if these actions significantly influence the results while their justification is difficult.

4 REVIEW OF EXISTING PSA LEVEL 2 ON GAPS AND INSUFFICIENCIES

The status of the PSAs Level 2 for the Fukushima Dai-ichi units can be summarized as follows: there was a limited scope Level 2 PSA, restricted to internal events and to the determination of the containment failure frequency (CFF) [96], [99]. Apparently, several severe accident management measures were considered within the limited scope PSA models, and found to be effective. However, the reliability assessment for these measures did not consider the potential influence of severe hazards impact or even severe accident conditions on site on the human reliability assessment for these measures. Consequently and with hindsight, the reliability assessment by TEPCO is seen as optimistic by PSA experts.

4.1 INITIATING EVENTS AND COMBINATION OF RARE EVENTS

PSA Level 2 starts with the plant damages states determined by the PSA Level 1. Since the PSA Level 1 for the Fukushima Dai-ichi plants did not comprise hazard impact scenarios (see section 3), these scenarios were not covered by the PSA Level 2 as well. Consequently, as even single hazard events were missing from systematic probabilistic consideration, no combinations of rare events were considered at all. Notably, this included respective deterministic assessments for the Fukushima Dai-ichi units as well.

In the following, the authors discuss lessons learned for the scope of PSA Level 2 and the treatment of rare events within the PSA Level 2 based on their experiences with such PSA models, the results of the ASAMPSA_E questionnaire [119] and the events during the Fukushima Dai-ichi accident.

The events at the Fukushima Dai-ichi plant during the accidental phase have highlighted a number of issues, which relate to assumptions usually made for PSA and especially for PSA Level 2 with respect to initiating events and accidental scenarios considered.

- The screening of events for (more in-depth) consideration in the PSA happens usually during the PSA Level 1 (see section 3.1). Consequently, Level 1 risk metrics related to frequency of core damage are applied for the screening. It has to be noted that with effective mitigative accident management, large accidental releases can be prevented with some chance of success. Conversely as demonstrated by the events for the Fukushima Dai-ichi site, there might be low probability/high impact scenarios, for which not only core damage but also large and/or early releases are almost inevitable. Moreover, these events can be screened out based on Level 1 risk metrics due to their small contribution to core damage states, but might be highly important contributors to specific Level 2 release categories, in particular release categories for large and/or early releases. Moreover, there are often no specific regulatory requirements on considering PSA Level 2 metrics for the screening of initiating events. Consequently, this currently is an issue for a number of PSA models.
- Obviously, the Fukushima Dai-ichi accident underscored the importance of performing PSA Level 2 investigations not only for internal events during full power operation but also systematically for shutdown modes, for hazard impacts, and for risk sources like the spent fuel pool. Based on the authors' experience, current PSA Level 2 models are often incomplete in this regard. Although e.g. IAEA SSG-4 [57] recommends performing probabilistic assessments for all plant damage states derived for all relevant sources, operating

modes, and for all initiating events, including hazards, national regulation and recommendations on PSA Level 2 have often been restricted to PSA Level 2 for internal events at full power operation. This situation is currently changing).

- The lesson learned from the accident has underscored the importance of analysing scenarios irrespective of their duration (“mission time”) until either an accidental situation is finalized or a controlled plant state can be justified. Based on the authors’ experience, accidental type sequences are sometimes not transferred from PSA Level 1 to the PSA Level 2 only because of the long period of time up to the accidental state (e.g. core damage). Sometimes PSA Level 2 is restricted as well to a mission time, neglecting sequences with late releases. This shortcoming is mostly motivated by concentration on large “early” releases. The experience with the Fukushima Dai-ichi releases clearly shows that neglecting late releases and restricting mission times should no longer be accepted.
- The lesson learned from the accident underscored the importance of sequences with containment failure causing offsite release. But it is important to note that neither the powerful earthquake nor the extreme tsunami seems to have caused containment failure. In this respect the Fukushima Dai-ichi experience confirms most existing PSA which identify external hazards as potentially cutting power supply or interrupting core cooling before the containment itself is destroyed. Containment failure in Fukushima Dai-ichi was a consequence of core melt impact associated to a lack of efficient containment heat removal possibility severe accident conditions. Taking into account that the NPPs in Fukushima Dai-ichi were neither designed against nor sufficiently upgraded to withstand severe accidents, the consequential containment failure after core melt had to be expected.
- Sequences triggered by (severe) hazard impacts are commonly regarded as candidates for containment failure before accidental conditions (e.g. core damage) have been reached. Based on the authors’ experience, these sequences are often estimated with comparatively small likelihoods to the Level 1 results (core damage frequency). They are thus either not transferred to the PSA Level 2 via an interface or are assigned to another interface state. In this case it has to be made sure that its representative scenario is not optimistic for these rare sequences.
- Concerning the initiating conditions to be considered in a PSA Level 2 (if it starts at core damage) and based on the Fukushima Dai-ichi accident conditions, situations of core melt from PSA Level 1 should be considered (in the PDS) while another or several reactors are already in severe accident conditions.

In addition, the authors have found useful to remind of some further issues associated to PSA Level 1 and 2 interface, although there is no direct connection to the Fukushima Dai-ichi accident.

- For this interface to be consistent, the definition of plant damage states needs to be common to both the PSA Level 1 and Level 2. Specifically, there is sometimes no clear agreement on the states with only partial core damage and the treatment of EOP and preventive severe accident measures during such conditions. Moreover, this issue is usually not specifically addressed in regulatory guides.
- If accidental scenarios for potential sources other than the core are investigated, an interface for “damage states” to the PSA Level 2 needs to be defined. This pertains particularly to the spent fuel pool and respective damage states. In light of the aforementioned issue partial damage scenarios for e.g. the spent fuel pool have to be included as well.

Moreover, it should be noted that there are potential sources in the plant for which fuel heat-up and melting (i.e. Level 2 issues) are not relevant at all. This includes e.g. mechanical damages to fuel assembly cladding

that are coolable by air or severe damage to radwaste processing facilities on site. These may directly lead to releases within the plant. In any case, the interface between PSA Level 1 and Level 2 (and possibly Level 3) has to be able to accommodate for these scenarios if they are considered relevant in terms of accident evolution, e.g. if they impair SAM actions due to radiation.

- The starting point of a PSA Level 2 event tree is the interface plant damage states as defined and characterized by the PSA Level 1. Interface plant damage states are defined by binning PSA Level 1 scenarios with similar properties regarding severe accident progression to limit the amount of modelling work needed for the continuation of the analyses in the PSA Level 2. For each plant damage state, a representative scenario is selected, which is then assumed in the further PSA Level 2 analysis. This is particularly relevant in the case a two-tiered approach for the PSA model is applied, where the PSA Level 1 software (and model) is actually different (or at least separated) from the PSA Level 2 software (and model). This kind of grouping or binning at an intermediary step of the PSA usually comes with a loss of information, e.g. on failed or available components or operator actions. If the representative scenario chosen for such a plant damage state is not the worst case scenario with all failures but a scenario with high importance for the interface group frequency; this can lead to optimistic assumptions on the availability of components or even systems in the further modelling of the PSA Level 2 with regard to specific binned sequences, which could e.g. be related to low probability/high impact scenarios. This deficiency might lead to overestimations of the reliability or even feasibility of specific accident management measures, and consequently might distort PSA Level 2 results for large and/or early release category frequencies. This issue could become important when analysing highly distorted plant conditions as in the Fukushima Dai-ichi case. This situation is currently changing thanks to the progress in PSA Level 2 methods and on severe accident considerations and knowledge.

Conclusions

- The scope of PSA Level 2 should be extended to include all operating modes, all events and hazards, and all relevant potential sources. National regulators should impose respective requirements.
- The screening of initiating events for detailed consideration in the PSA should be performed not only based on PSA Level 1 risk metrics but also on PSA Level 2 risk metrics like e.g. different release categories, including at least one risk metric for large releases and one for early releases. Screening thresholds on the risk measures for the Level 2 risk metrics should be defined and justified. Initiating events (including hazard scenarios) should only be screened out from the PSA, if they are screened out based on Level 1 and on Level 2 risk metrics. In addition, if a PSA Level 3 is intended, the screening process should include Level 3 risk metrics and thresholds as well.
- In order to assure consistency between the PSA Level 1 and Level 2, a common definition of “core damage” and other Level 1 interface groups shall be assumed. Moreover, partial core damage states should be considered and these should be treated consistently between PSA Level 1 and Level 2.
- In order to also take into account accidents in the spent fuel pool, appropriate definitions for these Level 1 end states, e.g. “fuel damage”, should be defined. The respective end states should be part of an appropriately defined interface to the PSA Level 2.
- The binning of sequences into Level 1 interface plant damage states should be restricted to those sequences that can be adequately and realistically subsumed into one scenario. All sequences within an interface group should have the same characteristics with regard to all branching points in the Level 2 accident progression event tree, i.e. not only with regard to severe accident phenomenology but also with regard to similar

characteristics for accident management measures and other operator actions as well as boundary conditions of the scenario.

- Concerning the initiating conditions to be considered in a PSA Level 2 (if it starts at core damage) and based on the Fukushima Dai-ichi accident conditions, situations of core melt from PSA Level 1 should be considered (in the PDS) while another or several reactors are already in severe accident conditions.
- All PSA Level 1 interface end states should be transferred to the PSA Level 2. If some end states are excluded from further analysis or are assigned to other, not fully representative groups, this should be done based on justified criteria, commensurate to the screening criteria and the objectives of the PSA. Level 1 end states with potential contributions to large or early releases should not be excluded from further analysis to the extent practicable. The latter routinely includes scenarios with containment failure prior to the accidental state (e.g. core damage).
- Accident type PSA Level 1 end states shall not be excluded from further consideration in a PSA Level 2 only based on the duration of the respective sequences up to the accidental state (“mission time”).
- As already pointed out (see PSA Level 1), grouping scenarios at different steps of the PSA process should avoid any significant “loss of memory” about the specific properties of the binned sequences [69], e.g. related to the initiating events, boundary conditions of the scenario, unavailability or availability of certain components, systems, or measures.

4.2 MEASURES AND SYSTEMS RELIABILITY AND CONDITIONAL UNAVAILABILITY FOR THE DiD LEVELS

Regarding the reliability of systems and measures in the PSA Level 2 the authors have some initial remarks. It has to be acknowledged that systems, which are assigned to DiD Levels 1 to 3 (i.e. operational systems up to design basis safety systems), can be relevant for further accident progression. This would be e.g. in the case of a previously failed operational system, which is repaired and then used during the accidental phase by manual operation. In that case, all issues already discussed for PSA Level 1 modelling are relevant as well for PSA Level 2. Conversely, certain operational or safety systems like ventilation systems usually not considered in a PSA Level 1 might open up release pathways in case of failures, which should be considered in a PSA Level 2. Moreover, there usually are dedicated systems and measures assigned to DiD Level 4. These fall squarely within the scope of the PSA Level 2, but might have been treated in the PSA Level 1 part already, if they were used to prevent an accidental state. What seems important is that the evaluation of the reliability of a given provision is made with the boundary conditions that characterize the operational state in which it is required, and those of the condition of a severe accident (DiD Level 4) are not necessarily equivalent of those that characterized the previous Level (DiD level 3).

Finally, the PSA Level 2 is restricted to on-site accident management. This, however, might be influenced by measure or events outside of the plant.

Finally, it has to be acknowledged that there was no detailed PSA Level 2 for hazard events for the Fukushima Dai-ichi units. The PSA Level 2 assessment was limited to the containment failure frequency for internal events only [99]. Consequently, there are few lessons which can be drawn directly from the accident with regard to PSA Level 2. There are, however, several issues which merit further consideration in light of the events of the Fukushima Dai-ichi accident.

4.2.1 MEASURES AND SYSTEMS RELIABILITY

The events during the Fukushima Dai-ichi accident have spotlighted several issues, which can be identified as potential weaknesses for current PSA Level 2 models based on the authors' experience. These are discussed in more detail in the following.

- The feasibility of severe accident mitigation measures is usually considered only for boundary conditions on the site and in the environment of the plant, which are reasonable during a scenario developing from an internal initiating event. Specific boundary conditions for hazard events (whether internal like e.g. fire or external like earthquake) and the effects on the feasibility of severe accident mitigation measures and the operability of respective equipment are usually not included in PSA Level 2 assessments. Indeed, reliability assessment of severe accident measures and systems done for the Fukushima Dai-ichi plant was performed under such boundary conditions. Importantly, this applied also to deterministic assessments of severe accident measures foreseen or back fitted for the units [99]. The whole issue of severe accident management and HRA for severe accident scenarios will be discussed in more detail in section 4.3 and 4.4, respectively. In this section, some fundamental assumptions for the reliability of measures and systems are further discussed.
 - By not considering the hazard impact on the site and its environment, important restrictions on the feasibility of measures and on the availability of equipment were not taken into account. Specifically, the single most important accident management measure foreseen at the plant was the restoration of AC power supply in case of a prolonged station blackout from the off-site grid. A situation, in which off-site power was unavailable for several hours or even days, was simply not anticipated. Similarly, these of a fire truck for emergency containment spray via the fire-fighting system for the containment rests on the premise that the truck can be brought into the right position on the site. This was proven to be difficult during the accident. These effects distort not only the results for Level 2 release categories but also the results of reliability assessment for the accident measures in question. Actually, a false impression of safety was instilled within the Japanese nuclear community with regard to the feasibility for said measures. This aspect will be further discussed in section 5. In any case, the boundary conditions for the feasibility and operability of specific measures or systems for accident mitigation play a crucial role. Although current regulatory guides on PSA stress the importance of assessing the reliability of systems and measures based on the plant conditions for their operation/execution, there is no extensive guidance on the specific issues discussed above. Consequently, current PSA Level 2 models have weaknesses in this regard.
 - Particularly for severe hazard impact scenarios, the conditions in the surroundings of the plant may be significantly altered compared to other scenarios. This affects e.g. access to the plant for additional emergency support staff; access to mobile resources stored off-site, the feasibility of changes of shifts, or resupply with commodities like diesel fuel or even food for on-site staff. These aspects were not considered for the Fukushima Dai-ichi plant, and they are not systematically considered in current PSA Level 2. Moreover, there are currently no specific requirements on this aspect by most regulators regarding PSA.
 - The reliability of measures and systems in accidental situations depends not only on the reliability of pre-planned actions and the availability of components, but also on operators not performing detrimental actions. During the Fukushima Dai-ichi accident operators on the site, despite their best intentions and following the operation manual, disabled e.g. the ICS of unit 1, although with hindsight this was identified as detrimental to the accident progression. Such detrimental actions

often play a role in major accidents to a larger (Three Mile Island, Chernobyl) or lesser extent. While the authors are not aware of obviously detrimental actions during the accidental phase for the Fukushima Dai-ichi accident, there is e.g. the example of external spent fuel pool cooling for unit 4, which was identified with hindsight as not urgent, thus draining resources from more advantageous actions. As already discussed in section 3.4 current PSA models lack a systematic consideration of detrimental actions. This is a weakness of current PSA Level 2 models as well.

- As demonstrated by the events in Fukushima Dai-ichi, the accidental phase and the time needed for controlling a severely damage core far exceeds a 24 hour or 48 hour fixed time window. Based on the authors' experience, several current PSA Level 2 models do have either an explicit or implicit cut-off for the scope of the modelling based on a fixed period of time. The modelling is not always extended up to a point where an accidental state has been reached which is either controlled based on justified criteria or for which further releases are demonstrated to be not relevant. This remains a potential weakness of PSA Level 2 models⁹.
- Further aspects pertain to the reliability of measures and systems with regard to DiD. For a start, most of the discussion in section 3.2.1 is directly applicable to severe accident mitigation measure on DiD Level 4. In the following, some aspects specific to the severe accident phase (DiD Level 4) are highlighted.
 - Although it has to be noted that all units were not designed to withstand severe accident conditions, the accident has exposed specific vulnerabilities in their severe accident behaviour. Most obviously were probably the weaknesses in the accidental venting function, which was not sufficiently operable under severe accident conditions so that delayed venting contributed to containment failures and subsequent hydrogen explosions in the reactor buildings. Similarly, operating rooms were no longer habitable soon after the first releases from the containment, and there were no fallback possibilities which would have allowed for remote operation of the most important systems. Moreover, there was a lack of reliable indications and measurements qualified for severe accident conditions and relevant scenarios. Unavailable or even misleading measurements and indications after the tsunami impact and particularly during the accidental phase impaired accident management measures. Such weaknesses might have been exposed with a more in-depth PSA Level 2. Moreover, there is still a lack of information about the accident progression and current state in the containments of units 1, 2, and 3.
 - The whole severe accident management strategy foreseen for the Fukushima Dai-ichi plant assumed the short-term availability of electric power, either from the grid or from other units. It has to be noted, though, that these power sources should be assigned to safety functions on DiD Level 1 to 3. Moreover, in order to utilize these sources working electrical cabinets and switchgears as well as related I&C have to be assumed. More detailed investigations could have exposed the level of interdependencies between the DiD Levels.
 - The high level of attentions to the spent fuel pool of unit 4 has highlighted the problem of simultaneous/correlated severe accident scenarios in the core and in the pool. Such a scenario would pose specific restrictions on mitigative actions, e.g. in the use of single redundancy severe accident measures like a mobile pump. Moreover, such a scenario would impact heavily on PSA Level 2 end

⁹ Note: This issue was already identified in ASAMPSA2 [69].

results as the source terms would be quite different - and possibly larger. Based on the authors' experience, a lack of investigations into spent fuel pool scenarios in general and into simultaneous spent fuel/core melt sequences in particular is a weakness of most current PSA Level 2 models.

- The issue of multi-unit sites with regard to the assessment of DiD Level 4 capabilities has been brought to the attention by the accident as well. Specifically, simultaneous accidents might challenge the assumed availability of systems or measures on DiD Level 4. As an example, cross-connections between the power supplies of different units were an important element of Fukushima Dai-ichi severe accident mitigation measures for coping with extended SBO for a single unit. Similarly, certain equipment foreseen for use in a severe accident situation was present with less than six redundancies like for e.g. fire trucks for emergency injection into the containment with 3 trucks on site for in total 6 units [99]. Additionally, the accident highlighted the availability of staff sufficiently trained to manage severe accident situations, which was one bottleneck on the Fukushima Dai-ichi site initially. The limitations due to shared resources for severe accident management are usually not included in the scope of current PSA Level 2 models to the best knowledge of the authors. Moreover, there are no specific regulatory requirements on this issue. Thus, this is another potential weakness of PSA models.

With regard to DiD assessment with PSA methods it should be recognized that DiD Level 4 as understood e.g. in WENRA Reference Levels [97] and IAEA SSR 2/1 [55] is aimed at mitigating the consequences of a severe accident, whereas DiD Level 5 is dedicated to off-site consequences. Thus, the end-points of a PSA Level 2, i.e. release categories, are at the boundary of DiD Level 4 considering the success of the corresponding “layer of provisions”.

Conversely, the interface plant damage states of PSA Level 1 are usually on the boundary from DiD Level 3 to DiD Level 4. In IAEA SSR 2/1 (Rev.1) [120] it is clearly stated that

“The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident.”

The key concern is the definition of the “severe accident” (fuel damage, partial or whole core melting) but once this metric defined, the interface plant damage states of PSA Level 1 are on the boundary from DiD Level 3 to DiD Level 4. Therefore, PSA Level 2 results sometimes can't be used directly for DiD Level 4 assessments.

However for dedicated mitigative measures or systems, which are only executed or operated after a core damage state has been reached, PSA results on e.g. system reliability may be applied directly. In this respect, PSA Level 2 models are often better tailored to PSA assessments of DiD than Level 1 models.

Conclusions

Based on the aforementioned discussion, the authors arrive at several recommendations as given in the following:

- The feasibility, operability, and reliability of severe accident mitigation measures should be systematically analysed with PSA Level 1 and PSA Level 2 models. This includes, but is not restricted to the evaluation of hazard impact on the site and the availability of off-site resources. Particularly, the availability of off-site electric power and the ultimate heat sink in the long term should be critically examined.

- Assessments of DiD Level 4 measures and systems should be done taking into account adequately detailed and comprehensive PSA model results. Particularly, the DiD Level 4 assessments should consider all operating modes and internal as well as external hazards.
- The degree of dependency of severe accident measures or systems to other (design basis) safety functions or measures, or to accident sequence boundary conditions, or even to other severe accident measures should be investigated using probabilistic methods. To the extent practicable, information about failed systems or components during the accidental scenarios from PSA Level 1 should be taken into account.
- Critically important instrumentation and measurements should be investigated using PSA methods on their availability during severe accident scenarios including scenarios developing from severe hazard impact. Importantly, adequate instrumentation and measurements should be available to the operators and crisis management crew for identifying, monitoring and assessing accidental situations in the reactor core and the spent fuel pool. Conversely, failure of such instrumentation and measurements should be part of PSA Level 2 models.
- PSA Level 2 analyses should systematically investigate potential detrimental actions or decisions by operators and additional emergency centre staff, which might aggravate an accidental scenario. To the extent practicable, such possibilities should be identified and included into PSA Level 2 models.
- PSA Level 2 models should consider the effect of (near) simultaneous accidental scenarios in the spent fuel pool and in the reactor core on the availability and reliability of dedicated systems or measures.
- PSA Level 2 modelling should be extended (like PSA Level 1 modelling) until either a controlled accidental state has been reached, e.g. if containment failure can be practically excluded, and/or until further additional releases can be demonstrated to be not relevant [13]. Respective criteria should be defined and justified for the PSA Level 2. Further independent failures should only be considered, if they are likely in the period of analysis and would significantly worsen the situation. This particularly applies to certain hazards. For example, the risk of strong aftershocks affecting the operability of key systems, whose structure may already be compromised [10], should be analysed in seismic PSA.
- For multi-unit sites, the dependencies between the units should be systematically included into the PSA Level 2 model. This includes, but is not restricted to, common parts of safety, support or operational systems, capacity and availability of common accident mitigation measures or systems for multiple units, availability of staff for performing measures in case of simultaneous accidental situations, effects of an accidental scenario in one unit on other units and the staff, etc.

4.2.2 MODELLING AND ASSESSMENT ISSUES

In this section, specific issues relate to PSA Level 2 modelling and assessments are discussed. However, PSA issues on severe accident measures and HRA are discussed in sections 4.3 and 4.4, respectively. In addition, most issues discussed already in section 3.2.2 for PSA Level 1 can be transferred to PSA Level 2. Nonetheless, there are some issues worth mentioning for PSA Level 2 modelling and assessment in light of the Fukushima Dai-ichi accident.

- The hydrogen explosions in the reactor buildings of units 1, 3, and 4 have underscored again the importance of adequately modelling the risk contribution of hydrogen deflagrations or detonations during a core melt scenario. While this issue has long been recognized as important for PSA Level 2, most models restrict the analysis to potential explosions within the containment or after containment failure. Some PSA models did investigate the respective risk for hydrogen in e.g. the venting lines. The accident development emphasized

the potential relevance of hydrogen explosions in rooms adjacent to the primary containment (i.e. reactor building) or connected via common air ducts (e.g. venting line). Although these explosions might not endanger primary containment integrity, they pose a significant risk to staff on the site. Consequently, accident mitigation can be hampered. Based on the authors' opinions, this is still an area with need for improvement for current PSA Level 2 models. Moreover, this can be an issue for further plant modifications for improving severe accident capabilities.

- Another issue relates to the modelling of long-term SBO scenarios in PSA Level 2. Based on the authors' experience, often (common cause) failures of specific components e.g. diesels and circuit breakers are assumed. Such a failure scenario might be adequate for internal events. For hazard events, more complex failure scenarios that affect whole cabinets, switchyards, and the related I&C are at least as relevant. These complex failure scenarios can prevent dedicated accident management actions which would otherwise be possible. Based on the authors' experience, PSA Level 2 models usually do not include a sufficiently detailed modelling of component failures to ensure that these effects are captured by the modelling itself. Indeed, this is an area for which proven methods are lacking. Consequently, this is an area of potential weaknesses for current PSA models as well as PSA Level 2 methodology.
- Complementary to the extension of the period of analysis (see above), the mission times for accident mitigation measures or systems have to be adapted in the PSA Level 2 modelling. Currently, component reliability models often assume fixed mission times in the range of at most several tens' hours. These time periods might be insufficient in order to demonstrate that a controlled state after an accident has been reached. In any case, these time periods are often inconsistent with the boundary conditions imposed by the specific accident sequence. Moreover, with extended mission times there can be increased demands on support systems (e.g. cooling, lubrication), fuel or power supply systems (e.g. batteries, compressed-air cylinders), or refilling of consumables like diesel fuel or water in storage tanks. These boundary conditions also affect the availability of measures. Based on the authors' experience, there is still room and necessity for improvement in current PSA Level 2 models on the aforementioned issues.
- Concurrently with extended analysis periods, the potential relevance of component and system repair is increased. Based on the authors' experiences such (beneficial) actions are usually not considered in current PSA Level 2 models, because the time needed for repair actions with a high chance of success under adverse conditions is often larger than the analysis time of the PSA Level 2. This conservative approach might no longer be merited in case of extended mission times, for which at least reasonably simple repair actions might have a good chance of success. Nevertheless each repair action modelling having a large impact on PSA Level 2 results has to be appropriately justified (e.g. availability of repairing components and staff). There is still a lack of effective modelling approaches for this issue of how to model appropriately the increasing chance of repair with time.
- Some PSA Level 2 analyses end with containment failure modes, as was the case for the models of the Fukushima Dai-ichi units. The analysis is typically carried on until all phenomena challenging the containment are over, within typical time scales of one to several days. However, when no source terms are defined, and respective criteria are lacking, there is neither any information about the release categories nor any assurance that accidental releases are covered until they become insignificant [69]. Indeed, the limitations of the modelling do not guarantee that all measures and phenomena with significant impact on release characteristics (amount and composition of radionuclides, release rate over time, etc.) are included in the modelling. In this respect, such Level 2 models might be of limited use for evaluating accident measures aimed at reducing releases.

- One issue highlighted by the accidents is the potential relevance of releases to the ground or to water in addition to aerial releases. Usually, only the latter are considered for defining (and assessing) release categories of a PSA Level 2. However, the accident at Fukushima Dai-ichi NPP has again reinforced the relevance of additional release pathways for the environmental impact. This is an area where many PSA Level 2 models can be improved based on the authors' experience [2]. Moreover, this issue is not specifically treated in related regulatory guidance (exception maybe in France, with importance given to the prevention of base mat penetration for Gen II reactors).
- For multi-unit sites, commonly used parts of systems, be they safety or operational systems or parts dedicated to severe accident management, are often considered in PSA models. However, for a lot of sites with multiple units - probably with exception of PSAs for CANDU type reactor sites - there usually is no explicit modelling of common system dependencies between different units at the fault tree/event tree level. Moreover, this issue is not clearly and specifically addressed in most regulatory guides on PSA. Consequently, there is still room and possibility for improvement for current PSA Level 2 models. Actually, there is a lack of methods for performing a site PSA for multi-unit sites [13]. Such site risk models are particularly important for scenarios which impact the site as a whole, e.g. most severe hazard impact event, and which can lead to complex scenarios simultaneously affecting several units.
- The issue of partial core damage states (or similar accidental states) at the interface from PSA Level 1 has already been raised. It should be noted, though, that such accidental states lead to specific event sequences with different success criteria for mitigative systems' performance, both in regard to preventing an aggravation into a more severe accidental state as well as in regard to maintaining containment integrity. Based on the authors' experience, current PSA Level 2 models are rarely sufficiently detailed to treat these specific properties. Moreover, there is no specific regulatory guidance on the treatment of partial core melt states in PSA Level 2 models. Consequently, this is an area for further improvements, and also an area for further improvement of methods.
- PSA Level 2 results are often associated with broad uncertainty bands (more than one order of magnitude) based on the authors' experience. This is even exacerbated for rare scenarios from e.g. severe hazard impact events, which themselves come with large uncertainties. This may affect the explanatory power of PSA Level 2 results, e.g. for decision making (cf. section 5). Effort to reduce these uncertainties is clearly merited. With regard to PSA modelling, it is important to actually include uncertainties into the models and provide traceable justifications on the Level 2 sources of uncertainty. Moreover, since there are also qualitatively different sources of uncertainty (lack of data, expert judgement, model uncertainty, etc.), the aggregation of uncertainties needs to be done with care. On these issues there is still room for improvement at PSA Level 2.

Conclusions

- The potential risk from all combustible gases detonation or deflagration should be investigated systematically. The risk of hydrogen detonations or deflagrations should include the risk from hydrogen accumulations outside of the containment, e.g. in the reactor building or in the venting lines as part of the PSA Level 2. In that respect, gas leakages from the containment and air ducts/ventilation lines should be investigated. If practicable, plant improvements should be realized to minimize the risk of hydrogen explosions. However, other combustible gases, such as carbon monoxide, which can be produced during molten core-concrete interactions, may also impose potential threat to hermetic containment integrity and should be investigated. The performance of hydrogen recombiners shall be analyzed and taken into account.

- Complex failure scenarios, which are especially relevant for severe hazard impact, should be adequately considered in the PSA Level 2 modelling. Specifically, these scenarios need to be considered in the reliability assessment of severe accident measures in case of hazard impact. There is a need for developing effective modelling approaches.
- PSA Level 2 models should include source term assessments for the release category end states. Branches in the accident progression event tree should be defined also in the light of the impact of systems, measures, or phenomena on release characteristics. Models limited to containment failure assessment should be extended as practicable.
- The mission times for accident mitigation measures needed to reach a controlled state after an accident should be used in the reliability assessment of components and as basis for HRA of operator actions.
- PSA Level 2 models should be extended to the extent practicable to include repairs of previously failed systems or components. The longer PSA Level 2 analysis and mission times become, the more important is the consideration of such repairs. Each repair action included in the modelling needs to be properly justified. Moreover, effective modelling approaches should be developed for this issue.
- PSA Level 2 models should include extended analysis times in the reliability models for systems, components and actions needed during the accident progression. Dependencies with support systems or supporting measures (like refilling fuel or water storage tanks), especially if induced by a longer mission time, should be systematically investigated and included into the Level 2 models to the extent sensible.
- For multi-unit sites, commonly used systems and resources should be systematically treated within the PSA Level 2 model. Most importantly, relevant restrictions on the availability or reliability of systems or resources have to be identified and included into the model. To the extent sensible and practicable, a site risk Level 2 model should be developed, especially for events which affect the whole site. In this regard, there is still need for further research on methods and good practices.
- PSA Level 2 models should include specific modelling related to partial core damage states and similar accidental states. Particularly, branches for the transitions into more severe states (e.g. full core melt) should be included in the APET with adequate success criteria for systems or measures.
- PSA Level 2 models should be extended to releases via the ground or to water in addition to aerial releases. Respective pathways need to be identified, releases need to be quantified. Consequently, necessary changes of the accident progression event tree modelling should be implemented in the models. This should be done on the basis of characteristics for dedicated release categories.
- PSA Level 2 results should include all sources of uncertainty. Large uncertainties for PSA Level 2 elements and results should be identified and reduced to the extent practicable. Additionally, relevant information on the effect of specific uncertainty sources on PSA results should be provided by sensitivity analysis.

4.3 SEVERE ACCIDENT MANAGEMENT PROCEDURES/GUIDELINES AND EVENT SPECIFIC BOUNDARY CONDITIONS

This section briefly discusses specific issues for severe accident management procedures and guidelines in light of the Fukushima Dai-ichi NPP accident. Importantly, the accident was characterized by a prolonged accidental situation on the site and an extended period of time for which severe accident measures had to be implemented and/or maintained. Some of the insights related to that aspect have already been discussed in section 4.2, so far

as they are relevant for PSA Level 2 systems reliability or modelling; and issue for HRA are discussed in section 4.4. In addition, the insights from section 3.3 for PSA Level 1 related issues can be transferred also to PSA Level 2.

After these remarks, the following issues are considered by the authors for further discussion.

- One insight from the analysis of the accident is that TEPCO staff was convinced of the effectiveness of the severe accident measures defined for the plant [99]. One contributing factor was the lack of comprehensive reliability assessments for these measures, e.g. under severe hazard impact boundary conditions. Based on the authors' experience, PSA assessments of severe accident management measures have in the past exposed potential vulnerabilities of the plant or the measure under consideration, raised awareness about the limitations of the respective measure and contributed to improving procedures and guidelines. There is, however, still room and necessity for improvement using PSA Level 2 insights for the assessment of foreseen or established SAMG, particularly with respect to hazard scenarios.
- Mobile equipment often is a critical element of mitigative accident management measures, because the physical separation usually protects it from the event/scenario, which led to the accidental situation. The Fukushima Dai-ichi accident gives good examples of scenarios, for which mobile equipment can't be successfully utilized due to e.g. blocked transport ways, inaccessibility of connection points, life-threatening danger related to potential accidental releases or further hydrogen explosions. These aspects were not considered in the assessment of measures for the plant [99], and based on the authors' experience are not considered in current PSA Level 2 models.
- Multi-unit site effects have impacted on the severe accident management measures during the accident. This underscores again the importance of considering all dependencies between the different units also for SAMG, i.e. dependencies due to commonly used systems or support systems, shared resources including operating personnel, impact on the accessibility and or operability of components or systems for the specific measures due to accidental conditions including releases in one unit, etc. There is potential for improvement for current PSA Level 2 models. This issue has also been discussed in section 4.2.
- Event specific boundary conditions, e.g. complex failure scenarios resulting from hazard impact, will influence the assessment results for specific accident management procedures. This has been demonstrated by the events during the Fukushima Dai-ichi accident as well. If assessments of severe accident management measures are performed with generic assumptions which can be optimistic for certain scenarios, this may lead to misleading, non-realistic optimistic results. Based on the authors' experience, a sequence specific assessment of measures, including specific HRA assessments, has not been performed for all current PSA Level 2 models. Based on the authors' experience current PSA Level 2 models can be enhanced in this regard.
- The accident at Fukushima Dai-ichi NPP gave salient examples about the importance of maintaining containment integrity in case of a core melt scenario. This is also the objective of important mitigative measures. The authors' acknowledge that assessing the risk of containment failure modes has always been one of the main objectives of PSA Level 2. Nonetheless, the accident reinforces its relevance, also for assessments related to DiD Level 4 and the independence of related measures foreseen on DiD Level 4 to other measures or systems on DiD Levels 1 to 3.

Conclusion

- Severe accident management measures should not only be included in PSA Level 2 models to the extent practicable, but conversely should also be checked and assessed with PSA Level 2 methods. Vulnerabilities and potentials for improvement found during such assessments should lead to the consideration of further improvement of plant safety.
- Severe accident management measures should be modelled and quantified within the PSA Level 2 based on scenario-specific boundary conditions to the extent practicable.
- Probabilistic investigation for mobile equipment should systematically identify and assess situations and scenarios, for which such equipment can't be successfully deployed. Exemplary reasons include blocked transport roads, access corridors, gates, collapsed constructions, inaccessibility of connection points, and common cause failure impact.
- Mitigative measures for maintaining containment integrity under accidental conditions should be systematically included into PSA Level 2 models. In addition, PSA methods should be used to demonstrate adequate independence of these DiD Level 4 measures from measures or systems on other DiD Levels.

4.4 HUMAN RELIABILITY ASSESSMENT AND EVENT SPECIFIC BOUNDARY CONDITIONS

HRA for PSA Level 2 considers post-core damage human actions aimed at preventing or mitigating radioactive releases to the environment. In the PSA Level 2 framework, HRA is used to determine Human Error Probability (HEP) values that reflect the reliability assessment of human actions under consideration of both decision-making error and error in the implementation of accident management measure actions. In general, PSA Level 2 applies the same HRA methodologies that can be used also for PSA Level 1. Therefore, the respective discussions in section 3.4 can be transferred also to PSA Level 2. In the following, HRA aspects specific to accidental situations (after e.g. core damage) are discussed.

As already discussed in section 3.4, current HRA methods are usually not well adapted for assessing complex situations, which require knowledge-based behaviour, which are evolving dynamically, at which operators act under very high Levels of stress, or when there is sufficient time for performing (complicated) actions like e.g. repairs of failed components. Consequently, it can indeed be questioned whether the methodologies used in HRA in PSA Level 2 can account for circumstances such as those present during the Fukushima Dai-ichi NPP accident. This is elaborated further in the following.

- HRA needs to include a more comprehensive and realistic assessment of influence of long-term post-core damage events. Long-term post-core damage sequences invoke new issues regarding the timing of operator actions. For example, in the Fukushima Dai-ichi NPP accident, the opening of containment vent valves was unexpectedly delayed by several hours by: 1) waiting for a nearby town to be evacuated, 2) hardware failures, and 3) harsh environment conditions that developed during the waiting time. It was also noted that the arrival of additional resources (e.g. from offsite) did not ensure rapid situation control. For these prolonged scenarios, potential time delays need to be accounted for in a realistic manner. The lack of contingency

procedures and pre-staged equipment impacted operator actions, so that operators had to operate outside the procedural space or formal training. Relevant performance shaping factors, such as fatigue (e.g., operators in the Fukushima Dai-ichi NPP event had long shifts with minimal food and rest) and “stress” in a very real sense (Fukushima Dai-ichi NPP operators were clearly worried about their personal safety e.g. due to potential hydrogen explosions and because of irradiation and contamination on the site, facing the dilemma of social safety or loss of assets [99]). Another potentially important aspect of long-term scenarios is the impact of shift changeover on the reliability of measure. Shift changeovers may lead to a loss of information or situational awareness, thus inducing additional sources of human error.

- Due to the on-site contamination and high radiation Levels in the accidental phase, staff had to perform actions under protective equipment and under high time pressure [99]. This aspect is not adequately addressed by current HRA methods - partly due to a lack of data. Based on the authors’ experience and the results of the ASAMPSA_E questionnaire [119], there is a need for further research on this issue.
- The accidental situation at the plant was characterized by a very complex picture of unavailable or outright destroyed systems and components, inaccessible areas, failed accident management equipment, etc. Moreover, information on the state of the units and the progression of the accident was mostly either lacking or even misleading (I&C failure; e.g. reactor water Level indications [99]). Operator guidance used in such scenarios (e.g., SAMGs) can call for a knowledge-based decision among a set of difficult choices and does not provide the same degree of direction as the Emergency Operating Procedures addressed in HRA for PSA Level 1. Moreover, SAMGs may not cover situations faced by the operators. Such situations have arisen during the Fukushima Dai-ichi NPP accident. For example, during containment venting, there were “a lack of contingency procedures for operating the vent system without power, as well as the lack of pre-staged equipment, such as an engine-driven air compressor” [102], p. 11, contributing to the delay in venting.
- For multiple-unit sites, there are specific issues for HRA for accident scenarios. One obvious concern is the potential impact the accident progression in one unit to measure for another unit as exemplified by the impact of the explosion in e.g. unit 4 (cf. also section 3.4). These specific performance shaping factors are usually not yet considered and not well understood. In addition, simultaneous accident in multi-unit sites can impose restrictions on the number of staff available for performing specific actions or time intervals during which these actions have to be performed. These aspects are usually not included in HRA assessments as well.
- As seen during the Fukushima Dai-ichi accident, in these situations there are typically multiple decision makers on-site (shift supervisor of a unit, head of on-site crisis centre) and off-site (utility crisis centre and senior management, local and national civil protection agencies, provincial and national government executives up to the Prime Minister) [99]. The treatment of different or multiple decision makers, including their interactions potentially resulting in distractions of plant personnel, is usually not considered in PSAs. The Fukushima Dai-ichi accident illustrates that: 1) decision makers might include government officials, 2) decision makers outside the control room can make mistakes (due to, for example, lack of understanding of the event-specific plant conditions, as well as NPP operations), and 3) organizational responsibilities may not be clear. Post-core damage sequences are further complicated by missing information (e.g. accurate containment pressure indications) and other instrument failures that are not expected or trained on. This can then lead to errors in the prioritization of the work, impose additional strains on critical on-site decision makers, and induce delays in the execution of severe accident mitigation measures. Based on the authors’ experience, current HRA methods are not well suited to capture such difficult decision making processes. Moreover, this aspect is usually not included in the scope of PSA analyses.

Conclusions

- HRA for PSA Level 2 should be extended to the extent practicable to consider long-term effects of accident scenarios, particularly performance shaping factors like fatigue or increased stress Levels, and the effects of shift changeover. HRA practitioners should participate in research on these issues.
- HRA for PSA Level 2 should consider performance shaping factors induced by exposure to irradiation and contamination as well as effects of related protective equipment and the need to perform actions on-site as quickly as possible. HRA practitioners should participate in research on these issues.
- HRA for PSA Level 2 should systematically analyse knowledge-based decisions and actions for mitigating an accident. PSA Level 2 should be extended to the extent practicable to cover such knowledge-based measures. Similarly, the potential for detrimental knowledge-based actions should be analysed and considered. Quantitative assessments should be treated under due consideration of their limitations. Consequently, HRA practitioners should participate in research on these issues.
- For multiple-unit sites, specific HRA of the actions and activities to be taken by staff shared between the units during a simultaneous severe accident should be performed.
- The potential impact of multiple decision makers (e.g. in the crisis organization) on the performance of severe accident measures should be considered in the HRA for the respective measures to the extent practicable. HRA methods for an efficient and reliable analysis of crisis organizations (internal and external to the site) should be developed. Their results should be integrated in PSA Level 2 models if relevant.

4.5 LESSONS LEARNED FOR LEVEL 2 PSA

This section summarizes the main lessons learned on Level 2 PSA based on the conclusions in the previous sections (see above). Following the topical structure of this section, the main insights regarding the different topics are given below.

4.5.1 INITIATING EVENTS AND COMBINATION OF RARE EVENTS

The Fukushima Dai-ichi NPP accident justifies the basic assumption of the ASAMPSA_E project of extending the scope of PSA Level 2 to include all operating modes, all events and hazards, and all relevant potential sources like e.g. the spent fuel pool. Consequently, all PSA Level 1 end states at the interface to the PSA Level 2 should be transferred to and treated within Level 2. Specifically, PSA Level 1 states with containment failure prior to core damage, e.g. due to hazard impact, should routinely be transferred. Moreover, the grouping and binning of interface states should be made not only in consideration of severe accident phenomenology but also regarding severe accident management measures and event boundary conditions. Any grouping into such intermediary states should be done in a way that avoids the loss of information about sequence characteristics like initiating events, availability of components or measures, and boundary conditions of the sequence to the extent practicable. Finally, screening of initiating events for the PSA should be done not only based on Level 1 risk metrics but also on adequate PSA Level 2 risk metrics including at least one metric for large releases and one for early release.

4.5.2 SYSTEMS RELIABILITY AND CONDITIONAL UNAVAILABILITY FOR THE DID LEVELS

PSA Level 2 models should be used to systematically analyse (mitigative) severe accident management measures in order to identify their limitations and potential weaknesses or areas for further improvement. Such analyses should be done for also (multiple) hazard impact scenarios and under consideration of the potential unavailability of off-site resources like power supply from the grid (off-site power supply) or unavailability of additional crisis response staff. The degree of dependency of severe accident measures or systems to other (design basis) safety functions or measures, or to accident sequence boundary conditions, or even to other severe accident measures should be investigated. In particular, the effects of the unavailability of critically important instrumentation or measurements need to be considered. The analysis should be extended to likely detrimental or aggravating actions, which operators or crisis management staff might erroneously derive based on their knowledge, existing SAMG and the available information during the accident.

Moreover, the scope of the accident sequence analyses should be extended until either a controlled state has been reached or until a state in which no additional releases is expected. In this respect, modelling of releases up to adequate release categories should be part of any PSA Level 2. Moreover, besides releases in the atmosphere also other release vectors (water, ground) should be considered. Containment failure and containment failure modes need to be treated comprehensively for the different accidental scenarios. All relevant release pathways, including those opened e.g. by hazard impact, should be part of the model.

Extended analysis times should be reflected in reliability assessments for systems and components - and their supporting systems - but also in HRA for operator actions. This should include the assessment of repairs to the extent practicable. Further challenges to the plant (e.g. aftershocks after an earthquake) should be considered in the model if they are sufficiently likely during the analysis period for the sequence and could impact on Level 2 results.

For multi-unit sites it is necessary to include all relevant dependencies into the PSA Level 2 model. This entails common systems or supporting systems, staff resources, mobile equipment, etc. To this end and for adequately covering complex scenarios simultaneously affecting several units, site risk PSA Level 2 models should be developed. Respective methods and tools need to be improved.

Large uncertainties for PSA elements and results need to be reduced to the extent practicable. In addition, results of sensitivity analysis should be used to provide relevant information on the influence of different sources of uncertainty on the PSA Level 2 results and their uncertainties.

Finally, the assessment of DiD Level 4 measures and systems should be done taking into account adequately detailed and comprehensive PSA model results. Particularly, the DiD Level 4 assessments should consider all operating modes and internal as well as external hazards.

4.5.3 SEVERE ACCIDENT MANAGEMENT PROCEDURES/GUIDELINES AND EVENT SPECIFIC BOUNDARY CONDITIONS

Several lessons learned on severe accident management have already been presented in section 4.5.2. In extension, severe accident management measures should be systematically included in PSA Level 2 under consideration of respective scenario-specific boundary conditions. Moreover, severe accident management measures and guidelines should be checked with PSA Level 2 methods on reliability, for identifying weaknesses in procedures as well as vulnerabilities of the plant and potentials for improvements. Simultaneously, PSA Level 2 results should be used to demonstrate reliability and adequate independence of DiD Level 4 measures. The objective of these assessments should be strengthening DiD (Level 4) in terms of performance and reliability of severe accident management.

4.5.4 HUMAN RELIABILITY ASSESSMENT AND EVENT SPECIFIC BOUNDARY CONDITIONS

For HRA, most of the lessons learned for the PSA Level 1 and discussed in section 3.5.4 can be transferred to PSA Level 2. Particularly with regard for HRA for PSA Level 2, it is necessary to consider performing shaping factors like exposure to high radiation fields, actions with protective equipment, and long term effects like fatigue or the effect of shift changeover. Since knowledge-based decisions and actions under stress play an important role during the accidental phase, they should be analysed with HRA methods. This extends to the assessment of potential detrimental or aggravating actions. In addition, the PSA Level 2 should consider the impact of multiple layers of decision makers internal to the plant (e.g. crisis organization) and external to the plant (e.g. company headquarters, government officials) on the accident management measure. As commonly accepted HRA methods are lacking on most of the aforementioned issues, HRA practitioners should participate actively in the related research.

5 USE OF PSA RESULTS IN DECISION MAKING

It is, of course, easy to be prudent in hindsight. Especially with regard to lessons learned from the decision making in the time before the Fukushima Dai-ichi accident, some well-known aspects (fallacies) of the human mind have to be mentioned as a start. Of particular importance are hindsight bias¹⁰, confirmation bias¹¹ (especially related to group think), oversimplification¹² as well as a number of probability-related fallacies (e.g. pseudo-certainty effect¹³, gambler's fallacy¹⁴, etc.). These have affected both the decision making before (and during) as well as the analysis of the accident after the fact - and they also apply to the authors of this report. However, in-depth discussions of representative heuristics are not the topic of this section. Instead, recommendations on improving decision making using PSA in light of the Fukushima Dai-ichi NPP accident are sought. And in order to form these recommendations, the authors have tried to include awareness about the aforementioned fallacies into their reasoning.

As a further preliminary remark, there is rather comprehensive guidance on the use of risk information, and in particular PSA information, in safety related decision making. The related concepts are usually subsumed into (integrated) risk-informed decision making (RIDM). Relevant publications include IAEA GSR Part 4 [54] and particularly INSAG-25 [105]. A good overview over a RIDM process in line with INSAG-25 gives the following Fig. 11. The generic process is commonly accepted and fits to the specific national approaches on RIDM, because it only excludes so called "risk based" decision making, which would define decision more or less exclusively on their expected utility as determined by a risk model, and decision making approaches neglecting all risk information. There is, however, no consensus in the scientific community and between licensees and not even between national regulators worldwide on the specific boundary conditions and criteria to be applied in such a RIDM process. Consequently, there are different probabilistic safety criteria and thresholds in use (e.g. [107]) or the relevance and use of PSA results in decision making (e.g. [108]). There are different requirements on the scope and level of detail of PSA studies for the support of safety-related decision making [108]. Moreover, the authors emphasize that a consensus has not yet been established even with the lessons learned from the Fukushima Dai-ichi accident. This report wants to contribute the view of the ASAMPSA_E project on some selected issues.

¹⁰Hindsight bias describes the tendency that humans will judge an event by its (known) outcomes. Consequently, the limitations of the decision makers in terms of knowledge and uncertainty are not adequately appreciated.

¹¹ Confirmation bias describes the tendency of humans to filter new information preferably for those bits and pieces that confirm their preconceptions and to ignore those parts that challenge or even contradict their preconceptions.

¹²For complex situations like the Fukushima Dai-ichi accident the tendency of humans to concentrate on specific aspects, compartmentalize and thus losing the view for the whole of the picture.

¹³ The tendency to make risk-seeking decisions to avoid (expected) negative outcomes, while making risk-averse decisions for (expected) positive outcomes.

¹⁴ The tendency for assuming a return period for random events where there is none (or in the case of Fukushima rather if it hasn't happened before it won't happen soon).

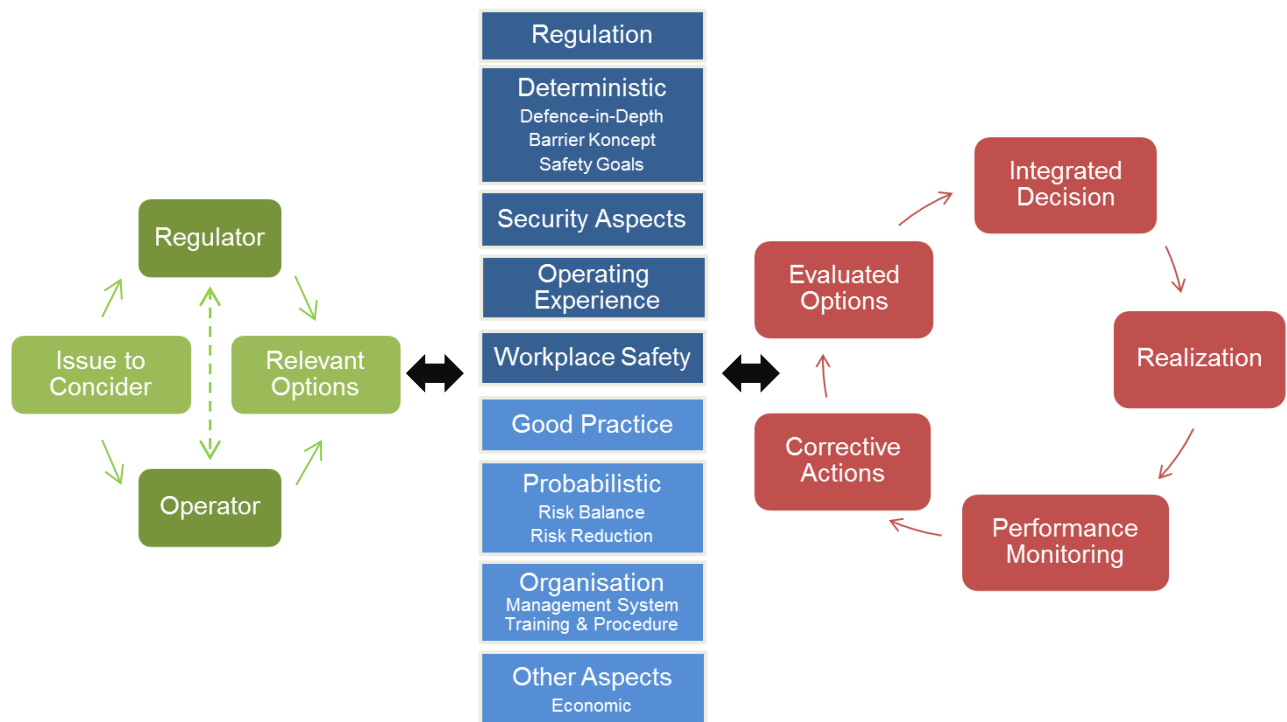


Fig. 1 Schematics of RIDM process in line with INSAG-25, taken from [106]

With respect to the use of PSA in decision making for the Fukushima Dai-ichi accident, there are some rather interesting aspects.

As already mentioned there was no detailed probabilistic analysis of beyond design basis risk for tsunamis (and correlated seismic events). Interestingly though, TEPCO updated assessments of the tsunami run-up height frequency of exceedance, which showed that potentially relevant scenarios could happen with a frequency comparable to or even larger than the CDF and CFF figures determined by internal events PSA models [99], albeit using tsunami hazard models not officially endorsed by the Japanese nuclear community. But this did not trigger further in-depth investigations; neither deterministic assessments of the design extension/beyond design basis accident range (cf. e.g. [55], [97]), nor probabilistic assessments were performed [99]. The latter decision is of interest here, and was explained with -amongst others - the following reasons. [99], [96].

- There was no officially endorsed tsunami PSA method. Thus, TEPCO was sceptical about the preliminary results and waited for external organizations like the Japan Society of Civil Engineers and updated regulatory guidance before taking potentially costly decisions. Moreover, the uncertainties associated with the beyond design tsunami hazard frequency of exceedance as determined by TEPCO were regarded as very high and the results to be unreliable.
- Further investigations of seismic hazard, e.g. Kashiwazaki-Kariwa NPP after the 2007 earthquake, limited TEPCO's resources for such analyses. This led to a postponement of further tsunami hazard investigations.

- As evidenced by plant improvements considered by TEPCO for mitigating tsunami risk after updates of tsunami hazard frequencies, TEPCO's staff and decision makers were aware of the basic weaknesses of the plant against external flooding. Consequently, there was a strong and partly subconscious motivation of not exposing such weaknesses to stakeholders (e.g. local communities) [96].
- The Japanese nuclear community had communicated to the public consistently that severe accident would "never" happen in their plants [96]. This had two effects. First, TEPCO staff (and the vast majority of the Japanese nuclear community) believed in their own propaganda. Second, TEPCO's staff was reluctant to release any information that could contradict this picture even to the regulator.
- The effects of confirmation bias and e.g. pseudo-certainty effect on decision makers should not be discounted.

It is important to point out that within the context of the decision it was not obviously wrong. The authors, however, disagree with the decision not to perform at least an exploratory PSA assessment. This is related to the use of PSA results in decision making and merits further discussion.

One approach of the use of PSA and its results in decision making assumes that PSA quantifies the level of risk from accidental releases for the nuclear facility. The systematic approach of PSA allows for detecting plant vulnerabilities and determining whether these amount to a level of risk unacceptable within the design basis of the plant. Often, the design basis level of risk is set by the regulator or amounts to the level of risk accepted with the original license of the plant¹⁵. If the risk is below that threshold, which does pertain to all beyond design basis accidents, PSA results might be used for cost-benefit analysis on the utility of corrective actions/safety improvements. Thus, mean values of PSA results are often the main results, while the underlying uncertainty distributions might play a minor role. In this context, quantitative PSA results should be sufficiently valid. Inaccurate or overly conservative results might induce potentially costly burdens on the licensee (who is responsible for performing plant specific PSA), whereas more refined assessments might fail to support the utility of these decisions. Especially with regard to rare events and accidental scenarios, which are demonstrated to be clearly below the accepted accidental risk threshold, there is no inherent need for (also costly) detailed probabilistic analyses, nor there a need to react to potential plant vulnerabilities for these scenarios.

Another approach to the use of PSA and its results in decision making assumes that the main purpose of PSA is identifying and assessing potential plant vulnerabilities, which would not be detectable e.g. by deterministic approaches. Quantitative PSA results are used for the ranking of different risk contributions and as supporting evidence for the effectiveness of proposed plant improvements. The risk level itself is used more as an informative figure and for determining those scenarios which can be practically excluded. Complementary to that approach there are often conditions, where the regulatory framework requires or informal agreements incentivize further plant improvements even in the beyond design basis risk area. Decisions on such improvements are taken more in the light of the effectiveness of these measures for highly ranked risks and the resulting improvements in the risk profile than on cost-benefit utility.

¹⁵ The importance of the risk accepted by the regulator with the operating license of the plant is rooted in administrative law principles. Basically, administrative bodies should not impose additional duties on a licensee or change conditions of the license without sound justification based on new evidence.

The two aforementioned positions are certainly extremes of a spectrum in risk-informed decision making (RIDM) approaches and most countries fall somewhere in between. However, the situation in Japan prior to the Fukushima Dai-ichi accident and the background of the decision makers was more similar to the former than to the latter approach. From the authors' point of view, the Fukushima Dai-ichi accident puts that position into question. There is a widespread agreement that even exploratory assessments of the risk for beyond design tsunamis would have exposed the plant vulnerabilities in that regard (placement of emergency diesel generators, flooding inducing an extended SBO, etc.). Indeed, plant improvement measures mentioned by TEPCO after re-evaluations of the design basis tsunami clearly indicate awareness of these issues [99]¹⁶. Additional considerations on the off-site effects of such a beyond design tsunami, which would likely be correlated to a strong earthquake, could have challenged the bias regarding availability of off-site power. Plant improvements on the vulnerabilities would likely have included ensuring water-tightness of compartments with safety critical equipment, elevated positions of (additional) air-cooled diesel generators, instrumentation and measurements qualified for severe accident conditions and independent power supply, etc. and more training of staff. In an environment with more emphasis on plant improvements even in the beyond design basis range the significant risk reductions/improvements for such a vulnerability would have been a strong argument for realizing these measures.

The authors conclude that this supports the basic assumption of the ASAMPSA_E project: extending the scope of PSA to all initiators and all relevant sources of accidental releases. Moreover, PSA should be used to identify plant vulnerabilities for all potentially relevant scenarios. In this case, relevance should be defined in terms of the overall risk profile of the plant and should specifically include all scenarios with large or early releases, which cannot be practically eliminated¹⁷. Moreover, PSA analyses should be used to demonstrate the effectiveness of respective plant improvements. PSA results should be used in a risk-informed process, which is fundamentally aimed at continuously improving plant safety to the extent practicable [27], [103]. While the importance of specific measures might be ranked under consideration of PSA results, general cut-off values for PSA results should not be sufficient by themselves to justify accepting known vulnerabilities. "Even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures to lower the risk further should be implemented." [74], p. 32. This should be consistently applied to new and existing reactors [97]. The ASAMPSA_E project will investigate this issue further and will publish further guidance on the use of PSA and PSA results in risk-informed decision making.

In addition to the fundamental issue on the role and use of PSA, there are several other aspects of PSA and its use in decision making, which shall be discussed in the light of the Fukushima Dai-ichi accident.

- As mentioned above, PSA results for the Fukushima Dai-ichi plant were used as support for the claim to Japanese stakeholders that there is "no risk" of a severe accident. The authors emphasise that certainties run contrary to the probabilistic approach. Similarly, translating PSA results like 10^{-5} per year into return periods like "one time in 100000 years" in e.g. stakeholder communication is not supported by the probabilistic approach and obfuscates and distorts PSA results. The authors find a need for better communication in this regard.

¹⁶ In this sense, the Fukushima Dai-ichi accident does not really qualify as a "black swan" or an unknown unknown. Treating it as such obfuscates the responsibility of decision makers in deciding that the beyond design tsunami risk to the plant was acceptable.

¹⁷ Practically eliminated should be understood as in SSR-2/1 [55] and in WENRA's positions for new reactors [74].

- In this context, PSA results are often narrowed down to very few numbers or even one risk-aggregate figure of merit. Such figures are often “core damage frequency” and/or “large early release frequency” (or containment failure frequency for the Fukushima Dai-ichi plant). While this certainly simplifies the problem space for the decision maker, this kind of risk aggregation can obfuscate or distort specific PSA results and related plant vulnerabilities. This problem will be discussed in more detail in the ASAMPSA_E project as respective results presentation to decision makers and stakeholders can be improved. In any case, an adequate set of PSA results needs to be used in risk-informed decision making for decision makers to fully understand the risk profile of their options.
- One important issue underscored again by the Fukushima Dai-ichi accident is the emergence of cliff-edge effects, if certain safety important parameters exceed threshold values (e.g. tsunami run-up height, limiting pressure for containment failure, etc.). Sufficient safety margins to such threshold values need to be maintained for all relevant scenarios, which is a common feature of DiD analysis. Safety margins need to be evaluated with PSA models or other probabilistic methods [44]; uncertainty distributions for safety margins and the probability of exceedance are important inputs for decision makers. Particularly, PSA needs to investigate safety margins to known or suspected cliff edge effects. Based on the authors’ experience, this application of PSA can be used more comprehensively.
- The treatment of uncertainty has been identified as an important problem for PSA with regard to decision making. Based on the authors’ experience, this is an open issue of decision theory in general. Since the authors do not aim to solve this fundamental problem in this report, a more limited issue is investigated. Uncertainty treatment in PSA Level 1 and Level 2 is usually done based on a (static) event tree/fault tree model with basic events. Probability distributions for reliability parameters (failure rate, failure probability, mission time, etc.) are assigned to the latter. Similarly, PSA Level 2 often includes specific phenomenological modelling that includes uncertainties distributions for keys parameters. Convolution of the uncertainty distributions of reliability parameters, usually based on minimal cut set solutions to the fault tree models generates uncertainty distributions for PSA results using a Monte Carlo sampling approach. This basic approach should be implemented for all elements of a PSA, to the extent practicable.
- PSA results should be understood first and foremost as uncertainty distributions. It needs to be emphasized that mean values are only one characteristic of these distributions, and they might be misleading if other distributions properties are neglected. Based on the authors’ experience, this probabilistic view of PSA results needs to be consistently communicated by PSA practitioners to other stakeholders. In addition, this issue applies not only to direct risk measures/metrics [109] (like e.g. core damage frequency) but also to secondary risk measures/metrics (like e.g. Fussell-Vesely importance). In light of the aforementioned discussion, such secondary risk metrics are particularly important for the ranking of risk. Therefore, they should be determined as uncertainty distributions as well. Based on the authors’ experience, this is not common practice for current PSA Level 1 and Level 2 models. Moreover, current PSA tools often do not support such calculations. This is another area for improvements.
- Current PSA models aggregate uncertainties for a range of different sources. Reliability data for component failures can often be determined from operating experience by applied statistics. Uncertainties for common cause failure data and human error probabilities depend on lack of data and knowledge, on expert judgement and on dedicated quantification models. The uncertainties for rare initiating events like e.g. severe hazard impact are similarly affected and might be in addition rely on multi-physics simulations for processes and phenomena, which are not well understood (e.g. slippage at the subduction zone of the Pacific plate in the

Japan trench region). Moreover, analyses of severe accident progression are also affected by the capabilities of simulation tools, limitations to the knowledge of severe accident phenomena and a dearth of data. The uncertainties assigned to these uncertain elements of a PSA Level 1 and Level 2 are often considered within PSA models even if respective distributions are the result of expert judgement. There are standard methods of sensitivity analyses, which allow to assess the relevance of the different sources of uncertainty on specific PSA results (be they produced for direct or secondary risk measures). Based on the authors' experience, these are not comprehensively applied, though, and current PSA tools offer only restricted support for sensitivity analysis. Moreover, the impact of different sources of uncertainty would have to be better communicated to decision makers and other stakeholders. It should be kept in mind that the interpretation of results is challenging, when they involve different degrees of conservatism.

Finally, are also modelling uncertainties related to the construction of event tree/fault tree models, selection of success criteria and mission times and other simplifications that are needed for constructing a manageable logic model of the plant. These modelling uncertainties are significantly harder to quantify, because this can only be done with alternative logic models. Nonetheless, there is room for improvement in this regard based on the authors' experience. PSA modelling uncertainties need to be determined and presented to decision makers and other stakeholders.

- As already mentioned in section 4, PSA Level 2 should be extended to determine accidental releases. Moreover, the Fukushima Dai-ichi accident has demonstrated that the long term release scenarios are highly relevant and therefore should be for decision makers. However, previous practices partly limited PSA Level 2 to determining the Large Early Release frequency (LERF), which is relevant mostly for short-term emergency measure planning. In light of the accident, PSA Level 2 needs to determine an appropriate set of release categories, including release categories for large releases and for early releases, as input for decision makers. This is an area of further improvement.

Moreover, more harmonized criteria for large and for early releases would be beneficial [69] for comparing PSA Level 2 results (and overall plant risk Level) between units and between design. This could further improve the overall validity and utility of PSA Level 2 results. In this context, the authors also see a need to better and more consistently present and communicate PSA Level 2 results to decision makers and other stakeholders.

- The authors note that there are also no commonly accepted risk criteria (and few risk metrics) [107]. In connection to the previous item, more harmonization would clearly be beneficial. However, the responsibility of decision makers for defining their acceptance criteria should not be abrogated artificially. Therefore, this issue will be discussed in more depth within the ASAMPSA_E project.
- PSA-based risk monitors are getting more and more common for nuclear power plants. In light of the Fukushima Dai-ichi NPP accident, risk monitor including PSA Level 2 models could have provided worthwhile information to decision makers on-site and particularly off-site. However, if risk monitors are fed with erroneous or misleading plant information - and the models do not consider and detect this possibility - they might also reinforce wrong assumptions about the state of the plant.

Conclusions

- PSA results should be used to systematically identify plant vulnerabilities for all scenarios which are not deemed to be practically eliminated. PSA results should be used to rank the priority of such investigations

based on the potential importance of the scenario to Level 1 and Level 2 results and under consideration of the risk profile of the plant.

- PSA investigations should be used to derive and/or assess the effectiveness of plant improvement measures towards reducing plant vulnerabilities.
- PSA results should be used as one input in a risk-informed decision making process regarding potential plant vulnerabilities in the design basis as well as in the design extension condition range. “Even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures.
- lower the risk further should be implemented.” [74], p. 32 Thus, the decision making process should be geared towards continuously improving plant safety as far as reasonably practicable.
- Risk informed decision making processes should consider an adequate set of PSA risk measure/metrics for Level 1 and Level 2 in order to fully appreciate the risk profile of each option.
- PSA results for all risk metrics should be understood and presented as uncertainty distributions. Adequate characterizations of these distributions (in addition to mean value) should be provided.
- Uncertainty analysis for PSA results should be accompanied by comprehensive sensitivity analyses. The effects of major sources of uncertainty on PSA results distributions should be clearly demonstrated. This should entail sources from expert judgement, quantification models, simulation tools, scientific uncertainty and - to the extent practicable - variations of fault tree/event tree modelling.
- PSA Level 2 results used for decision making should include risk metrics on the accidental release and in particular should cover long term release scenarios.
- PSA practitioners should continue to further define a common and harmonized understanding of risk metrics and related risk criteria. Similarly, communication on risk metrics and risk criteria to decision makers and stakeholders by PSA practitioners should be consistent and perspicuous.
- PSA results should be used in on-site and off-site risk monitors, including PSA Level 2 results, to the extent practicable.

6 SUMMARY

6.1 MAIN CONCLUSIONS

“The Fukushima Dai-ichi NPP accident is a sequence of equipment, planning and institutional failures resulting in releases of radioactive materials, following the [Great East Japan Earthquake and the subsequent tsunami(s)]” [10], p. 1. Although the seismic hazard was considered both in the site evaluation and design of the Fukushima Dai-ichi NPPs, the impact from the earthquake on 11 March 2011 exceeded the licensing based design basis ground motion. More importantly, although the tsunami hazard was considered both in the site evaluation and design of the Fukushima Dai-ichi NPPs, the related risk was underestimated. Subsequent additional protective measures taken as result of a re-evaluation after 2002 were insufficient to cope with the tsunami run-up values on 11 March 2011 and related phenomena (hydrodynamic forces, debris impact, site flooding) [70]. Therefore, the plants were not able to withstand the tsunami impact.

In this report, the implications from the Fukushima Dai-ichi NPP accident for PSA Level 1 and Level 2 and to decision making using PSA results have been investigated in the framework of the ASAMPSA_E project. Since the scope of PSA in Japan in general as well as for the Fukushima Dai-ichi units did not extend to the relevant scenarios, direct lessons to be learned on these issues are limited. Therefore, the authors have used their experience on the current status of PSA Level 1 and Level 2 models worldwide and in Europe as well as the insights gained from the ASAMPSA_E questionnaire [119] for identifying further gaps of PSA methodologies and for derived related conclusions and recommendations.

In the following, the main lessons learned on PSA Level 1 and Level 2 as well as decision making using PSA results is briefly summarized. Moreover, a numbered list of the conclusions and recommendations contained in this report is provided in section 6.2.

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

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

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

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

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

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

Another important field is the assessment of human reliability (HRA) for the purposes of PSA. HRA needs to include a more comprehensive and realistic assessment of the effect of hazards on human performance. Despite numerous HRA methods being available, there is a lack of methods for the assessment of knowledge-based actions like e.g. recovery action, of action in high-stress situation like e.g. operability under accidental conditions, and of potentially aggravating actions during and before the event. Particularly with regard for HRA for PSA Level 2, it is

necessary to consider performing shaping factors like exposure to high radiation fields, actions with protective equipment, and long term effects like fatigue or the effect of shift changeover. Moreover, the impact of multiple layers of decision makers on accident management should be assessed.

PSA models for multi-unit sites should systematically include relevant dependencies on the systems levels, e.g. via shared support systems or buildings, as well as dependencies on the accident sequence level, e.g. via the impact of a severe accident in one unit on measures or systems in another unit, into their PSA models. In addition, shared staff resources, mobile equipment, etc. have to be considered. This might require dedicated human reliability analysis. For adequately covering complex scenarios simultaneously affecting several units, site risk PSA models should be developed.

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

The insights in this report confirm that safety related decision making should be made within in risk-informed context, encompassing deterministic, probabilistic and other information. The fundamental approach used for decision making should be the continuous improvement of plant safety to the extent reasonably achievable [27]. In that sense, “even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures to lower the risk further should be implemented.” [74], p. 32. Thus, PSA results should be used to systematically identify plant vulnerabilities for all scenarios which are not deemed to be practically eliminated, and to demonstrate the effectiveness of potential plant improvements.

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

In summary, the Fukushima Dai-ichi NPP accident justifies the basic assumption of the ASAMPSA_E project of extending the scope of PSA to include all operating modes, all events and hazards, and all relevant potential sources like e.g. the spent fuel pool. It has to be acknowledged that extended PSA models, which cover all the scenarios and events recommended above, will require a lot of work on the development of efficient PSA methods, collection and generation of (site / plant-specific) data, further research on such diverse areas as human reliability, geosciences, and severe accident phenomena, and on the improvement of PSA models themselves. In this sense, the PSA community is faced with a series of complex and difficult problems. “But the fact that this

problem¹⁸ is complex can no longer be an excuse for doing nothing.” [110]. The ASAMPSA_E project tackled the aforementioned issues in different deliverables of the project.

¹⁸ The remark was in reference to gun control issues in the U.S.A after the Newtown massacre.

6.2 LIST OF CONCLUSIONS AND RECOMMENDATIONS

The purpose of below listed recommendations is not to put too much burden on the PSA scope and PSA analyst, but to stress that PSA is an important tool for assessing the nuclear safety aspects that need further improvements.

- 1) Hazard frequency assessment should take into account all events occurred in the immediate vicinity of the plant and, if relevant, in wider regions around the plant;
- 2) The frequency assessment should take into account all correlation mechanisms;
- 3) A necessary precondition for hazard identification for PSA is sufficient scientific knowledge about rare hazard scenarios with a potentially high impact. It has to be recognized that geosciences have not yet arrived at the level of understanding desirable for PSA assessment in a lot of cases but this cannot justify neglecting this area of risks. Obviously, further research in these fields in on-going and PSA experts on hazard assessment for nuclear facilities should establish strong links to geoscience researchers and integrate the best available scientific insights into their risk assessments.
- 4) Since hazard identification needs to be site-specific, the original sitting analyses have to be updated regularly for PSA purposes as well as for deterministic assessments. Site specific hazard identification has to be systematically extended to scenarios in the design extension conditions range (cf. WENRA Reference Levels), especially for the purposes of an extended PSA.
- 5) Hazard identification should be extended beyond the already established hazards like flooding or internal fire. All natural hazards that might affect the site shall be identified; a wide spectrum of rare events should be assessed (cf. WENRA Reference Levels).
- 6) There is a lack of accepted methods for ‘extrapolating hazard intensity’ over ‘frequency of exceedance curves’ in the range (frequencies smaller than approximately 10^{-4} per year) that can usually not be supported by actual data. There is on-going research in this area and PSA experts for nuclear facilities should be actively involved therein. Moreover, improved methods and better data are needed for limiting uncertainty bands for such extrapolated rare event frequencies.
- 7) The lack of methods to assess hazard consequences should not be utilized to skip a hazard scenario, which is deemed physically plausible by experts. If relevant, the margins of the plant to severe accident scenarios and conditional core damage/large release probabilities should be estimated with a probabilistic approach. Expert judgement should be used as needed.
- 8) More attention should be paid to worldwide operating experience in the nuclear industry as well as other industries regarding precursor hazard events and near misses. These insights should be systematically used in the site-specific hazard identification.
- 9) Hazard identification should be performed not only in regard to the risk to fuel in the core but extended also to the risk of spent fuel in dry or wet storage on the site.
- 10) A realistic set of combinations of hazards should be identified on the basis of a list of individual internal and external hazards. It should be done through a systematic check of dependencies, by identifying (in decreasing order of priority):
 - a) Potential induced effects by hazards (e.g. tsunami or dam failure induced by earthquake, internal flood induced by missiles;
 - b) Correlated hazards occurring in the same conditions (e.g. strong winds and extreme snow pack, icing);
 - c) Independent frequent internal events occurring during hazard period (e.g. if a hazard situation persists).

- 11) The screening process should consider credible frequencies for the hazards of relatively high magnitude, especially if they have never been observed in the past in the plant vicinity. The impact of correlated hazards should be carefully considered.
- 12) The set of screening criteria should ensure screening in low probability/high impact scenarios to the extent practicable.
- 13) Screening criteria should include suitable risk metrics for covering accidental release risk like e.g. large release frequency or conditional containment failure probability.
- 14) Screening should be done by combining fixed threshold values (e.g. for frequency of exceedance) with criteria relative to the risk level of the plant (e.g. using metrics like CDF, LRF, CFF, etc.).
- 15) Probabilistic hazard assessment should be systematically performed to support design extension and Level 2 PSA significance for the risk of radioactive releases. Respective safety assessment practices should be established.
- 16) Sufficiently detailed (probabilistic) hazard assessments are required to identify existing plant vulnerabilities particularly for low probability/high impact events.
- 17) Detailed probabilistic assessment of hazards to the extent screened in should be performed up to a controlled safety state, which is defined by clear criteria for plant parameters and availability of essential safety functions. Challenges to such a controlled state should require additional, independent events in PSAs modelling.
- 18) The community of hazard assessment and PSA experts should work towards establishing effective probabilistic hazard assessment approaches.
- 19) Significant research effort is still needed for further improving the methods and tools needed for probabilistic hazard assessment, which requires long-term funding for public bodies and involvement of fundamental research institutions as well as end-users.
- 20) Hazard PSAs need to be extended to risk sources other than the reactor core, in particular to a spent fuel pool. Respective initiating events have to be mapped to relevant hazard scenarios. Spent fuel pool related events should be considered in at-power PSAs as well. Waste treatment facility related events should be considered in addition, even if they do not require necessarily a PSA modelling.
- 21) Hazard PSAs for other risk sources than the reactor core necessitate the development of PSA models on internal and external events for these sources. If such models are unavailable, the internal events PSA of a plant should be extended.
- 22) The occurrence of further initiators during the time frame of the PSA analysis (specifically for correlated and long-term hazards) as well as the implementation of some recoveries should be considered.
- 23) Regulators should ensure that actions taken and resources relied upon at one level of DiD are as far as possible independent from the other levels in order to minimize the potential for same failures propagating from one level to another as occurred at the Fukushima Dai-ichi NPP. Specifically, assessment of these issues with PSA methods to the extent appropriate should be done.
- 24) System reliability assessments with PSA methods should be extended to the design extension conditions regime. Similarly, DiD assessments for severe accident management measures, procedures, or systems should be performed using PSA methods as appropriate. Consequently, Level 1 and Level 2 PSA models should be considered for such assessments.
- 25) Best practices for using PSA for DiD assessments need to be gathered. This issue will be treated by the ASAMPSA_E project with the scope of a separate technical report. In any case, there is still need for further

research into how PSA models can be efficiently used to do DiD assessments. Moreover, related criteria need to be defined.

- 26) Potentially relevant detrimental actions by operators before an accidental state has been reached, e.g. disabling safety systems or aggravating accidental consequences, should be systematically investigated. Potentially relevant actions should be included in the systems reliability assessment and the fault tree/event tree modelling to the extent practicable.
- 27) PSA analysis times should be extended until a stable controlled state or an accidental stage has been reached. Success criteria for a controlled state in the long term after an event should be defined. Justified analysis times should form the basis for systems or component specific mission times in the fault tree modelling dependent on the scenario. This may necessitate changes to some PSA software tools.
- 28) Consequential failures induced by hazards impact need to be systematically addressed considering site-specific conditions, particularly for detailed PSA assessments. As this task includes also spatial interactions (fire and flood spreading, impact of collapsed SSC), I&C interactions (faulty signals), and system interdependencies (e.g. supporting systems), it can be very complex. Moreover, erroneously established dependencies (e.g. due to faulty operator actions prior to or during the event scenario), should be considered in PSA Level 1 if relevant. Also, in addition to failed barriers or protective measures, degraded states should be included into detailed PSA assessments. Of particular importance are containment failure modes due to hazard impact, i.e. prior to accidental states. These should be systematically investigated in the Level 1 PSA; respective pathways need to be described. On all these issues, new and improved methods as well as reliability/fragility estimations need to be developed.
- 29) The dependencies of barrier effectiveness as well as safety systems effectiveness to non-safety class functions, which are in turn dependent on the plants operating status, should be investigated systematically. There is a need for new and improved methods as well as data.
- 30) Similarly, failure and degradation mechanisms of qualified and non-qualified equipment for specific hazard impacts and their secondary effects need to be investigated in more detail. Dynamic loads (e.g. vibration, overpressure, etc.) should be considered as well. Consequently, respective failure modes and eventually basic events have to be defined. For this, probabilistic methods have to be improved.
- 31) The analysis period assumed for system reliability (as well as event progression) should not be limited to 24 h (conventional scrutation duration for static Boolean models). Instead, mission times should be chosen in a realistic way based on the time the system performance is needed for controlling a scenario. Respective success criteria should be defined and justification should be provided, particularly on why a controlled state has been reached. The mission time should be used in basic event models and for quantification of e.g. certain common cause failures. Consistency with accident progression analysis should be maintained.
- 32) For multi-unit sites, the interdependencies between the units, including dependencies on component or system level, should be included into the event tree/fault tree modelling. This includes dependencies between the units due to existing connections (e.g. shared turbine building, cable trenches, ventilation ducts, spatial interactions between plant units compartments or interfaces), which are usually neglected for PSA purposes. Potentially relevant dependencies can arise due to failed isolation or erroneously opened/closed connections. On these issues, further developments are needed. In addition, appropriate conditional probabilities and/or event correlations have to be established for PSA modelling and quantification. This constitutes a significant challenge; methods and data for this task have to be developed.
- 33) In system reliability modelling, a particular focus should be on consequential failure analysis due to hazard impact (whether direct or indirect, by environmental conditions or as an area event, etc.).

- 34) The probabilistic assessment of EOPs and preventive AM procedure/measures in Level 1 PSA should systematically consider accessibility and operability of equipment as well as feasibility of measures in case of hazard impacts. There is a need for more sophisticated methods and for better data on these issues.
- 35) Similarly, Level 1 PSA for multi-unit sites should systematically consider the impact of a severe accident scenario in one unit on the accessibility and operability of equipment for other units. In addition, simultaneous availability of staff for performing actions needs to be taken into account. There is a need for more sophisticated methods and for better data on these issues.
- 36) Identification and treatment of “errors of commission” (i.e. performance of inappropriate actions that may aggravate an accident scenario) involving intentional disabling of safety systems (e.g. intentional isolation of the Isolation Condenser system at Fukushima Dai-ichi NPP as per operation manual). However, EOCs along with the associated contexts that would make such errors probable are not included in most PSA models except for the quite obvious scenarios. There are HRA methods capable of treating some aspects of EOCs (e.g., ATHEANA), and such methods (or at least their key underlying concepts) should be useful when searching for cognitively challenging human failure events. These practices need to be improved.
- 37) Assessment of the feasibility of recovery actions and delays in performing these actions (including accessibility and operability under accidental conditions; long time window needed to complete action). This aspect needs to be considered more systematically in PSA models and HRA methods and data need to be further improved in this regard; as minimal all recovery actions modelled in a PSA should be precisely described, justified and their impacts on the PSA final results explained.
- 38) Assessment of the effects of lack of or even misleading information (including loss of instrumentation and control equipment) and related uncertainties on decision making and operator actions. This aspect should be better included into PSA models. Particularly for knowledge-based decision making, development of practicable and qualified HRA methods is needed.
- 39) Assessment of the variability in plant crew performance. This aspect needs to be accounted for in the uncertainties assigned to HEP, and there is a need for better data to that effect.
- 40) Adequate treatment of cognitive ‘between-person’ and ‘within-person’ dependencies among sequential or parallel, operator actions due to weak knowledge about dependencies. There is still a strong need for the development of efficient, practicable methods on this aspect.
- 41) Analysts need to find a balance in the application of initial (conservative) screening values and of (more realistic) values based on sophisticated HRA methods for the basic events for operator actions in the PSA model in order to prevent skewed results.
- 42) HRA analysts should be sufficiently experienced, be informed about available assessment methods and should have access to expert level knowledge on plant behaviour, procedures, handling of components, etc. as appropriate for each assessment.
- 43) The scope of Level 2 PSA should be extended to include all operating modes, all events and hazards, and all relevant potential sources. National regulators should impose respective requirements.
- 44) The screening of initiating event for detailed consideration in the PSA should be performed not only based on PSA Level 1 risk metrics but also on Level 2 PSA risk metrics like e.g. different release categories, including at least one risk metric for large releases and one for early releases. Screening thresholds on the risk measures for the Level 2 risk metrics should be defined and justified. Initiating events (including hazard scenarios) should only be screened out from the PSA, if they are screened out based on Level 1 and on Level 2 risk metrics. In addition, if a Level 3 PSA (or Level 2+ with few off-site consequences analysis) is intended the screening process should include Level 3 risk metrics and thresholds as well.

- 45) In order to assure consistency between the PSA Level 1 and Level 2, a common definition of “core damage” and other Level 1 interface groups shall be assumed. Moreover, partial core damage states should be considered and these should be treated consistently between Level 1 and Level 2 PSA.
- 46) In order to also take into account accidents in the spent fuel pool, appropriate definitions for these Level 1 end states, e.g. “fuel damage”, should be defined. The respective end states should be part of an appropriately defined interface to the Level 2 PSA.
- 47) The binning of sequences into Level 1 interface plant damage states should be restricted to those sequences that can be adequately and realistically associated with regard to all branching points in the Level 2 accident progression event tree, i.e. not only with regard to severe accident phenomenology but also with regard to similar characteristics for accident management measures and other operator actions as well as boundary conditions of the scenario.
- 48) Concerning the initiating conditions to be considered in a Level 2 PSA (if it starts at core damage) and based on the Fukushima Dai-ichi accident conditions, situations of core melt from Level 1 PSA should be considered (in the PDS) while another or several reactors are already in severe accident conditions.
- 49) All PSA Level 1 interface end states should be transferred to the Level 2 PSA. If some end states are excluded from further analysis or are assigned to other, not fully representative groups, this should be done based on justified criteria, commensurate to the screening criteria and the objectives of the PSA. Level 1 end states with potential contributions to large or early releases should not be excluded from further analysis to the extent practicable. The latter routinely includes scenarios with containment failure prior to the accidental state (e.g. core damage).
- 50) Accident type Level 1 PSA end states shall not be excluded from further consideration in a Level 2 PSA only based on the duration of the respective sequences up to the accidental state (“mission time”).
- 51) As already pointed out (see Level 1 PSA), grouping scenarios at different steps of the PSA process should avoid any significant “loss of memory” about the specific properties of the binned sequences, e.g. related to the initiating events, boundary conditions of the scenario, unavailability or availability of certain components, systems, or measures.
- 52) The feasibility, operability, and reliability of severe accident mitigation measures should be systematically analysed and checked for adequacy with PSA Level 1 and PSA Level 2 models. This includes, but is not restricted to, the evaluation of hazard impact on the site and the availability of off-site resources. Particularly, the availability of off-site electric power and the ultimate heat sink cooling in the long term should be critically examined.
- 53) Assessments of DiD Level 4 measures and systems should be done taking into account adequately detailed and comprehensive PSA model results. Particularly, the DiD Level 4 assessments should consider all operating modes and internal as well as external hazards.
- 54) The degree of dependency of severe accident measures or systems to other (design basis) safety functions or measures, or to accident sequence boundary conditions, or even to other severe accident measures should be investigated using probabilistic methods. To the extent practicable, information about failed systems or components during the accidental scenarios from Level 1 PSA should be taken into account.
- 55) Critically important instrumentation and measurements should be investigated using PSA methods on their availability during severe accident scenarios, including scenarios developing from severe hazard impact. Importantly, adequate instrumentation and measurements should be available to the operators and crisis management crew for identifying, monitoring and assessing accidental situations in the reactor core and the

spent fuel pool. Conversely, failure of such instrumentation and measurements should be part of Level 2 PSA models.

- 56) Level 2 PSA analyses should systematically investigate potential detrimental actions or decisions by operators and additional emergency centre staff, which might aggravate an accidental scenario. To the extent practicable, such possibilities should be identified and included into PSA Level 2 models.
- 57) Level 2 PSA models should consider the effect of (near) simultaneous accidental scenarios in the spent fuel pool and in the reactor core considering the availability and reliability of dedicated systems or measures.
- 58) Level 2 PSA modelling should be extended (like Level 1 PSA modelling) until either a controlled accidental state has been reached, e.g. if containment failure can be practically excluded, and/or until further additional releases can be demonstrated to be not relevant. Respective criteria should be defined and justified for the PSA Level 2. Further independent failures should only be considered, if they are likely in the period of analysis and would significantly worsen the situation. This particularly applies to certain hazards. For example, the risk of strong aftershocks affecting the operability of key systems, whose structure may already be compromised, should be analysed in seismic PSA.
- 59) For multi-unit sites, the dependencies between the units should be systematically included into the Level 2 PSA model. This includes, but is not restricted to, common safety related systems, support or operational systems, capacity and availability of common accident mitigation measures or systems for multiple units, availability of staff for performing measures in case of simultaneous accidental situations, effects of an accidental scenario in one unit on other units and the staff, etc.
- 60) The potential risk from all combustible gases detonation or deflagration should be investigated systematically. The risk of hydrogen detonations or deflagrations should include the risk from hydrogen accumulations outside of the containment, e.g. in the reactor building or in the venting lines as part of the PSA Level 2. In that respect, gas leakages from the containment and air ducts/ventilation lines should be investigated. If practicable, plant improvements should be realized to minimize the risk of hydrogen explosions. However, other combustible gases, such as carbon monoxide, which can be produced during molten core-concrete interactions, may also impose potential threat to hermetic containment integrity and should be investigated.
- 61) Complex failure scenarios, which are especially relevant for severe hazards impacts, should be adequately considered in the Level 2 PSA modelling. Specifically, these scenarios need to be considered in the reliability assessment of severe accident measures in case of hazard impact. There is a need for developing effective modelling approaches.
- 62) Level 2 PSA models should include source term assessments for the release category end states. Branches in the accident progression event tree should be defined also in light of the impact of systems, measures, or phenomena on release characteristics. Models limited to containment failure assessment should be extended as practicable.
- 63) The mission times for accident mitigation measures needed to reach a controlled state after an accident should be used in the reliability assessment of components and as basis for HRA of operator actions.
- 64) Level 2 PSA models should be extended to the extent practicable to include repairs of previously failed systems or components. The longer Level 2 PSA analysis and mission times become, the more important is the consideration of such repairs. Moreover, effective modelling approaches should be developed for this issue to model appropriately the increasing chances of repair with time available.
- 65) Level 2 PSA models should include extended analysis times in the reliability models for systems, components and actions needed during the accident progression. Dependencies with support systems or supporting

measures (like refilling fuel or water storage tanks), especially if induced by a longer mission time, should be systematically investigated and included into the Level 2 models to the extent sensible.

- 66) For multi-unit sites, commonly used systems and resources should be systematically treated within the PSA Level 2 model. Most importantly, relevant restrictions on the availability or reliability of systems or resources have to be identified and included into the model. To the extent sensible and practicable, a site risk Level 2 model should be developed, especially for events which affect the whole site. In this regard, there is still need for further research on methods and good practices.
- 67) PSA Level 2 models should include specific modelling related to partial core damage states and similar accidental states. Particularly, branches for the transitions into more severe states (e.g. full core melt) should be included in the APET with adequate success criteria for systems or measures.
- 68) PSA Level 2 models should be extended to releases via the ground or to water in addition to aerial releases. Respective pathways need to be identified, releases need to be quantified. Consequently, necessary changes of the accident progression event tree modelling should be implemented in the models. This should be done on the basis of characteristics for dedicated release categories.
- 69) PSA Level 2 results should include all sources of uncertainty. Large uncertainties for PSA Level 2 elements and results should be identified and reduced to the extent practicable. Additionally, relevant information on the effect of specific uncertainty sources on PSA results should be provided by sensitivity analysis.
- 70) Severe accident management measures should not only be included in PSA Level 2 models to the extent practicable, but conversely should also be checked and assessed with PSA Level 2 methods. Vulnerabilities and potentials for improvement found during such assessments should lead to the consideration of further improvement of plant safety.
- 71) Severe accident management measures should be modelled and quantified within the PSA Level 2 based on scenario-specific boundary conditions to the extent practicable.
- 72) Probabilistic investigation for mobile equipment should systematically identify and assess situations and scenarios, for which such equipment can't be successfully deployed. Exemplary reasons include blocked transport roads, inaccessibility of connection points, and common cause failure impact.
- 73) Mitigative measure for maintaining containment integrity under accidental conditions should be systematically included into PSA Level 2 models. In addition, PSA methods should be used to demonstrate adequate independence of these DiD Level 4 measures from measures or systems on other DiD Levels.
- 74) HRA for PSA Level 2 should be extended to the extent practicable to consider long-term affects of accident scenarios, particularly performance shaping factors like fatigue or increased stress levels, and the effects of shift changeover. HRA practitioners should participate in research on these issues.
- 75) HRA for PSA Level 2 should consider performing shaping factors induced by exposure to radiation and contamination as well as effects of related protective equipment and the need to perform actions on-site as quickly as possible. HRA practitioners should participate in research on these issues.
- 76) HRA for PSA Level 2 should systematically analyse knowledge-based decisions and actions for mitigating an accident. PSA Level 2 should be extended to the extent practicable to cover such knowledge-based measures. Similarly, the potential for detrimental knowledge-based actions should be analysed and considered. Quantitative assessments should be treated under due consideration of their limitations. Consequently, HRA practitioners should participate in research on these issues.
- 77) For multiple-unit sites, specific HRA of the actions and activities to be taken by staff shared between the units during a simultaneous severe accident should be performed. The options for personnel support from other

NPPs shall be studied as well. It is also important to analyse how shifts of personnel call by emergency on the site can obtain information for the on-going situation and can take over the control of the facilities.

- 78) The potential impact of multiple decision makers (e.g. in the crisis organization) on the performance of severe accident measures should be considered in the HRA for the respective measures to the extent practicable. HRA methods for an efficient and reliable analysis of crisis organizations (internal and external to the site) should be developed. Their results should be integrated in PSA Level 2 models if relevant.
- 79) PSA results should be used to systematically identify plant vulnerabilities for all scenarios which are not deemed to be practically eliminated. PSA results should be used to rank the priority of such investigations based on the potential importance of the scenario to Level 1 and Level 2 results and under consideration of the risk profile of the plant.
- 80) PSA investigations should be used to derive and/or assess the effectiveness of plant safety improvements aimed to reduce the plant vulnerabilities.
- 81) PSA results should be used as one of the inputs in a risk-informed decision making process regarding potential plant vulnerabilities - at the design basis stage, as well as in the design extension condition range. "Even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures to lower the risk further should be implemented." [74], p. 32 Thus, the decision making process should be oriented and accelerated towards continuously improving plant safety as far as reasonably practicable.
- 82) Risk informed decision making processes should consider an adequate set of PSA risk measures/metrics for Level 1 and Level 2 in order to fully appreciate the risk profile of each option.
- 83) PSA results for all risk metrics should be understood and presented as uncertainty distributions. Adequate characterizations of these distributions (in addition to mean value) should be provided.
- 84) Uncertainty analysis for PSA results should be accompanied by comprehensive sensitivity analyses. The effects of major sources of uncertainty on PSA results distributions should be clearly demonstrated. This should entail sources from expert judgement, quantification models, simulation tools, scientific and statistical uncertainty and - to the extent practicable - variations of fault tree/event tree modelling.
- 85) PSA Level 2 results used for decision making should include risk metrics on the accidental release and in particular cover long term release scenarios.
- 86) PSA practitioners should continue to define a common and harmonized understanding of risk metrics and related risk criteria. Similarly, communication on risk metrics and risk criteria to decision makers and stakeholders by PSA practitioners should be consistent and perspicuous.
- 87) PSA results should be used in on-site and off-site risk monitors, including PSA Level 2 results, to the extent practicable.

The table below provides a list of PSA issues (relevant to ASAMPSA_E project scope) identified in this report and related recommendations for PSA Level 1, Level 2 and use of PSA results:

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

7 REFERENCES

- [1] IAEA, IAEA-TECDOC-1341, Extreme external events in the design and assessment of nuclear power plants, 2003, Vienna.
- [2] <http://ensreg.org/EU-Stress-Tests>
- [3] NRA, Enforcement of the new regulatory requirements for commercial nuclear power reactors, July 8, 2013
- [4] NRA, How PSA results are to be utilized in new nuclear regulation in Japan, PSAM Topical Conference in Tokyo, April 15, 2013
- [5] TEPCO, Lessons Learned from Fukushima Dai-ichi Accident, PSAM Topical Conference in Tokyo, April 15, 2013
- [6] NRA, Outline of new regulatory requirements for light water nuclear power plants, Provisional Translation, April 3, 2013
- [7] http://www.aesj.or.jp/en/release/committee_for_investigation_of_nuclear_safety.shtml
- [8] <http://www.nsr.go.jp/english/>
- [9] http://www.aesj.or.jp/sc/english/rk004e_2011_en.html
- [10] W. Epstein, A Probabilistic Risk Assessment Practitioner looks at the Great East Japan Earthquake and Tsunami, <http://woody.com/wp-content/uploads/2011/06/A-PRA-Practitioner-looks-at-the-Great-East-Japan-Earthquake-and-Tsunami.pdf>
- [11] US Nuclear Regulatory Commission, PRA Procedure Guide: A Guide to the performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, 1983.
- [12] WENRA, Stress test specifications, April 2011
- [13] A. Olsson, Lloyd's Register Consulting (On behalf of the Nordic PSA Group (NPSAG)), Identification of potential focus areas regarding development of PSA methodologies as lessons learned from Fukushima, 2012 Dai-ichi , NPSAG Autumn Seminar, October 2012
- [14] A. Lyubarskiy, I. Kuzmina, M. El-Shanawany, NOTES on Potential Areas for Enhancement of the PSA Methodology based on Lessons Learned from the Fukushima Dai-ichi Accident, September 2011
- [15] ENSREG, Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, June 2012
- [16] WENRA, Updating WENRA Reference Levels for existing reactors in the light of TEPCO Fukushima Dai-ichi accident lessons learned, November 2013
- [17] WENRA, Conclusions arising from Consideration of the Lessons from the TEPCO Fukushima Dai-ichi Nuclear Accident, 2012
- [18] OECD/ NEA, Nuclear Energy Agency (NEA) activities in follow-up to the TEPCO Fukushima Dai-ichi Daiichi nuclear accident, 2012
- [19] OECD/NEA, The Fukushima Dai-ichi Daiichi Nuclear Power Plant Accident: OECD/NEA Nuclear Safety Response and Lessons Learnt, 2013
- [20] IAEA, 2nd Extraordinary Meeting of the Contracting parties to the Convention of Nuclear Safety. - final summary report, August 2012, Vienna, Austria
- [21] Convention on Nuclear Safety - National Report of Japan for the Second Extraordinary Meeting, 2012
- [22] ONR, Japanese earthquake and tsunami: Implementing the lessons for the UK's nuclear industry, October 2012
- [23] IAEA, "Seismic Hazard in Site Evaluation for Nuclear Installation", Specific Safety Guide No. SSG-9, August 2010

- [24] SNETP (Sustainable Nuclear Energy Technology Platform) - Identification of Research Areas in Response to the Fukushima Dai-ichi Accident, January 2013
- [25] ASME, The ASME Presidential Task Force on Response to Japan Nuclear Power Plant Events - Forging a New Nuclear Safety Construct, June 2012
- [26] US NRC - Recommendations for Enhancing Reactor Safety in the 21st Century - the Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident, July 2011
- [27] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006)
- [28] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996)
- [29] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999)
- [30] <http://www-ns.iaea.org/standards/concepts-terms.asp>:
- [31] Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety standards for protecting People and the Environment , Specific Safety Guide No. SSG-2, IAEA Vienna 2009
- [32] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna (2000)
- [33] IAEA CN-205-T2-04 Safety analysis in design and assessment of the physical protection of the OKG NPP, Pär Lindahl, IAEA-CN-205 Vienna 21-24 Oct 2013.
- [34] The PSA Approach for the Safety Assessment of Low power and Shutdown States, D.Müller -Ecker, GRS,
- [35] <http://www.iaea.org/ns/tutorials/regcontrol/assess/assess3213.htm>, Regulatory control of Nuclear Power Plants, 3. Assessment of Safety
- [36] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA Vienna, 2000
- [37] http://nuclear.inl.gov/deliverables/docs/ineri_pdf_report_on_sharing_of_systems_and_structures_august_2007_complete_%20report.pdf , Oak Ridge National Laboratory, ORNL/LTR/INERI-BRAZIL/06-01, Design Strategies and Evaluation for Sharing Systems at Multi-Unit Plants Phase I , August 2007
- [38] Post-Fukushima Dai-ichi accident Peer review report Stress Test Peer Review Board Stress tests performed on European nuclear power plants, ENSREG, v12h, 2012-04-25
- [39] Directive from 13.6.2013: COM(2013) 343 final, Council Directive amending Directive 2009[71]EURATOM establishing a Community framework for the nuclear safety of nuclear installations
- [40] <http://www.ensreg.eu/nuclear-safety/prevention-accidents>
- [41] S. Guentay ASAMPSA2: Workshop on Review of the ASAMPSA2 Guideline on Level2 Development and Applications, Synthesis of the L2 PSA End-Users Evaluation of the “Best-Practices Guidelines for L2 PSA Development and Applications (Part I), Espoo, Finland, March 7-9 2011
- [42] Safety Report Series No.52, Best estimate Safety Analysis for Nuclear Power Plants: Uncertainty evaluation; http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1306_web.pdf
- [43] ASAMPSA_E, “The link between the Defence-in-Depth Concept and Extended PSA”, Technical report ASAMPSA_E/WP30/D30.7/2017-31 volume 4, PSN-RES/SAG/2017-00019.

- [44] IAEA-TECDOC-1332, Safety margins of operating reactors Analysis of uncertainties and implications for decision making, IAEA January 2003.
- [45] American National Standards Institute (ANSI), External Events in PRA Methodology, ANSI/ANS 58.21-2007, 2007.
- [46] American Society of Mechanical Engineers (ASME), Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, AMSE/ANS RA-Sa-2009, 2009.
- [47] J. J. Bevelacqua, "Nuclear Regulation in the United States and a Possible Framework for an International Regulatory Approach", International Nuclear Safety Journal, Vol.1, No.1 (2013)
- [48] K. N. Fleming, "On the Issue of Integrated Risk - A PRA Practitioners Perspectives", Proceedings of the ANS International Topical Meeting on Probabilistic Safety Analysis, San Francisco, CA., USA, Sep. 11-15, 2005.
- [49] IAEA Safety Series No.118, Safety Assessment for Spent Fuel Storage Facilities, IAEA, Vienna, 1994.
- [50] T.E. Collins and G. Hubbard, Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants, NUREG-1738, U.S. Nuclear Regulatory Commission, January 2001.
- [51] Joon-Eon Yang, Development of an Integrated Risk Assessment Framework for Internal/External Events and all Power Modes, Nuclear Engineering and Technology, Vol. 44 No.5 June 2012
- [52] Burgazzi L., Addressing the challenges posed by advanced reactor passive safety system performance assessment, Nuclear Engineering and Design, 241, pp. 1834-1841, May 2011
- [53] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007
- [54] IAEA, General Safety Requirements Part 4, GSR Part 4, 2009
- [55] IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1, 2012
- [56] IAEA, Development and Application of Level 1 Probabilistic Safety Assessment for nuclear Power Plants, Specific Safety Guide, SSG-3, 2010
- [57] IAEA, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide, SSG-4, 2010
- [58] IAEA, 2011. Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations. Specific Safety Guide No. SSG-18, Vienna.
- [59] IAEA, Site Evaluation for Nuclear Installations. Safety Requirements, NS-R-3, 2003.
- [60] IAEA, 2002. External Human Induced Events in Site Evaluation for Nuclear Power Plants. Safety Guide No. NS-G-3.1, Vienna.
- [61] IAEA, NS-G-3.3, Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna.
- [62] IAEA, NS-G-3.6, Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants, Vienna.
- [63] IAEA, NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Vienna.
- [64] IAEA, NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants, Vienna.
- [65] IAEA, Severe Accident Management Programs for Nuclear Power Plants, NS-G-2.15, 2009
- [66] U.S. NRC, Guidance for Assessment of Flooding Hazards due to Dam Failure, JLD-ISG-2013-01, July 29, 2013
- [67] WENRA RHWG, Reactor Safety Reference Levels, 2008
- [68] WENRA RHWG, Safety Objectives for New Power Reactors, 2009
- [69] ASAMPSA2, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors, ASAMPSA2/WP2-3/D3.3/2013-35
- [70] IAEA, Mission Report - The Great East Japan Earthquake Expert Mission - IAEA International Fact Finding Expert Mission Of The Fukushima Dai-ichi NPP Accident Following The Great East Japan Earthquake And Tsunami, 24 May - 2 June 2011

- [71] Dominique Delattre (IAEA), “Safety Standards and their Role, IAEA Response to the TEPCO’s Fukushima Dai-ichi NPPs Accident”, EC Workshop how to improve safety in regulated industries, What could we learn from each other?, Luxemburg, 16-17 October 2012
- [72] Javier Yllera (IAEA/NSNI), “Safety Requirements / Design Criteria for SFR, Lessons Learnt from the Fukushima Dai-ichi accident ”, 3rd Joint GIF-IAEA ,Workshop on Safety Design Criteria for Sodium-Cooled Fast Reactors Vienna, 26-27 February 2013
- [73] Nathan Siu, Don Marksberry, Susan Cooper, Kevin Coyne, Martin Stutzke (US NRC), “PSA Technology Challenges Revealed by the Great East Japan Earthquake”, PSAM Topical Conference in Light of the Fukushima Dai-ichi accident, Tokyo, Japan, April 15-17, 2013
- [74] WENRA RHWG, Report Safety of new NPP designs, March 2013
- [75] DS462 DPP. Revision through addenda of GSR Part 1, NS-R-3, SSR-2/1, SSR-2/2 and GSR Part 4.
- [76] IAEA, A Methodology to Assess the Safety Vulnerabilities of Nuclear Power Plants against Site Specific Extreme Natural Hazards, 2011.
- [77] AESJ, Implementation Standard Concerning the Seismic Probabilistic Risk Assessment of Nuclear Power Plants (in Japanese), 2014
- [78] US NRC, NUREG 1150, 1990
- [79] V.L. Sailer, K.R. Perkins, J.R. Weeks, and H.R. Connell, Severe Accidents in Spent Fuel Pools in Support of Generic Safety Issue 82, NUREG/CR-4982 and BNL-NUREG- 52093. Brookhaven National Laboratory, Upton, N.Y., July 1987.
- [80] BNRA, European “Stress Tests” for NPPs, National Report of Bulgaria, December 2011.
- [81] BNRA, EUROPEAN “STRESS TESTS” Kozloduy NPP, National Action Plan of Bulgaria, December 2012.
- [82] BNRA, EUROPEAN “STRESS TESTS” Kozloduy NPP, National Action Plan of Bulgaria, January 2014.
- [83] B. Marinova, et all, Main Results and Conclusions of PSA Level 1 for Units 5 and 6 of “Kozloduy”NPP, Proceedings of the 9th International Conference on Nuclear Option in Countries with Small and Medium Electricity Grids , Zadar, Croatia, 3-6 June 2012.
- [84] BNRA, Regulation for ensuring the safety of NPPs, Sofia, Published SG, No. 66 of 30 July 2004, amended SG No. 46 of 12 June 2007, and amended SG No. 53 of 10 June 2008.
- [85] BNRA, Safety Guide “Use of PSA to Support the Safety Management of NPPs”, 2010.
- [86] IAEA, “Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes”, IAEA-TECDOC-1144, 2000.
- [87] NUREG-1842 “Evaluation of Human Reliability Analysis Methods Against Good Practices”, 2006
- [88] BMU, Bekanntmachung der “Sicherheitsanforderungen an Kernkraftwerke” vom 22. November 2012, BAnz AT 24.01.2013 B3
- [89] ENSI, Probabilistische Sicherheitsanalyse (PSA): Qualität und Umfang, ENSI-A05, 2009
- [90] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes - Leitfaden Probabilistische Sicherheitsanalyse, vom 30. August 2005, BAnz No. 207a (57), 2005.
- [91] S. Sperbeck, M. Türschmann, GRS - Recent Research on Hazards PSA Results and Applications, PSAM 12, 2012
- [92] Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, October 2005.
- [93] Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke, Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-38/05, October 2005.

- [94] Stress tests performed on European nuclear power plants. Bulgaria. Peer review country report. Post-Fukushima Dai-ichi accident. ENSREG, 2011.
- [95] Summary report on the impact and experience feedback of the previous ASAMPSA2 project. "NUCLEAR FISSION", Safety of Existing Nuclear Installations. Contract 605001. 2013.
- [96] A. Suzuki, Managing the Fukushima Challenge, Risk Analysis 34 (2014), p. 1240-1256
- [97] WENRA, "WENRA Safety Reference Levels for Existing Reactors", 24 September 2014
- [98] ASME, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plants Applications", ASME/ANS RA-S-2008, 2008
- [99] Tokyo Electric Power Company, Inc. (TEPCO), "Fukushima Nuclear Accident Analysis Report", June 20, 2012, http://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf
- [100] Holmberg, J., J. Nirmark, "Risk-informed Assessment of Defence in Depth, LOCA Example, Phase 1: Mapping of Conditions and Definition of Quantitative Measures for the Defence in Depth Levels", Rev. 0, SKI report 2008:33, February 2008
- [101] Hellström, P. M. Knochenhauer, R. Nyman, "SSM Research Project on Defence-in-Depth PSA - Assessing Defence-in-Depth Levels with PSA Methods" in: 10th International Probabilistic Safety Assessment and Management Conference (PSAM10), 2010
- [102] INPO, "Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station", Rev. 0, INPO 11-005, November 2011
- [103] European Council, Council Directive 2009/71/EURATOM of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations, Official Journal of the European Union, L172/18, 2.7.2009
- [104] Müller-Ecker, D., "WENRA and Its Expectations on the Safety of New NPP", INPRO Dialog Forum on Global Nuclear Energy Sustainability, Licensing and Safety Issues for Small- and Medium-sized Reactors (SMRs), Vienna, 29 July - 2 August 2013
- [105] IAEA, "A Framework for an Integrated Risk Informed Decision Making Process, A report of the International Nuclear Safety Group", INSAG-25, 2011
- [106] Einarsson, S., A. Wielenberg, "An Integrated Risk Informed Decision Making Approach for Germany", Proc. of PSAM11/ESREL2012, 25 - 29 June 2012, Helsinki, 2012
- [107] OECD/NEA, "Probabilistic Risk Criteria and Safety Goals", NEA/CSNI/R(2009)16, December 2009
- [108] OECD/NEA, "Use and Development of Probabilistic Safety Assessment, An Overview of the Situation at the End of 2010", NEA/CSNI/R(2012)11, January 2013
- [109] Johansen, I.L., M. Rausand, "Foundations and Choice of Risk Metrics", Safety Science, Vol. 62, (2014), p. 386-399
- [110] B. Obama, "Remarks by the President in a Press Conference" from 19 December 2012, Press Office of the White House, December 2012 (published online)
- [111] SSM, Swedish action plan for NPP, Response to ENSREG's request, Dec 2012
(<http://www.stralsakerhetsmyndigheten.se/Global/Pressmeddelanden/2012/%C3%85tg%C3%A4rdsplaner/swedish-action-plan.pdf>)
- [112] Ds 2012:18 Convention on nuclear safety 2012 extra ordinary meeting - The Swedish National Report, Regeringskansliet, Ministry of the Environment.
(<http://www.regeringen.se/content/1/c6/19/73/60/2c6a4dce.pdf>)
- [113] SSM, Investigation of long-term safety in the Swedish nuclear power industry and measures owing to the accident at Fukushima Dai-ichi, 31-10-2012

(<https://www.stralsakerhetsmyndigheten.se/Global/Pressmeddelanden/2012/Investigation-of-long-term-safety-eng.pdf>)

[114]Sweden's sixth national report under the Convention of Nuclear Safety, Ministry of the Environment, Ds 2013:56, Stockholm 2013.

(https://www.riksdagen.se/sv/Dokument-Lagar/Utdredningar/Departementsserien/Swedens-sixth-national-report_H1B456/?text=true)

[115]Japan Nuclear Safety Institute (JANSI), "Lessons Learned from Accident Investigation Reports on the Fukushima Daiichi Accident and JANSI's Supporting Activities", December 2013

(http://www.genanshin.jp/english/report/lessonslearned/data/F1jiko_kyokun_r1.pdf)

[116]AESJ, "The Fukushima Daiichi Nuclear Accident Final Report of the AESJ Investigation Committee", August 2014

[117]NRA, "Analysis of the TEPCO Fukushima Daiichi NPS Accident", Interim Report, October 2014

(https://www.nsr.go.jp/english/library/data/special-report_20141104.pdf)

[118]ASAMPSA_E, "Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA", Technical report SAMPSA_E/WP30/D30.7/2017-31 volume 2, PSN-RES/SAG/2017-00017

[119]ASAMPSA_E, "Synthesis of the initial survey related to PSAs End-Users needs", ASAMPSA_E D10.2, January 2015, Technical report ASAMPSA_E/WP10/D10.2/2014-05, Reference IRSN PSN-RES/SAG/2014-00193

[120]IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1)

8 APPENDIX 1 - LESSONS LEARNED (EXAMPLES)

8.1 BULGARIA-I

(Contributed by TUS)

The Fukushima Dai-ichi nuclear disaster on March 11, 2011 was an energy accident in the Fukushima Dai-ichi I Nuclear Power Plant that raised a lot of questions and prompts the countries all over the world to reconsider the conditions and requirements to the design and operation of the NPPs. As well in Bulgaria there are working units of nuclear power plants in Kozloduy NPP, Bulgarian authorities are joined to the wide-world enforces in correspondence increased requirements the nuclear reliability and safety.

The regulations concerning nuclear safety and radiation protection in Bulgaria are based on the Act on the Safe Use of Nuclear Energy (ASUNE) since June 2002. This act concerns the main principles of independence of the regulatory authority, of clear regulatory environment in correspondence nuclear safety, radiation protection, physical protection and emergency planning based on evaluation of all safety aspects and regulatory inspections. On this basis there are relevant actions for implementation of different administrative measures [94] that determines the need to study, use and to apply of the lessons learned from the Fukushima Dai-ichi accident.

Before the Fukushima Dai-ichi accident a Program for further modernization of the 5th and 6th Units of Kozloduy NPP was developed and in addition on the basis of the periodic safety reviews a lot of improvements were begun in 2008. Concerning the severe accidents, the program consists of measures which were defined earlier and confirmed during the periodic safety review, for instance:

- Monitoring the temperature of the reactor vessel by installation of temperature sensors.
- Closing the ionization chamber channels in the walls of the reactor vessel shaft (this is a weak point for potential penetration of molten corium in case of a severe accident).

Also there were planed measures that are identified as a result of the periodic safety review by implementation of safety accident management, implementation of symptom based emergency operating procedures for reactor shutdown conditions with closed and open primary circuit, updating, verification and enforcement of safety accident management, taking into account the state of the plant, etc.

On the other hand the subject for influence and experience from Fukushima Dai-ichi is covered by the project ASAMPSA2, as was concluded from a PSA perspective point of view that PSA should no longer be limited to a certain set of events or sequences (concerning the plant status, external events like floods, etc.) [95]. Also, ASAMPSA_E presents that the PSA and its results could be utilised to provide justification for the hazard events or phenomena, and also that the severe external events that cause accidents (as in the case of Fukushima Dai-ichi accident or aircraft impact) can lead to limitation of availability of plant staff, consequently human reliability analysis in this case have to be considered. There are identified significant gaps of knowledge in the fields of nuclear safety that not found much attention until now as accident sequences in shut down mode, including open reactor pressure vessel, accidents in the spent fuel pool, fission product behaviour, reducing the existing large

uncertainties in release fractions to the environment, accident prevention and mitigation by unconventional human actions.

After the Fukushima Dai-ichi accident in 2011 stress tests were performed on European nuclear power plants, including the Bulgarian Kozloduy NPP. On the basis of the defined lessons learned from the accident and from the stress tests in process of planning of the improvement measures in Bulgaria were initiated and accelerated a lot of measures. In addition, a Program for implementation of recommendations following the stress tests on nuclear facilities at Kozloduy NPP was defined. Practically a new improvement program was developed. The program was approved by the Bulgarian Nuclear Regulatory Agency (BNRA) and is currently under implementation. There are a number of improvements, some of which were identified before or as a result of the periodic safety review of 2008, and some of which are new improvements on the basis of lessons learned from the Fukushima Dai-ichi accident, which are in correspondence with the problems associated with accident management.

The additional improvements for severe accident managements in 5th and 6th units of Kozloduy NPP are in result to “Program for Implementation of Recommendations Following the Stress Tests Carried Out on Nuclear Facilities at Kozloduy NPP plc”. The main of them are:

- Construction of a new emergency management system, outside the Kozloduy site;
- Development of technical means for direct water supply to the steam generators;
- Development of technical means for direct water supply to the spent nuclear fuel ponds in the spent fuel storage facility;
- Closing the ionizing chamber channels in the walls of the reactor cavity;
- Implementation of the symptom based emergency operating procedures for the shutdown states with open reactor;
- Implementation of severe accident management guidelines;
- Installation of additional hydrogen recombiners in the containment;
- Measuring channels for monitoring of vapour and oxygen concentrations in the containment;
- Installation of a wide range temperature sensors for monitoring the temperature of the reactor vessel;
- Improving on-site and off-site emergency plans, taking into account difficulties in accessing the emergency control rooms, providing alternative routes for evacuation, transport of fuels and materials, access of the staff, etc.;
- Study of the options for localizing the molten core in case of a severe accident;
- Development and implementation of the spent fuel pool severe accident management guidelines.

The Bulgarian national report [80] identifies modifications for further enhancements as possible measures to increase robustness of the plant which have to be on one hand planned and implemented in the next period and on another hand to be subject of an extended PSA. The most important from them are:

- Development of measures for prevention of water intake in the plant drainage network in case of valley flooding.
- Development of an emergency procedure for personnel actions in case of wall ruptures of waterpower dams on the Danube River (Jelezni Vrata 1 and 2).
- Modernization of the draining and sewage systems in accordance with the planned design for reconstruction of the system from the modernization program of 5th and 6th units of Kozloduy.
- Investigation of possibilities to protect the equipment of bank pumping station 2 and 3 of external flooding with maximum water level equal to 32.93 m, and etc.

Taking into account the results of discussions during the country and the peer review in the period after the Fukushima Dai-ichi accident, the following areas for further improvements (weak points) could be also presented:

- To be considered the lack in the implementation of measures in the area of accident management, such as mitigation of hydrogen risk and prevention of the containment melt-through;
- To be investigated the possibilities for solutions for the management of liquid releases in the events of a severe accident;
- To be further assessed the effectiveness of severe accident management with the currently available hardware with aim for mitigation of severe accidents;
- For the aim of severe accident management should be investigated in more detail the consequences of possible adverse effects of earthquakes;
- It needs to be reconsidered the simultaneous core melt/fuel damage accidents in different installations, during or after decisions on complete list of measures for mitigation of severe accidents;
- To be developed severe accident management that fully covering shutdown states, including those with open reactor;
- Generally the potential accidents in spent fuel pool are not analysed in detail. There is no severe accident management data for spent fuel pool accidents, but the development is defined by the recently adopted improvement program.

The extreme weather conditions and the combinations with other hazard events still need to be considered. With this regard, BNRA requested Kozloduy NPP to perform a consolidated review of extreme weather hazards in correspondence with IAEA requirements and guidance and for development of a plan to monitoring and identification of the improvements. On the other hand authorities consider provision of a monitoring and alert system for extreme weather with aim adequate operating procedures in those cases.

The Kozloduy NPP is in compliance with the licensing and Bulgarian national regulations on nuclear energy and radiation safety and deterministic as well as the probabilistic assessment studies have been developed for all operational units in order to confirm the design basis and the defence-in-depth. On the other hand the result from the existed probabilistic safety assessment (PSA) does not include external flooding or extreme weather that was determinative in the case of Fukushima Dai-ichi accident. In particular, the lack of regulatory criteria about the extreme weather is not described in the national report of Bulgaria. The PSA results presented in the national

report for 5th and 6th units of Kozloduy NPP do not address the external flooding and extreme weather, consequently it should be included in the next PSA updates. Then for example the approach of evaluations re-assessment of the seismic hazard is made and should continue in the future.

Generally, the consequences from Fukushima Dai-ichi accident, determines to be taken into account all the operation modes in PSA, as well all postulated events as severe weather conditions (a combination of extreme weather conditions), fire, flooding and seismic events, etc. These events shall be addressed in the design of eventual new plant and for existing NPP in one extended PSA of the plant, using probabilistic combinations and to set recommendations for consolidated review of extreme external hazards in correspondence to current nuclear safety guidance.

8.2 BULGARIA-II

(Contributed by INRNE)

Immediately after the accident in the Fukushima Dai-ichi nuclear power plant in Japan on March 11, 2011, the European Union decided to reassess the level of nuclear safety in all nuclear power plants in the EU. This was done in close cooperation with ENSREG, the group of national safety authorities of all Member States.

The stress tests [80] were performed in Bulgaria on the nuclear facilities, located on Kozloduy NPP site. The stress test is defined as a targeted reassessment of nuclear safety margins in the light of events occurred at Fukushima Dai-ichi NPP, as a result of the impact of extreme weather phenomena, requiring the performance of the safety functions of the plant and leading to a severe accident. In general, stress test consists in determining the preparedness of a nuclear power plant to respond to the consequences of the occurrence of extreme natural phenomena.

Based on the results of the stress tests, at the end of December 2012, the BNRA issued the National Action Plan of Bulgaria [81] which included timetables for implementation of defined measures. In January 2014 the BNRA updated the status of the National Action Plan of Bulgaria towards 31 December 2013 with included a new Part IV: “New Measures and Activities” and issued a new revision [82].

The National Action Plan of Bulgaria unites all technical and organizational measures, and joint actions at the level of Kozloduy NPP site and on the institutional level, resulting from the safety reassessment of the nuclear facilities in operation (the nuclear reactors and the spent fuel pools of units 5 and 6, and the spent fuel storage facilities). The PSA studies in Bulgaria are periodically updated to reflect both the current state of the plant, after numerous upgrades, and development of the analyses methods.

In 2010, an update of PSA Level 1 for units 5 and 6 of Kozloduy NPP [85] for all operational states (full power, low power and shut down) was completed, including the state with the nuclear fuel located in the spent fuel pool. The PSA reflects the configuration of units 5 and 6 towards the end of 2007. Kozloduy NPP units 5 and 6 PSA Level 1 covers the determination of the fuel damage frequency for the following categories: internal IEs; internal fires; internal floods; seismic hazards. External initiating events other than seismic effects are not accounted for in the PSA.

In 2006, PSA Level 2 for full power was completed. It covers internal events, internal flooding, internal fires and earthquakes. Presently, the Probabilistic Safety Assessment Level 2 is being updated and available results are not updated. Upgraded version of the PSA Level 2 for units 5 and 6 will be covered for all operational states and will be based on the interface with PSA Level 1 developed in 2010.

The development of the Severe Accident Management Guides (SAMGs) in Bulgaria began in 2003-2004, following an extensive study. The SAMGs were implemented in practice at the end of 2012, following a successful process of verification, validation and operators training. The SAMG in Kozloduy NPP are unit based, and thereby each nuclear facility on the site is capable to react independently to the symptoms in case of severe accident. The National Action Plan based on the stress tests, the analyses of the phenomena, resulting from a severe accident in the spent fuel pool (SFP) and in the shutdown open reactor, will be completed. On this basis SAMGs will be developed for SFP and shutdown open reactor.

The updates of the PSA studies were planned to reflect the lessons learned from the Fukushima Dai-ichi accident. The following topics were planned and will be included in the next upgrades of the PSAs: list of relevant external hazards, including tornado and external flooding (included as measures in the National Action Plan); multi units PSA.

The regulations [84] and guidelines [85] concerning PSA in Bulgaria covered: all internal and external hazards which are applicable for the NPP site; fuel in the reactor core and in the spent fuel pool; all operational states of the units.

Analysis of extreme weather conditions on the KNPP site, using probabilistic methods according to the IAEA methodology, and considering combinations of extreme weather conditions was planned.

The regulations and guidelines concerning the PSA in Bulgaria are developed based on the IAEA safety standards and reference levels for harmonization of the safety requirements for nuclear power plants, defined by the Western European Nuclear Regulator's Association (WENRA). They were established before accident was happened in the Fukushima Dai-ichi NPP. After the accident, the BNRA has taken action on the regulatory framework in order to reflect lessons learned. The BNRA is the regulatory body for nuclear safety in Bulgaria.

As is stated in the National Action Plan of Bulgaria, the next measures related to the legislative framework were planned and into implementation:

- Develop a programme to review the regulatory requirements taking into account the lessons learned from the NPP Fukushima Daiichi accident. Finalization - December 2013. This measure was implemented.
- Revise the existing regulatory requirements upon issue of new IAEA documents that consider the lessons learned from the accident. Finalization: On a regular basis.
- Revision and update of the regulatory guidelines to consider the lessons learned and the relevant new documents of the IAEA and the European Commission. Finalization - December 2014.

8.3 GERMANY

(Contributed by GRS)

The reactor accidents at the Fukushima Dai-ichi plant occurred in the last phase of the development of the new German “Safety Requirements for NPP” [88], promulgated in early 2013. The lessons from the accident were incorporated into the new German regulation, leading to a number of changes, particularly related to the deterministic safety assessment approach. With regard to PSA, the role of PSA insights in the provision of evidence and regulatory decision making outside of the PSR was strengthened. For the first time in Germany, qualitative criteria for the application of PSA Level 1 in frame of safety assessments outside of the PSR were defined. However, no specific requirements on PSA were newly introduced because of the Fukushima Dai-ichi accident.

Within the German (regulatory) framework, the guidelines for performing and reviewing PSA up to Level 2 are developed by the “Facharbeitskreis Probabilistische Sicherheitsanalysen” (FAK), an advisory body to the federal regulator “Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit” (BMUB). The FAK is currently developing supplementary guidance documents to the existing technical documents on PSA methods [92] and data [93], which in turn supplement the German PSA Guide (“Leitfaden PSA”) of the BMUB, issued in 2005 [90]. These additional supplements will give more detailed requirements on the scope and methods for PSA on a number of specific issues, e.g. hazard assessment. In particular, the following issues have been emphasized/ introduced based on the lessons learned:

- Applying a fixed analysis time of e.g. 24 h for PSA (Level 1) and assuming that scenarios will be contained due to successful emergency measures, if core damage does not occur before, is no longer accepted. It has to be demonstrated that a controlled plant state has been reached that can be maintained for a prolonged time period barring additional (probabilistic) failures.
- The reliability of the spent fuel pool cooling has to be included into the scope of the PSA.
- The scope of the PSA Level 1 is extended to “fuel damage states” (cf. ENSI-A05 [89] for a similar concept, which specifically covers damages to fuel elements outside of the reactor core). This extension is in line with the German Safety Requirements [88], where PSA Level 1 “core damage” frequency is defined to include all initiators and all plant operating states.
- According to [88] and as a result of the lessons learned, the scope of PSA has been extended to perform a systematic site-specific screening of hazards to be analysed, also extending to combinations of initiating events. This is specifically requested for combinations of external as well as internal hazards.
- For the probabilistic assessment of the reliability of emergency operating procedures as well as of severe accident management actions, the specific boundary conditions of each scenario (accessibility/operability of equipment, environment/high radiation areas, etc.) have to be taken into account.
- Hydrogen issues outside of the containment should be covered in PSA Level 2 investigations, both for releases by containment venting and for other hydrogen releases into the containment (containment failures).

In addition, GRS is performing research into specific issues for a PSA with an extended scope. One focus is on a systematic and efficient extension of detailed PSA Level 1 assessment to internal and external hazards. To this end, three aspects are mentioned [91]: Analysing the hazards and their combinations with respect to relevance and frequency (of exceedance); defining initiating events induced by each relevant hazard; extending the plant

model to include the hazard induced failures and unavailability of SSC. Another research issue is the extension of PSA Level 2 analyses to low-power and shutdown operating states and severe accident scenarios in the SFP.

8.4 ITALY

(Contributed by ENEA)

ENEA lessons learned from the Fukushima Dai-ichi accident for the development of extended PSA.

The Fukushima Dai-ichi accident of Japan in 2011 has discovered various gaps related to the current PSA approach usage for plant risk assessment. This makes some issues to be re-considered and/or implemented in the PSA application and state of practice: these include, for instance, PSA for extreme external events, site-wide risks (including multiple units and spent fuel pools), extended accident scenarios (including long-term station blackout, SBO, and loss of ultimate heat sink), implying, for instance, consideration for prolonged mission times. An additional important point relates to the identification of the dependencies between the external hazards and their modelling within the PSA framework.

An assessment of the lessons learnt from the Fukushima Dai-ichi nuclear accident for implementing PSA methodology will address some foundational notions related to a number of factors, as highlighted by the event:

- The dependency between seismic events and tsunamis (and, more generally, between certain classes of external hazards);
- Plant vulnerability to SBO;
- The risk significance of long term SBO;
- Risk associated with multi-unit events, including handling of CCF events, unit-to-unit interactions and dependencies, human error assessment in multiunit plant sites;
- Risk associated with spent fuel pools;
- Need for a stable, long term, ultimate heat sink;
- Consideration for prolonged mission times;
- Performance assessment of passive systems and their role for the mitigation of external events implying the SBO;
- The role of operator under severe accident conditions (human reliability);
- The considerations for rare events;
- Re-assessment of DID, in terms of weaknesses and gaps between the different Levels.

L2 PSA, as well, has to be extended to cover external hazards, in the frame of the full scope PSA development, and specifically the related aspects, as coming out from the analysis.

- Plant Damage States under external hazards
- Loss of containment function failure modes
- Accident phenomenology investigation
- Hydrogen explosion
- The role of operator under severe accident conditions and human reliability
- SAMG implementation
- Site risk issue
- Risk associated with spent fuel pools

- Consideration for prolonged mission times
- Role of passive systems relevant for the mitigation of severe accidents
- Re-assessment of DID, in terms of weaknesses and gaps between the different levels
- PSA application to all power plant status, e.g. low power and shutdown: full scope PSA
- Uncertainties evaluation

Recapitulating, the issues emphasized within the present study are to be tackled to use the results of the PSA appropriately in future risk-informed decision making processes.

Focus should be on the risk itself, rather than just frequency, and all risk contributors are to be covered appropriately as far as possible in a consistent and exhaustive manner.

In order to solve some incompleteness issues, research on extreme external hazards, risk assessment of the spent fuel pool and site risk is required. These are the emerging issues after the Fukushima Dai-ichi accident.

8.5 SWEDEN

(Contributed by Lloyd's Register)

Following the severe accident at the Fukushima Dai-ichi nuclear power plant in 2011 and the EU stress tests completed in 2012, a Swedish national action plan [111] covering all Swedish nuclear power plants has been developed to implement lessons learned from the accident and to deal with the conclusions from the second extraordinary meeting [112] under the Convention on Nuclear Safety in 2012. The Swedish action plan mainly contains crosscutting and comprehensive measures and presents investigations whose aim is to determine and consider which technical and administrative measures are fit for purpose, how they shall be implemented and the appropriate time schedule for implementation. The measures listed in the Swedish national action plan [111], which consists of further analyses and investigations, are scheduled in three different categories, 2013, 2014 and 2015, corresponding to the year when the measures shall be completed. This categorization is based on an assessment of the urgency of the measures' implementation as well as the complexities of these measures.

In addition to the national action plan, a number of measures to increase the level of safety at Swedish nuclear power plants were implemented within a year after the accident at the Fukushima Dai-ichi nuclear power plant. These measures were mainly identified in connection with investigative work linked to the licensees' international forum, WANO, and in connection with the stress test assessments conducted by Swedish nuclear facilities [113]. A majority of the measures had been completed by the end of 2012. These measures are relatively straightforward measures, feasible to take in the short term to increase the likelihood of preventing a serious incident, while also reinforcing the work on severe accident management including emergency response organizations [114].

Below, a summary is provided of some of the Swedish actions taken, or to be taken, in the light of the Fukushima Dai-ichi nuclear power plant accident.

External Events and Natural Hazards

As a result of the stress test assessments, some areas of improvement for the Swedish NPPs have been identified by the licensees while others have been identified by the regulator when reviewing licensee reports. Swedish Radiation Safety Authority (SSM) followed the work of WENRA and ENSREG to develop a methodology for assessing margins for cliff-edge effects due to external events.

The following areas define the measures to be performed by Swedish licensees in relation to natural hazards:

- Seismic plant analyses,
- Investigation regarding secondary effects of an earthquake,
- Review of seismic monitoring,
- Investigation of extreme weather conditions,
- Investigation of the frequency of extreme water levels,
- Flooding margin assessments,

- Evaluation of the protected volume approach,
- Investigation of an improved early warning notification,
- Investigation of external hazard margins,
- Develop standards to address qualified plant walk-downs.

The following areas define the measures to be performed by Swedish regulator:

- Research project regarding the influence of paleoseismological data,
- Estimation of extreme weather conditions.

1) Accident management and recovery

It must be mentioned that the severe accidents involving core melt and melt-through of the reactor pressure vessel are design basis accidents for the consequence mitigating systems at Swedish NPPs where the system for filtered containment venting is the main component. The containment filtered venting systems, including relevant instrumentation, are designed for passive operation over at least 24 hours.

2) Risk Assessment

According to the safety regulations SSMFS 2008:1, all Swedish reactors have to be analysed with probabilistic methods to supplement the basic deterministic safety studies. All power reactors have to perform complete Level 1 and Level 2 PSA studies including all operating modes and all relevant internal and external hazards for the sites. Today, all power reactors have performed Level 1 and Level 2 studies. The Level 1 studies have been updated continuously with regard to plant modifications. Work has been performed to fill gaps in the Level 1 studies and to finalize studies for low power operation, area events and external hazards.

The basic PSA studies are expected to be updated every year taking into account the past year's plant modifications which have an impact on the PSA-result. In principle most licensees are moving towards practising a so-called "Living PSA". PSA results are also used routinely by the licensees to support decisions concerning significant modification of the designs, modification of operations, documentation and assessment of events.

As mentioned in earlier national reports, the numerical PSA figures are not regarded as a definitive and exact value of the actual risk level. There are no requirements related to numerical PSA results, although the licensees have such safety objectives. The studies should be sufficiently detailed, comprehensive and realistic to identify weaknesses in the designs and to be used to assess plant modifications, modifications of technical specifications and procedures as well as assessment of the risk significance of events.

2.1) Earthquakes

SSM assesses that the licensees have not taken the measures required under the Authority's regulations for certain reactors. It has for example not been fully demonstrated that important functions needed to bring all reactors to a safe state will perform as intended during and after an earthquake.

Also, the licensees need to complete the in-depth analyses required for evaluating the safety margin for safe shutdown and implementation of the improvements identified in the updated comprehensive risk and safety assessments. As far as concerns 2 of the sites, a more detailed analysis also needs to be conducted in terms of earthquake-induced flooding.

2.2) Flooding

All the nuclear power plants are capable of withstanding a rise in sea water level of 3 metres, which the licensees estimate has a probability of once per 100,000 years (10⁻⁵/year). In the assessment of SSM, this estimate should be evaluated with further measures.

Combination effects of waves and high water levels have not been taken into account for all facilities. This is why further analyses are needed to take these combinations into consideration as well as to shed light on potential dynamic effects in connection with flooding phenomena.

2.3) Extreme Weather Conditions

The comprehensive risk and safety assessments demonstrate the nuclear power plants' resilience against the conditions that might arise at the plants as a result of different kinds of extreme weather conditions. The comprehensive risk and safety assessments nevertheless show that a number of areas contain major uncertainties or for some other reason should be investigated further to make it possible to identify opportunities to further strengthen the facilities' protection in connection with these events. For example, the procedures for the working staff in terms of requisite measures in the event of large quantities of precipitation and extreme temperatures should be reviewed. Also, no in-depth analyses of combinations of different weather phenomena have been conducted, such as extreme snowfall together with extreme winds.

Furthermore, it has been established that there is a lack of detailed and thorough descriptions of how the nuclear power plants are impacted in connection with possible ice storms. One engineering assessment, however, is that an extreme ice storm might cut offsite power and risk blocking ventilation systems and hampering access to the site. The fact that in-depth analyses have not been conducted is assessed as a deficiency in relation to current regulations and must consequently be performed.

2.4) Consequence-Mitigating Systems

The comprehensive risk and safety assessments demonstrate the importance of consequence-mitigating systems, for example accident filters and the independent functions for containment spray. This mainly applies in connection with power failures and a loss of heat sink, or a combination of both these events. However, it has been observed that there are uncertainties in the analyses of consequence-mitigating system performance in a long-term sequence, so it needs to be ensured that these systems are capable of performing during long-term accident sequences in addition to all the conditions applying to the scenarios in which the systems are credited. This for example applies to the conditions arising if these systems are used for transferring heat from the reactor core to the atmosphere.

2.5) Power Failures

All Swedish nuclear power plants have alternative reserve power systems in the form of gas turbines within or close to the site. However, these reserve power systems have not been safety classified, meaning that lower requirements on quality and testing apply than for safety systems. As the comprehensive risk and safety assessments indicate that an alternative reserve power system could be crucial during a sequence of events where all offsite power and ordinary reserve power is unavailable, the need to strengthen these systems should be investigated, particularly when considering situations where several reactors are affected simultaneously.

In the event of a loss of all alternating current (i.e. a loss of offsite power in addition to loss of ordinary and alternative reserve power); only the power systems with battery back-up for instrumentation and manoeuvring of components remain operational. At the present time, requirements are imposed on the batteries working for one to four hours, although analyses and support documentation show that they can work for a longer period of time. Thus it has been deemed crucial to review the potential for increasing the current battery capacity by qualifying the batteries for longer periods of operation or, alternatively, disconnecting the batteries from non safety-critical equipment while also examining the potential to recharge the batteries using mobile equipment.

It must be possible to use mobile equipment if there is a loss of all alternating current, but the capacity and number of mobile units are insufficient for all kinds of events, particularly if several reactors are affected simultaneously. This is why it is considered essential that the licensees take stock of their mobile units to ensure that they have an adequate quantity of units, that they offer sufficient capacity and are available in the event of severe accidents.

The comprehensive risk and safety assessments also show that there may be a need to refill lubricant within a few days at some facilities, which is why a sufficient supply of lubricant should be ensured at the site.

2.6) Loss of main heat sink

All Swedish nuclear power plants are dimensioned to be brought to a safe state if the seawater inlet is blocked, also to keep the plant in this state. It was nonetheless shown from the comprehensive risk and safety assessments that this has not been fully verified as far as concerns some of the power plants, so this work remains to be done.

Simultaneous blockage of both inlet and outlet channels has not been taken into account previously as part of the analyses of these plants and the comprehensive risk and safety assessments now show that these conditions necessitate a number of manual measures. It has been established that an in-depth analysis of manual measures that may be necessitated by accident sequences that have been taken into account needs to be performed, in addition to an evaluation of available resources. These analyses should consider access to the facility on the basis of assumed accident sequences and their potential impact on the work environment.

The comprehensive risk and safety assessments now also demonstrate the major significance of independent core cooling functions, where both permanent and alternative systems as well as mobile units raise the level of the

facilities' safety and robustness. For the purpose of ensuring the availability and performance of these systems, in-depth analyses should be performed to evaluate present independent core cooling functions and to identify a potential need for additional improvements or implementation of new systems.

In order to maintain cooling of the fuel pools in accident situations, manual measures are needed; at the same time, however, lessons learned from Fukushima Dai-ichi show that access to reactor buildings can be hampered during severe accidents. This is why it is considered essential that the licensees evaluate the potential to implement alternative solutions for cooling of fuel pools by implementing both permanent installations and mobile units. A key prerequisite in connection with these investigations is to take into consideration the personnel's capability to carry out potential manual measures in connection with these events/accidents.

2.7) Emergency response management and emergency preparedness

The comprehensive risk and safety assessments demonstrate the importance of the consequence-mitigating systems, where the accident filters are key. In an accident situation where residual heat removal has failed and the reactor core is melting through the reactor vessel, the pressure in the containment will rise until valves to the accident filter open and relieve the pressure from the containment into the atmosphere. This filter has been designed so that a considerable proportion of the radioactive substances that may be present in the gases passing through the accident filters are captured, thus largely preventing ground contamination.

The accident filters were originally designed for 24 hours of operation without operator actions. As the lessons learned from the accident at Fukushima Dai-ichi have demonstrated that accident sequences can be prolonged and that it can be difficult in these situations to carry out manual actions within 24 hours, the licensees need to evaluate the accident filters in terms of long-term operation.

In Sweden, work has long been underway to develop the facilities for the purpose of preventing hydrogen explosions. It has nonetheless been established that the licensees have not conducted a detailed and thorough study of the risk of hydrogen leakage to the reactor building, which in fact did occur from the reactors of Fukushima Dai-ichi. For this reason, the licensees must investigate these risks further. Above all, these investigations should focus on the risk of hydrogen accumulation in reactor buildings, as well as the need for additional monitoring to assist operators and other working staff. Beyond this, dealing with hydrogen over a long-term perspective needs to be taken into account.

Strategies for emergency response management are at the present time oriented at sequences where the consequence-mitigating systems protect containment integrity and thus prevent large and uncontrolled radiological discharges into the environment. Lessons learned from the accident at Fukushima Dai-ichi nevertheless indicate that pre-planned strategies are also needed covering accidents involving failure of the containment function and where considerable releases of radioactive materials are unavoidable.

When updating existing strategies for emergency response management, an in-depth analysis of the accident response organisation's structure and staffing also needs to be performed to ensure that it is capable of dealing with all situations, in particular situations where several reactors are affected simultaneously.

8.6 LITHUANIA

(Contributed by LEI)

The stress tests performed in Lithuania on the Units 1 and 2 of Ignalina NPP (currently under decommissioning) and the spent fuel interim storage facilities translated into a series of measures to enhance the safety of the nuclear facilities. Several provisions pertain to the seismic hazard, such as the prevention of spent fuel cask tip-over, seismic alarm and monitoring system, emergency preparedness for the existing and new spent fuel interim storage facilities. Other address the power supply to the instrumentation and control system in the spent fuel storage pools, the fuel supply for assuring long-term operation of diesel generators and the upgrading of the information system to improve the information transfer on the spent fuel storage pools of both units to the main control room, the accident management centre and the Lithuania's State Nuclear Power Safety Inspectorate (VATESI).

Activities of TSOs and lessons learned following the accident at Fukushima Dai-ichi NPS

Organisation	Activity/Project	Results/Reports	Lessons learned (reference to document, website, etc.)
Lithuanian Energy Institute	<p>Ignalina NPP spent fuel coolability analysis in the spent fuel pools.</p> <p>Participation in the SARNET-II (Network of Excellence for a Sustainable Integration of European Research on Severe Accident Phenomenology and Management - Phase 2), in Work Packages:</p> <ul style="list-style-type: none"> “ASTEC Code Assessment”; “Bringing research results into reactor application”. 	<p>SARNET report on the modelling and analysis of results of processes in the spent fuel pools.</p> <p>ERMSAR 2013 paper “Activity in the syntheses of spent fuel pool accident assessments, using severe accident codes” (together with other SARNET partners)</p>	<p>Performing the safety assessment of spent fuel pools at Ignalina NPP the additional failures were added to the initiating events.</p> <ul style="list-style-type: none"> http://www.sar-net.eu/ Kaliatka A., Ognerubov V., Vileiniškis V., Ušpuras E. Analysis of the Processes in Spent Fuel Pools in Case of Loss of Heat Removal due to Water Leakage // Science and Technology of Nuclear Installations, Vol. 2013, Article ID 598975, 11 pages, 2013. Kaliatka A., Uspuras E., Vileiniskis V. Analysis of heat removal accidents in the spent fuel pools of Ignalina Nuclear Power Plant // The 15th International Topical Meeting on Nuclear Reactor Thermal-Hydraulics (NURETH-15), Pisa, Italy, May 12-17, 2013, CD p. 1-12.
Lithuanian Energy Institute	<p>Assessment of Potential Visaginas NPP Construction Sites in Respect of External Events (analysis of the following external factors: human induced events, meteorological phenomena and site flooding) performed according the agreement between JSC Visaginas NPP and LEI.</p>	<p>Reports prepared in 2012:</p> <ul style="list-style-type: none"> Assessment of unintentional human induced events, meteorological and flooding hazards. Survey of Statistical Data and Probabilistic Methods. 	<p>Results performed during research may greatly contribute to making decisions regarding specific VNPP construction site and planning its risk management.</p> <ul style="list-style-type: none"> http://www.vae.lt/projektas/en/ Alzbutas R., Povilaitis M., Vitkutė J. Application of probabilistic uncertainty analysis for modeling of gas pipeline explosion // 11th international probabilistic safety assessment and management conference and the annual European safety and reliability conference (PSAM11 ESREL2012), Helsinki Finland, June 25-29, 2012. IAPSAM & ESRA, 2012.

Organisation	Activity/Project	Results/Reports	Lessons learned (reference to document, website, etc.)
		<ul style="list-style-type: none"> Update of the evaluation of man-made unintended events. Update of the evaluation of meteorological hazards. Technical note: Review of statistical data and probabilistic methods. Final reports: Assessment of ultimate heat sink characteristics and flooding risks and detailed assessment of gas explosion. 	<p>ISBN 978-1-62276-436-5, p. 5561-5570.</p> <ul style="list-style-type: none"> Česnulytė V., Alzbutas R. Probabilistic modelling and uncertainty analysis of extreme weight of snow // 11th international probabilistic safety assessment and management conference and the annual European safety and reliability conference (PSAM11 ESREL2012), Helsinki Finland, June 25-29, 2012. IAPSAM & ESRA, 2012. ISBN 978-1-62276-436-5, p.1243-1252. Ušpuras E., Rimkevičius S., Povilaitis M., Iešmantas T., Alzbutas R. Hazard analysis and consequences assessment of gas pipeline rupture and natural gas explosion // Management of natural resources, sustainable development and ecological hazards. Ravage of the planet III: third international conference on management of natural resources, sustainable development and ecological hazards / Ed. C.A. Brebbia, S.S. Zubir. Ashurst, Southampton : WIT Press, 2012. ISBN 978-1-84564-532-8, p. 495-504.