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

"NUCLEAR FISSION"

Safety of Existing Nuclear Installations

Contract 605001

ASAMPSA_E guidance for level 2 PSA

Volume 2

Implementing external Events modelling in Level 2 PSA

Reference ASAMPSA_E

Technical report ASAMPSA_E/WP40/D40.7/2017-39 volume 2

Reference IRSN PSN/RES/SAG/2017-0002

E. Cazzoli (CCA), J. Vitázková (CCA), H. Löffler (GRS), L. Burgazzi (ENEA)

CCA, GRS, ENEA, NUBIKI, JSI, TUS, JANSI, IRSN have contributed to this report

Period covered: from 01/01/2015 to 31/12/2016	Actual submission date: 31/12/2016	
Start date of ASAMPSA_E: 01/07/2013	Duration: 42 months	
WP No: 40	Lead topical coordinator : Horst Löffler	His organization name : GRS

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

ASAMPSA_E Quality Assurance page

Partners responsible of the document:	**GRS, CCA, ENEA, IRSN**
Nature of document	Technical report
Reference(s)	Technical report ASAMPSA_E/WP40/D40.7/2017-39 volume 2 Rapport IRSN-PSN-RES/ SAG/2017-002
Title	Implementing external events in L2 PSA
Author(s)	E. Cazzoli (CCA), J. Vitázková (CCA), H. Löffler (GRS), L. Burgazzi (ENEA)
Delivery date	31/12/2016
Topical area	L2 PSA, severe accident management, external hazards
For Journal & Conf. papers	No

Summary:
The objective of the present document is to provide guidance on the implementation of external events into an "extended" L2 PSA. It has to be noted that L2 PSA addresses issues beginning with fuel degradation and ending with the release of radionuclides into the environment. Therefore, the present document may touch upon, but does not evaluate explicitly issues that involve events or phenomena which occur before the fuel begins to degrade.
Following the accident at Fukushima Dai-ichi, the nuclear safety community has realized that much attention should be given to the areas of operator interventions and accidents that may develop at the same time in more than one unit if they are initiated by one or more common external events. For this reason and to fulfill the PSA end-users' wish list (as reflected by an ASAMPSA_E survey), the attention is mostly focused on interface between L1 and L2 PSA, fragility analysis, human response analysis and some consideration is given to L2 PSA modeling of severe accidents for multiple unit sites, even though it is premature to provide extensive guidance in this area.

The following recommendations, mentioned in various sections within this document, are summarized here:

1. Vulnerability/fragility analyses should be performed with respect to all external hazards and all structures, systems and components potentially affected that could be relevant to L2 PSA,
2. Importance should be given to the assessment of human performance following extreme external events; for extreme circumstances with high stress level, low confidence is justified for SAM human interventions and for such conditions, human interventions could be analyzed as sensitivity cases only in L2 PSA,
3. Results presentation should include assessment of total risk measures compared with risk targets able to assess all contributions to the risk and to judge properly the safety (see document [15] for recommendations on PSA results presentation),
4. Total risk measures shall be associated to appropriate information on all uncertainties, simplifications and conservatisms that appear today to be inherent to any extended PSA,
5. Because NPPs on multi-units sites are in general not fully independent, verification and reassessment of current single PSAs is needed before developing multi-units PSA,
6. Because established methodologies for multi-unit sites L1-L2 PSA analysis are not yet available (even if multi-unit sites L1-L2 PSA analysis are now on-going in some countries), it is recommended to use first a simplified method. The boundary between L1 and L2 PSA shall be defined appropriately and some relevant adaptations/simplifications in both L1 and L2 PSA may be considered (in a first step) to limit the complexity of the multi-unit sites L1-L2 PSA development.

Visa grid

	Main author(s) :	**Verification**	**Approval (Coordinator)**
Name (s)	E. Cazzoli, J. Vitázková,	H. Löffler	E. Raimond
Date	13.12.2016	14.12.2016	28.12.2016

CHANGE HISTORY

Revision	**Date**	*Author*	*Pages or paragraphs changed*	*Nature of the changes*
1	28.08.2015	E. Cazzoli		Draft
2	14.11.2015	E. Cazzoli		Addenda: Contribution ENEA, Comments ENEA, TUS, JSI, GRS ; added Summary and Conclusions
3	29.02.2016	J. Vitazkova	Conclusions	Modifications on text due to comments in meeting in Paris 23rd-27th Nov. 2015, Chapters 2.6 and 5. added, Chapter 4 modified. All later comments and contributions taken into account. Version for final reviews by project leaders.
4	11.03.2016	H. Löffler with J. Vitazkova	2.6, 2.7.2	According to review by the work package leader, modifications have been agreed with CCA.
5	29.03.2016	H. Löffler		Work package leader has duly considered comments by JSI and NUBIKI
6	28.04.2016	E. Raimond, N. Rahni	All	Final review. Few modifications proposed before report issuance. An example of fragility analysis and compliance of the report with the PSA End-Users Needs is also proposed in appendix.
7	09.05.2016	H. Löffler	Summary, 2.8.2	Modifications as agreed between CCA and IRSN accepted.
8	04.10.2016	H. Löffler	7.3	Update according to the ASAMPSA_E end-user's workshop September 2016 (summary of conclusions below): The interest and feasibility of a PSA modeling exactly each DiD level (especially levels 1 and 2) has to be investigated ; proposal for a L2 PSA for multi-unit site seems interesting but needs further developments to be used as it is presented. Recommendations (1) consider all reviewers' comments (2) promote "graded" approach for the development of L2 PSA for external events (3) introduce the discussion on low quality data for rare IE events (natural hazards) and how it considered for L2 PSA development (shall we exclude such IE from L2 PSA ?, how to be consistent in risk metrics applications ? Shall ASAMPSA_E promote full-scope integrated PSA (all IE in one PSA) or promote separated PSA (one PSA for each type of IE in order to avoid mixing situations with different quality in IE data) (4) Comment more precisely the choice to be done between L1-L2 integrated or separated methodologies in the context of external hazards).
9	2.11.2016	J.Vitazkova	all 2.2 7.2	Modifications according to comments of Tractebel, LEI, JANSI and EDF – mostly format, formulations Added paragraph on source terms Merged added Section 7.3 with 7.2 evaluating End User's needs
10	28/12/2016	E. Raimond	Few	Approval reading, consistency with other ASAMPSA_E reports and End-users' recommendations.

LIST OF DIFFUSION

European Commission (Scientific Officer)

Name	First name	Organization
Passalacqua	Roberto	EC

ASAMPSA_E Project management group (PMG)

Name	First name	Organization	
Raimond	Emmanuel	IRSN	Project coordinator
Guigueno	Yves	IRSN	WP10 coordinator
Decker	Kurt	Vienna University	WP21 coordinator
Kumar	Manorma	LRC	WP22 coordinator
Wielenberg	Andreas	GRS	WP30 coordinator until 2016-03-31
Löffler	Horst	GRS	WP40 coordinator WP30 coordinator after 2016-04-01

REPRESENTATIVES OF ASAMPSA_E PARTNERS

Mustoe	Julian	AMEC NNC
Grindon	Liz	AMEC NNC
Pierre	Cecile	AREVA
Godefroy	Florian	AREVA
Dirksen	Gerben	AREVA
Kollasko	Heiko	AREVA
Pellisseti	Manuel	AREVA
Bruneliere	Hervé	AREVA
Hasnaoui	Chiheb	AREXIS
Hurel	François	AREXIS
Schirrer	Raphael	AREXIS
Gryffroy	Dries	Bel V
De Gelder	Pieter	Bel V
Van Rompuy	Thibaut	Bel V
Jacques	Véronique	Bel V
Cazzoli	Errico	CCA
Vitázková	Jirina	CCA
Passalacqua	Roberto	EC
Bonnevialle	Anne-Marie	EDF
Bordes	Dominique	EDF
Vasseur	Dominique	EDF
Panato	Eddy	EDF
Romanet	François	EDF
Lopez	Julien	EDF

Gallois	Marie	EDF
Hibti	Mohamed	EDF
Brac	Pascal	EDF
Jan	Philippe	EDF
Nonclercq	Philippe	EDF
Bernadara	Pietro	EDF
Benzoni	Stéphane	EDF
Parey	Sylvie	EDF
Rychkov	Valentin	EDF
Coulon	Vincent	EDF
Banchieri	Yvonnick	EDF
Burgazzi	Luciano	ENEA
Karlsson	Anders	FKA
Hultqvist	Göran	FKA
Pihl	Joel	FKA
Ljungbjörk	Julia	FKA
KÄHÄRI	Petri	FKA
Wielenberg	Andreas	GRS
Loeffler	Horst	GRS
Hage	Michael	GRS
Sperbeck	Silvio	GRS
Serrano	Cesar	IEC
Benitez	Francisco Jose	IEC
Del Barrio	Miguel A.	IEC

Apostol	Minodora	INR
Nitoi	Mirela	INR
Stefanova	Antoaneta	INRNE
Groudev	Pavlin	INRNE
Laurent	Bruno	IRSN
Clement	Christophe	IRSN
Duluc	Claire-Marie	IRSN
Leteinturier	Denis	IRSN
Raimond	Emmanuel	IRSN
Corenwinder	François	IRSN
Pichereau	Frederique	IRSN
Georgescu	Gabriel	IRSN
Bonneville	Hervé	IRSN
Denis	Jean	IRSN
Bonnet	Jean-Michel	IRSN
Lanore	Jeanne-Marie	IRSN
Espargilliere	Julien	IRSN
Mateescu	Julien	IRSN
Guimier	Laurent	IRSN
Bardet	Lise	IRSN
Rahni	Nadia	IRSN
Bertrand	Nathalie	IRSN
Duflot	Nicolas	IRSN
Scotti	Oona	IRSN
Dupuy	Patricia	IRSN
Vinot	Thierry	IRSN
Rebour	Vincent	IRSN
Guigueno	Yves	IRSN
Prošek	Andrej	JSI
Volkanovski	Andrija	JSI
Alzbutas	Robertas	LEI
Rimkevicius	Sigitas	LEI
Olsson	Anders	LRC
Häggström	Anna	LRC
Klug	Joakim	LRC
Kumar	Manorma	LRC
Knochenhauer	Michael	LRC
Kowal	Karol	NCBJ
Borysiewicz	Mieczyslaw	NCBJ
Potempski	Slawomir	NCBJ
Vestrucci	Paolo	NIER
La Rovere	Stephano	NIER
Brinkman	Hans (Johannes L.)	NRG
Bareith	Attila	NUBIKI
Lajtha	Gabor	NUBIKI
Siklossy	Tamas	NUBIKI
Caracciolo	Eduardo	RSE
Gorpinchenko	Oleg	SSTC
Dybach	Oleksiy	SSTC
Grondal	Corentin	TRACTEBEL
Claus	Etienne	TRACTEBEL
Oury	Laurence	TRACTEBEL
Dejardin	Philippe	TRACTEBEL
Yu	Shizhen	TRACTEBEL
Mitaille	Stanislas	TRACTEBEL
Zeynab	Umidova	TRACTEBEL
Bogdanov	Dimitar	TUS
Ivanov	Ivan	TUS
Kubicek	Jan	UJV
Holy	Jaroslav	UJV
Kolar	Ladislav	UJV
Jaros	Milan	UJV
Hustak	Stanislav	UJV
Decker	Kurt	UNIVIE
Prochaska	Jan	VUJE
Halada	Peter	VUJE
Stojka	Tibor	VUJE

REPRESENTATIVE OF ASSOCIATED PARTNERS (External Experts Advisory Board (EEAB))

Name	First name	Company
Hirata	Kazuta	JANSI
Hashimoto	Kazunori	JANSI
Inagaki	Masakatsu	JANSI
Yamanana	Yasunori	TEPCO
Coyne	Kevin	US-NRC
González	Michelle M.	US-NRC

SUMMARY

This document provides guidance in the implementation of external events modeling in extended L2 PSA and is a complement of the ASAMPSA2 guidelines in this area. The conclusions of the ASAMPSA_E end-users survey and of technical meetings of WP10, WP21, WP22, and WP30 at Vienna University in September 2014 which are relevant for L2 PSA have been reflected in the content of the present document and are being taken into account as much as it is possible with the current status of knowledge.

Issues that belong only to Level 1 PSA analyses in general are not discussed, and it is assumed that the only relevant issues to be resolved according to the end-users' wish list are those subsequent to core damage and/or fuel degradation, i.e. after permanent loss of core cooling and/or decay heat removal functions. Following the accident at Fukushima Dai-ichi, the nuclear safety community has realized that much attention should be given to the areas of operator interventions and accidents that may develop at the same time in more than one unit if they are initiated by one or more common external events. For this reason and to fulfill the PSA end-users' wish list, the attention is mostly focused on interface between Level 1 and Level 2, human response analysis and some consideration is given to Level 2 modeling of severe accidents for multiple unit sites, even though it is premature to provide extensive guidance in this area.

ASAMPSA_E PARTNERS

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

1	Institute for Radiological Protection and Nuclear Safety	IRSN	France
2	Gesellschaft für Anlagen- und Reaktorsicherheit mbH	GRS	Germany
8	Cazzoli Consulting	CCA	Switzerland
9	Italian National Agency for New Technologies, Energy and the Sustainable Economic Development	ENEA	Italy
14	NUBIKI	NUBIKI	Hungary
24	Jožef Stefan Institute	JSI	Slovenia
27	Technical University of Sofia – Research and Development Sector	TUS	Bulgaria

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

Not Applicable

GLOSSARY

ACWS	Auxiliary Cooling Water System
AESJ	Atomic Energy Society of Japan
APET	Accident Progression Event Tree
BWR	Boiling Water Reactor
DiD	Defence in Depth
CCF	Common Cause Failure
CD	Core Damage
CDF	Core Damage Frequency
CDS	Core Damage State
CRT	Common Risk Target
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat (Swiss Federal Nuclear Safety Inspectorate)
EOP	Emergency Operating Procedure
FCI	Fuel Coolant Interaction
FCVS	Filtered Containment Venting System
FP	Fire Protection
HRA	Human Reliability Analysis
L1	Level 1
L2	Level 2
MCCI	Molten Core Concrete Interaction
MCS	Minimal Cut-Set
PDS	Plant Damage State
PSA	Probabilistic Safety Analysis
RCS	Reactor Coolant System
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SFP	Spent Fuel Pool
SSC	Structures, Systems and Components

1 INTRODUCTION

The objective of the present document is to provide guidance on the implementation of external events into an "extended" L2 PSA and is intended as a complement to the L2 PSA ASAMPSA2 guidelines [5]. Some considerations to "extended" PSAs for multi-units sites are also included. The following sub-sections define more precisely the boundaries and the conditions to which this specific guidance is aimed.

It has to be noted that the present document is related to L2 PSA which addresses issues beginning with fuel degradation and ending with the release of radionuclides into the environment. Therefore, the present document may touch upon, but does not evaluate explicitly issues that involve events or phenomena which occur before the fuel begins to degrade and that should be covered by the L1 PSA assessments. Such questions that belong to L1 PSA, will define boundary conditions for the L2 PSA and are addressed by other documents within ASAMPSA_E.

The objectives of the report as defined in [26] accordingly to the End-Users needs ([3], [4]) have been fulfilled as much or as reasonably as possible with respect to "extended" L2 PSA, i.e. the impact of external initiating events and multi-units sites on the performance of L2 PSA.

1.1 EXTERNAL EVENTS UNDER CONSIDERATION

A complete list of events to be considered for extended PSA has been proposed by the ASAMPSA_E project in [1]. It has been decided [2] to group most of them into six main groups that are discussed within the ASAMPSA_E guidelines in separate documents, and these are shown in Table 1.

Nevertheless, from the point of view of L2 PSA the specific initiator is not important, since the analysis starts at the time of "core damage", and what is important is to know the boundary conditions at that time (i.e., it is important to know how the accident reached that point, regardless of what initiated the chain of failures). Therefore, it should be kept in mind that the present L2 PSA guidance is not just specific to the six groups of events shown in Table 1, but covers all events that result in core or fuel damage due to loss of coolant level and/or decay heat removal functions.

Table 1 Groups of external initiating events considered in details in ASAMPSA_E

Initiator group	Initiating events or natural phenomena included
Seismic	Seismo-tectonic events
External floods	Extreme precipitation; events that cause swelling of waterways and/or lakes (in general including elevation of sea level); failure of dams; tsunami
Extreme weather	Effects of high or low temperature; high wind and tornadoes; excess snow
Lightning	Stroke of lightning on power lines, switchyard, transformers, electromagnetic disturbances to electronic components
Biological hazards	Biological (animal, plant) infestation within the installations and water supplies
External explosion, aircraft crash, external fires	Man-made events such as external explosions, civilian and military aircraft (large and small, including crop dusters) crashes, external fires

1.2 IMPACT OF EXTERNAL EVENTS ON L2 PSA ISSUES

It is assumed that the team or teams performing the L2 PSA for external events will be already familiar with the procedures and protocols to be used in the analysis for internal events. All the relevant information can be found in Vol. 1 of the ASAMPSA2 guidelines ([5], Sections 2.1 through 2.15) and the technical approach is discussed in Vol. 2 ([5], Sections 2 through 7).

It should be noted that other current L2 PSA guidelines (e.g. the IAEA [11] and Swiss ENSI guidelines [6], [41]) have no *specific* requirement and *very few* recommendations for the performance of L2 PSA for external events, indicating that the expected impact of external events on the performance of L2 PSA is not as great as it is for the performance of L1 PSA. It can reflect also the fact that performance of external hazards L2 PSA is not yet a common practice.

However some specific issues are to be considered and must be discussed (also in response to some of the End-Users needs). These are detailed in the following sections.

2 EXTERNAL EVENTS SPECIFIC ISSUE IMPACTING L2 PSA

2.1 DEFINITION OF PLANT DAMAGE STATES (PDS)

The content of this section is relevant mostly if the L1 and L2 PSA analyses are not integrated. Moreover, the discussion of definition of PDS is valid for the analyses of initiating events occurring at full power and low power (which normally is part of the shutdown analyses). Since the definition of, and collection of data for the PDS are tasks that may fall upon different teams that perform the analyses (L1 and L2 PSA teams), this section provides a general summary intended primarily for L2 PSA analysts.

This section summarizes some views for the definition of PDS which are common to all external hazards.

It must be stressed, as was done for analyses of internal events, that this task involves close interaction between the teams performing the analyses. L2 PSA team has knowledge about boundary conditions necessary for characterization of accidents after core damage, and L1 PSA team know how accidents progressed up to that point and why core damage occurred. Therefore, this part of the works profits from feedback and potentially iterative work between the two teams in the course of defining the PDSs.

To this point, it is recommended that the L2 PSA team in general takes cognizance and understands thoroughly the definition of systems success criteria used in the Level 1 study, and in particular for accidents initiated by external events, what are the potential initiator-dependent systems failures (failure of systems that occurred as a direct impact from the initiator) and independent failures (failure of systems that may have occurred after accident initiation, at a time that for the most part cannot be specified by Level 1 analyses).

It is also strongly recommended that the L2 PSA team familiarizes itself with the results of Level 1 in terms of individual accident sequences or Minimal Cut-Sets (MCSs) that show the chain of failures (initiator, initiator severity, dependent systems failures, component failures, and operator errors) that ended in core damage.

Operator errors in L1 PSA are of particular importance for L2 PSA analyses if anticipated operator interventions that could be considered as part of SAMGs are introduced in L1 PSA in conjunction with interventions that are part of EOPs. This is the case for instance for containment venting, initiation of containment sprays, or initiation of firewater (or equivalent emergency system) injection in the RCS prior to core damage in BWR plants. In these plants for example, since many of the accident sequences from external events result in L1 PSA consequences similar to complete Station Blackout accidents with failure of all safety high pressure injection systems, the only option for preventing core damage would be to depressurize the RCS and initiate firewater as soon as possible. The danger is that this system may be over-credited in Level 2, if accident progression to the time of core damage is not thoroughly understood by the L2 PSA teams.

In addition, it is also strongly recommended that the L2 PSA team responsible for the definition of PDSs understand the role of auxiliary systems (such as compressed air, auxiliary and component cooling water systems, etc.) in the process of preventing core damage in particular accident scenarios, since these may fail as dependent on the initiator, without immediate failure of the primary safety systems.

For the purpose of “presentation of results” and “analysis of results” (especially for importance analysis) it is strongly suggested to include one additional characteristic in the definition of PDSs that describes the group of initiators. For instance, the following groups of initiators can be identified: internal fires, internal floods, seismic, aircraft crash, floods, tornadoes/high winds and corresponding identifiers to these should be used in the PDS codes in the analysis to differ them in order to recognize within the analysis, which PDS is addressed to which initiator, since the same sequence can be related to more types of initiators.

Moreover, if a group of initiators is subdivided in L1 PSA models into severity classes (e.g. seismic initiators class 1 or S1 considers seismic events with ground acceleration between 0.1 and 0.2 g, seismic class 2 or S2 considers events with ground acceleration between 0.2 and 0.3 g, etc.; or aircraft crash class 1 or A1 considers potential impact of small civilian airplane including crop dusters, class 2 or A2 considers impact of small military airplane, etc.), it is recommended that the PDS characteristic preserves the division into these classes.

The definition of PDSs that has been used for the internal events analysis has to be verified for applicability to L1 PSA accident sequences that are initiated by specific external events. The combination of dependent and independent systems failures due, for instance, to seismically induced sequences may require the definition of additional PDSs that were not considered possible for internal events. In addition, all external events may induce additional failures that were not considered for internal events (such as direct containment failure, containment isolation failure, piping failure inside or outside the containment, unavailability of main control room).

Finally, site personnel may be required to perform actions (such as venting of the containment prior to core damage) that would not be considered under accidents initiated by internal events and that change the status of the containment before the beginning of Level 2 analyses.

Note that some of these boundary conditions (especially with respect to the status of the containment function and attempts to perform interventions that could be considered as part of accident management, hence as part of Level 2) may in general not be of interest specifically to the Level 1 models, therefore it is the responsibility of the Level 2 analysts to alert their Level 1 colleagues on the need to tag or flag accident sequences where containment has been challenged and failed, or where some accident management actions have been exhausted.

It should be noted however that, when here it is stated that the Level 1 analyses can provide information that is important to define boundary conditions for the Level 2 analyses, especially where the containment status is concerned, it is meant always within the bounds of Level 1 specific analyses and competences. For instance, a specific structural analysis for failure of the containment due to earthquake has to be performed for Level 1 and is required e.g. by the Swiss ENSI Section 4.6.2.1 of [6], [41] to discuss the SSC fragility analyses, and it is stated that both structural failure of the containment and failure of pipes that would lead to containment bypass must be considered and assessed. These fragility assessments however are meant to provide information relevant to failures that can influence reactor systems or operations of related components (e.g., in the example of requirements given in [6], [41] there is no specific mention of fragility analyses for pipes exiting the containment whose failure would not lead to a loss of reactor coolant and containment bypass but which could lead to loss of containment isolation). Even with the ENSI requirements, as far as containment failure is concerned, only gross structural failure is normally considered in Level 1, because this may cause failure of pipes and components (or even the reactor vessel) housed within the containment. The potential for cracks and leaks of the containment is not generally included, and therefore the Level 1 SSC fragility studies cannot provide this information. Responsibility for the assessment of leaks from the containment, including failure of penetrations, following an

external initiating event should be assigned to the Level 2 assessment. This issue is discussed in detail in Sections 2.2, 2.4 and 2.5.

Severe accident management strategies aim at protecting the containment during the accident progression: the L2 PSA teams shall identify precisely what is needed for this purpose (reactor building integrity, pipes and penetration tightness, primary circuit depressurization equipment, containment venting, instrumentation, recombiners, valves, electrical or air supply, human access to some rooms for some manual actions …) and examine if the external hazards can induce damage. This information shall then be available in the PDS characteristics.

Considering the Fukushima Dai-ichi accident, also additional structures should be taken into account in addition to containment status – e.g. status of spent fuel storage/pool, which, in current analyses may not be commonly included, except e.g. for the Swiss Mühleberg one-unit BWR plant where a complete analysis was performed in 2010-2013 including all external events, all operational modes including fuel damage in the fuel pool (for details see: [30], [31], [32]). The location of the spent fuel storage should be considered and included in PDS characteristics – if outside the containment or inside the containment. Location of the spent fuel pool outside the containment represents a quite significant potential source of risks in case of hydrogen generation and its immediate release into reactor building with no additional measures from the point of view of defence-in-depth (missing last physical barrier of confinement).

Additional characteristics for defining PDS with particular importance for L2 PSA do not seem to be needed. Any example we could think of would be an accident with somehow catastrophic consequences in Level 1 (everything fails), so that any issue impacting Level 2 would be “mute”. For instance fires after large aircraft impact in the reactor building would have no additional meaning, since in this case either the containment is penetrated / fatally damaged (failure of all pipes assumed due to failure of reactor building and systems located in the building), or the fire should have been taken into consideration in Level 1 (failure of equipment due to fire following the aircraft impact).

2.2 CONTAINMENT ANALYSIS, PHENOMENA AND SOURCE TERMS

2.2.1 GENERAL CONSIDERATIONS

In order to address the potential of leaks from the containment following an external initiating event, it is recommended that, in addition to containment fragility analyses for events that occur within the containment (missiles, internal pressurization, explosions, etc.) fragility analyses should be performed within Level 2 to assess:

- the probability of cracks crossing and traversing the entire wall of the containment resulting in leaks and isolation failure following specific external events initiators (a complement of Level 1 seismic fragility analyses),
- the probability of failure of any of the containment penetrations (cable, pipeline) leading to containment isolation failure in case of specific external events initiators, and
- the probability of failure of any of the containment access doors (man-holes, hatches) leading to containment isolation failure in case of specific external events initiators.

These analyses should be performed only with respect to external initiating events that have a direct impact on the containment (e.g., they need not be done for biological infestation events, lightning, external explosions ...). In case these specific analyses cannot be performed satisfactorily, section 2.5 provides some suggestions for the quantification of these probabilities.

Additional mechanistic codes analyses will be needed in case new or additional external-events specific PDSs have been identified. Protocols and best-practices applicable to these processes are found in sections 2, 3 and 4 of [5] (Vol. 2). For PDSs that are common between internal and external events, there could be an impact of external events on physical phenomena in Level 2 after core damage; e.g. the timing of events could be affected. These two issues however can be covered by the present ASAMPSA2 methodology for internal events [5].

In general, the vast majority of core damage sequences induced by external events behave as sequences that are induced by a loss of power event or loss of ultimate heat sink. A smaller number of sequences (especially for the most severe initiators with extremely large consequences) behave as containment bypass or containment failure prior to core damage. Therefore, there is no need of new methodologies or approaches to treat source terms with respect to external hazards.
It is recommended that a limited set of specific accident sequence sensitivity analyses should be performed to verify that the results of analyses for internal events apply at least for risk dominant Level 2 sequences within the uncertainty bounds. All phenomena related to in-vessel accident progression, vessel failure, and ex-vessel accident progression should be then reviewed, including source terms.
Nevertheless, in case of multi-unit L1-L2 PSA, specific consequences analyses are needed to assess the impact of one damaged reactor on the other ones. Such consequences analyses shall be similar to those done for a single unit PSA (impact of environmental conditions on human actions and equipment survivability) but shall be applied to a vast set of multi-units site conditions.

2.2.2 EXAMPLES

2.2.2.1 Containment PSA against earthquake in Japan

Note: The example (proposed by JANSI) shown below is a preliminary estimate. In the L2 seismic PSA to be conducted for existing NPPs in compliance with the recommendation by the regulator after Fukushima Dai-ichi accident, more detailed analyses are to be conducted.

(1) Failure mode of Containment

In the AESJ seismic PRA standard [37] [38], accident scenarios concerning loss of containment function by the earthquake is mentioned when conducting L2 PSA for seismic event. Accident sequences leading to the loss of containment function are identified considering the following items:

- Failure of CV (containment vessel) structure due to earthquake;
- Degradation pressure capacity of CV due to earthquake;
- Failure of CV isolation due to earthquake;
- Loss of pressure suppression function due to earthquake;
- Loss of decay heat removal function due to earthquake;
- Loss of FP release suppression function due to earthquake.

As for steel containments, buckling of the containment and pipe penetration damage is considered as main failure mode. In L2 PSA, occurrence of buckling of the CV is considered as failure mode (loss of containment function) in many cases.

As for Reinforced Concrete or Prestressed Concrete, overall structural failure due to shear failure of the containment is a dominant failure mode. Anti-leak function is secured by the steel liner, and large deformation by shear failure leads to the ductile failure of the liner and the loss of anti-leak function.

For every type of containment, failure of reactor building is assumed to lead to containment failure.

Seismic fragility of the containment for overall structure failure and local failure can be evaluated based on the seismic design where response analyses for design basis earthquakes are conducted.

(2) Example of fragility analysis of CV [37]

In the examples of fragility analysis for steel containments shown in AESJ seismic PRA standard [37], fragility analysis is focused on buckling failure.

● Earthquake response analysis

Reactor building including the containment is modelled in the response analysis, soil-structure interaction is considered as well.

In the fragility analysis applying “the method based on realistic capacity and realistic response” (explained below), earthquake ground motions of different levels (e.g., seven levels) are used as input motions, and time history response analyses are conducted.

In the earthquake response analysis of NPP building, as well as in fragility analysis, usually a stick model has been used. With multiple stick models structures and members (e.g. shear wall, containment vessel, etc.) comprising the reactor building are represented. If floor flexibility cannot be ignored, a multiple stick model considering floor flexibility (e.g., connecting sticks with springs) is used.

● Fragility analysis: Response (earthquake response)

In the fragility analysis, realistic response and capacity are estimated probabilistically. To evaluate realistic response three methods are mentioned in the AESJ standard:

(a) method based on realistic capacity and realistic response (based on earthquake response analysis),

(b) method based on realistic capacity and response factors,

(c) method based on capacity factor and response factor.

In the methods (b) and (c), which are based on the response obtained in the design, response factors F_1, F_2, F_3, F_4 are used to estimate realistic response, which takes into account uncertainties included in the evaluation of the response:

F_1: earthquake ground motion at the free surface (where design earthquake ground motion is specified),

F_2: earthquake input to building and structure,

F_3: earthquake response of building and structure,

F_4: earthquake response of components (CV).

In the methods based on response factors (methods (b) and (c)), all these factors are used.

In the method (a) only F_4 is used generally, as the result of time history response analyses with earthquake ground motions of different levels (e.g., seven levels) are used.

F_4 is modelled as the product of seven random variables (sub-factors) as,

$F_4=F_{ESS} \times F_D \times F_{EM} \times F_{MOD} \times F_{EMC} \times F_{ECC} \times F_\mu$

where,

F_{ESS}: factor for input to equipment (CV)

F_D: factor for damping of equipment (CV)

F_{EM}: factor for modelling of equipment (CV)

F_{MOD}: factor for response of higher mode (of CV)

F_{EMC}: factor for mode combination (of CV)

F_{ECC}: factor for earthquake component combination

F_μ: factor for plastic energy absorption (of CV)

In the example shown in refs. [37], [38], some of above factors are not considered, or median is set to 1.0 as the response is estimated based on time history response analysis.

● Fragility analysis: Capacity (buckling strength)

Buckling strength is evaluated by the formula for thin-walled cylindrical shell subject to axial compressive load (vertical earthquake response in vertical direction is considered) and bending moment.
In the example, the median yield stress of steel is assumed as 1.2 x Sy (Sy: design yield stress). Using this median yield stress value in the formula, the median of buckling stress is estimated.
Uncertainties of the buckling capacity are evaluated based on experimental data from which the formula is developed assuming log-normal distribution and logarithmic standard deviations β_R (aleatory uncertainty) and β_U (epistemic uncertainty) are given.

Using realistic response and realistic capacity, fragility of the containment for buckling as a failure mode is estimated.

2.2.2.2 Confinement PSA at IRSN (France)

IRSN is performing research to extend the scope of its existing L2 PSA for the French PWRs to internal or external hazards. Due to limited available resources, the concept of "confinement PSA" is applied: the objective is to calculate conditional failure for the confinement function depending on the external hazards intensity. In 2016, this is being applied to earthquake and internal fires.

The global approach can be summarized as follow:

- define list of system, structure and components (SSC) that are needed to fulfill the confinement function,
- select limited number SSCs that must be studied in details because they are requested for the confinement function (e.g. containment steel liner, SG steam line, sump recirculation lines, RCS depressurization system, FCVS …),
- define the failure modes for each SSCs associated to the hazards,
- develop SSC failure analysis,
- develop probabilistic assumptions (conditional failure probability, event tree, …).

Some details of an on-going seismic analysis for a PWR steam generator main steam line are presented in Appendix 1.

2.3 HUMAN RELIABILITY ANALYSIS

2.3.1 GENERAL CONSIDERATIONS

The techniques used to assess human actions in L2 PSA are discussed in detail in Chapter 3 of the ASAMPSA2 guidelines, Vol. 2 [5] (At this time, it is expected that the same techniques and models will be used for "extended PSA" (including external events initiators). For the most part, the current models are adequate for analyses of multi-units accidents, but some points that are specific to the conditions to be expected during accidents initiated by these events should be carefully reviewed as discussed below.

L2 PSA accident sequences that are induced by external events should be examined in order to verify and take into account whether site personnel interventions have not already been credited in Level 1 either as part of the EOPs or as recovery actions (see also the previous section on definition of PDSs). In addition, the availability of systems that may be credited for Level 2 may be impacted by the specific initiators (availability of signals, non-plausible/misleading signal(s), failure of components, loss of site personnel, problems with the Technical Support Center). Special attention should be given to the availability of sufficient resources (systemic and human) for multi-units sites. After some adaptation, existing HRA methods should be able to cope with Level 2 issues after external impact.

However, the real challenge seems to be proper modelling of the actual situation. As by definition of Level 1 PSA, the external event has been so powerful that it may have caused failure of systems, structures, signals etc., resulting in core damage. Therefore, the staff might have to face extremely serious conditions and degradation of plant systems, possibly including disrupted communication lines, inaccessibility of resources, and missing personnel. In addition, external or internal radioactivity levels may preclude interventions that involve work outside or inside the buildings. It is obvious that human reliability under such conditions is very uncertain.

The HRA methods and data used in the analyses should be critically examined with regard to their applicability under the described circumstances. Potential screening criteria (or additional criteria and performance shaping factors for the quantification of probabilities of operator failure) for this task may be:

- is only the plant itself affected by the external event (e.g. aircraft impact), or is the whole region affected (seismic, flooding, typhoon), which would leave the plant without external support?
- is the external event fast (e.g. aircraft impact, seismic), or slow (e.g. heat wave), and was there an opportunity for preparation against the external event?
- is the external event itself also affecting human performance (e.g. extreme storm, snow, smoke, debris, radioactivity or bodies of casualties and injured persons on the site)?
- how is the crisis team (who is in charge of ordering and initiating the SAM actions) going to respond to the potentially extreme conditions?
- how efficient can be the rescues teams from outside of the plant for considering the amplitude of damages, kinetics of accident, radiations, …
- how is accident management affected by interventions performed potentially by unskilled or not properly trained personnel?

With respect to the last concern in the list given above, it must be re-iterated that some actions may have to be performed by unskilled operators (e.g. the fire brigade). A large weight should be given to the issues of training and skill of the operators or personnel who are involved in the management actions, and much less weight to the time available to perform them, even though in many cases this time may be very long. It should be noted that relatively long time available needs not necessarily be an asset, since a longer time for implementation might

mean also more potential mistakes or may induce a too optimistic or lax attitude of the personnel involved (including the crisis team).

It seems quite clear that L2 PSA assumptions for HRA will depend on the quality of training of the utility emergency teams and on the existence of procedures that would allow crisis team to take decision in due time and avoid an aggravation of the situation.

Given all the uncertainties introduced by the quantification of the potential shaping factors that would properly describe and characterize the SAM interventions (see the next section for details), and given that the SAM actions in L2 PSA *per-se* are implemented for mitigative purposes, it might be advisable in sequences with extremely high level of stress to perform the basic analysis without consideration of SAM human interventions, especially if the utility has not implement a specific training program for such conditions. Under such adverse conditions SAM should be investigated in sensitivity analyses that would show what are the potential (but not assured!) benefits of the implementations. This will also provide good information of the resilience of the plant containment safety function.

Some other issues, listed in the section on quantification of the event trees, could also be included in the HRA assessment as specific and separate performance shaping factors (or equivalent HRA modeling technique), or alternatively they may be separately quantified in some of the nodes of the event trees, since they actually belong to general plant specific and accident specific conditions, more than to intervention (SAM) specific conditions.

Specific detailed discussion on performance shaping factors and implementation of SAMG is to be found in the next section. Some recommendations for improvements in the models or development of new methodologies are also provided.

2.3.2 HRA SHAPING FACTORS

The previous section mentioned some of the factors that are most evident and obvious in the difficulties of implementing operator interventions following an external initiating event. This section provides a more systematic look at the specific performance shaping factors that are used in HRA analyses.

The examination of the factors that drive human responses under severe accident conditions is essential for integrating SAMGs and for implementing HRA approaches in light of external hazards.
The list of human performance shaping factors for L2 PSA that should be carefully reviewed before implementation in the models includes (see also deliverable D40.5 [16] relative to SAMG implementation):

- physical and psychological stressors that are likely to influence performance in severe accidents need to be realistically modelled; if the accident is extending over multiple days it will impose severe mental and physical fatigue on control room operators, field staff, and personnel in the plant's emergency response

centre; note that "level of stress" per se may not be modelled as a performance shaping factor, nevertheless the issue is whether stress is properly taken into account especially for accidents initiated by external events.

- control room operators and field personnel are also exposed to physical stressors (e.g., loss of lighting and high radiation) as well as psychological stressors associated with risk to their health and lives and those of their co-workers and families, posing an extra load on the control room operator performance;
  in particular operator actions need to consider the possible environmental factors, posed by the extreme harsh working environment conditions, including radiation levels and high temperatures;
  for example, operators could not take critical some control actions from the control room; instead, they should take manual actions in the field; radiation releases in the plant and limited access of the personnel to equipment could hamper the ability of personnel to perform their duties, both in the control room and in the field; some field activities could require multiple teams because of difficult onsite conditions; flooding, debris, and other hazards caused by the external event and by the severe accident phenomena, like the hydrogen explosion, limit access to some parts of the reactor buildings and challenge the field response.

- communication to transmit information and instructions in an accurate and timely manner plays an important role in shaping actions at certain points during the accident response;
  this item encompasses communications and real-time information systems to support communication and coordination between control rooms and technical support centres, control rooms and the field, and between onsite and offsite support facilities; it should be noted, that the hierarchy of responsibility for some actions and issuing instructions should be known and clear to everybody; to this aim the availability of the communications equipment that the staff will need to effectively respond to the accident (e.g., radios for response teams, cellular telephones, and satellite telephones) must be ensured;

- operators training: the operators could encounter situations that go well beyond their training for responding to off-normal conditions; in responding to severe accidents at nuclear plants, operators are likely to face complex, unanticipated conditions (e.g., multiple interacting faults, failed or degraded sensors, goal conflicts, and situations not fully covered by procedures) that require them to engage in active diagnosis, problem solving, and decision making to determine what actions to take; this implies that emergency response procedures should involve all the scenarios which include core damage and operator training should routinely exercise the whole range of SAMG response options and involve as well multiple unit scenarios;
  here is a need for HRA methods that more accurately model the kinds of complicating situational aspects that are likely to arise in severe accidents and the psychological processes that underlie performance in these situations.

- real-time information about conditions at nuclear plants for monitoring critical thermodynamic parameters related to the severe accident progress and phenomenology, as fuel rod – water interaction, hydrogen build up and combustion, fission product release, molten fuel relocation and MCCI (molten core concrete interaction), etc.; it should be also noted that based on some conditions (e.g., radiation levels), all operations in the open on site may be stopped and non-necessary personnel evacuated.

The qualification of all the related instrumentation for the diagnosis of severe accident and monitoring at deteriorated plant conditions should be taken into account in the probability of human interventions.
The proper working of the related measurements would be assumed until the loads do not exceed the designed values. The considerations must not be limited to seismic loads only, but also take into account vibrations of various levels, humidity, temperatures, electric current frequency peaks (lightning, events caused by immediate switch-off of some electric devices in/outside of the plant, …) etc. with respect to all considered external hazards.
The role of personnel in accident recovery is to be opportunely modelled in HRA, given evidence that people are a source of system resilience because of their ability to adapt creatively in response to unforeseen circumstances even with unavailability of major physical safety systems to mitigate the accident ("heroic" actions). Nevertheless, creativity and improvisation may also have a very negative impact, so crediting any "heroic" action should be done very cautiously.

2.4 EVENT TREE MODELLING

Additional Accident Progression Event Tree (APET) analyses may be needed in case external-events specific PDSs have been identified. Protocols and best-practices applicable to these processes are found in Sections 2, 3 and 4 of [5] (Vol2).
In general, the vast majority of core damage sequences induced by external events behave as sequences that are induced by a loss of power event (due to loss of transformers or loss of the switchyard, which are the SSCs most exposed to the effects of external events). A smaller number of sequences (especially for the most severe initiators with extremely large consequences) behave as containment bypass or containment failure prior to core damage.
Additional event trees had to be modeled if the event trees for internal events are not adequate to describe accident progression of external events-induced sequences and the combinations of system failures. However as indicated above in the section on PDSs (Section 2.1), the present opinion is that there will be no L2 PSA accident evolution (regarding progression of physical phenomena) which is principally different from the traditional L2 PSA sequences. Either the accidents behave as some already analyzed internal initiated sequences, or they need no special trees, because they lead directly to containment failure or bypass.

Containment fragility analyses should be performed for Level 1 (fragility due to external loads during accident initiation) and Level 2 (fragility due to internal loads during accident progression) to provide also data with respect to containment fragility for formation of deep cracks and containment penetrations failures induced by external events.

This fact was recognized already in the NUREG-1150 analyses [12]. In the Level 2 APETs developed for the five plants, provision was made to model these potential additional containment failure modes with the addition of a top event that allowed for quantification of the conditional probability of "Pre-existing containment leaks and containment isolation failure" prior to accident initiation, in addition to the quantification of the other modes of potential containment failure before and during accident progression that were provided by one of the PDS

characteristics (status of the containment). In fact, the possibility for these additional modes of containment failure was recognized also for accidents initiated by internal events, since cracks or failure of penetrations may develop after the last periodic containment leak-tightness tests and prior to accident initiation.

Quantification of this top event is discussed briefly in the next section.

2.5 QUANTIFICATION OF EVENT TREES

This section deals only with assessment of the conditional probabilities of the branches in the accident progression event trees. A basic necessary precondition for this task is proper estimation of physical phenomena including containment performance, and of human reliability. The quantification approach is, in principle, similar for external hazards and the conventional PSA.

However, some particular remarks have to be formulated:
Experiences with real core melt events (Jaslovske Bohunice A1, TMI 2, Fukushima Dai-ichi) indicate that operator and staff interventions crucially influence the accident evolution, together with other specific characteristics of any plant (such as plant design, size or power level, design of systems, etc.). As already mentioned in the section on human reliability, the success probability of human actions under the conditions of an externally initiated accident is extremely uncertain and difficult to estimate. Furthermore, since in many cases the external event was powerful enough to cause so many failures in SSCs to almost assuredly (if not assuredly) induce core melt, it is not at all certain whether equipment needed for SAM (if not designed for that conditions) or any other action is available and functional. In this case, the role of personnel and the crisis teams in fact becomes insignificant, as occurred at Fukushima Dai-ichi.

An example of problems connected with SAM interventions is containment venting: even if the venting system is designed properly to cope with core melt accidents initiated by internal events (e.g. if it can manage steam, hydrogen, fission products, and can retain volatile radionuclides), and even if the actions necessary to operate a venting system are simple and very quick; nevertheless the impact of the external event may have affected e.g. valves, piping, filters, or the stack. The consequence of misled venting exhaust containing hydrogen has been clearly visible in the Fukushima Dai-ichi accident.

This example shows that adequate quantification of event tree branches may be much more complicated when taking into account disturbances from external impacts. Given the restraints in time and budget which normally exist when performing PSA, it seems to be not realistic to expect a complete quantification of a full set of external event sequences. At best, it may be possible to address particular selected issues, e.g. the conditional probability of successful venting after a certain initiator (e.g. external events initiators with relatively low intensity). Facing

the difficulty of quantifying the event tree, one might assume that accident management actions will not be possible at all, which could be an unjustified conservatism.
For this reason, it would be advisable to separate higher intensity initiating events (i.e. duplicate event trees and quantify them differently for core damage sequences due to higher intensity external initiators), and assume that for these accident management actions will not be possible at all, due to multiple reasons, some of which may be or may not be quantifiable through a fragility analysis. The event trees with lower intensity events should then try to assign some success probability to accident management, including the following issues:

- potential damage to instrumentation and control devices,
- potential damage to structures where the necessary equipment is stored,
- potential damage to the equipment itself,
- impairment or even death of key personnel, and
- disruption of communications and means and ways to move the equipment around the site.

Note that these issues may also be added as performance shaping factors (or equivalent method-dependent model) in the HRA models that calculate the probabilities of success of SAM interventions. They have been separated to this section because these issues are certainly a function of severity of initiators and it may be easier to quantify them separately from the general issues that pertain more specifically to HRA.

Looking specifically at the quantification of potential failure modes that cannot be or that are not addressed by containment fragility analyses performed in L1 and L2 PSA (containment leaks and penetration failures due to external initiating events), if it is found that a specific analysis is not feasible, the quantification of this issue (or APET top event, see the previous section) should be performed using some engineering judgment as was done in the NUREG-1150 analyses [12] for internal events.

In these studies the analysts judged that the possibility of containment failures to develop after the latest leak-tightness test was “unlikely” and thus quantified it accordingly to the NUREG-1150 scheme (“unlikely” = 1E-3). For external events initiated accidents, it could be argued that the conditional probability of leaks is at least equal to the conditional probability of gross failure, if provided by the L1 PSA fragility analyses. In this regard, the separation of PDSs into different accident initiator severity classes (as done in L1 PSA analyses, see the recommendations on PDS development) is of importance.

2.6 DEFENCE-IN-DEPTH UNDER EXTERNAL EVENTS LOADS

It should be noted, that defence in depth is related to deterministic analyses, performed for DBA purposes as it follows from the IAEA definition in ([7], Chapter ACCEPTANCE CRITERIA): Deterministic approach: The deterministic approach is based on the two principles: leak tight barriers and the concept of defence-in-depth (DiD).

Paragraph 7.13: "Thus a deterministic safety analysis alone does not demonstrate the overall safety of the plant, and it should be complemented by a probabilistic safety analysis. [*Emphasis added*]"
Paragraph 7.14: "While deterministic analyses may be used to verify that acceptance criteria are met, probabilistic safety analyses may be used to determine the probability of damage for each barrier. [*Emphasis added*] "Probabilistic safety analysis may thus be a suitable tool for evaluation of the risk that arises from low frequency sequences that lead to barrier damage, whereas a deterministic analysis is adequate for events of higher frequency for which the acceptance criteria are set in terms of the damage allowed."

Document [34] adds: "The review showed that the fundamental safety requirements are generally based on a deterministic, defence-in-depth safety philosophy. The use of risk based safety goals [*Emphasis added*], in combination with deterministic safety goals, provides a way to develop balanced, technology neutral, expectations for the protection of worker and public health and safety and a means for an independent and integrated assessment of plant safety."

In accordance with the principles quoted above, L2 PSA have identified several deficiencies in existing plants with regard to severe accidents, although these plants apply the DiD concept. This is not surprising because practically no existing plants (Generation I and II NPPs) were designed against such events. Identified issues include also instances where DiD is not or not well implemented for such conditions. One example is the fact that the fuel cladding made out of Zr, which is considered to be a reliable second physical barrier within the first safety layer of DiD concept under normal operation as well as under conditions of Design Basis Accidents, becomes a source of risk at beyond design basis temperatures because together with steam it is a source of hydrogen. From this point of view the fuel cladding should not be considered to be a safety barrier with respect to severe accident conditions or PSA. Another example is, for many plants, the insufficient containment pressure load capacity in severe accident conditions, which leads to the necessity of a venting system. This means that the containment, which constitutes the last barrier in the DiD, is not well suited to manage severe accident conditions, except if the filtration capacity of the venting system is so good that offsite impact becomes negligible. Nevertheless, the severe accident which occurred in the TMI plant demonstrated a successful DiD concept: The inner barriers were lost due to fuel melting, but the containment remained intact and functional.

The large majority of severe accidents initiated by external hazards can be represented by sequences which are very similar to transients initiated by internal initiators, or loss of offsite power sequences. For such external hazard scenarios the DiD issue is not different from the well-known internal initiator topics. There is, however a subsection of external hazard scenarios which can directly threaten the containment, i.e. the outermost (last) barrier in the first place. If this last barrier fails first, it may be difficult to demonstrate that the remaining inner barriers still constitute adequate protection levels. Therefore, the validity of the DiD concept may be questioned under such conditions.

Motivated by the major severe accidents in Chernobyl, and also after Fukushima the DiD concept should be analyzed and undergo improvements complying with IAEA INSAG-10 [14] and INSAG-12 [10] to assure the IAEA Safety Principle 8 to be met: *"Defense in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defense in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability."* It is to be recognized that IAEA does not specify what is a "harmful effect", nevertheless a single failure after an initiating event leading directly to offsite releases, whatever the consequences may be, constitutes failure of all DiD barriers. More detailed discussions about current DiD and safety margins can be found in [33] as well as in report [43]of the ASAMPSA_E project on the link between defence in depth concept and extended PSA.

From the PSA point of view, however, this is no particularly difficult issue. The level 2 event trees simply have to contain paths where the containment (or also the next barriers) are not functional right from the beginning, rather than being challenged by phenomena later in the sequences.

2.7 ANALYSIS AND PRESENTATION OF RESULTS

The ASAMPSA2 document (Vol. 2, [5]) contains an extended section on this topic. In spite of this, the present sections are a complement to and re-enforcement of the discussions given in [5] because the need for proper analysis and presentation of results is of crucial significance for PSA quality and some rare external events can be considered in some way to be special. The major task of this document is to cover the impact of external events on L2 PSA which are potentially followed by immediate destruction of all barriers (MCSs of first grade with only initiator) or, much more than accidents initiated by internal events, might include only one additional failure, e.g. a human error, both leading to large releases. Furthermore, external events have a potential for affecting more than one single unit on a site, which implies the issue of how to characterize L2 PSA results with respect to more than one accident sequence.

Therefore in this context the results should be carefully analyzed taking into account some of the major deficiencies in most current PSAs, i.e. missing confrontation and comparison with the IAEA 10 safety principles [35], the three safety objectives [14], assessing total risk of releases and comparison to a common risk target. Some solutions in this respect are offered for example by the CRT method for evaluation of total risk of releases [9], [27], [28], which is discussed in detail in WP30. Even though these issues are addressed in other ASAMPSA_E documents as well, these topics are expanded here as integral part of the performance of L2 PSA.

The sections that follow discuss separately what results should be given, how the results should be analyzed, and how they should be presented and interpreted, respectively. Note that many of the arguments relating PSA, DiD and INES (e.g. in [8]) and shown below are relatively new, hence they require a more extended discussion.

2.7.1 L2 PSA RESULTS AND HARMONIZATION

WP30 of ASAMPSA_E is involved in a general discussion of risk metrics and PSA results [15]. In addition to this work, the present section concentrates on those topics which are of particular relevance for L2 PSA and external events. Probabilistic risk/safety assessment is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity (see for instance [13], section 11.2, pg. 438). It has been developed as a tool to identify vulnerabilities of a plant and to demonstrate safety of nuclear power plants comparing the results with safety goals/limits and one of its main objectives according to ([11] §1.2, page 1) is to evaluate all radiation risks (i.e. from all operational modes and from whatever activity involves radiation sources in a facility as a whole, and not from just a single unit):

“The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined.” ([11], para. 1.2).

In IAEA INSAG-3 [10], chapter 3.3.4, item 84, the following paragraph can be found:
“Probabilistic analysis is used to evaluate the likelihood of any particular sequence and its consequences. This evaluation may take into account the effects of mitigation measures inside and outside the plant. Probabilistic analysis is used to estimate risk and especially to identify the importance of any possible weakness in design or operation or during potential accident sequences that contribute to risk (which should be more precisely interpreted as: that might cause excessive contribution to risk).”

Therefore, the results should be provided at least partly in form of risk(s). For PSA we should accept in general (i.e. irrespectively of specific risk measures) the definition of risk as defined in INSAG-12 [10] §14, pg. 8: “the risk associated with an accident or an event is defined as the arithmetic product of the probability of that accident or event and the adverse effect it would produce”.

An important deficiency noted in analyses, as concluded within ASAMPSA2 project, is that in spite of the IAEA definitions and requirements, the results are currently depending on PSA objective, and “risk” evaluation complying with one of the IAEA fundamental principles is currently performed in various ways because there is no common understanding of the “adverse effect”. The second deficiency related to L2 PSA results is, that no common harmonized risk comparative parameter (safety goal) exists to compare the level of safety. As a surrogate, currently a frequently used parameter is LERF (Large Early Release Frequency), which is only semi-

quantitative without an exact definition of “Large” and “Early” and without harmonized values of frequency throughout the European countries.

A third deficiency has been underlined during the second ASAMPSA_E End-Users workshop (September 2016) : while extending the scope of PSA (internal initiating events, internal or external hazards, multi-unit PSA …), it appears that the quality of data (hazards characterization and impact, human and component reliability, failure rates …) supporting the different parts of an extended PSA is heterogeneous and can overshadow the agglomeration results in a total risk assessment: therefore, it is questionable whether such agglomeration is sensible at all. Nevertheless this real difficulty shall not be an excuse to not try to present a complete view of risks through PSAs.

The observations mentioned above apply to the status of many present-day PSAs. Considering these shortcomings in traditional PSA, it is justified to discuss adequate risk metrics within the “extended” scope of ASAMPSA_E.

Within the ASAMPSA2 project the idea of Common Risk Target (CRT) was proposed by Jirina Vitazkova and Erik Cazzoli representing the CCA company within the project ASAMPSA2, described in Chapter 6 of the ASAMPSA2 Guidelines (Vol. 1, [5]). The methodology used to derive the proposed Common Risk Target (CRT) was fully worked out within a dissertation thesis [9] and published in 2013 in the journal Nuclear Engineering and Design [27]. The methodology is based on grouping sequences leading to releases according to INES scale grades. This helps to recognize if the plant is really balanced – i.e. if none of the release groups causes a significant contribution to the total risk. The CRT parameter is based on the constant risk principle (Farmer’s curve) and its quantitative value is comparable with other industrial risks by transforming releases in TBq to consequences. In the context of the CRT (and the IAEA INES definition [8]) it is necessary to use radiological equivalent toxicity of I_{131} and include all the released radioactive elements.

CRT is technically derived and not only assigned without justification. This method ensures that some of the objectives of PSA are fulfilled, such as identification of weaknesses, identification of outliers that dominate risk results and proper analysis of results in comparison with IAEA safety principles and objectives including consideration of multi-unit sites.

The CRT method is mentioned here as an example for calculating the total risk because it is in particular related to L2 PSA. Within WP30 of the ASAMPSA_E project there is a more comprehensive discussion of various risk metrics ([15]) and the CRT method itself with its derived value of CRT target is discussed. An example, why the L2 PSA results should be shown as risk contributions (in the sense explained above), is given below and discussed in detail in [15] and [42] of the ASAMPSA_E project.

2.7.2 ANALYSIS OF RESULTS

Consideration of beyond design basis accidents of nuclear power plants (NPPs) is an essential component of the defense in depth approach which underpins nuclear safety. Beyond design basis accidents that may involve significant core degradation are of particular interest for accident management - a set of actions taken during the

evolution of a beyond design basis accident made to prevent the escalation of the event and to mitigate the consequences of a severe accident and to achieve a long term safe stable state.

Existing PSA methodology is able to provide results for any type of risk metrics. As it is discussed in [5], various results in various forms are produced within the L2 PSA assessments depending on the scope/objective of L2 PSA; among these the most commonly analyzed are:

- Frequency of containment failure - first containment failure, dominant containment failure modes.
- Individual containment failure modes and related frequencies.
- Magnitude and frequency of releases for the different containment failure modes.
- Frequency of releases - based on releases, in/out of APET evaluation, based on kinetics, on containment failure time, on delay before obtaining an activity release limit; this category covers L(E)RF.
- Containment matrix (probability of containment failure modes as a function of accident initial conditions or CDS).

This means that the results, by showing different phenomena or parameters, are usually not comparable in a process of cross-checking and thus consistency and comparability of the results of different L2 PSA studies cannot be ensured.

L2 PSA should carefully check the local requirements. Several panels have been, and are still, compiling and comparing the various practices. In this respect different limits and practices in different countries exist and it depends on local authorities what kind of results they ask for and indeed what quality, depth and extent of the analysis of results is required.
If, for instance, in the local legislation LERF is used for L2 PSA results, then it depends, what else the authority asks in the legislation to show about the results (importance analysis, contribution of chosen PDSs to final frequency, contribution of chosen containment failure modes to final frequency etc. …). Sometimes nothing more than LERF results are specifically required.

As previously stressed, the IAEA document [36] states that “Probabilistic analysis is used to evaluate the likelihood of any particular sequence and its consequences. This evaluation may take into account the effects of mitigation measures inside and outside the plant. Probabilistic analysis is used to estimate risk and especially to identify the importance of any possible weakness in design or operation or during potential accident sequences that contribute to risk (which should be more precisely interpreted as: that might cause excessive contribution to risk).” However, since for the most part regulatory requirements concentrate on the demonstration that a target on large release frequency is met, and no demonstration is asked for total risk or even risk profile (frequency versus releases), accident sequences may not be analyzed according to their contribution to total risk. Then it is not possible to conclude that the plant is really balanced thus complying with the general safety objective, i.e. there are no specific sequences identified with a significant contribution to total risk. Consequently, decision making focusing

on limited risk metrics will dismiss other accident related consequences. Even though the results might be in accordance with safety requirements of an authority (e.g. LERF or LRF values), they might not satisfy some of the basic safety principles and objectives as mentioned above, and decisions made on such basis may be misleading.
Unfortunately, however, no harmonized or unanimously accepted risk metrics exists. The related discussion is provided in reports [43], [15] or [43] of the ASAMPSA_E project, where also recommendations are given for suitable results presentation.

2.7.3 PRESENTATION OF RESULTS

The ASAMPSA2 guidelines ([5], Vol.2, section 2.6) provide examples on presentation of L2 PSA results. Following Fukushima, the "Lessons learned" included statements to the effect that some deficiencies had been noted in the area of presentation and interpretation of results in the Japanese PSAs (*see WP30*, [15]). In addition, the community started to feel the necessity of correlating work on DiD and PSA (also *WP30,* **Erreur ! Source du renvoi introuvable.**). The technical reasons for analyzing and presenting results to show relationships with the objectives of PSA, including finding deficiencies in DiD, are also given in **Erreur ! Source du renvoi introuvable.**. It is to be recognized that many of the risk measures discussed are functional to and dependent on the tools and methodology used. For instance, importance analysis of magnitude of releases with respect to system, components and operator errors may be possible only if the PSA Level 1 – Level 2 are fully integrated. On the other hand, importance analysis with respect to PDSs may not be possible if the analysis is integrated. Nevertheless, L2 PSA should strive to calculate and show risk assessment in terms of releases in order to comply with the objectives of properly identifying plant weaknesses and areas which could merit a closer look to point out remedial measures (including plant back-fits) to reduce risks, i.e. all the results relevant not only to social and environmental risks but to economic risks which include reduction of eventual wrong investments.

2.8 ISSUES INVOLVING MULTI UNITS SITES

2.8.1 GENERAL CONSIDERATIONS

Most of the plants currently operating are multi-unit sites and it is really urgently needed to consider this issue in PSA. No complete satisfactory methodology or guidance exists as of the date this was written. This document has made full use of the information that can be gathered from [19] and the related literature, which includes experience from Canadian PSAs. Some countries like Korea are now considering very seriously these issues and are developing specific projects [20],[21],[22]. Although it is a general issue for PSA, it is addressed here in the section on external events because external events seem to be the most significant contributor to sequences affecting more than one unit.

The accident at Fukushima has shown that accidents at multi-units sites should be given special consideration, given the possibility of common cause failures among the different plants in different states of operation.

Moreover, it is possible that the units at a site are in different operation modes: in one unit, the risk may be due to the SFP (core unloaded), in the other unit, the core may be the main threat.
Each of the plants at the site behaved differently and final consequences (releases to the environment, at least according to current information) varied for each of the units at the site. The different behavior and responses of the units and final core status including extent and type of containment damages in Fukushima Dai-ichi prove that even though the units are identical or very similar and they are at the same place and being threatened simultaneously by the same initiator, there are many unforeseen factors that may influence the progression and final result of a severe accident. All these factors may raise the doubt whether the current PSAs are "realistic" at all even for a single unit, and perhaps the community should return to a more conservative approach. Nevertheless, this section attempts to provide, if not guidance, some points that should be considered when addressing multi-units in PSA, and some suggestions on procedures for resolving some of the issues connected with such PSAs.

At first glance a PSA for multi-units sites seems to be merely a technical issue and a question of resources to simply adding and combining sequences in more than one unit on a site. However, when looking more closely it becomes clear that significant challenges are involved. These challenges arise from the fact that a plant housing more than one unit can be subjected to the following sets of problems arising from intra-unit (i.e. within individual units) and inter-units (i.e. from connections among units) dependencies or correlated phenomena:

- **Common cause initiator:** an event (external or internal) affects more than one unit on the site (common initiating event); some SSCs fail due to the initiator, but these dependent (on the initiator) failures occur randomly and in different combinations in the units; consequently, the accident progresses in different ways in each unit; no other common dependent failure occurs, either in systems, components or structures; all recovery actions by the operators progress completely independently in each unit; one or more units may reach core damage conditions while the others do not (Level 1); after core damage, accident progression still goes on independently within each unit, and SAM interventions proceed independently (Level 2); if such a scenario could be irrefutably proven, then the results for the whole site are only a matter of combinatorial analysis.
- **Common cause failure of systems:** there could be inter-connections among systems, and common cause failure of systems as a whole could occur due to the same initiator; one simplistic example which is valid for BWRs and PWRs is as follows: the Auxiliary Cooling Water System (ACWS) of two or more units could share the intake from sea or river; if the intake is blocked, the ACWS and cooling of the components in the secondary side (PWRs) or in the balance of plant (BWRs) is lost for all units; after the common initiating event that essentially trips all cooling pumps in all units, other failures may occur in each unit independently and therefore the accidents in the units start along the same path and then progress according to the other failures; the list below provides more examples of systems that are typically in common.

- **Common cause failure of operator actions:** resources for recovery may be shared among the units; if the resources are not available for one unit, due to initiator or other causes, they are not available for any other unit; the accidents in the units will probably end in the same way (the same PDS); here it might be noted that maybe only one unit is affected by e.g. a seismic/external initiator and the other/others not, but an operator failure causes the failure of the originally non-affected units (this being however a L1 PSA issue).
- **Potential correlations and dependencies between components, systems and operator actions**: this could be considered an analogy of the common cause failure of components already considered in L1 PSA for internal events: the initiating event could induce the same type of failure in components due to latent reasons, such as poor maintenance in all units or partial failure of components due to the initiating event.
- **The crisis center that guides the management of accidents is shared among the units**: the issue is whether the crisis center can cope with managing more than one severe accident at a time, and whether, if a wrong decision is reached for one unit, the same wrong decision will be reached for all units (e.g., venting the containment when not necessary).

The last two points are mostly relevant for L2 PSA. Integrated and very detailed models such as have been developed to analyze single unit L2 PSA, or which are suggested within the ASAMPSA2 guidelines ([5]) cannot be developed for analyses of accident progression of more than one unit at the same time. This fact has been recognized by the community and [19] (summary of the 2014 meeting in Ottawa on multi-unit PSA) recommends developing very simplified models.

Examples of common systems for twin units/more units which could be affected by a common initiator:

I. L1 PSA (all) and L2 PSA (most):

1. Backup/emergency power supplies of various sorts - lines - e.g. 110 kV, transformers, bus bars, switchboards, diesel generators, mobile diesel generators, automatic standby start, regulation/control of voltage and reactive power …
2. Ultimate heat sink
3. Compressors/refrigerant pumps
4. Auxiliary feed water system
5. Essential service water system
6. Hardware of common control and computer systems and computer network for “twin unit” including their ventilation and cooling systems, monitors, communication lines
7. Central electric control room - control of auxiliary electric supplies for one “twin-unit” communication lines within NPP with their power supplies
8. Fire system control and computer systems including its ventilation and cooling systems and their communication with main control room

9. Communication system to fire brigades and their head-quarters/regional board of managing directors outside of NPP
10. Personnel organization/occupation

II. Systems not normally considered in PSAs or systems that are not considered to be safety systems:

1. System of radioactive wastes - pipes, tanks ….,
2. System and control of spent fuel containers and disposal site
3. Circulation cooling water pumps and cooling towers
4. High pressure air system (affecting various equipment including fast acting/air-operating valves)
5. Sewage water purification systems
6. Drinking water system (important for personnel during SA)
7. System of physical control/safeguards

Items in group I. definitely may be affected by some common initiators and therefore have to be carefully modeled in L1 PSA because they will increase the individual CDF and will also increase the potential for concurring severe accidents with CD.

Group I also shows systems /subsystems etc., which may be affected by common initiator and which, after CD, may be con-causes for increasing the severity of the accident in more than one unit at the same time; i.e., they show systems with "hidden correlation" failures more than just "common cause failures", and should be carefully considered and modeled in L2 PSA.

The second group shows systems etc. which are not even (normally) considered in PSA L1 or L2, but which may have bearing to and/or negative impact on accidents initiated by external events.

Moreover, as is recognized by e.g. [17], supporting or adjunct mechanistic or probabilistic models for multi-units analyses are lacking at this time (both for study of accident progression and of consequences). A general guidance for performance of PSA is forthcoming (also from [17]) however, for now the ASAMPSA_E guidelines need to point out that the following more specific issues need to be addressed when considering multi-unit sites:

- all sources (e.g. [17] and [18]) seem to agree: What is the proper definition of “risk” to a site? In ASAMPSA2 ([5]) risk is defined relative to hazards or accidents. Risk associated with the hazard is a combination of the probability (or frequency) of the hazardous event and the magnitude of the consequences. The consequences can be represented in several dimensions. A usual engineering definition of risk associated with an event i is: Risk(event i) = “the probability of an event i” x “the consequences of an event i”. In case of multi-unit site, the risk associated to a nuclear accident (radioactivity release) is the integral of all accident consequences multiplied by frequencies for all radioactivity sources including spent fuel pools. This is discussed more precisely in [15].

- the units on a site are not totally independent: at a minimum they share the crisis center and at least external energy supplies/electric grid/transformers and switchyards which are interconnected for back

connections and jumps which are used not only for "OUT" energy but also "IN" energy in case of loss of production necessary for self-consumption; the dependencies and feedback between units can be properly modeled only if a single dynamic super-model that can track accident progression in all units at the same time is used; this is practically impossible either because of code limitations or because of the complexity that would be introduced in such a model; therefore, modeling accident progression in one unit at a time seems to be the only solution.

- if the units are not independent - how should the dependence be modelled? Note that in practice the units on one site often are not identical; given that analyses should be performed one unit at a time, the only solution may be to introduce dependencies in an iterative way, by re-quantifying some nodes in the APETs according to results of a single unit; this would also take care of the fact that units at a site are not necessarily of the same type and make.

- the final maximum released quantity of an accident in two units is about twice the maximum release from a single unit (which implies in fact that the risk, whatever may be the definition of risk, posed by a site with N units may be in first approximation N times the risk posed by a single unit site, and the analysis could be stopped there: when compared to the other uncertainties in releases and frequencies this factor of two or even N is insignificant). So, it does not really appear justified to spend much effort on detailed multi-unit analyses for accidents that progress in more than one unit, and analyses should be simplified as much as is reasonable, and introduction of conservatisms should be considered (as already noted). Please note that even this first approximation is valid ONLY if Level 1 PSA can provide a defensible and complete analysis of all inter- and intra-units connections, dependencies and correlations that could trigger conditions conducive to CD in all units at the same time, even for internal initiating events. This is not currently taken into consideration. One example of such potential incompleteness in current Level 1 analyses would be that auxiliary feedwater systems are commonly shared among units in some designs, however only one unit is considered, and therefore the internal event initiator "Loss of Feedwater" (LOF) MUST be in that case considered as common-cause initiator for multi-units sites.

2.8.2 PROPOSAL FOR MULTI-UNIT SITE ANALYSIS

From the point of view of striving for completeness and defensibility of results (related to the previous observation) any PSA guideline should stress the necessity for a proper process of quality assurance. Here by quality assurance is meant not just the formal ISO process, but a thorough checking and understanding of the results and the implications of the results, to verify the contribution to total risks and to verify that the analyses are proper and consistent including compliance with the 10 IAEA safety principles [35], e.g. the requirement that a single failure would not lead to core damage and releases or significant contribution of particular sequences to final risk (not PDSs only and not contribution to frequency only). This is currently not always done.

At the present time, it seems to be already clear that modelling common cause failures (caused by the external event) in more than one unit opens a large field of practical modeling (especially the probabilistic models and tools capable of accommodating the potential size of combinations) and computational problems (extension of existing mechanistic and probabilistic consequence codes): the potential results in terms of release categories become extremely complicated, if e.g. each unit has 10 potential different release categories, and if the accident sequences in a site with just two units are not identical (which seems to be obvious from Fukushima), this could in theory result in 100 different release category combinations. Obviously there is a need to properly group such a large variety and detailed and integrated models as recommended by ASAMPSA2 guidelines for single units cannot be fully implemented (i.e. currently it seems impossible to analyze with single super event trees the parallel failures and accident progressions in more than one unit and therefore potential inter-dependencies, especially in operator interventions, may not be correctly modeled). All these layers of complexity may actually be sufficient to warrant stopping at the first approximation of risk estimates (total site risk equal to N times the single unit risk).

At the time this document was prepared (mostly winter 2016) no satisfactory and complete integrated and detailed methodology for performance of Level 1 and Level 2 for multi-unit sites has been published. ASAMPSA_E suggests some approximations, introduction of conservatism and simplifications as discussed in the next section below. Please note that the scheme shown here is only a suggestion that can resolve some of the issues detailed above.

For these suggested procedures here to be valid it is necessary that L1 PSA provides adequate information about accidents that occur or are under way at the same time in more than one unit. It must also be remembered that L1 PSA for the most part deals with prevention of core damage and thus does not necessarily cover all possible sequences potentially significant and in progress after core damage, while Level 2 deals only with mitigation of releases and consequences from severe accidents that cannot be prevented.
Bearing then in mind that models as suggested by sources (summary provided in [19]) should be simplified, and assuming that the only inter-unit dependencies during accident progression after core damage are in the area of SAM operator interventions, the following procedure is suggested:

1. Clearly establish major objectives of calculations in terms of the risk measures that should be provided (see [15]), bearing in mind that not all risk measures may be actually calculated. Nevertheless, the end product should be the estimation of overall RISK (probability that adverse consequences from all accidents at one site will occur in a given period of time, as defined by IAEA) and comparison with appropriate safety targets. This is supported, as already mentioned in Chapter 2.6, by IAEA [34]: The use of risk based safety goals, in combination with deterministic safety goals, provides a way to develop balanced, technology neutral, expectations for the protection of worker and public health and safety and a means for an independent and integrated assessment of plant safety.

2. Simplify existing single-unit models (APETs), keeping them compatible with the objectives (risk measures compatible with common risk targets) that must be provided (e.g., one potential simplification could be a broad characterization of release classes as performed by EDF [15], rather than characterization of releases by specific release modes). Analyze APETs one unit at a time (i.e., it is not envisioned that super models may be developed even with a very simplified scheme of characterizing release modes).
3. Identify, from L1 PSA results, accidents that are expected to occur simultaneously in more than one unit: specific super-PDSs should be provided. It is necessary here to define where L1 PSA stops and where L2 PSA starts: a simple approach can be to consider that L2 PSA starts when fuel damage has occurred in one of the site NPP (or simultaneously on several NPPs due to common causes) and then to consider additional impacts on the other NPPs with the L2 PSA approach.
4. Define consequence/release dominant containment failure modes from analyses of single-unit APETs and source terms assessment and prioritize these modes in the quantification of APETs: which are the "very large", "large", "medium"… release modes, and in which time frame they are expected to occur. The INES scheme [8] (Farmer's curve) should be used for reference of what is "large", "medium" etc.
5. Assume that the unit which is expected to fail in one of the failure modes conducive to large releases actually fails first (by containment bypass, by failure of containment isolation, by early containment failure…..). Here an example is given for a two-unit site. The time of release defined in point 4 determines which unit should fail first. For example, in a combination of PDSs in which unit 1 fails in a bypass mode, and unit 2 fails as Station Blackout, the containment failure of and releases from unit 1 certainly precede any possible containment failure of unit 2, and any intervention in the open for unit 2 is thus precluded (see next point). If both units fail as Station Blackout, the conditional probability of early containment failure of unit 1 defines in first approximation the dependent failure probability of interventions in the open for unit 2 (see next point).
6. After the failure in one unit as described in point 5 conservatively assume that, due to the large releases occurring from the first failure, all accident management interventions for all other units that need working in the open will completely cease or will be impeded for an extended period of time (this assumption takes also care of uncertainties in the decision of intervening correctly and at the appropriate time by the crisis center), and therefore will likely fail for all the other units.
7. Quantify event trees according to the assumptions made in point 6.
8. Eventually iterate the tasks 3 through 8 to arrive at consistent results.
9. Integrate results for the calculations of the various failure modes for all units.

This proposed model only assumes that the APETs are built and run for individual units and the multi units effects and consequences are calculated separately by appropriate integration tools (EXCEL spread sheets can be useful). Note that some inter-unit CCFs (the potential containment system CCFs, if the systems are not independent) are taken into account if the PDS characteristics are properly defined, because the failure of containment systems can be calculated before Level 2 through appropriate systems analysis (that can be taken from the existing Level 1 models). Iterations may be necessary only for sites with more than two units.

3 COMPLIANCE WITH END-USER'S NEEDS

The appendix (section 7.2) proposes an overview of the End User expectations for external hazards L2 PSA and their handling in the present reports.

The present document discusses some Level 2 issues that may be impacted by external events (i.e., analysis of containment performance through mechanistic codes, event tree modeling, and quantification of event trees), and treats more in depth some issues that are to be considered as integral parts of a PSA, namely selection of results, analysis of results, and presentation of results, all issues which are completing the ASAMPSA2 guidelines.

4 CONCLUSIONS

The nuclear accident in Fukushima, Japan, resulted from the combination of two correlated extreme external events – earthquake and induced tsunami affecting more than one unit at the same time. The consequences went beyond what was considered in the initial NPP design. ASAMPSA_E project aims at providing best practice guidelines for the identification of such situations with the help of "extended" L1 and L2 PSA and for the definition of appropriate criteria for decision making in the European context. According to [29] an extended PSA applies to a site with one or several NPPs and to its environment, and it intends to calculate the risk induced by main sources of radioactivity like reactor core, spent fuel storages inside or outside of containment, or other potential sources.

In particular, the following conclusions were reached for the modeling of external events in L2 PSA:

a) from the point of view of procedures/methods/approaches used currently in L2 PSA, there is no need of new methodologies in terms of PDSs, accident progression event trees development and evaluation;

b) the present guidelines identify the need of additional vulnerability/fragility analyses of systems, structures and components (like spent fuel pool, reactor containment, instrumentation, FCVS, etc.) needed for SAM strategies application in relation to all external hazards of various degrees of loads and intensity;

c) from the point of view of HRA more and higher stressors should be taken into account, e.g. within HRA models that use shaping factors. Assessment of human actions related to external events should be critically evaluated. SAM human interventions in particular seem to be appropriate as sensitivity analyses only in case of extreme conditions, especially if the utility has not implemented a specific training program for such conditions.

d) from the point of view multi-unit site analyses, it was concluded that:

- no practical methodology exists to treat the problem,
- no completely INDEPENDENT units on sites with several units are in operation; therefore, existing PSAs need QA re-assessment with respect to commonalities (and not only the potential common cause initiating events),
- a new methodology is necessary to be developed first for the L1 PSA and clearly defined boundary conditions for L2 PSA must be defined there, considering that risk (and not only "site" frequency) of the whole site should be evaluated [29]; some discussion on L2 PSA is provided with respect to Canadian CANDU reactors, but, unfortunately, it might be valid for this type of reactors ONLY.
- a major conclusion in this respect was made: simplification of models is inevitable,
- nevertheless a proposal for performance of L2 PSA (in section 2.8.2) is introduced to potentially solve this issue, given that the proper L1 PSA boundary conditions are provided,

e) from the point of view of proper analysis of results, it was found to be useful to assign one additional identification character to the PDS codes keeping track of each and every internal and external hazard in

order to make it possible to analyze at the end the contributors to the total risk by initiator related to the given PDSs,

f) from the point of view of proper analysis of results an application of proper risk metrics is necessary in order to make the best possible use of the PSA findings, especially to identify the main sources of risks and to support well founded decision making. In this respect an integral risk metric like e.g. the CRT method could be helpful. (See WP30 document [15] on risk metrics).

5 RECOMMENDATIONS

Main recommendations, mentioned in various sections within this document, are summarized here:

1. Vulnerability/fragility analyses should be performed with respect to all external hazards and all structures, systems and components potentially affected that could be relevant to L2 PSA,
2. Importance should be given to the assessment of human performance following extreme external events; for extreme circumstances with high stress level, low confidence is justified for SAM human interventions and for such conditions, human interventions could be analyzed as sensitivity cases only in L2 PSA,
3. Results presentation should include assessment of total risk measures compared with risk targets able to assess all contributions to the risk and to judge properly the safety. See document [15] for recommendations on PSA results presentation,
4. Total risk measures shall be associated to appropriate information on all uncertainties, simplifications and conservatisms that appear today to be inherent to any extended PSA,
5. Because NPPs on multi-units sites are in general not fully independent, verification and reassessment of current single PSAs is needed before developing multi-units PSA,
6. Because established methodologies for multi-unit sites L1-L2 PSA analysis are not yet available, it is recommended to use first a simplified method. The boundary between L1 and L2 PSA shall be defined appropriately and some relevant adaptations/simplifications in both L1 and L2 PSA may be considered (in a first step) to limit the complexity of the multi-unit sites L1-L2 PSA development.

6 LIST OF REFERENCES

[1] List of external hazards to be considered in ASAMPSA_E - K. Decker (UNIVIE), H. Brinkman (NRG) - ASAMPSA_E/WP21/D21.2/2015-10 IRSN PSN-RES/SAG/2015-00085 dated 2015-02-26

[2] Minutes of the ASAMPSA_E WP10 WP21 WP22 WP30 technical meetings - 8th-12th September, 2014 - Hosted by Vienna University - Reference ASAMPSA_E: WP5/2014-06 Reference IRSN: PSN/RES/SAG/2014-00318 – dated 25-09-2014 – E. Raimond (IRSN), K. Decker (Vienna Univ), Y. Guigueno (IRSN), J. Klug (LRC), M. Kumar (LRC), A. Wielenberg (GRS)

[3] ASAMPSA_E - Synthesis of the initial survey related to PSAs End-Users needs - Y. Guigueno and al. IRSN PSN-RES-SAG-2014-00193, ASAMPSA_E/WP10/D10.2/2014-05, dated 23-01-2015,

[4] Minutes and recommendations of the Uppsala End-Users workshop (26-28/05/2014) - reference ASAMPSA_E/WP10/2014-07 PSN-RES/SAG/2014-00335

[5] Best-Practices Guidelines for L2PSA Development and Applications, (Volume1 – General - Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors - Volume 3 – Extension to Gen IV reactors) - Reference ASAMPSA2, Technical report ASAMPSA2/ WP2-3-4/D3.3/2013-35, IRSN/PSN-RES/SAG/2013-00177, dated 2013-04-30 (www.asampsa.eu, www.asampsa2.eu)

[6] "Probabilistische Sicherheitsanalyse (PSA): Qualität und Umfang, Richtlinie für die schweizerischen Kernanlagen," ENSI A-05, Ausgabe Januar 2009.

[7] IAEA Safety Standards for protecting people and the environment, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2, IAEA, Vienna 2009.

[8] IAEA: INES: The International Nuclear and Radiological Event Scale User's Manual, 2008 Edition, Non-Serial publications, IAEA-INES-2009, 206 pp., Vienna 2009

[9] J. Vitazkova: METHODOLOGY OF COMMON RISK TARGET ASSESSMENT AND QUANTIFICATION FOR SEVERE ACCIDENTS OF NUCLEAR POWER PLANTS BASED ON INES SCALE, Slovak University of Technology, Bratislava, June 2014

[10] BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS 75-INSAG-3 Rev. 1, INSAG-12, A report by the International Nuclear Safety Advisory Group, 1999

[11] IAEA Safety Standards for protecting people and the environment, Development and Application of Level2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, SSG-4, STI/PUB/1443, ISBN 978-92-0-102210-3, ISSN 1020-525X, Vienna 2010

[12] US Nuclear Regulatory Commission (USNRC), “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants”, NUREG-1150 (1990).

[13] Ajit Kumar Verma, Srividija Ajit, Durga Rao Karanki: Reliability and Safety Engineering Springer Series in Reliability Engineering, ISSN 1614-7839, ISBN 978-1-84996-231-5, DOI 10.1007/978-1-84996-231-2, Springer Verlag London Limited 2010.

[14] http://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e_web.pdf, INSAG10

[15] ASAMPSA_E - Risk Metrics and Measures for an Extended PSA, ASAMPSA_E/WP30/D30.7/2017-31 volume 3

[16] ASAMPSA_E "Guidance on the verification and improvement of SAM strategies with L2 PSA ASAMPSA_E/WP40/D40.7/2017-39 volume 3

[17] K. N. Fleming, "A Technical Approach to Meeting Challenges in Multi-Unit PSA", from Proceedings of International Workshop on Multi-Units Probabilistic Safety Assessment (PSA), Ottawa, Canada, November 17-20, 2014.

[18] M. Modarres, "Significance of Multi-Unit Nuclear Plant Risks and Implications of the Site-Level Quantitative Health Objectives", from Proceedings of International Workshop on Multi-Units Probabilistic Safety Assessment (PSA), Ottawa, Canada, November 17-20, 2014.

[19] G. Georgescu and R. Georghe (nuclearsafety.gc.ca), "Summary of Session 3, Experience wim Multi-Unit PSA, Part 3", from Proceedings of International Workshop on Multi-Units Probabilistic Safety Assessment (PSA), Ottawa, Canada, November 17-20, 2014.

[20] Ho-Gon Lim, Sang-Hoon Han (KAERI), "Construction of Site Risk Model using Individual Unit Risk Model in a NPP Site", Transactions of the Korean Nuclear Society Spring Meeting, JeJu, Korea, May 12-13, 2016

[21] Dong-San Kim, Jin Hee Park, Ho-Gon Lim (KAERI), "the contribution to site core damage frequency from independent occurrences of initiators in two or more units: How low is it? ",Transactions of the Korean Nuclear Society Spring Meeting, JeJu, Korea, May 12-13, 2016

[22] Dong-San Kim, Jin Hee Park, Ho-Gon Lim (KAERI), Multi-Unit Initiating Event Analysis for a Single-Unit Internal Events Level 1 PSA, Transactions of the Korean Nuclear Society Spring Meeting, JeJu, Korea, May 12-13, 2016

[23] Mercurio, D., Podofillini, L., Zio, E., Dang, V.N., 2009. Identification and classification of dynamic event tree scenarios via possibilistic clustering: application to a steam generator tube rupture event. Accident Analysis and Prevention 41, 1180–1191.

[24] IAEA TEC-DOC-626, 1991. Safety related terms for advanced nuclear power plants. September 1991.

[25] Burgazzi, L., Addressing the challenges posed by advanced reactor passive safety system performance assessment, Nuclear Engineering and Design 241 (2011) 1834–1841.

[26] IRSN/PSN-RES-SAG/15-00168 Technical report ASAMPSA_E/ WP40/ D40.3/ 2015-11 21/66 Report proposing the content of future L2 PSA guidance to be established within ASAMPSA_E

[27] Vitazkova, J., Cazzoli, E. Common Risk Target for severe accidents of nuclear power plants based on IAEA INES scale. Nuclear Engineering and Design, Vol.262, Pages 106-125; ISSN 0029-5493, September 2013

[28] Vitázková J., Cazzoli E.: Safety Goals and Safety Targets for Severe Accidents in View of IAEA Recommendations. Proceedings of ISAMM 2009, Implementation of Severe Accident Management Measures, Schloss Bottstein, Switzerland, October 26-28 2009, Salih Guentay PSI, PSI Bericht Nr. 10-07, October 2010, ISSN 1019-0643, Nuclear Energy and Research Department Laboratory for Thermal Hydraulics, pp. 340-355.

[29] Raimond, E. European ASAMPSA_E project, Advanced Safety Assessment: Extended PSA, available on http://asampsa.eu/wp-content/uploads/2014/10/ASAMPSA_E-project_status_October_2014.pdf

[30] Vitazkova J., Cazzoli E.: Probabilistic Safety Assessment KKM Shutdown Internal Floods, September 2010

[31] Cazzoli E., Vitazkova J.: Assessment of Impact of DIWANAS backfits on LERF, KKM LEVEL2 PSA update, September 2013

[32] Cazzoli E., Vitazkova J.: Probability Safety Assessment, KKM LEVEL2 PSA update, August 2013

[33] J.Vitázková, E. Cazzoli: The principle of Defence-in-Depth in the perspective of Probabilistic Safety Analyses in wake of Fukushima, Risk Analysis IX, Book series: WIT Press, 9th International Conference on Risk Analysis and Hazard Mitigation, ISBN:978-1-84564-92-6, ISSN: 1746-4463, June 2014

[34] MDEP STC Sub-committee on Safety Goals, January 2011, The Structure and Application of High level safety goals Report, January 2011, IAEA Safety Series 115 (In revision as DS 379)

[35] International Atomic Energy Agency (IAEA), "Fundamental Safety Principles", IAEA Safety Fundamentals, No. SF-1, IAEA, Vienna (2006).

[36] International Atomic Energy Agency (IAEA), "BASIC SAFETY PRINCIPLES FOR NUCLEAR POWER PLANTS", Safety Series No. 75-INSAG-3, A report by the International Nuclear Safety Advisory Group, Vienna, 1988.

[37] Atomic Energy Society of Japan, A Standard for Procedure of Seismic Probabilistic Risk Assessment for Nuclear Power Plants: 2015 (in Japanese)

[38] A. Yamaguchi, S. Nakamura, et al., Revision of the AESJ Standard for Seismic Probabilistic Risk Assessment (3) Fragility Evaluation, PSAM 12, 2014

[39] ASAMPSA_E – End-users review - Questionnaire - ASAMPSA_E/WP10/D10.4/2016-18 rev.2, IRSN PSN/RES/SAG/2016-00184 rev.2, Y. Guigueno and al,

[40] ASAMPSA_E/WP10/D10.5/2017-40, Synthesis report of the End-Users survey and review of ASAMPSA_E guidance, and final workshop conclusions. Identification of follow-up useful activities after ASAMPSA_E, Y. Guigueno and al, IRSN PSN/RES/SAG/2017-0003

[41] Probabilistic Safety Analysis (PSA): Quality and Scope, Guideline for Swiss Nuclear Installations", ENSI-A05/e. Edition March 2009.

[42] ASAMPSA_E/WP30/D30.7/2017-31 volume 1, Final WP30 guidance document (decision-making based on extended PSA)

[43] ASAMPSA_E/WP30/D30.7/2017-31 volume 4, PSA and Defense in Depth concept

7 APPENDIX

7.1 APPENDIX 1 - EXAMPLE OF AN ON-GOING SEISMIC FRAGILITY ANALYSIS AT IRSN (MAIN STEAM LINE OF A PWR)

Fragility curves express the conditional probability of failure of a structure or component for a given seismic input motion parameter. In the framework of the containment seismic PSA, IRSN is developing a methodology to determine the fragility curve of a component supported by a structure, by means of numerical calculations. The main steps of this methodology are the following:

1) develop suite of seismic time histories representing variation of ground motion spectra;
2) build numerical models (for the supporting structure and the component);
3) define failure criteria;
4) propagate uncertainties and compute mechanical responses: uncertainties due to seismic loads as well as model uncertainties are taken into account and propagated using Monte Carlo simulation (this step is not yet started);
5) compare responses to failure criteria (uncertain threshold values) and derive fragility curves (this step is not yet started).

Ground motion

Nonlinear response history analysis (RHA) is nowadays widely used to quantify the seismic performance of structures and components.

For this study, acceleration time histories (accelerograms) are considered as inputs. They are issued by probabilistic seismic hazard analysis assessment (PSHA) and by using the spectrum matching technique ([A1], [A2]). These accelerograms are consistent with the uniform hazard spectra (UHS) of a specific NPP site. Seven return periods (from 1000 to 10 000 000 years) and several fractiles are considered, which leads to generate more than 100 accelerograms with three components: North-South, East-West and Up-Down.

The input motion is applied at the base of the supporting structure modelling. Peak Ground Acceleration (PGA) has been chosen to characterize seismic ground motion level.

Mechanical models

The study considers a coupled model consisting of a supporting structure (the containment building), and a secondary system representing the steam line (from the steam generator inside the containment to the stop downstream from isolation valve located outside the containment, Figure 2).

The containment building is represented by a stick model that has been identified from the respective finite elements 3D model (Figure 1). The stick model takes into account soil structure interaction and allows fast calculations.

The steam line is modeled by means of beam elements (Figure 3), taking in consideration the steel steam line, and several valves, supporting devices and stops at different elevations.

A previous analysis showed that the maximum stress is located in the containment penetration area. Then an additional local model of the penetration has been developed (Figure 4) considering the non-linear behavior of steel.

The response of the steam line is calculated in two stages:

- the response of the containment structure to ground motion is obtained by using the stick model; in particular, displacements of the stop and supports are assessed;
- these displacements are given boundary conditions (in red on Figure 3) for the beam model representing the steam line.

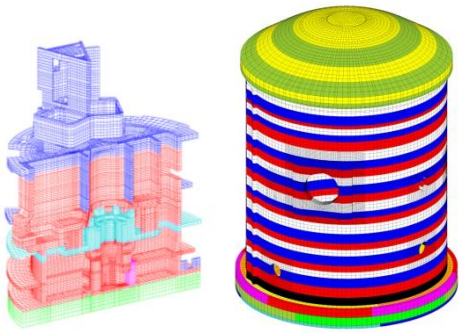

Fig. 1/ Containment 3D model

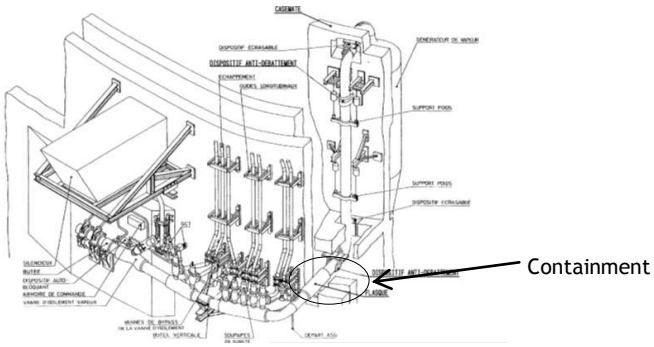

Fig.2/ Main steam line with stop and supporting devices (schematic view)

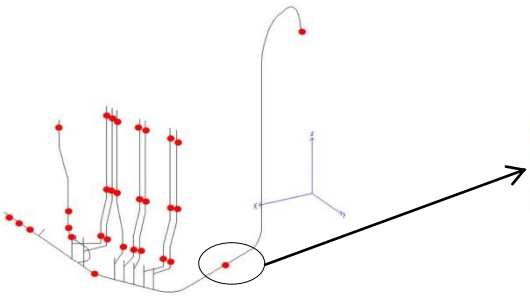

Fig.3/ Steam line beam model

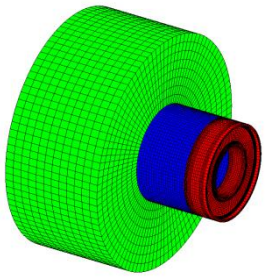

Fig.4 / Containment penetration model for the steam line

Mechanical failure criteria

First, the steam line integrity is verified: for each time and each node of the line, a linear calculation is performed; the equivalent stress is calculated according to the French nuclear construction code requirements (RCC-M[1]) and compared to the admissible stress.

In case of exceedance, a new calculation is done taking into account the nonlinear steel behavior. The Von Mises stress is compared to the ultimate strength (for each accelerogram and uncertain parameters sampling) and the fragility curve is derived.

[A1] Abrahamson NA (1992) - Non-stationary spectral matching. Seism Res Lett 63(1): 30
[A2] Al Atik L, Abrahamson NA (2010) - An improved method for nonstationary spectral matching. Earthquake Spectra 26(3): 601-617 doi: 10.1193/1.3459159

[1] Design and Construction Rules for Mechanical Components of PWR Nuclear Islands code.

7.2 APPENDIX 2 - COMPLIANCE OF THE REPORT WITH THE PSA END-USERS NEEDS

This document attempts to fulfill the requirements that emerged from the end-users' survey and meeting as much or as reasonably as possible with respect to "Extended" L2 PSA, i.e. the impact of external initiating events and multi-units sites.

7.2.1 End User's needs as identified at the beginning of the project

Only the issues listed in Table 1 of [26] which are relevant to performing L2 PSA are shown:

"1. GENERAL CONSIDERATIONS RELATED TO L2 PSA FROM END-USERS' DISCUSSIONS; GENERAL CONSIDERATIONS ON EXTENDED PSA

Concerning the scope of the ASAMPSA_E project, ASAMPSA_E shall at least address the 10 more important external hazards for the End-users:

- Earthquake
- Flooding
- Extreme air temperatures
- Snow pack
- Lightning
- Storm (tornadoes, hurricane, …)
- Biological infestation
- Aircraft crash
- External fire
- External explosion.

ASAMPSA_E shall consider also:

- Internal fires, floods and explosions,
- heavy load drops, high energy line break (HELB), missiles, chemical releases;
- other extreme weather conditions,
- transport of dangerous substances, accidents in facilities located in the vicinity of NPP"

The consideration of external events has been done in Section 1.1 of this document, working on the reduced list of classes that are considered in WP22. L1-L2 PSA interface recommendations have been provided for the six classes of events in Section 2.1. One discussion for each class of events has been provided by WP40 partners to the individual documents produced by WP22 in the form of an Appendix.

"ASAMPSA_E shall also examine the interest of integrated (all hazards and IE) or separated PSA model"

In this work it is assumed that the PSA will be performed in an integrated platform (in this case, "integrated" means that ALL events that may cause a hazard are considered in a single model; it is NOT in reference to L1-L2

integrated analyses). The "integrated" in the sense of "single model" is a specific requirement of some authorities (e.g., the Swiss ENSI[6], [41]). The report insists on the interest to calculate a total risk measure to fulfill the IAEA safety objectives.

"ASAMPSA_E shall address methodology for simultaneous accident progression in core and SFP".

This wish by end-users cannot be addressed because a common approach for accidents in core and in SFP has not yet been developed. No state-of-the-art exists, and it would be premature to define something like "best practice". The end-user's wish might be transferred into an appropriate research activity.

"2. INTRODUCTION OF HAZARDS IN L2 PSAs

ASAMPSA_E shall identify issues associated to external hazards that may need significantly different treatments in comparison with L2 PSA methodologies for internal IE, e.g.

- Induced effects (internal hazards) by external hazards,
- Earthquake aftershocks,
- External hazards impact on containment function."

This end-user's wish has been addressed where appropriate (see interface L1-L2, Section 2.1 and see comment below, and comments that are already in the summary of items to be treated).

"Level 2 comment on induced effects and aftershocks
The end-users recommend that these issues should be addressed by L2 PSA, but it seems that they are more relevant for L1 PSA and should be covered there. In addition, it seems extremely ambitious to provide good practice for such issues. Guidance in terms of screening criteria in order to reduce complexity might be provided though."

"3. COMMON ISSUES FOR MULTI-UNITS PSA

ASAMPSA_E shall clearly identify deficiencies of single units PSA and promote development of multi units PSA".

This is done to the extent possible in Section 2.8, since ASAMPSA-E seems to arrive ahead of any other set of guidelines on the issue of multi-units sites. Experience from Canadian PSAs (from Toronto meeting in 2014) has been taken into account.

"ASAMPSA_E shall consider experience of countries like Canada having already developed multi-units PSA."

This is done (all relevant information from meeting in Canada taken into consideration), Section 2.8. Note that however the Canadian experience (for CANDU-type plants) is somehow limited, if compared to the needs of all other types of plants.

"ASAMPSA_E shall in particular examine HRA modelling demand for multi-unit PSA (e.g. team sufficiency if shared between units, site management complexity, equipment restoration possibilities, inter-reactor positive or negative effects …)"

This is done in Section 2.7.

"ASAMPSA_E shall examine how to improve HRA modelling for external hazards conditions to tackle the following issues:

- the high stress of NPP staffs,
- the number of tasks to be done by the NPP staffs,
- the impossibility, for rare events, to generate experience or training for operators actions (no observation of success/failure probability (e.g. simulator),
- the possible lack of written operating procedures (or non-precise procedures),
- the possible wrong information in the MCR or maybe the destruction of the MCR,
- the methodologies applicable to model mobile barrier installation (for slow developing event),
- the methodologies available to model use of mobile equipment (pumps, DGs) and conditional failure probability (human and equipment),
- the methodologies applicable to model equipment restoration (long term accident sequences, specific case of multi-units accidents, …)".

This is done wherever it is possible to discuss (specifically in Section 2.8, reinforced by the general discussions on HRA in Section 2.3), since there are no advances in any of the areas in the list, the suggestion is for the most part to use caution and conservatisms.

7.2.2 End User's comments as identified in the survey at the end of the project

This section is summarizing comments to the report as they emerged from the end-users' questionnaire [39] and workshop [40]. Related to this present document, the following comments have been given in the questionnaire. Answers are provided subsequently:

"There are neither new approach proposed, nor practical recommendations in the report."

It has been pointed out several times that from the point of view of L2 PSA (which is the subject of the present report) there is almost no issue which is significantly different for external initiators in comparison with internal ones. Therefore, there is almost no need for new approaches or practical recommendations beyond existing ones (see e.g. the ASAMPSA2 documents). Some differences might be expected for human reliability and for multi-unit sites.
This is why these topics are addressed in the present report. The issue is very different and difficult for L1 PSA, and there are several reports within ASAMPSA_E addressing the L1 issues.

The authors of the report have considered that the fragility analysis for the NPP confinement function following an external or internal hazard shall be performed in L1 PSA, even if results are used in L2 PSA. This choice, which has been controversially discussed during the ASAMPSA_E project, simplifies the L2 PSA guidance. Some partners, like IRSN, have pointed out the difficulty to perform this fragility analysis for the confinement function because failure criteria (containment leakage) are not equivalent to those applied in L1 PSA (in general, equipment malfunction).

"It appears to be clear that the subject needs more research, experience and discussion."

According to the authors' opinion, more research for L2 PSA regarding external events is not needed – see answer above. However it is obvious that experience of external hazards analysis and multi-unit L2 PSA is still largely missing today in the nuclear safety community. Experience and discussions in this area, based on applications, shall be promoted during the coming years. This may lead to a better basis for guidance to be developed.

"The need for this topic in the ASAMPSA_E project should be clarified."

The comment is not quite clear – what topic. As far as L2 PSA practices – except recommendations towards

- additional vulnerability/fragility analyses,
- specific human behavior analyses,
- multi-unit site issues,
- together with some practical recommendations related to coding of sequences, grouping initiators by intensity, etc.

no needs for new approaches related specifically to external hazards were identified.

Anyway, within ASAMPSA_E project no new methods were expected to be developed, the project has been supposed to provide best practices. Since full scope PSAs including external hazards are not yet performed widely best practices are difficult (maybe impossible) to provide. The recommendations are based on practical experiences of authors of this document, who also proposed within the document some outlines for multi-unit site issue resolutions (CCA).

Moreover, the following recommendations have been given during the workshop in September 2016 in Vienna. Appropriate answers are given subsequently:

"Consider all comments introduced by the reviewers into the document before the workshop."

Pertinent updates in the text had been performed including comments after the workshop, which are incorporated in the current text of the document.

"The interest and feasibility of a PSA modeling exactly each DiD level (especially levels 1 and 2) has to be investigated."

This topic seems to be of less importance for L2 PSA (where per definition all barriers preventing core melt have failed) than for L1 PSA. Anyway, the problems identified with respect to the issue has been related to dependencies of systems and quality of currently defined DiD. More details are to be found in [43].

"Proposal for a L2 PSA for multi-unit site seems interesting but needs further developments to be used as it is presented."

According to the author's opinion, multi-unit PSA are not yet state-of-the-art. As it was not the task of ASAMPSA_E to develop new approaches, the rough outline of the method was proposed by CCA voluntarily to show how the issue might be potentially resolved.

"Promote "graded" approach for the development of L2 PSA for external events."

The graded approach is recommended in IAEA Safety principle 3 [SF-1, Vienna, 2006]:

"3.15. Safety has to be assessed for all facilities and activities, consistent with a graded approach. Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to ***control the hazard****, and the* ***design and engineered safety features are assessed to demonstrate that they fulfil the safety functions*** *required of them. Where* ***control measures or operator actions*** *are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the* ***arrangements made are robust and that they can be relied on****. A facility may only be constructed and commissioned or an activity may only be commenced once it has been demonstrated to the satisfaction of the regulatory body that the proposed safety measures are adequate.*

3.16. The ***process of safety assessment for facilities and activities is repeated in whole or in part as necessary later*** *in the conduct of operations in order to take into account* ***changed circumstances (such as the application of new standards or scientific and technological developments), the feedback of operating experience, modifications and the effects of ageing****. For operations that continue over long periods of time, assessments are* ***reviewed and repeated as necessary****. Continuation of such operations is subject to these reassessments demonstrating to the satisfaction of the regulatory body that the safety measures remain adequate.*

3.17. Despite all measures taken, accidents may occur. ***The precursors to accidents have to be identified and analysed, and measures have to be taken to prevent the recurrence of accidents****.* ***The feedback of operating experience*** *from facilities and activities — and, where relevant,* ***from elsewhere — is a key means of enhancing safety****. Processes must be put in place for the feedback and analysis of operating experience, including initiating events, accident precursors, near misses, accidents and unauthorized acts, so that lessons may be learned, shared and acted upon. "*

It means that the analysis should be always performed **gradually** in steps **and the tasks should be split** in order to get as good result as possible to take into account all possible phenomena. The graded approach described in this report is represented e.g.

- at the level of external initiators graded by intensity;
- by sequences assigned to particular initiators in order to keep track to the end and to see in results also the initiators, since identical sequences may be assigned to more initiators;
- at the level of results – sequences graded by level of releases (INES) – see the CRT method recommended in [15];
- recommended revision of current PSAs with respect to IAEA Safety principles (feedback), …etc.

Anyway, this request was not part of initial End User's needs. The "graded approach" has been highlighted by some end-users (from industry) in the second end-user's workshop to overcome the difficulties of data quality and resources needed to extend PSA: sometimes, it may be appropriate to develop simplified PSA with conservatisms

in order to keep some consistency between the resources in PSA development, the quality of the final PSA results and their applications. For some end-users, high uncertainties could justify not developing some parts of PSA. In the context of the ASAMPSA_E project, it appears reasonable to promote as an important objective the "total risk assessment" with PSA (in the sense that PSA shall check (as far as possible) that no risk is unduly neglected) and to recognize that in some cases some simplifications are justified in PSA. The recommendations 3 and 4 are formulated in that direction. There is no recommendation to limit the PSA scope to the parts where uncertainties are not too high.

"Introduce the discussion on low quality data for rare IE events (natural hazards) and how it considered for L2 PSA development (shall we exclude such IE from L2 PSA?, how to be consistent in risk metrics applications ? Shall ASAMPSA_E promote full-scope integrated PSA (all IE in one PSA) or promote separated PSA (one PSA for each type of IE, to avoid mixing situations with different quality in IE data)"

It has to be admitted that it is not state of the art to precisely determine frequencies of rare natural hazards. However, this fact must not be used to justify that such issues are to be dismissed in PSA. Rather, it should encourage research and development in this field – perhaps with the consequence to devote fewer resources to well-established issues. Meanwhile, it is recommended to perform such analyses based on the present limited knowledge base. If the associated results are very different in quantity or quality to common PSA practice, these analyses might be presented and discussed separately

Regarding methodologies (integrated vs. separated), these have advantages and disadvantages, and both are routinely applied. In principle the interface from level 1 to level 2 becomes very complex if much information has to be transferred through this interface (e.g. status of human reliability, availability of systems for accident management, status of neighboring units, future development of an external hazard, …). It is a challenge for both approaches to handle such complexity. The success depends more on resources, user skills and technical tools than on the simple discrimination of integrated vs. separated approach.