Insights from PSA Comparison in Evaluation of EPR Designs

Ari Julin[*a], Matti Lehto[a], Patricia Dupuy[b], Gabriel Georgescu[b], Jeanne-Marie Lanore[b], Shane Turner[c], Paula Calle-Vives[c], Anne-Marie Grady[d], Hanh Phan[d]

[a] Radiation and Nuclear Safety Authority (STUK), Finland
[b] Institute of Radiological Protection and Nuclear Safety (IRSN) , France
[c] Office for Nuclear Regulation (ONR), United Kingdom
[d] Nuclear Regulatory Commission (USNRC), United States of America

Abstract: The paper describes the outcome of a limited probabilistic safety assessment (PSA) comparison on the following EPR designs: Olkiluoto 3 Nuclear Power Plant (NPP) in Finland, Flamanville 3 NPP in France, UK EPR design, and U.S. EPR design. The objective of this PSA comparison was to identify differences in the modeling aspects and results of EPR PSAs, as well as to assess the rationale for these differences. The comparison covered various types of initiators challenging a broad scope of safety functions. Insights from the EPR PSA comparison and rationale for the differences originated from modeling assumptions, applied reliability data, designs, and operational aspects. The EPR designs chosen for comparison represents various design and licensing stages, as well as level of detail, which gives the main rationale for the identified differences. The outcomes and lessons learned from the EPR PSA comparison have been used to facilitate the regulatory reviews and assessment work of various EPR designs and to enhance the scope, level of detail, and quality of EPR PSA models and documentation.

Keywords: PSA, EPR, Licensing, Regulation, Design Evaluation

1. INTRODUCTION

The EPR is an Evolutionary Pressurized Water Reactor (a.k.a. European Pressurized Water Reactor), whose design takes benefit from operating experience especially in France and Germany. Design improvements have been introduced to enable more reliable prevention and mitigation of severe accidents. EPR PSA development was initiated from the beginning of the conceptual design stage. At the end of the basic design phase, Level 1 PSA for internal initiating events as well as the so called Level 1+ PSA, to estimate the frequency of potential failures of the containment, taking into account measures for severe accident mitigation were completed. Later, Level 2 PSA and hazards PSA were developed. PSA has been used during the design process in order to optimize the design with respect to safety and availability [1].

EPR PSA comparison was performed by the Radiation and Nuclear Safety Authority of Finland (STUK), Institute of Radiological Protection and Nuclear Safety (IRSN) of France, Office for Nuclear Regulation (ONR) of the United Kingdom, and United States Nuclear Regulatory Commission (USNRC) within the Multinational Design Evaluation Program (MDEP) design specific working group on the Evolutionary Power Reactor (EPR). The comparison was conducted on the following EPR designs: Olkiluoto 3 Nuclear Power Plant (NPP) in Finland, Flamanville 3 NPP in France, UK EPR design, and U.S. EPR design, respectively.

MDEP was established in 2006 as a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities who are currently or will be tasked with the review of new reactor power plant designs. The Organization for Economic Co-Operation and Development (OECD) Nuclear Energy Agency (NEA) facilitates MDEP's activities by acting as technical secretariat for the program.

[*] ari.julin@stuk.fi

The objective of this PSA comparison was to identify differences in the modeling aspects and results of EPR PSAs, as well as to assess the rationale for these differences. The PSA comparison exercise was aimed to provide support for safety evaluations and PSA reviews in MDEP member countries.

The scope was limited to the following four initiating events (IEs): medium loss-of-coolant accident (LOCA), loss of offsite power (LOOP), steam generator tube ruptures (SGTR), and loss of cooling chain (LOCC). The selection covered various types of initiators challenging a broad scope of safety functions. The comparison focused on the IE definition, modeling of accident sequences (i.e., timing, safety functions, automatic and manual actions, etc.), minimal cut sets, importance measures, and quantitative results.

2. LICENSING AND PSA REQUIREMENTS

The licensing process is country specific, but it contains many similarities. PSA is a licensing document and a full scope PSA is required at the latest in the operating license phase. Licensing steps, status of licensing process and the role of PSA in France, UK, USA and Finland are described in more detail in the following subsections.

France

In accordance with the "Technical Guidelines" [2], the safety demonstration for the nuclear power plants of the next generation has to be achieved in a deterministic way, supplemented by probabilistic methods. In the frame of the construction license application of Flamanville 3 (FA3) reactor (2006) EDF provided a Level 1 PSA for internal events for the reactor and fuel pool, and a Level 1+ PSA and simplified analysis for internal and external hazards. For the FA3 operating license application, EDF will provide, according with the French safety requirements, a full scope Level 1 and Level 2 PSA (internal events and hazards). Some of these PSAs are already being reviewed by IRSN in the frame of so called "anticipated instruction" of the operating license.

UK

ONR has developed a process of generic design assessment (GDA) [3] for new reactor designs. Under the GDA process ONR assesses the safety case for the generic design of a specific type and make of reactor. ONR expects that the submission for design acceptance should include a full scope Level 1 and Level 2 PSA. The PSA should be used to help show that the design satisfies the requirement to reduce risk as low as reasonably practicable (ALARP). A Level 3 PSA relevant to the generic site will also be expected. The PSA for the UK EPR was assessed by ONR as part of GDA [4].

Prior to start of nuclear safety-related construction of a new reactor the responsible body (the licensee) would have to hold a nuclear site license [5]. ONR will then ordinarily use the primary power provided by License Condition (LC) 19 (4) [6] to specify that the licensee should not commence nuclear safety-related construction without a regulatory Consent. Throughout construction and installation, ONR may employ LC19 (4) to identify further 'hold points' where ONR Consent is required before the licensee may proceed from one stage to the next. For each stage, a safety case would be submitted to support the licensee's request to move from one stage to the next. Safety cases commonly produced include: pre-construction safety case, pre-inactive commissioning safety case, pre-active commissioning safety case, pre-operational safety case and operational safety case. For each safety case ONR expects that a full scope, site specific Level 1, 2 and 3 PSA would be included. This PSA would need to be aligned to the relevant reference design for the specific stage. The licensee has submitted to ONR an initial pre-construction safety report (PCSR) for the construction of two EPRs at Hinkley Point C [7]. However, this PCSR will be updated by the licensee prior to requesting consent to start construction of the nuclear island at Hinkley Point C.

Ultimately it is ONR's expectation that a full scope site specific Level 1, 2 and 3 symmetric PSA is produced to support operation that is consistent with international good practice and is capable of supporting a risk monitor application.

ONR expectations relevant to PSA can be found in its Safety Assessment Principles [8] (SAPs) and in the ONR technical Assessment Guide (TAG) on PSA, TAG 030 [9]. ONR is also guided in its safety case assessments by certain numerical targets in the SAPs. In assessing against these, ONR will seek sufficient information for it to be able to judge that the targets are likely to be achieved and that the overall risk is ALARP.

USA

The PSA is performed to support the design certification of the U.S. EPR. The principal objectives of this analysis are:

- to demonstrate that the design poses an acceptably low risk of core damage accidents;
- to identify opportunities for effective and timely improvements during the design phase, through a systematic assessment of the design;
- to provide the foundation for a plant-specific PSA for the combined operating license (COL) and operating phases.

The COL applicant that references the U.S. EPR design certification will either confirm that the PSA in the design certification bounds the site-specific design information and any design changes or departures, or update the PSA to reflect the site-specific design information and any design changes or departures.

This PSA is a Level 1 and Level 2 PSA and addresses the risks associated with nominal full-power operation, low-power operation, and shutdown conditions. The PSA assesses both internal and external events (except acts of sabotage).

The PSA assesses risk for comparison against the Commission's safety goals: core damage frequency (CDF) less than 1E-4/year and large release frequency (LRF) less than 1E-6/year; and containment performance goals: containment integrity be maintained for approximately 24 hours following onset of core damage for the more likely severe accident challenges and the conditional containment failure probability (CCFP) less than approximately 0.1 for the composite of all core damage sequences assessed in the PSA.

The design certification application for U.S. EPR is still under review. USNRC has completed phase three out of six in the safety review process. It is not known when the final safety evaluation report will be available.

Finland

The foundation for the risk informed safety management is laid in the nuclear safety legislation. Detailed regulations called YVL Guides are issued by STUK. As a necessary complement to the deterministic safety design, a PSA is required to verify the reliability of all vital safety functions and the balance of the design features.

A plant specific, design phase Level 1 and 2 PSA is required as a prerequisite for issuing the construction license, and a complete Level 1 and 2 PSA for issuing the operating license. The plant specific PSA includes internal initiators, internal hazards (fires, floods, missiles, etc.) and external hazards (harsh weather conditions and seismic events, etc.) analyzed in all operating modes. In each licensing phase PSA has to be used to demonstrate that the following probabilistic design objectives, specified in the Regulatory Guide YVL A.7 [10], will be met:

- mean value of CDF is less than 1E-5/year; assessed and verified in full scope Level 1 PSA;
- mean value of LRF is less than 5E-7/year; assessed and verified in full scope Level 2 PSA.

PSA will be complemented during construction as the detailed design of the plant unit will be finalized. Design has to be modified unless these objectives are met. If dominant risk factors are identified after issuing a construction license, all reasonable efforts have to be taken to reduce the risk.

During construction, PSA shall be updated to comply with the detailed design information of systems, structures and components (SSC) and more detailed modeling of plant response to various initiating events. The fulfillment of the aforementioned numerical criteria for CDF and LRF has to be demonstrated as well.

In addition, several PSA applications have been required in Regulatory Guides as a condition for construction and operating licenses. Examples of required risk informed PSA applications include Pre- and In-Service Inspection (RI-PSI/ISI), In-Service Testing (RI-IST), Technical Specifications (RI-TS), Safety Classification of SSCs (RI-SC), staff training, and identification of potential design changes and/or plant modifications.

In Olkiluoto 3 (OL3) project, risk informed approach has been applied in a large scale for the first time in the design, construction and commissioning of a new NPP unit in Finland.

3. EPR PSA COMPARISON

3.1. Development of EPR PSAs

The first Level 1 PSA for internal initiating events was completed at the end of the basic EPR design in 1999. This PSA model and documentation has been utilized in the further development of the first versions of EPR PSAs for Olkiluoto 3 and Flamanville 3 NPPs. Since then, the OL3 construction license PSA (2004) has been updated several times in the course of the detailed design process more or less independently from other EPR PSAs. OL3 PSA (2004) was used in the development of U.S. EPR PSA for Design Certification process in 2007. PSA for UK EPR GDA process was at least partially based on the three aforementioned PSAs: OL3 (2004), FA3 (2006) and U.S. EPR (2007). Although EPR PSA developers are exchanging PSA information and findings, each EPR PSA has been extended and updated in accordance with his own project specific requirements while the licensing and/or the detailed design processes have progressed.

3.2. Information on Selected EPR PSAs and Documentation

The analysis of internal initiating events constitutes the backbone of any plant specific PSA. EPR designs under the review represent various stages of the design process, licensing process, as well as level of modeling detail. Some PSAs are more or less so called full scope PSAs in terms of the coverage of initiating events i.e. internal IEs, and internal and external hazards are included in the analyses. The others include somewhat limited analysis of hazards. Therefore internal events PSAs were selected for EPR PSA comparison effort. The following subsections provide more information on the status and details of PSAs and related documentation chosen for the comparison. The source of the background information on the EPR PSAs is summarized in Table 1.

Table 1: EPR PSA Models and Documentation

	PSA information source (design stage)
FA3	Final Safety Analysis Report (FSAR) (2010)
UK EPR	GDA step 4 (2011) [4], GDA PCSR (2011) [11]
OL3	pre-Operating License Application (pre-OLA, v104, 2010)
U.S. EPR	Design Certification (DC) rev. 5 + PSA (2013)

Flamanville 3 NPP

The FSAR 2010 version of the Level 1 PSA internal events is an update of the PSA version provided by EDF and analyzed by IRSN in the frame of the construction license application in 2006. It considers the conclusions of the 2006 instruction and the design evolution until 2009. The updated version of this PSA provided by EDF in the frame of the operating licensee, will include the results of the "anticipated instruction" by IRSN (done in 2010 and 2013) of the FSAR 2010 version and of the subsequent updates as well as the final design and operation. However, due to inherent difficulties in developing a design PSA, some aspects will be finalized later, before starting commercial operation (like for example, the detailed human reliability analysis (HRA) based on the finalized procedures or the detailed modeling of maintenance).

UK EPR

The UK EPR GDA PCSR 2011 [11] version of the PSA model was considered as part the comparison exercise. This was assessed by ONR during the GDA process. This is a Level 1, 2 and 3 PSA that considers both internal events, and internal and external hazards. The Level 1 PSA also includes consideration of all non-power operating states. The scope of this PSA excluded any requirement on the PSA modeling that needed detailed design information or site specific data beyond the scope of GDA.

Updates have since been made to the PSA model to account for site specific features at Hinkley Point C, including, for example, site specific heat sink modeling, site specific loss of ultimate heat sink frequency and site specific loss of off-site power frequencies. The revised PSA has been provided to ONR to support the licensee's initial site specific pre-construction safety report [7]. Further updates to the PSA are anticipated as the detailed design progresses and as procedures are developed.

U.S. EPR

The U.S. EPR Level 1 PSA 2013 is a revision of the original 2009 Level 1 PSA, and is based on the design input through September 2012 and its supporting documentation. The 2013 PSA also reflects some modeling and data changes. The 2009 and 2013 PSA significant initiating event contributions to CDF for internal events are quite similar, with LOOP and small LOCA (SLOCA) still among the most important contributors.

Design changes resulting from earlier PSA insights include: increased safety related chiller capacity; each component cooling water header can provide seal cooling to all four reactor coolant pumps (RCPs); and, the four emergency feed water system (EFWS) storage tanks cross tie valves have been closed.

Pending design changes will be assessed against the PSA model periodically and the cumulative impact on the CDF will be determined and documented. If the impact on the cumulative CDF is less than 10 percent (positive or negative), then no further action will be taken. If the impact on the cumulative CDF is greater than 10 percent (positive or negative), then further impact on the PSA will be evaluated.

Olkiluoto 3 NPP

OL3 PSA has been updated several times during the construction and detailed design process. Hundreds of design changes ranging from minor to major have been implemented since the start of the construction in 2005. The PSA documentation and model chosen for EPR PSA comparison is based on the situation around the end of 2010 and the so-called pre-operating license application FSAR documentation.

Changes in the OL3 risk profile are foreseen due to the finalization of the detailed instrumentation and control (I&C) design and more detailed and realistic modeling of internal hazards, especially fires.

3.3. Main Results of EPR PSAs

Table 2 presents the results of four different EPR designs' internal events PSAs for power operating modes. The total CDFs are fairly similar but the risk profiles are not identical. Based on the experience from previous PSA comparisons performed e.g. in France and Finland, it was evident that the comparison should not focus on only those IEs, which CDF differs the most. Even with similar CDFs, significant difference may be identified related to IE frequencies, most important cut sets, modeling details, most important basic events, assumptions etc. Therefore the selection of candidate IEs was focused on those initiators challenging a broad scope of safety functions. Finally, the following four initiating events were chosen for comparison: medium loss-of-coolant accident, loss of offsite power, steam generator tube rupture(s), and loss of cooling chain.

Table 2: EPR PSA internal events CDF (1/a)

IE	DESCRIPTION	FA3	UK EPR[A]*	U.S. EPR*	OL3*
LOOP	**Loss of Offsite Power**	**1,40E-07**	**2,97E-07**	**1,23E-07**	**1,33E-07**
LOCA	Loss of primary coolant accident	5,70E-08	1,06E-07	4,48E-08	7,08E-08
MLOCA	***Medium LOCA***	***(3,6E-08)***	***(9,2E-09)***	***(9,1E-10)***	***(3,1E-08)***
V-LOCA	LOCA leading to containment bypasses	6,50E-10	3,70E-09	2,99E-09	1,50E-08
Prim-Tr	Primary circuit transients	2,00E-08	5,25E-08[D]	-	1,07E-08
Sec-Tr	Secondary circuit transients	4,60E-09	1,63E-08	1,37E-08	8,37E-08
Sec. Br.	Secondary circuit breaks	1,80E-08	1,3E-08	1,66E-09	8,88E-09
SGTR	**Steam Generator Tube rupture(s)**	**1,10E-08**	**1,02E-08**	**2,63E-08**	**2,21E-08**
LOCC	**Loss of cooling chain or heat sink**	**8,80E-08**	**9,46E-08**	**3,61E-08**	**1,94E-08**
ATWS	Anticipated Transient w/o Scram	1,00E-07	2,14E-08	8,95E-09	*(1,84E-08[B])*
LV-bus	Loss of low voltage busbars	2,50E-09	-	-	-
I&C	Spurious I&C actions	3,50E-08	-	-	-
IND SGTR	Induced SGTR	-	4,35E-09	8,50E-09	-
BDA	Loss of 6.9kV Power from Bus BDA	-	-	1,14E-08	-
GT	General Transient (Includes Turbine Trip and Reactor Trip)	-	-	2,02E-08	-
CCI-SAC	Loss of SAC divisions 3 & 4 due to CCF	-	-	-	2,50E-09
PSD	Planned Shutdown (pseudo IE) [C] *- I&C passive CCFs dominate the result*	-	-	-	1,18E-07
	TOTAL	**4,8E-07**	**6,2E-07**	**3,0E-07**	**4,8E-07**

[A] *PSA for a UK EPR™ at Hinkley Point C [7]*
[B] *Modeled together with related transients, not as a separate IE*
[C] *Event sequences which may occur (only) during a planned shutdown maneuver*
[D] *This includes some contribution for non at power operating states*
[*] *At power operating states*

3.4. Medium LOCA Comparison

IE definitions and plant response

Following a LOCA there are several scenarios possible depending on the break size. The definition of the LOCA categories is based on the accident mitigation means required depending on the impact of the break size on the reactor and given by the results of thermal-hydraulic analysis performed to support the PSA.

During at-power states, the LOCA scenarios typically modeled in the EPR PSAs studied result in a depressurization of the reactor coolant system, a decrease of pressurizer level and an increase in the pressure in the containment. This results in a reactor and turbine trip, and the initiation of the safety injection systems. In particular, the partial cooldown is initiated in order to decrease the reactor coolant system pressure to allow the required safety injection. Cooldown is performed by releasing the steam from the steam generators (SG) via the steam dump to the condenser or to the atmosphere.

Typical accident sequences and progression

The accident scenarios are similar in all the compared PSAs. Following a medium LOCA, partial cooldown is initiated in order to allow medium head safety injection into the cold legs. If partial cooldown fails, actuation of the primary circuit feed and bleed function is necessary.

The safety injection system accumulators discharge cold water to ensure complete quenching.

If the medium head safety injection system trains are unavailable, fast secondary cooldown can be manually actuated to reduce reactor coolant system pressure sufficiently to allow low head safety injection into the cold legs.

IRWST cooling is performed with one residual heat removal system train or containment heat removal system (CHRS) train.

Main differences

The main differences identified were the assumed medium LOCA frequencies. There is a significant difference between OL3/FA3 and UK/US medium LOCA frequencies. The UK and US medium LOCA frequencies' data source is NUREG 1829. The medium LOCA frequencies used in the FA3 and OL3 medium LOCA models have their origin in studies developed in France or in Germany respectively.

The conditional core damage probability is similar in all the PSAs. However, the following important differences have been identified:

- There are differences in the range of break size considered in the medium LOCA category. The main reason for this difference seems to be the thermal-hydraulic support studies available to the PSA analysts. The support studies are specific to each project except for the UK EPR PSA. The OL3 and the UK EPR PSAs studied in this comparison share the same support studies. However, some small differences exist in LOCA category definition between both PSAs. According to the information provided by the "EPR family", these differences seem to be due to modeling assumptions regarding the break spectrum.
- There are differences in the reliability data and human error probabilities. The impact in the overall medium LOCA results is negligible. However, the impact of these differences on the overall CDF may be more significant, but it was not in scope of the comparison exercise.
- There seems to be important differences in the treatment of digital I&C amongst the different models. Some of these differences may be due to modeling assumptions, the detailed design information available during the development of the PSA and potential design differences.

- The main difference identified in the success criteria is that the four steam generators (no additional feed) are required to ensure the cooldown functions in the U.S. EPR PSA as opposed to one steam generator (with additional feed) required in the other PSAs studied. Although this is different, it is not necessary contradictory as the same objective could be achieved by different means. However, it is important to note that differences in the supporting analysis may result in a different pressure in the containment after a medium LOCA. Depending on the protection system design, differences in the containment pressure may have an impact on the state of the main steam isolation valves (open or close). This would have an impact on the number of steam generators required to ensure the cooldown function. On the basis of the information available for the study it was not clear if there are different settings in the logic to control the main steam isolation valves between the different EPRs. The requirements for secondary feed would depend on the number of steam generators claimed in the PSA. As indicated previously, a review of the supporting analyses was considered as out of scope of the comparison exercise. *NOTE!: The success criteria for the U.S. EPR has been changed. Similarly to the other EPRs PSA studies, one steam generator is required, a difference in the U.S. EPR PSA is that no additional feed is required.*
- There are also differences regarding the need for primary bleed (during primary feed and bleed) in case of the partial cooldown failure, between the UK PSA and the rest of the PSA models.

Potential reason(s) for differences

The main reasons for the differences identified seem to be differences in modeling assumptions and thermal-hydraulic analyses. There was insufficient information available to realize any significant design differences that could impact the results.

Areas and topics that require additional information

Assumptions regarding the thermal-hydraulic analyses were not considered in this comparison exercise. These studies are not fully representative of all the EPR designs at this stage so a comparison at this stage may not be meaningful.

There was insufficient information to understand the differences in reliability data and human error probabilities. It is recommended to study these differences for the dominant contributors to the overall PSA results. Furthermore, there was insufficient information regarding I&C modeling and design differences. In view of the I&C significance for most of the CDF scenarios, it is recommended to study specific differences in the I&C modeling and design.

3.5. Loss of Off-site Power Comparison

IE definitions and assumptions

The external electrical power supply of the EPR plant is provided by two electrical grids: main grid designed for the normal operating conditions; auxiliary grid in case of "main grid" failure. In general, three types of LOOP initiating events can be analyzed in the EPR PSAs:

- loss of main grid: this initiator is defined as the loss of the external main power supply only;
- short term loss of offsite power: total failure of the main and auxiliary grid for a short term;
- long term loss of offsite power: total failure of the main and auxiliary grid for a longer term.

All compared PSAs consider these initiating events, but the frequency and grouping of initiating events are slightly different. It was decided to continue the comparison only for the initiating events Short LOOP and Long LOOP. In all PSAs the recovery times considered for these two initiating events are 24 hours for the long LOOP and 2 hours for short LOOP. The origin of 2 hours border between short and long term LOOP is that, for EPR reactor, the diesel generators are not needed

before 2 h (if no RCP seals LOCA). The IE frequencies used in the different PSAs are very similar, although coming from different specific data sources.

Typical accident sequences and progression

The accident scenarios are similar in all compared PSAs. Following the loss of the main and auxiliary grids the plant will be transferred to House Load Operation. In case of unavailability of the house load, the reactor trip is triggered. The turbine trip and the closure of Main Feed Water (MFW) large flow lines are also triggered. The Emergency Diesel Generators (EDGs) are started and connected to the safety busbars automatically. Since the MFW and the Startup and Shutdown System (SSS) pumps are not supplied by the EDGs, the SG level decreases leading to EFWS automatic actuation. The SG regulation is automatic. In case of EFWS unavailability primary Feed and Bleed (F&B) is necessary to avoid core damage. As the Component Cooling Water System (CCWS) and Chemical and Volume Control System (CVCS) are supplied by the EDGs, the reactor coolant pumps seals injection and the thermal barriers cooling is maintained (Note! In the U.S. EPR, CVCS is supplied from the station blackout DGs). In case of failures of these systems or theirs support systems, the Stand Still Sealing System (SSSS) will be automatically actuated in order to maintain the primary circuit integrity.

Similarities and differences

There is a large consistency among the four PSAs as regards to:

- the initiating events considered: short (2h) and long (24h) LOOP;
- the main CD sequences: in the four studies the main functional sequences are either a loss of heat removal (EFWS and F&B failure) mainly due to the failure of all the diesel generators, or a seal LOCA followed by a total loss of water injection;
- the overall results are very similar: about 1.3E-07 /year for the CDF relating to LOOP (as presented in Table 3 below) and a dominant contribution of LOOP to the total CDF.

Table 3: CDF (1/a) related to LOOP IE

	FA3	**UK EPR**	**U.S. EPR**	**OL3**
Short LOOP (<2h)	3,4E-08	1,4E-07	1,2E-07	1,1E-07
Long LOOP (< 24h)	9,5E-08			2,1E-08
Total	**1,3E-07**	**1,4E-07***	**1,2E-07**	**1,3E-07**

* *Result from PSA for GDA 2011 PCSR [11] inclusive of consequential LOOP. Note, PSA for Hinkley Point C, LOOP CDF ≈ 3E-07 /a*

However, with a more detailed analysis, differences were identified which could have an impact on results, especially in case of risk informed decision making (e.g. design optimization, TechSpecs, maintenance programs):

- Differences in success criteria and strategy in degraded situations: for example F&B is considered as possible with LPSI only in U.S. EPR PSA, the actuation of SBO diesel generators is possible only after the loss of all EDGs for FLA3. These differences seem to be due to procedures and to support calculations.
- Differences in the level and detail of modeling: for example modeling of ventilations, of electrical interconnections, of manual alignment of headers or other manual actions could lead to significant contributions.
- Differences in modeling and role of batteries, especially the need for 2h batteries for SBO diesels actuation and the CCFs between batteries.
- There are some differences in the reliability data and human errors probabilities, but it seems that they have not an important impact on the comparison.
- Significant differences appear in modeling and quantification of I&C: the CCFs identified and quantified, the account for diversified means (non-computerized) are not similar. The differences seem to arise from different modeling, assumptions and design.

It can also be underlined that some dominant results rely on similar assumptions in the four studies, especially the treatment of the seal LOCA risk and the CCFs between EDGs. For this last point all the PSAs consider a CCF between the four main diesels and a CCF between the SBO diesels, but no CCF between the two categories (assumption of adequate diversity), and since the loss of the six diesel generators is a dominant cut-set for all the studies, this assumption of diversity is very important.

Areas and topics that require additional information

Some of the identified differences between the compared PSAs, like the I&C, ventilations and CCF modeling may have an important impact on the PSA results and applications. However the available information was not sufficient for a detailed comparison. Especially I&C, which is an important and cross-cutting issue, needs a particular attention.

3.6. Steam Generator Tube Rupture Comparison

IE definitions and assumptions

The initiating event is a steam generator tube rupture (SGTR), for: the double ended rupture of a single tube; the double ended rupture of two tubes; and an induced rupture of multiple tubes, following a secondary side break. The multiple tube rupture is modeled as ten ruptured tubes in a single steam generator. The SGTR causes a loss of inventory from the primary to the secondary side of the SG, leading to a primary pressure decrease and a level increase in the affected SG.

Typical accident sequences and progression

The accident scenarios are similar for all four PSAs. The case of a single tube rupture, which was evaluated by all four PSAs, is described below.

Upon diagnosing the SGTR, operators trip the reactor, then isolate the faulted SG and initiate cooldown with the intact SGs. Failure to isolate the faulted SG means there is a LOCA outside containment and the operators must cool down, depressurizing the reactor cooling system (RCS). If the faulted SG is not isolated, an automatic signal initiates MHSI, which ensures primary circuit makeup and extends the time available for operators to cool down. Secondary cooldown can be accomplished by utilizing either the startup and shutdown system (SSS) or the emergency feed water system. If secondary cooldown fails, the operator initiates feed and bleed using MHSI, opening all the pressurizer safety valves (PSV) or one of the severe accident depressurization valves (PDV). Long term cooling (LTC) is either provided by one train of LHSI or a single train of the severe accident heat removal system (SAHRS i.e. CHRS in FA3/OL3/UK EPR) and the IRWST. Operator aligns and initiates residual heat removal via secondary circuit before IRWST is lost.

Similarities and differences

The four PSA models are largely similar, with respect to:

- the initiating events considered a single tube leak (all), a double tube leak (all but US), and multiple tube leaks (US and FA3);
- the main core damage sequences are failure to initiate fast secondary cooldown and failure of primary feed and bleed;
- the overall results for the single tube rupture, with the exception of the UK EPR, are similar ~ 2E-08 /year and are presented in Table 4 below. For the UK EPR, the CDF resulting from single tube ruptures has increased to 6,24E-09 /year in the PSA for a UK EPR™ at Hinkley Point C as a result of a correction to the PSA model [7].

Table 4: CDF (1/a) related to SGTR at power

	FA3	UK EPR*	U.S. EPR	OL3
Single tube rupture	5,5E-09 (1,0E-08 incl. small SGTR)	2,2E-10	2,6E-08	2,2E-08
Double tube rupture	7,7E-10	4,0E-09	N/A	9,0E-12
Multiple tube ruptures (following sec. side break)	4,4E-09 (SGTR SSB)		8,5E-09 (IND SGTR)	

* *Results from PSA for GDA 2011 PCSR [11]*

Areas and topics that require additional information

Potential design changes from I&C, especially in the U.S. EPR, need to be reflected in the PSA.

3.7. Loss of Cooling Chain Comparison

The Loss of Cooling Chain (LOCC) initiating events cover several failure modes, including pipe breaks and leaks, of the Component Cooling Water System (CCWS) and of the Essential Service Water System (ESWS). There are two common user headers (CH) in CCWS, each connected to two CCWS trains. There is also an interconnection between CHs for RCP thermal barrier cooling in all other EPR designs, except for OL3.

IE definitions and assumptions

In EPR PSAs, partial or total loss of cooling chain is treated as a so called common cause initiator (CCI). A common cause initiator is defined as an event which either causes a reactor trip or requires a shutdown of the reactor, and which at the same time degrades one or several of the safety functions which are required for the shutdown.

LOCC events are categorized in following main groups, presented in Table 5 below. Note, loss of one CCWS/ESWS alone do not lead to a CCI if the switchover to the standby train is successful. The number of LOCC IE groups in EPR PSAs varies from one to seven. For example, in OL3 PSA, seven IE groups were modeled in the construction license PSA (2004). Later, six of these were screened out based on frequency screening, more realistic modeling and taking into account that many of the event combinations are modeled in the fault trees i.e. there is no need to model each combination as a separate IE. According to EPR vendors, the modeling of LOCC IEs in EPR PSAs may evolve towards similar direction than in OL3 PSA.

Table 5. IE group frequencies (1/a) for LOCC events

	FA3	UK EPR	U.S. EPR**	OL3*
Loss of one train	4,7E-1	***	2,7E-3	-
Loss of one common header	5,8E-3[2]	***	2,0E-1[1]	3,5E-3[3]
Loss of all trains	1,8E-7	***	2,4E-6	-

* *Seven IE groups were modeled in construction license PSA (2004)*

** *The U.S. EPR values for these IE group frequencies are based the older model; in the 2013 revision all the LOCCW IEs are integrated into the model through a single initiating event fault tree*

*** *Not published*

1. *spurious openings of safety valves contribute 93% and leaks contribute 5%*
2. *Spurious opening of safety valves and leaks contribute each other to about 50% (EDF operating experience)*
3. *includes mechanical failure of one train and failure of switchover to the standby train*

Typical accident sequences and progression

Loss of one CCWS/ESWS train leads to unavailability of corresponding train in following safety systems (through lack of cooling):

- Medium Head Safety Injection
- Residual Heat Removal
- Low Head Safety Injection *(valid for pumps in safety trains 2 and 3, pumps in trains 1 and 4 have diversified cooling)*

The consequences of losing one common user header are:

- for OL3: loss of cooling for two RCP (thermal barrier and motor, motor bearing, pump thrust bearing) which leads to an automatic trip of these two RCP and consequential automatic reactor & turbine trip; for other EPRs either common header can cool all four RCPs (interconnection)
- shutdown of the operating charging pump (make-up) and automatic startup of the standby charging pump.

The consequences of losing two common user headers are:

- loss of cooling for all RCP (thermal barrier and motor, motor bearing, pump thrust bearing) which leads to an automatic trip of the RCP and consequential automatic reactor & turbine trip;
- loss of all charging pumps.

A failure of RCP trip may lead to a RCP seal LOCA. Residual heat removal would in both aforementioned cases be performed automatically via the secondary side feed & bleed with all secondary systems available with the exception that emergency feed water system train(s) may be affected via loss of room cooling in the corresponding trains in which the CCWS/ESWS failure(s) occur.

Following the LOCC the pressure in the main steam lines increases until the main steam by-pass (MSB) is automatically opened. If the MSB is not available the main steam release trains (MSRT) are opened. If the main feed water is not available, the start-up and shutdown (SSS) feed water pump is actuated. If both the MFW and the SSS fail the emergency feed water system (EFWS) pumps are automatically actuated.

Similarities and differences

In general, the plant response to LOCC IEs is fairly similar in all EPR PSAs. Significant differences exist in the grouping of IEs. The number of LOCC IEs varies from one IE group in OL3 up to seven IE groups e.g. in UK EPR. There are also differences in the exact definition of LOCC IEs, their frequencies, as well as in data sources and in the se of operating experience (pipe breaks and leaks).

Some of the differences in IE groups and frequencies may be explained by conservative modeling, choice of modeling approach (use of fault trees and/or calculation of IE specific frequencies) or data source.

In some cases the consequences of losing one or two common user headers in CCW system may vary due to design differences e.g. in air conditioning and ventilation systems. In OL3 NPP, the room cooling in the safeguard buildings was diversified by adding new heat exchangers cooled by CCWS. Examples of other design differences are given below.

- CCWS common user header (CH) valves
  - U.S. EPR: CCW CH valves need two divisions (trains) to open/close these valves (Div1 and 2 “OR” Division 3 and 4); specific combinations of double failures could fail all valves;

    - FA3, OL3, UK EPR: The solenoid valves are power supplied from the division the main valve belongs to. Thus the main valve closes (common user header will be isolated) if the power supply of the respective division is lost.
- There is an interconnection between common user headers for RCP thermal barrier cooling in all EPR designs, except for OL3 NPP. Adding this design feature in OL3 would have no significant impact on the risk.

Insufficient information was available for more detailed comparison of LOCC events in EPR PSAs.

Areas and topics that require additional information

The treatment of software failures and spurious signals of I&C systems as well as their impact on the results and the most important cut sets is still under review by some regulators. Another important modeling issue is the RCP seal LOCA. Based on the comparison, there are clear differences in the modeling. Complexity of potential failure combinations and assumption related to the leakage potential of the RCP seals need to be studied in more detail before drawing any definitive conclusions on identified differences.

4. EPR DESIGN DIFFERENCES

The MDEP EPR specific PSA working group has held joint meetings with EPR vendors exchanging information related to regulatory review findings, modeling details, design differences and potential new design changes. The work is still on-going, especially related to the identification of design differences affecting the risk. The aim is to find rationale for differences in EPR PSAs, whether their origin is in design, PSA modeling or data.

Examples of known differences, which are implemented due to regulations, site, operator, industry or project timing (not all of these are directly related to the PSA comparison exercise):

- Different SGTR management strategy in OL3: aim is to minimize steam release into environment, i.e. faulty steam generator automatically isolated at the end of partial cooldown (time < 10min). In other EPR designs isolation is done around 60 minutes post fault.
- Differences in system design, e.g. air conditioning and ventilation systems, extra boration system, fuel pool cooling system, EDG size and cooling, fire design, and some of the I&C systems.
- Full rupture (2A LOCA) of reactor cooling systems (RCS) is not the design basis for ECCS in all EPR designs,
- There are differences in RCS insulation material (mineral vs. glass wool).
- There are design differences related to severe accident management, for example:
    - Fulfillment of single failure criterion in severe accident systems is required in OL3.
    - Diversity between severe accident and design basis accident equipment is not required in all EPR designs.
    - Redundancy in severe accident depressurization is not required in all EPR designs.
    - Severe accident containment filtered venting is not required in all EPR designs.

5. CONCLUSIONS

One of the most important reasons for the identified differences is due to the fact that compared EPR PSAs represent various stages of the design process, licensing process, as well as level of modeling detail. Some PSAs are so called full scope PSAs in terms of the coverage of initiating events, i.e. internal IEs, and internal and external hazards are included in the analyses. The others include somewhat limited analyses of hazards.

Comparison of the numerical results of different EPR design PSAs is not straightforward. Firstly, each PSA represents various phases of licensing and detailed design processes. Secondly, there are differences in EPR designs, which affect the risk. Thirdly, studying the numerical results alone does not reveal the definitions and assumptions related to the modeling of IE groups and the accident progression.

The differences in the details and assumptions related to the modeling of I&C systems explain some of the identified differences. In addition, the detailed design of the OL3 I&C system is still under development and some changes are foreseen. The treatment and assumptions concerning software failures and spurious actions of I&C systems as well as their impact on results and most important cut sets is to be reviewed. Comprehensive fault analyses are needed for more detailed and realistic modeling of I&C systems.

The outcomes and lessons learned from the EPR PSA comparison have been used to facilitate the regulatory reviews and assessment work of various EPR designs and to enhance the scope, level of detail, and quality of EPR PSA models and documentation.

References

[1] J-L. Caron et al. "*The Use of PSA in Designing the European Pressurized Water Reactor (EPR)*", Proceedings of the 5th International Conference on Probabilistic Safety Assessment and Management (PSAM-5), November 27–December 1, 2000, Osaka, Japan.

[2] Letter ASN, "*Options de sûreté du projet de réacteur EPR" (2004) endorsing the "Technical guidelines for the design and construction of the next generation of nuclear power plants with pressurized water reactors*"

[3] ONR, New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-001 Revision 0, August 2013, (www.hse.gov.uk/newreactors/ngn03.pdf).

[4] ONR, Generic Design Assessment – New Civil Reactor Build, Step 4 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR™ Reactor, ONR-GDA-AR-11-019, Revision 0, 10 November 2011, (www.hse.gov.uk/newreactors/reports/step-four/technical-assessment/ukepr-psa-onr-gda-ar-11-019-r-rev-0.pdf).

[5] ONR, Licensing Nuclear Installations, Second edition: August 2013, (www.hse.gov.uk/nuclear/licensing-nuclear-installations.pdf).

[6] ONR, Licence condition handbook, Issue Date: October 2011, (www.hse.gov.uk/nuclear/silicon.pdf).

[7] Hinkley Point C Pre-Construction Safety Report 2012, (http://hinkleypoint.edfenergy consultation.info/public-documents/hinkley-point-c-pre-construction-safety-report-2012/).

[8] ONR, Safety Assessment Principles for Nuclear Facilities, 2006 Edition, Revision 1 SAPs, (www.hse.gov.uk/nuclear/saps/saps2006.pdf).

[9] ONR, Nuclear Safety Technical Assessment Guide, Probabilistic Safety Analysis, NS-TAST-GD-030 Revision 4, June 2013, (www.hse.gov.uk/nuclear/operational/tech_asst_guides/ns-tast-gd-030.pdf).

[10] Regulatory Guide YVL A.7, *"Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant"*, Radiation and Nuclear Safety Authority (STUK), 2013.

[11] UK EPR pre-construction safety report, Chapter 15, probabilistic safety analysis, 2011, (www.epr-reactor.co.uk/scripts/ssmod/publigen/content/templates/show.asp?P=290&L=EN).