MDEP

Technical Report

TR-EPRWG-04

EPR Working Group

Limited Comparison of EPR™ Probabilistic Safety Assessment (PSA)

Participation

Regulators involved in the MDEP working group discussions:	ASN (France), STUK (Finland), ONR (UK), NRC (USA), NNSA (CHN)
Regulators which support the present report:	ASN (France), STUK (Finland), ONR (UK), NRC (USA), NNSA (CHN)
Compatible with existing IAEA related documents:	Yes

CONTENTS

Executive Summary

The Multinational Design Evaluation Programme (MDEP) was established in 2006 as a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities that are currently or will be tasked with the review of new nuclear power reactor designs. The main objectives of MDEP is to enhance multilateral co-operation within existing regulatory frameworks, to encourage multinational convergence of codes, standards and safety goals and to implement the MDEP products in order to facilitate the licensing of new reactors. The MDEP incorporates a broad range of activities including the exploration of opportunities for harmonisation of regulatory practices and especially the co-operation on the safety reviews of specific reactor designs.

The MDEP now comprises five design-specific working groups for the EPR™, AP1000™, ABWR™, VVER™, and APR1400™ designs and three issue-specific working groups (vendor inspection cooperation, codes and standards, and digital instrumentation and controls (I&C)). The EPR Working Group (EPRWG) has five technical expert subgroups (TESGs): digital I&C, accidents and transients, severe accidents, probabilistic safety assessment and commissioning activities. The Organization for Economic Co-Operation and Development (OECD) Nuclear Energy Agency (NEA) facilitates MDEP's activities by acting as technical secretariat for the programme.

This EPR PSA comparison report, prepared by the EPR PSA TESG, describes the outcome of a limited 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. Originally, Taishan NPP Unit 1 (TSN, China) was not part of the comparison but it was later added for the comparison of I&C, HVAC and fuel pool cooling systems. The objective of this comparison was to identify differences in the modelling 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 modelling 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 main comparison work was performed a few years ago and therefore the most recent developments in the EPR design and PSA models are not reflected or discussed in this report.

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.

1 Background

1.1 Introduction

The EPR is an European Pressurized Water Reactor (a.k.a. Evolutionary Pressurized Water Reactor), whose design takes benefit from operating experience especially in France and Germany. Design improvements have been introduced to aim for 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, United States Nuclear Regulatory Commission (U.S. NRC) and National Nuclear Safety Authority (NNSA) of China within the Multinational Design Evaluation Program (MDEP) design specific EPR working group (EPRWG). 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, U.S. EPR design, and partly also Taishan NPP (China) 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 programme.

In MDEP, regulatory review and technical assessment information has been exchanged among its member countries to increase cooperation and improve the effectiveness and efficiency of the regulatory design review and licensing process for new reactor design and construction applications. However, one of key principles governing the MDEP program is that each regulatory entity retains sovereign authority over licensing and regulatory decisions for the new reactor design and construction applications under review in the member countries. For EPRWG, each national regulatory body is fully responsible for approving the EPR design and/or its construction application in its own country. One of the main purposes of establishing the MDEP program is to help each regulatory authority make informed decisions through multinational co-operation.

The objective of this PSA comparison was to identify differences in the modelling 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 (MLOCA), loss of off-site 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, modelling of accident sequences (i.e., timing, safety functions, automatic and manual actions, etc.), minimal cut sets, importance measures, and quantitative results.

1.2 EPR Safety Features

The EPR design is based on the experience from French and German PWRs, especially the N4 and Konvoi designs. Systematic use of the well-known design principles of redundancy, diversity and separation is an essential factor to meet the safety goals. Starting from the early conceptual design, probabilistic insights have been used to support the design of safety systems and to improve the provisions against internal and external hazards.

EPR design includes several features strongly contributing to low risk and well balanced design of a nuclear power plant. Examples of such design features include:

- Four redundant, separated safety trains (divisions)
- Diversity in systems design and safety functions
- Physical separation against internal & external hazards
- Station Black-Out (SBO) diesel generators (diverse of EDGs)
- Reactor Coolant Pump (RCP) stand-still seal system, back-up for normal seal system
- Double-wall containment with steel liner

Following twofold safety approach is applied in EPR design:

- To improve the preventive measures against accidents.
- To mitigate Severe Accidents consequences, even if their probability has been further reduced.

The safety approach includes a strong deterministic basis complemented by probabilistic analyses.

Accident Prevention measures are enforced by:

- Simplification of the safety systems
- Generally 4-train design of safety systems
- Elimination of common mode failures by physical separation and diverse back-up functions for safety functions
- Increase of grace periods for operator actions by designing components (e.g. pressurizer and steam generators) with larger water inventories to moderate transients

- Less sensitivity to human errors by an optimized man-machine interface by digital instrumentation and control systems and information supplied by modern operator information systems.

Low probability events with multiple failures and coincident occurrences up to the total loss of safety-grade systems are considered in addition to the deterministic design basis.

Two categories of events for risk reduction were introduced in EPR design:

- Prevention of core damage
- Prevention of large releases.

Design provisions for the reduction of the residual risk are:

- Primary Feed and Bleed in case of total loss of secondary side cooling
- Features for corium spreading and cooling, for hydrogen recombination, and for containment heat removal in case of severe accidents.

Consequently, the EPR design incorporates the following features for core damage mitigation and the prevention of large releases:

- Prevention of high pressure core damage by high reliability of decay heat removal systems, complemented by a dedicated primary depressurization
- Prevention of hydrogen combustion by reducing the hydrogen concentration in the containment at an early stage by catalytic Hydrogen (H2) –recombiners
- Control of the containment pressure increase by a dedicated containment heat removal system (CHRS), which consists of a spray system and which allows recirculation through the cooling structure of the melt retention device
- Collection of all leaks and prevention of any bypass of the confinement is achieved by a double wall containment.

The safety systems design is based mainly on four redundant subsystems, each with a 100% nominal capacity. Regarding emergency cooling systems the use of four redundancies is compatible with the N+2[1] design criterion. To minimize the effect of common cause failures (CCF), diversity is mainly used on safety function level, but also within some safety systems. Some examples of OL3 functional diversity are given in Table 1.

Systematic physical separation has been applied in the EPR design. Each of the four trains of the safety systems is located in a separate safeguard building. EPR design provides protection against a collision of a large passenger jet and a fighter plane. The reactor building, fuel building and two out of four safeguard buildings are protected by thick double concrete walls. The other two safeguard buildings and some support system buildings are protected by distance separation. These buildings are heavily built to withstand debris from airplane crash.

[1] *N+2 redundancy criterion gives the number of subsystems needed when a random single failure in one subsystem and preventive maintenance in another subsystem is postulated*

Table 1: Examples of Safety System Diversity in OL3 EPR

Safety grade systems	Diverse System Functions				
Emergency feedwater system + secondary relief	Primary side bleed via pressurizer safety valves	+	Feed with Medium Head Safety Injection System		
Emergency core cooling with the Medium Head Safety Injection System	Fast depressurization via secondary side	+	Accumulator Injection System	+ Low Head Safety Injection System	
Emergency Diesel Generators	SBO Diesels		On-site Gas Turbines		

EPR Designs in Member Countries participating in PSA Comparison

Olkiluoto NPP Unit 3 (OL3) in Finland was the first EPR-based nuclear power plant to begin construction. The licensee, the utility company Teollisuuden Voima Oyj (TVO) initially submitted an application in November 2001 to build the OL3 EPR plant and the Finnish Government granted the construction license for OL3 in February 2005. The construction for OL3 officially started in July 2005. OL3 is currently expected to enter commercial operation by the end of 2018.

In France, the EPR-based Flamanville Unit 3 (FA3) is the first Generation III+ plant in France. Électricité de France (EDF), applied to build the FA3 EPR plant and the French government issued the construction license for FA3 on April 11, 2007. Its construction officially began in December 2007. FA3's fuel loading is now scheduled in 2018.

In UK, EdF/AREVA requested that the Office for Nuclear Regulation (ONR) perform a Generic Design Assessment (GDA) on the UK EPR generic design in July 2007. ONR issued a Design Acceptance Confirmation (DAC) in December 2012 indicating the design is suitable for construction in the UK. Assessment reports on the UK EPR are available on the ONR website (*www.onr.org.uk/new-reactors/uk-epr/reports.htm*). Further work is required to close out GDA assessment findings, provide a safety case for items that are out of scope for the GDA (e.g. site specific heat sink), and show suitability for specific sites.

In U.S., AREVA NP submitted an application in December 2007 to the U.S. NRC for certification of the U.S. EPR standard design, which is modified to meet the U.S. regulatory requirements. In January 2010, the U.S. NRC staff issued a Phase 2 safety evaluation report with open items for the U.S. EPR Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation". Four organizations initially submitted applications in 2007 and 2008 to obtain a combined license (COL) to build U.S. EPR-based nuclear power plants. However, three of them (Callaway, Calvert Cliffs and Nine Mile Point) were withdrawn in 2013 and 2015. In February 2015, AREVA requested the NRC to suspend its safety review of the U.S. EPR design certification (DC) application. AREVA did not define an end date for the suspension period and said that it would contact the NRC prior to restarting the DC review.

2 Licensing and PSA Requirements in Member Countries

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 Finland, France, UK and USA are described in more detail in the following subsections.

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.) analysed 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[2] [9], will be met:

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

PSA will be complemented during construction as the detailed design of the plant unit is 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 modelling of plant response to various initiating events. The fulfilment 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.

[2] Reg. guide YVL Guide A.7 is an update of YVL 2.8, which is used for the licensing of OL3, The criterion for CDF and LRF are same in both guides.

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.

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 has provided, according with the French safety requirements, a full scope Level 1 and Level 2 PSA (internal events and hazards). According to the technical guideline, a probabilistic safety assessment has to be performed with the following objectives at the design stage : supporting the choice of design options, including redundancy and diversity in the safety systems, well-balanced safety concept and valuation of deviations from present safety practices, appreciation of the improved safety level compared to existing plants.

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 (HPC). 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 symmetrical 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 [7] (SAPs) and in the ONR Technical Assessment Guide (TAG) on PSA, TAG 030 [8]. 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 regulations require that a design certification (DC) application must contain a final safety analysis report (FSAR) that includes a description of the design-specific PSA and its results. The principal objectives of this assessment are to:

- Identify and address potential design features and plant operational vulnerabilities
- Reduce or eliminate the significant risk contributors of existing operating plants applicable to the new design
- Select among alternative features, operational strategies, and design options.
- Demonstrate that the risk associated with the design compares favorably against the Commission's goals of less than 1.0E-4/a for core damage frequency (CDF), less than 1.0E-6/a for large release frequency (LRF), and less than 0.1 for the conditional containment failure probability for the composite of all core damage sequences assessed in the PSA
- Obtain risk-informed safety insights based on systematic evaluations
- Describe the design's robustness, levels of defense-in-depth, tolerance of severe accidents initiated by either internal or external events, and risk significance of potential human errors associated with the design.

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.

Currently, the safety review of the U.S. EPR design certification application is suspended. The U.S. NRC has completed Phase three out of the six-phase safety review process.

3 Evolution and 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.

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 modelling detail. Some PSAs are more or less so called full scope PSAs in terms of the coverage of operating modes and 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 2.

Table 2. EPR PSA Models and Documentation

	PSA information source (design stage)
FA3	Final Safety Analysis Report (FSAR) (2010)
OL3	Pre-Operating License Application FSAR and PSA documentation (2010) and PSA model v104
UK EPR	GDA step 4 (2011) [4], GDA PCSR (2011) [10]
U.S. EPR	Design Control Document (DCD) Rev. 7 and PSA Rev. 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 analysed 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, includes 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 modelling of maintenance).

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 modelling of internal hazards, especially fires.

The scope of PSAs is more or less similar in all EPR projects (see Table 3). Biggest differences are in modelling of Level 3 PSA, handling of seismic hazards and treatment of non core melt sequences. These differences originate from each member country's national requirements related to the licensing of NPPs.

UK EPR

The UK EPR GDA PCSR 2011 [10] version of the PSA model was considered as part of 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 modelling 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 (HPC), including, for example, site specific heat sink modelling, 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 was updated in 2013 to reflect the integrated effects of individual changes that occurred between the 2009 U.S. EPR final safety analysis report (FSAR) and the 2013 U.S. EPR FSAR mark-ups. These changes occurred as a result of the numerous U.S. EPR design changes implemented in the five year period between September 2007 and September 2012.

Some of these design changes were identified by the PSA as opportunities to reduce risk. The most important area of improvement identified in the previous PSA revision was connected to the high contribution to risk from the heating, ventilation and air conditioning

(HVAC) systems. Improvements in this area resulted in the following PSA initiated design changes:

a. Increased capacity of the safety chillers - to provide more redundancy in the HVAC model, capacity of the safety chillers was increased so that one Safety Chilled Water System (QKA) chiller can cool two divisions.

b. Relocation of Class 1E inverters - the Class 1E inverters were moved from the direct current (DC) switchgear rooms to the alternating current (AC) switchgear rooms to reduce a heat load in the rooms. This design change has increased time available for HVAC recovery in safeguard building electrical rooms to longer than four hours.

In addition to the above design changes, some changes to the PSA model were also implemented in order to remove excessive conservatism, reduce non-conservatism, and correct model limitations. Important changes included in the PSA update were:

a. Initiating events - integrated initiating event fault trees: loss of component cooling water, loss of electrical bus, loss of balance of plant, and interfacing systems loss of coolant accidents into the PSA model, enabling more realistic importance rankings, and integrated uncertainty distributions.
b. Data/values - updated data, preventive maintenance parameters, human reliability analysis (HRA) error probabilities and dependencies.
c. System models - the systems with the largest changes in the updated PSA were: HVAC system, electrical system, I&C, RCP thermal barrier, emergency feedwater system, safety injection system (SIS) medium head safety injection/low head safety injection (MHSI/LHSI), control of emergency core cooling system flow, and core cooling system.

The 2009 and 2013 PSA significant initiating event contributions to CDF for internal events are quite similar, with LOOP and small LOCA (SLOCA) being still among the most important contributors.

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.

Table 3. Scope of PSA Models [11]

	FA3 FSAR	**OL3** Oper.License	**UK EPR** GDA	**U.S. EPR** DC
Level 1	x	x	x	x
Level 2	x	x	x	x
Level 3	simplified	-	simplified (full scope by HPC)	Full scope in support of Environmental Report (not in DC)
Internal Events	x	x	x	x
Internal Hazards	x	x	at power operating states	x
External Hazards	x	x	limited	x
Seismic	simplified	Seismic PSA	PSA based SMA	PSA based SMA
Fuel Pool Accident	x	x	x	-
LCHF*	x	-	x	-

** Scenarios with Low consequence and high frequency (no core damage)*

4 Main Results of EPR PSAs

Table 4 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. Largest differences in the initiating event group specific results are close to two orders of magnitude even if their contribution to the overall risk is small. The rationale for some of the identified differences is discussed in the following sections.

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, modelling 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 4. EPR PSA internal initiating events CDF (1/a)*

IE	DESCRIPTION	FA3	OL3	UK EPR	U.S. EPR
LOOP	**Loss of Offsite Power**	**1,40E-07**	**1,33E-07**	**1,48E-07**	**1,23E-07**
LOCA	Loss of primary coolant accident	5,70E-08	7,08E-08	1,18E-07	4,48E-08
MLOCA	***Medium LOCA***	***(3,6E-08)***	***(3,1E-08)***	***(9,2E-09)***	***(9,1E-10)***
V-LOCA	LOCA leading to containment bypasses	6,50E-10	1,50E-08	4,80E-09	-
Prim-Tr	Primary circuit transients	2,00E-08	1,07E-08	8,17E-08[C]	-
Sec-Tr	Secondary circuit transients	4,60E-09	8,37E-08	1,79E-08	1,37E-08
Sec. Br.	Secondary circuit breaks	1,80E-08	8,88E-09	1,3E-08	-
SGTR	**Steam Generator Tube rupture(s)**	**1,10E-08**	**2,21E-08**	**4,2E-09**	**2,63E-08**
LOCC	**Loss of cooling chain or heat sink**	**8,80E-08**	**1,94E-08**	**1,2E-07**	**3,61E-08**
ATWS	Anticipated Transient w/o Scram	1,00E-07	*(1,84E-08[A])*	2,14E-08	8,95E-09
LV-bus	Loss of low voltage busbars	2,50E-09	-	-	-
I&C	Spurious I&C actions	3,50E-08	-	-	-
IND SGTR	Induced SGTR	-	-	4,3E-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 common cause initiator	-	2,50E-09	-	-
PSD	Planned Shutdown (pseudo IE) [B] *- I&C passive CCFs dominate the result*	-	1,18E-07	-	-
	TOTAL	**4,8E-07**	**4,8E-07**	**5,3E-07**	**2,9E-07**

* *Data source: documentation presented in Table 2*
A *Modelled together with related transients, not as a separate IE*
B *Event sequences which may occur (only) during a planned shutdown maneuver*

[c] *This includes some contribution for non at power operating states*

5 PSA comparison of selected Initiating Events

5.1 Introduction

The objective of this PSA comparison was to identify differences in the modelling 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.

Detailed comparison of large and comprehensive PSAs is a very labour intensive job. It was necessary to first limit the comparison scope and to enable the allocation of resources to the most important aspects in PSAs. Thus the comparison was limited to level 1 PSA at full power and 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 and systems. The comparison focused on the IE definition, modelling of accident sequences (i.e., timing, safety functions, automatic and manual actions, etc.), minimal cut sets, importance measures, and quantitative results.

EPR designs under the review (see Section 3) represented various stages of the design process, licensing process, as well as level of modelling detail.

5.2 Loss Of Off-site Power (LOOP)

5.2.1 IE definitions and assumptions

The external electrical power supply of the EPR plants is provided by two electrical grids: main grid designed for the normal operating conditions; auxiliary grid in case of “main grid” failure. Both grids are designed to provide sufficient power for the safe shut down of the plant.

In general, three types of LOOP initiating events can be analysed in the EPR PSAs:

- Loss of main grid: this initiator is defined as the loss of the external main power supply only. The auxiliary grid supply is assumed to be potentially available. If the switchover to house load operation or to auxiliary grid is successful, no safety system is needed to cope with this event.
- Short term loss of offsite power: this initiator is defined as the total failure of the main and auxiliary grid for a short term.
- Long term loss of offsite power: this initiator is defined as the total failure of the main and auxiliary grid for a longer term.

In the four compared PSAs these three types of initiating events are particularised as follows:

- FA3:
  - Loss of main grid: 0.1/a.
  - Short LOOP (recovery time < 2h): 2,09E-2 /a.
  - Long LOOP (recovery time < 24h): 1,77E-3 /a.
- OL3:
  - Short LOOP (recovery time < 2h): 6E-2 /a.
  - Long LOOP (recovery time < 24h): 1E-3 /a.
- UK:
  - Short LOOP (recovery time < 2h): 6E-2 /a.
  - Long LOOP (recovery time < 24h): 1E-3 /a.
  - Induced by reactor trip (or others initiators leading to reactor trip):
    - Short LOOP (recovery time < 2h): 3,3E-4 (conditional prob. after reactor trip)
    - Long LOOP (recovery time < 24h): 6,6E-4 (conditional prob. after reactor trip)
- US:
  - Long LOOP (recovery time < 24h): 1,91E-2 /a.

    Note: The initiator "Long LOOP" is split in the PSA in three scenarios:
    - recovery before 1h (0.5 probability),
    - recovery before 2h (0.3 probability),
    - recovery before 24h (0.3 probability),

    Based on the recovery probabilities the equivalent initiating events frequencies can be estimated as:
    - Short LOOP (recovery time < 2h): 1,3E-2 /a.
    - Long LOOP (recovery time < 24h): 6E-3 /a.

    These equivalent values were used for the comparison purpose.

In all PSAs, the recovery times are considered as being:

- maximal duration for the long LOOP (24 hours),
- mean times for short LOOP (2 h).

  Note: In fact, for OL3 PSA, the 2 h recovery time for short LOOP is defined as being maximal time, but a recovery human error before 2 hours is considered.

The origin of 2 hours border between short and long term LOOP is that, for EPR reactor, the emergency diesel generators are not needed before 2 h (if no RCP seal LOCA). The emergency feed water system (EFWS) is necessary after the depletion of the steam generator inventory (~1h30min) and the primary heat transport (PHT) heat up time (~30min).

The data sources for the initiating events quantification are the followings:

- FA3: EDF operating experience,
- OL3: Finish specific data.

- UK: Specific data for induced LOOP, EUR data for the other initiators,
- US: NUREG CR 6890,

At this stage, taking into account the relative diversity of LOOP initiating events, it was decided to continue the comparison only for the initiating events Short LOOP and Long LOOP. The frequencies of the selected initiating events are presented in the following table:

Table 5. LOOP Frequencies

	FA3	OL3	UK EPR	U.S. EPR
Short LOOP (<2h)	2.1E-2	6.0E-2	6.0E-2	1.3E-2
Long LOOP (< 24h)	1.8E-3	1.0E-3	1.0E-3	6.0E-3

5.2.2 Modelling and description of accident sequences and progression

5.2.2.1 Accident scenario

The accident scenarios are similar in all compared PSAs.

Following the loss of the main and auxiliary electrical grids, the plant will be transferred to House Load Operation, if initially the plant is at full power. House Load Operation is not credited in the version of the UK PSA used in the comparison study. In case of unavailability of the house load (failure or reactor not at full power), the reactor trip is triggered, for example on low main cooling pumps speed, low reactor coolant flow or high steam generators (SG) pressure.

After the reactor trip, the turbine trip and the closure of Main Feed water (MFW) large flow lines are also triggered.

The Emergency Diesels Generators 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 diesels, the steam generator level decreases, leading to Emergency Feed Water System (EFWS) automatic actuation. The steam generator regulation is automatic. In case of EFWS unavailability, primary feed and bleed is necessary to avoid core damage.

As the Component Cooling Water System (CCWS) and Chemical and Volume Control System (CVCS) are supplied by the emergency diesel generators, the RCP seal injection and the thermal barriers cooling is maintained. 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.

5.2.2.2 Main operator actions

No operator actions are necessary on the success path at short and medium terms. The first operator action is necessary before the emptying of EFWS tanks (at ~24 hours) to supply the EFWS tanks or to connect the residual heat removal (RHR).

Nevertheless, in case of failure of front line or support systems, several operator actions are necessary. In general, important operator actions, as shown by PSAs, are the followings:

- Manual starting and connection of Station Black-Out (SBO) Diesels,
- Manual Partial Secondary Cooldown (PCD) to ensure the SSSS integrity in case of unavailability of primary pump seals injection and thermal barriers cooling,
- Manual Fast secondary Cooldown in case of Medium Head Safety Injection System (MHSI) unavailability,
- Primary Feed and bleed if the secondary cooling is not available.

Moreover the comparison, as showed in Sections 5.2.3.3 and 5.2.4, highlighted some other important operator actions specific only for some PSAs.

The differences between the different PSAs are analysed in the Section 5.2.4.

5.2.3 Results

5.2.3.1 Core damage frequency

The core damage frequency (/a) obtained for the LOOP initiating events family are presented in the following table:

Table 6. LOOP CDF

	FA3	OL3	UK EPR	U.S. EPR
Short LOOP (<2h)	3,4E-8	1,1E-7	5.7E-8	1,2E-7
Long LOOP (< 24h)	9,5E-8	2,1E-8	4.3E-8	
Total	1,3E-7	1,3E-7	1,0E-7	1,2E-7

The conditional core damage probabilities (CCDP, core damage frequency divided by initiator frequency) are presented in the following table:

Table 7. LOOP CCDP

	FA3	OL3	UK EPR	U.S. EPR
Short LOOP (< 2h)	1.6E-6	1.8E-6	0.96E-6	6E-6
Long LOOP (< 24h)	5E-5	2.1E-5	4.3E-5	

5.2.3.2 Dominant accident sequences

Short LOOP (< 2h)

- FA3
  - Failure of all diesels (4 main diesels and of 2 SBO diesels): 6.3E-9 /a.
  - Failure of EFWS and failure of feed and bleed: 5.4E-9 /a.
- OL3:
  - Failure of all diesels (4 main diesels and of 2 SBO diesels): 8.7E-8 /a.
  - Failure of EFWS and failure of feed and bleed 1.4E-8 /a.
- UK:
  - RCP seals LOCA followed by failure of safety injection: 3.9E-8 /a.
    - PCD failure (I&C) or,
    - MHSI failure and failure of the manual fast cooldown.
  - Failure of EFWS and failure of feed and bleed: 1.1E-8 /a.
- US: not available

Long LOOP (<24h)

- FA3:
  - Failure of all diesels (4 main diesels and of 2 SBO diesels): 4.6E-8 /a.
  - Seals LOCA followed by failure of 3 main diesels and of the remaining MHSI train: 1.6E-8 /a.
- OL3:
  - Common Cause Failure (CCF) of 4 EFWS pumps and feed and bleed failure: 1.4E-8 /a.
  - Seals LOCA followed by MHSI failure and fast cooldown failure: 4.8E-9 /a.
- UK:
  - Failure of all diesels (4 main diesels and of 2 SBO diesels): 5E-8 /a.
  - Seals LOCA followed by MHSI failure and Fast Cooldown failure: 1.6E-8 /a.
- US:
  - Failure of all diesels (4 main diesels and of 2 SBO diesels): 7.2E-8 /a.

5.2.3.3 Important post-accident human actions

The study of the importance measures (mainly Fussell-Vesely) showed that the following post-accident human actions are important contributions to the core damage frequency:

- FA3:
  - Starting of the SBO diesels.
  - Primary Feed & Bleed in case of secondary cooling unavailability.
  - Manual PCD before 2h in order to keep the SSSS integrity.
  - Starting of the SBO diesels and Fast secondary Cooldown in case of LOCA in SBO conditions.
- OL3:
  - Providing power from on-site Gas Turbine.

  - Opening of EFWS headers valves at long term.
  - Primary Feed & Bleed in case of secondary cooling unavailability.
  - Using of cross connections between electrical trains.
  - Switching to fresh air supply in case of failure of ventilation cooling.
  - Controlling EFWS if case of automatic control (PS) failure.
  - Manual start of stand-by rectifiers (short LOOP).
  - Manual start of SBO diesels (short LOOP).
- UK :
  - Using of the cross connection between electrical trains to open the main steam relief train (MSRT) in SBO conditions.
  - Starting of the SBO diesels.
  - Fast cooldown in case of MHSI unavailability.
  - Control EFWS in case of automatic control (protection system, PS) failure.
  - Primary Feed & Bleed in case of secondary cooling unavailability.
  - Opening of EFWS headers valves within 6 hours.
- US:
  - Connecting and loading SBO diesels (SBO and non SBO conditions).
  - Recovering room cooling locally in case of ventilation failure.
  - Switching chiller cooling in case of main cooling failure (ventilation failure).
  - Primary Feed & Bleed in case of secondary cooling unavailability.
  - Controlling EFWS if case of automatic protection system (PS) control failure.

5.2.3.4 Important systems and components

The study of the importance measures (mainly Fussell-Vesely) showed that the following systems and components are important contributions to the core damage frequency:

- FA3:
  - Stand Still Sealing System.
  - Main diesels.
  - Diesels SBO.
  - Safety Injection System.
  - Emergency feed water system.
  - TXP (SPPA-T2000).
- OL3:
  - Gas turbine.
  - Main diesels.
  - Stand Still Sealing System.
  - Emergency feed water system.
  - Computerized I&C (mainly for short LOOP).
- UK:
  - Stand Still Sealing System.
  - Protection System.
  - Main diesels.
  - Diesels SBO.

- US:
  - Main diesels.
  - Diesels SBO.
  - Stand Still Sealing System.
  - Batteries.

5.2.4 Similarities and differences

The comparison of models and the results showed that they are globally quite similar. However, there are some assumptions or design differences which, although the global results are in the same range, can lead to different PSA output in the context of a decision making processes (design optimization, Technical Specifications, maintenance programs…).

The most important aspects are presented in the following paragraphs 5.2.4.1 - 5.2.4.4.

5.2.4.1 Modelling Methods

All the PSAs use the event trees/fault trees modelling, although the size and the structure of the trees are rather different. For example the event trees of FA3 are very large compared to the others. However these differences, mainly related to the detail of the analysis, have no (or a limited) impact on the results.

5.2.4.2 Initiating events

The definition of initiating events is the same in all compared PSA:

- short LOOP, with a medium recovery time of 2 hours,
- long LOOP, with a maximum recovery time of 24 hours.

The PSAs do not study longer LOOPs than 24 hours. However, for FA3 and for UK EPR, specific studies consider a longer LOOP duration (100 hours and 192 hours): these specific studies are not considered in this comparison report.

The frequency of initiating events are of the same order of magnitude (~1E-2 /a. for the short LOOP and ~1E-3 /a for the long LOOP), but some differences between the different PSA exist, explained mainly by different local conditions. Also, the UK EPR PSA considers the induced LOOPs with a frequency of 4.9E-4 /a for short LOOP and 9.7E-4 /a for long LOOP. Short induced LOOP has not an important contribution to the CDF, but long induced LOOP has a contribution similar to other long LOOP initiating event (4.2E-8/a).

5.2.4.3 Accident sequences modelling

Heat removal by secondary side

- Short term

In all PSAs, except FA3 PSA, it is assumed that the EFWS is not needed before 2-2.5[3] hours. The steam generator inventory and the delay before PHT heat-up allow to start-up the EWFS only after 2 hours.

In FA3 PSA, it is considered that, in case of unavailability of all main diesels, EWFS needs to be started (power supplied by SBO diesels) before 1h30, in order to avoid the emptying of steam generator which leads to feed and bleed initiation criteria (which cannot be performed if all main diesels are unavailable).

The reason of this difference seems to be related either to the depth of the analysis or different accident procedures (the design looks similar). This aspect is important mainly for determining the operator available time to manually start the SBO diesels.

- Medium term
  In all PSAs it is considered that water supply of the EFWS tanks is not necessary (the accident sequences mission time is limited to 24 h).

  The main difference between the models is that in all PSAs, except FA3, the opening of the EFWS common headers is considered necessary in case of unavailability of some EFWS trains (loss of power supply or train failure).

Primary Feed and bleed and success criteria

The primary feed and bleed success criteria are fairly different in different PSAs.

- The feed and bleed cannot be performed with LHSI, except for US PSA.
- The cooling can be performed either by one LHSI train (in all PSAs) or by containment heat removal system (CHRS). In all PSAs, one CHRS train is sufficient for feed and bleed (in the US design there is only one CHRS train, in other designs there are two CHRS trains).
- The success criteria for the injection with MHSI is also different:
  - FA3:
    - 2/4 MHSI pumps, or,
    - 1/4 MHSI pumps and 4/4 Accumulators, or,
    - 1/4 MHSI pumps, 1/2 CVCS and 1/4 LHSI (or 1/4 Accumulators),
    - in case of seals LOCA: 3/4 MHSI, 1/4 Accumulators and 2/2 CVCS pumps,
  - OL3:
    - 2/4 MHSI, or,
    - 1/4 MHSI pumps and 4/4 Accumulators.
  - UK:
    - 2/4 MHSI pumps or 1/4 MHSI pumps and 4/4 Accumulators
  - US:

[3] In OL3 PSA, grace period of 2.5 hours is used based on support analyses.

  - 1/4 MHSI pumps and 1/4 Accumulators, or,
  - 1/4 LHSI pumps and 2/4 Accumulators,
  - in case of seals LOCA: 1/3 MHSI pumps and 1/3 Accumulators or 1/3 LHSI pumps and 1/3 Accumulators,
- The success criteria for Primary Depressurization System (PDS) is the same in all PSAs (1/2 valves). In all PSAs, except FA3 PSA, it is considered that the opening of 3/3 Pressurizer valves is a redundancy for the PDS.

The above differences are mainly generated by the different support studies (or by assumptions taken in absence of support studies) and the definition of core damage. Even if the numerical results are similar, these modelling differences can lead to different conclusions in the frame of a decision making process. This subject may be further analysed (possibly in connection with other EPR MDEP groups).

Modelling of short mission times for the main diesel

The main diesels reliability for short mission times (short LOOP) is modelled in a different manner in the different PSAs:

- In FA3 PSA, EDF considers a correction factor which takes into account the possibility that the main diesels may not fail simultaneously and consequently quantify the probability to recover the external power supply before the failure of the last main diesel.
- In OL3 PSA a 24 hours mission time is considered for both short and long LOOP.
- In UK PSA a 2 hours mission time is considered.
- In US PSA a 12 hours mission time is considered.

It is difficult to assess the impact of this modelling difference on the overall results, but it seems that, in general, the EDGs mission time is an important parameter for the core damage frequency in case of LOOP. In fact, the frequency of the short LOOP and the expected duration seems to be a dominant contributor for the LOOP family.

Station Black-Out Diesels

a) Strategy to use the SBO diesels

The strategies for using the SBO diesels have some differences. In all PSAs except for FA3, it is considered that the SBO diesels will be used in case of corresponding electrical train main diesel failure. For FA3, the starting of SBO diesels is possible only if all the main EDGs are unavailable. This aspect explains the FA3 dominant accident sequence: seals LOCA followed by failure of 3 main diesels and of the remaining MHSI train, since the fast cooldown cannot be performed with only one EFWS train.

This accident procedure strategy difference can have an important impact on the results.

b) Strategy in case of RCP seals LOCA in SBO conditions

In case of RCP seals LOCA in SBO conditions two problems are raised:

- The strategy to reach the LHSI injection conditions and further to inject by LHSI (since one SBO diesel cannot supply LHSI and EFWS pumps simultaneously, a careful power management is necessary):
  - In FA3 PSA and UK PSA it is considered that fast secondary cooldown will be engaged, by using two EFWS pumps, then the operator will switch at least one SBO diesel to supply a LHSI train.
  - In US PSA it seems that the strategy is to initiate the primary bleed (opening of primary depressurization valves) followed by primary injection with one LHSI train and at least two accumulators. This strategy raises the question of available support studies.
  - In OL3 PSA two SBO diesels are necessary (conservative assumption because in OL3 PSA, one SBO is enough for decay heat removal). However even in no LOCA situation, OL3 PSA considers that two SBO diesels are necessary.
- The available time to perform the manual actions.
  - In FA3 PSA it is considered that the available time is 1h30. However, recent support studies show that the available time before emptying the steam generators is about 30 minutes if the PCD (opening of the main steam relief valves (MSRV)) is automatically initiated by the safety injection signal.
  - In OL3 PSA and US PSA it is considered that, in case of seal LOCA, the available time to start and connect the SBO diesels is 1 hour.
  - In UK PSA the available time is 30 minutes.

This aspect may be one of the most important for the LOOP initiators family. However, the available information seems insufficient to definitely draw a conclusion.

c) Support systems needed to start and connect the SBO diesels

In all PSAs it is considered that the SBO diesels can be manually started and connected from the main control room if the 2h batteries are available. In all PSAs, except US PSA, if the 2h batteries are unavailable, the local starting and connection of SBO diesels is possible (by using the SBO dedicated batteries, capacity ~12 h). In US PSA it is considered that the SBO diesels cannot be started and connected without the 2 hours batteries

It seems that this aspect is coherent in three PSAs (FA3, OL3 and UK). However, the “local actions” are not detailed (for example, if the local action should be performed in one place or in several places).

d) Diversity main diesels / diesels SBO:

Since no common cause failure (CCF) grouping together the main and SBO diesels is considered, it seems that in all PSAs the main diesels and the SBO diesels are considered as being diversified.

However, in the US PSA, the probability to lose all diesels seems more important than in the other PSA. This may be induced by the CCF of batteries (and by the assumption that the SBO diesels cannot be started and connected without the 2 hours batteries), and by possible other high functional dependency between the main diesels and the SBO diesels.

SSSS reliability

The reliability model of the standstill sealing system (SSSS) device itself looks like being similar in all PSAs.

Similarly, for all EPR, in order to ensure the SSSS leak tightness, some other automatic and manual actions are also necessary: main pumps shutdown, closure of the seals leak-off line, manual PCD before 2 or 3 hours. These actions involve I&C systems and power supply systems.

However the modelling and the level of detail seem to be different in different PSAs:

- The model of the SSSS device itself is more (UK PSA) or less detailed (FA3); however the final results are similar.
- Manual PCD:
  - In all PSAs the manual PCD action is considered (delay available: 2 hours). In OL3, PCD within 2 hours guarantees SSSS leaktightness for 30 hours according to test results).
- I&C and electrical power supply:
  - In FA3 PSA and UK PSA the I&C for the SSSS actuation and other associated automatic actions is modelled (COMPACT model) but the electrical power supply of the valves (mainly the seals leak-off line isolation valves) is not explicitly modelled.
    Note: this aspect is important since functional dependency between the electrical trains may be highlighted by the PSA.

In general, it seems that the available information on the detailed modelling of the systems and actions to ensure the SSSS leaktightness is not sufficient for a complete detailed analysis of this aspect.

Use of inter-trains electrical cross connections

In UK PSA and in OL3, PSA the possibility to use the interconnection between the electrical divisions is considered:

- UK – to make possible the actuation of the MSRT if some of the electrical division are available,
- OL3 – to supply the ventilation systems of the train for which the electrical power is not available.

Since in FA3 PSA the electrical power supply of the solenoid valves needed to actuate the MSRV is not modelled, the need for using the interconnection to other electrical division, in case of failure of the current division powers supply, is not highlighted by the PSA. Moreover since the design of the power supply of the MSRT systems (valves itself and solenoid valves) is different between different EPR project, as presented by AREVA, it is difficult at this stage to draw a conclusion regarding the overall importance of using the interconnection between the electrical divisions for this purpose in case of failure of one or more electrical divisions. However, this aspect might be important for the CDF.

Also, in the FA3 and in the UK PSA the ventilation systems are not modelled, consequently the impact of the ventilation unavailability is not highlighted by PSA. This aspect can be also important for the CDF.

In U.S. EPR PSA: information not available.

Note: the need or not to use the inter-connections between the electrical divisions, in case of failure of one or more electrical divisions, especially to ensure the I&C or ventilations power supply, may be an important aspect which needs to be considered in the NPP design and in the accident procedures.

Ventilations modelling

The ventilation systems are modelled in OL3 PSA and in U.S. EPR PSA. They are not modelled in FA3 PSA and in UK EPR PSA. Moreover, the ventilations design is slightly different for different EPRs (for example, in OL3, ventilation cooling diversity is provided in divisions 1 and 4).

For U.S. EPR FSAR, it was considered that a loss of HVAC to safeguard buildings SB1 and SB4 leads to loss of Division 1 & 4 (the divisions that supply the running CCW pumps) and this results in loss of HVAC to all safeguard buildings.

The actual modelling in OL3 PSA and in U.S. EPR PSA highlights the importance of the ventilations and of the recovery actions of the ventilations (local “not-detailed” recovery in US PSA or using of the electrical interconnection between the electrical divisions in OL3 PSA).

In conclusion, it is not easy to compare the PSAs regarding the ventilations since the models and the designs are different. Nevertheless, the importance of the ventilations on CDF is highlighted by the PSAs where this aspect is considered.

The assumptions regarding the external temperatures considered in the PSAs (high temperatures and low temperatures) were not checked in the frame of this PSA comparison study.

I&C modelling

Globally, the digital I&C seems to have an important impact on LOOP results in some study but less in others. This point may probably be similar for other Initiating Events so it may be important to have more details about the I&C model in each study (assumptions, reliability, CCF). It may be interesting to have a special analysis of this subject in a further comparison exercise.

Model used:

The modelling of I&C is based on the COMPACT model for FA3, UK and USA PSA, and on the super component model for OL3.

CCF considered:

Several I&C CCFs are considered in the different PSAs with different numerical values, and it is not easy to identify from the minimal cut sets (MCS) what part of the I&C is concerned and what are the functional consequences.

Moreover the modelling of a hardwired backup system (HBS, non-digital) is clearly introduced for OL3 and for UK PSA. In UK PSA, this processing part of the Non-Computerised Safety System (NCSS) is considered as one unique part (no distinction is made between specific or non-specific logic parts) common to all NCSS channels: automatic functions and manual actions. A failure of this processing part leads to the total loss of all NCSS actions. This event captures failure of the hardware and software of the processing system (instrumentation, actuation, support systems (electrics etc.) are modelled separately).

The following CCFs are identified:

- FA3:
  - PS: failure of common logic: 1E-5
  - TXP: failure of common logic: 1E-4
  - No CCF between PS and TXP
- OL3:
  - Failure of computerized I&C: 2E-6
  - CCF TXP (hardware failure): 4.37E-6
  - CCF TXS (hardware failure): 3.43E-5
- UK:
  - Failure of common logic of protection system
  - Failure of SPPA-T2000 (TXP) logic part

  - CCF between PS and SPPA-T2000 logic parts: not explicitly modelled but is considered as covered by the PS and SPPA-T2000 failure probabilities
  - Total failure of NCSS is introduced (no indication of the numerical value)
- US:
  - CCF on safety automation system (SAS) divisions: 5E-7
  - CCF PS Diversity Groups A&B software: 1E-5
  - TXS Operating System or Other Common Software: 1E-7

The I&C treatment is very important since it appears in the dominant MCS for at least two PSAs (UK, US).

- The CCF modelled for software failures are different (identification and quantification), although these differences do not correspond clearly to a design difference. This finding illustrates the part of judgment and the subsequent uncertainty in this PSA aspect which, even if there is no significant effect on the base case results, has to be kept in mind in case of risk informed decision making.
- There is a non-digital backup modelled in two PSAs (NCSS for UK, HBS for OL3) with an important impact on the results. The importance of the non-digital back-up is of course highly related to the values used in different PSAs to quantify the software failures.

Common cause failures

The modelling of CCF groups is slightly different in the compared PSAs. The aspects having an impact on the LOOP initiating events family are:

- The CCF of the safety busbars (LH) is considered in:
  - FA3 - induced by the simultaneously start-up of the safety systems – it is an important contributor,
  - US – induced by CCF on under voltage sensors,
  - Not considered in the other PSAs.
- The “2 hours” batteries CCF are considered as following:
  - US – 4 batteries CCF is considered (1.6E-7) (additionally it is considered that the starting and coupling of SBO diesels is not possible without “2 hours” batteries),
  - OL3 – 4 batteries CCF is considered (1.5E-7) (it is also considered that the starting and coupling of SBO diesels is possible without “2 hours” batteries),
  - FA3 and UK – two groups of two “2 hours” batteries are considered (no CCF on 4 batteries is considered and it is also considered that the starting and coupling of SBO diesels is possible without “2 hours” batteries).
- EDGs: all PSAs consider two groups: one group for the main diesels and one group for the SBO diesels. In conclusion, all PSAs consider that the main and SBO diesels are completely diversified.
- CCF on EFWS control valves:
  - Modelled in OL3 PSA and looks as being one important aspect.
  - Not modelled in FA3 and UK PSA.

- CCF of rectifiers after LOOP
  - Modelled in OL3 PSA: it highlights the importance of the manual connection of stand-by rectifiers.
  - Not modelled in FA3 and UK PSA.

In conclusion, some of the modelled CCF groups are different in different PSAs. The impact of these differences is difficult to assess since some assumptions (relating or not to design differences) are different, leading to different importance of the CCF groups. As mentioned previously, the differences highlight PSA uncertainties which have to be considered in a decision making process.

Reliability data

The reliability data of components are slightly different in different PSA projects. However it seems that the impact of these differences (except the I&C reliability) on the results is limited.

Human factor modelling and quantification

The human factor is quantified by using the same method in all PSAs (Swain screening method). However, some of the operator available times to perform actions are different, leading to different quantification of the error probabilities.

The dependencies between post-accident human errors are systematically considered in all PSAs. In FA3 and UK PSA, the total dependencies are considered (the second operator action is not credited if the first action has failed).

Maintenance

The preventive maintenance is considered in all compared PSAs.

The corrective maintenance seems to be explicitly considered only in U.S. EPR PSA.

The contribution of the maintenance to CDF is more important in US PSA (however the details are not available to draw a conclusion).

5.2.4.4 Results

CDF

The CDF is very similar between the four compared PSA LOOP initiating event families (~1E-7 /a).

However the conditional core damage probability is different between OL3 and FA3 on one side (~1E-5) and UK and US on the other side (~1E-6). The differences can be explained

by different PSA assumptions but also by the slightly different designs, as already mentioned in the previous chapters.

Dominant sequences

For the short LOOP initiating event, the dominant accident sequences are in general the failure of all diesels or the failure of secondary cooling followed by the failure of feed and bleed.

In the UK PSA, the RCP seals LOCA sequence is the dominant one (not dominant in the other PSAs). The difference can be explained by a higher failure probability of the PS in UK PSA, leading to increasing the contributions of sequences involving automatic safety injection (triggered by PS).

For the long LOOP initiating event, the dominant accident sequences are in all PSAs the failure of all diesels or seals LOCA sequences.

As a conclusion, the dominant accident sequences are similar, except UK PSA where, as the reliability of I&C is different, the seals LOCA sequences are more important for short LOOP initiating events.

Importance of systems and components

The most important systems/components, for the LOOP initiating events family, are similar in different PSA: main and SBO diesels, SSSS, EFWS. However in some PSAs, due to different design or assumptions, some other systems/components are also highlighted: PS (UK), TXP (SPPA-T2000) (FA3), “2 hours” batteries (US), on-site Gas turbine (OL3), computerized I&C (OL3).

In general, it looks that, even if it is not modelled in the same manner, the aspects related to I&C are important.

Importance of human factor

In general, all PSAs identified the starting and connection of SBO diesels as a dominant human action. Also, the primary Feed & Bleed action in case of secondary cooling unavailability was identified as an important operator action.

The identification of other important operator actions depends on the specificities of each PSA (design, assumptions, ...):

- Manual regulation of EFWS: the modelling of EFWS automatic regulation failure in PSAs highlighted the importance of this manual action (except FA3 PSA where the EFWS automatic regulation failure is not considered).
- Using of the cross connection between electrical trains (UK and OL3 PSA) – but for different purposes (I&C / ventilation).

- Ventilation recovery actions (US and OL3 PSA).
- Opening of EFWS headers valves (UK and OL3 PSA).
- Fast secondary cooldown in case of MHSI unavailability or SBO conditions (UK and FA3 PSA).
- Manual PCD before 2h in order to keep the SSSS integrity (only FA3).
- Providing power from Gas Turbine (only OL3).

In conclusion, the differences in terms of human actions importance are in general driven by other differences in PSA and design. Some of the actions are design specific, such as to provide power from Gas Turbine, specific for OL3 design. Other actions should be similar, but due to modelling simplifications / assumptions they are not identified in all PSAs.

It appears that, in the success branch, generally there is no human action necessary in short term, except in some particular cases as for example the cross-connection of EFWS lines (UK) or the alignment of EFW tanks before 6 hours (US).

5.2.5 Conclusions

5.2.5.1 Main findings:

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

- The initiating events considered: short (2h) and long (24h) LOOP.
- The functional accident sequences: in the four studies the functional sequences are a loss of heat removal (EFWS and feed and bleed 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-7 /a. for the CDF relating to LOOP.
- LOOP initiating event family has a dominant contribution to the total CDF.

However, with a more detailed analysis, differences were identified which could have an impact on results, especially in case of risk informed decision making:

- Differences in success criteria and strategy in degraded situations: for example primary feed and bleed is considered as possible with LPSI only in US PSA, the actuation of SBO diesel generators is possible only after the loss of all main diesel generators for FA3. These differences seem to be due to procedures and to support calculations.
- Differences in the level and detail of modelling: for example modelling of ventilations, of interconnections between electrical divisions, of manual alignment of EFWS headers or other manual actions could lead to significant contributions.
- Differences in modelling and role of batteries, especially the need for 2h batteries for SBO diesels actuation and the CCFs between batteries.
- Significant differences appear in modelling and quantification of I&C: the considered CCFs, the account for diversified means (non-computerized) are not

similar. The differences seem to be due both to modelling and assumptions differences (considered software CCFs and associated quantification) as well as design differences (existence of a non-computerized back-up).

These differences, which illustrate some important PSA uncertainties, have to be taken into account for PSA applications and decision making.

In 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 diesel generators. 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 sufficient diversity). Since the loss of the six diesel generators is a dominant cut-set for all the studies, this assumption is very important.

5.2.5.2 Further work:

Some points could be further investigated: role of ventilations, of batteries, manual actions. These investigations include the supporting calculations. In particular the modelling of I&C appears as an important topic needing more details, and a specific comparison could be carried out in the future.

5.3 Medium Loss of Coolant Accident (MLOCA)

5.3.1 IE definitions and assumptions

Loss of coolant accidents (LOCA) deal with initiating events corresponding to breaks in the reactor primary coolant system where other systems are not capable of maintaining the water inventory. The consequences of a break in the reactor primary coolant system depend on the reactor state. The whole spectrum of LOCAs is analysed for at-power states. In this report we have only considered at-power states.

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. LOCAs are therefore usually modelled in PSA by considering a number of discrete sizes, for example:

- Very small LOCA (VSLOCA)
- Small LOCA (SLOCA)
- Medium LOCA (MLOCA)
- Large LOCA (LLOCA)
- Reactor Pressure Vessel Failure

The break size for a given category of LOCA is usually defined to be consistent with the results of thermal-hydraulic analysis performed to support the PSA. For the MLOCA Figure 1 summarises the range of break sizes assumed in each of the compared PSAs. The

LOCA categories compared in this comparison exercise are highlighted in Figure 1 and are discussed in the following sub-sections.

Max area	FA3	U.S. EPR	UK GDA	OL3
2 cm^2	**VSLOCA** • Steam generators (SG) required for 24 hours mission • 1 train of medium head safety injection (MHSI) with partial cooldown	**SLOCA** • SGs required for 24 hours mission • 1 MHSI with partial cooldown	**SLOCA** • SGs required for 24 hours mission • 1 MHSI with partial cooldown	**SLOCA** • SGs required for 24 hours mission • 1 MHSI with partial cooldown or primary bleed and feed with 2 MHSI in case of failure of partial cooldown
20				
45	**SLOCA** • SGs required for 24 hours mission • 1 MHSI and 1 accumulator with partial cooldown			**MLOCA** • SGs required for 24 hours mission • 1 MHSI with partial cooldown OR primary bleed and feed with 2 MHSI and 1 accumulator and 1 CVCS in case of failure of partial cooldown
100		**MLOCA** • Only initial SG inventory required • 1 MHSI with partial cooldown	**MLOCA** • SGs required for 24 hours mission • 1 MHSI with partial cooldown OR 2 MHSI and 1 accumulator and 1 chemical volume control system (CVCS) in case of failure of partial cooldown	
180	**MLOCA** • Cold leg: SGs not required if 2 MHSI OR 1 MHSI and 3 accumulators • Hot leg: SGs not required if 3 MHSI and 3 accumulators 1 MHSI and 1 accumulator		**MLOCA** • SGs not required • 1 MHSI and 2 accumulators and 1 low head safety injection (LHSI) OR 2 MHSI	**LLOCA** • SGs not required • 1 MHSI and 2 accumulators and 1 LHSI OR 2 MHSI
830		**LLOCA** • SGs not required • 1 MHSI, and 1 accumulator and 1 LHSI OR 2 accumulators and 1 LHSI	**LLOCA** • SGs not required • 1 MHSI and 1 accumulator and 1 LHSI OR 2 accumulators and 1 LHSI OR 1 accumulator and 2 MHSI	
>830	**Negligible**		**2A** • SGs not required • 2 MHSI and 3 accumul- and 2 LHSI	**LLOCA** • SGs not required • 1 MHSI and 2 accumulators and 1 LHSI OR 2 MHSI

Figure 1. LOCA categories for the different EPRs
(Categories included in the comparison marked in yellow)

FA3

In this PSA comparison, we have compared the small LOCA at FA3 with the other PSA models; this LOCA is defined as having a break size in the range 45–125 cm^2. Below 45 cm^2, fast secondary cooldown can be claimed to successfully mitigate the LOCA in case of MHSI failure. This is not the case above 45 cm^2 as the support studies indicate there is insufficient time for operators to undertake fast secondary cooldown. Above 125 cm^2, secondary cooldown is assumed not to be required.

OL3

The MLOCA is considered to have a break size in the range 20 to 100 cm^2. The UK EPR and OL3 PSAs share the same thermal-hydraulic studies so the same principles as for the UK EPR PSA apply here. However, the breakdown of the break sizes is different for the lower end of the range. A less conservative approach has been taken in the OL3 PSA for LOCA with a break size in the range 20-45 cm^2. The grace time to start depressurization (bleed) is shorter for 20-45 cm^2 breaks than for 2-20 cm^2 breaks according to thermal-hydraulic analyses. Thus by modelling together the 2-20 and the 20-45 cm^2 in the UK EPR PSA and using the grace time associated with 20-45 cm^2 in the whole category, it leads to a slight conservatism for the 2-20cm^2 category in the UK PSA results as the probability of failure to depressurize (bleed) increases when the grace time decreases.

UK EPR

Medium LOCAs are assumed to have a break size of between 45 cm^2 and 180 cm^2. This group is divided into two sub-categories:

- Large MLOCA between 100 cm^2 and 180 cm^2. This size of break is sufficient to depressurise the primary side to the medium head safety injection (MHSI) pressure without secondary partial cooldown. Above 180 cm^2 the LOCA leads to a rapid and significant depressurisation of the primary side down to the low head safety injection (LHSI) pressure; this is considered as a large LOCA.
- Small MLOCA between 45 cm^2 and 100 cm^2. The lower end of the range is assumed to be large enough to depressurise the primary side to the MHSI injection pressure without secondary partial cooldown. However, although secondary partial cooldown is not required, it is assumed in the PSA to improve the likelihood of MHSI success.

U.S. EPR

The MLOCA is considered to have a break size in the range 45 to 180 cm^2. So lower bound break size for a medium LOCA is defined as a break large enough that water supply to the steam generators is not required for secondary cooldown (other than the initial steam generator inventory). Above 180 cm^2 is large enough to lead to a rapid and significant depressurisation of the primary side down to the LHSI pressure; steam

generators are assumed not to be required. It is noted that this definition may have changed since the point in time when this comparison exercise was carried out.

5.3.2 Descriptions of plant response to IE and prevention of core damage

During at-power states, the LOCA scenarios typically modelled in the EPR PSAs studied result in a depressurisation of the reactor coolant system, a decrease of pressuriser 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. These safety injection systems provide water to the primary circuit to successfully cool the fuel and prevent core damage. Furthermore, cooldown is initiated (depending on the size of the break) 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.

The EPR has the following safety injection systems:

- Chemical and volume control system (CVCS). Under certain small break LOCA conditions, the CVCS helps maintain the required water inventory in the reactor coolant system.
- Safety injection system. This consists of four trains (one for each loop) and each consists of the following injection systems: accumulators, MHSI and LHSI. MHSI and LHSI take water from the in-containment refuelling water storage tank (IRWST). The water in the IRWST is cooled by either the containment heat removal system (CHRS) or for the LHSI, by the residual heat removal system via the LHSI heat exchanger. Accumulators take water from accumulator tanks. The accumulator safety injection is initiated once pressures fall below approximately 47 bar of the operating primary circuit pressure. The medium head safety injection is initiated at pressures below 97 bar and the low head safety injection is initiated at pressures below 20 bar.

To reduce the reactor pressure quickly enough to allow successful safety injection, secondary cooldown may be required to remove heat from the primary circuit (depending on the break size). The steam generated in the steam generators is released via the steam dump to the condenser or to atmosphere. The following are considered (depending on the break size):

- Partial secondary cooldown – one steam generator fed by the emergency feedwater system (EFWS) and one out of four main steam relief trains (MSRT) or two out of eight main steam safety valves (MSSV).
- Fast secondary cooldown – at least two steam generators fed by the EFWS and two out of four MSRTs. Fast secondary cooldown is manually actuated.

In the case that secondary cooldown fails, bleed may be required in order for the reactor pressure to be reduced low enough to allow timely feed (from the CVCS) of the primary circuit in order to prevent core damage.

The LOCA is assumed to render one train of safety injection unavailable as a result of the fault, therefore three trains are assumed available (fully planed state).

5.3.3 Typical accident sequences and progression

Figure 2 shows generic event trees to illustrate the typical accident sequences and progression following an MLOCA; the trip and shutdown functions are ignored. Two event trees are shown for the small and large MLOCA. Differences in how these are modelled in each of the PSAs is discussed in Section 5.3.4, although the accident scenarios are similar in all the compared PSAs.

Following an MLOCA, 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.

For small MLOCA (break size between 45 and 100 cm^2) the following are typically required:

- one train of partial cooldown, one train of MHSI and one train of IRWST cooling;
- with MHSI unavailable, operator to initiate fast secondary cooldown (two trains), one train of accumulators and one train of LHSI; or
- with partial secondary cooldown unavailable, two trains of MHSI, one accumulator and one train of CVCS and one train of IRWST cooling.

For large MLOCA (break size above 100 cm^2) the following are typically required:

- one train of MHSI, two trains of accumulators and one train of LHSI;
- if accumulators unavailable, two trains of MHSI and one train of IRWST cooling; or
- If LHSI unavailable, two trains of MHSI and one train of IRWST cooling.

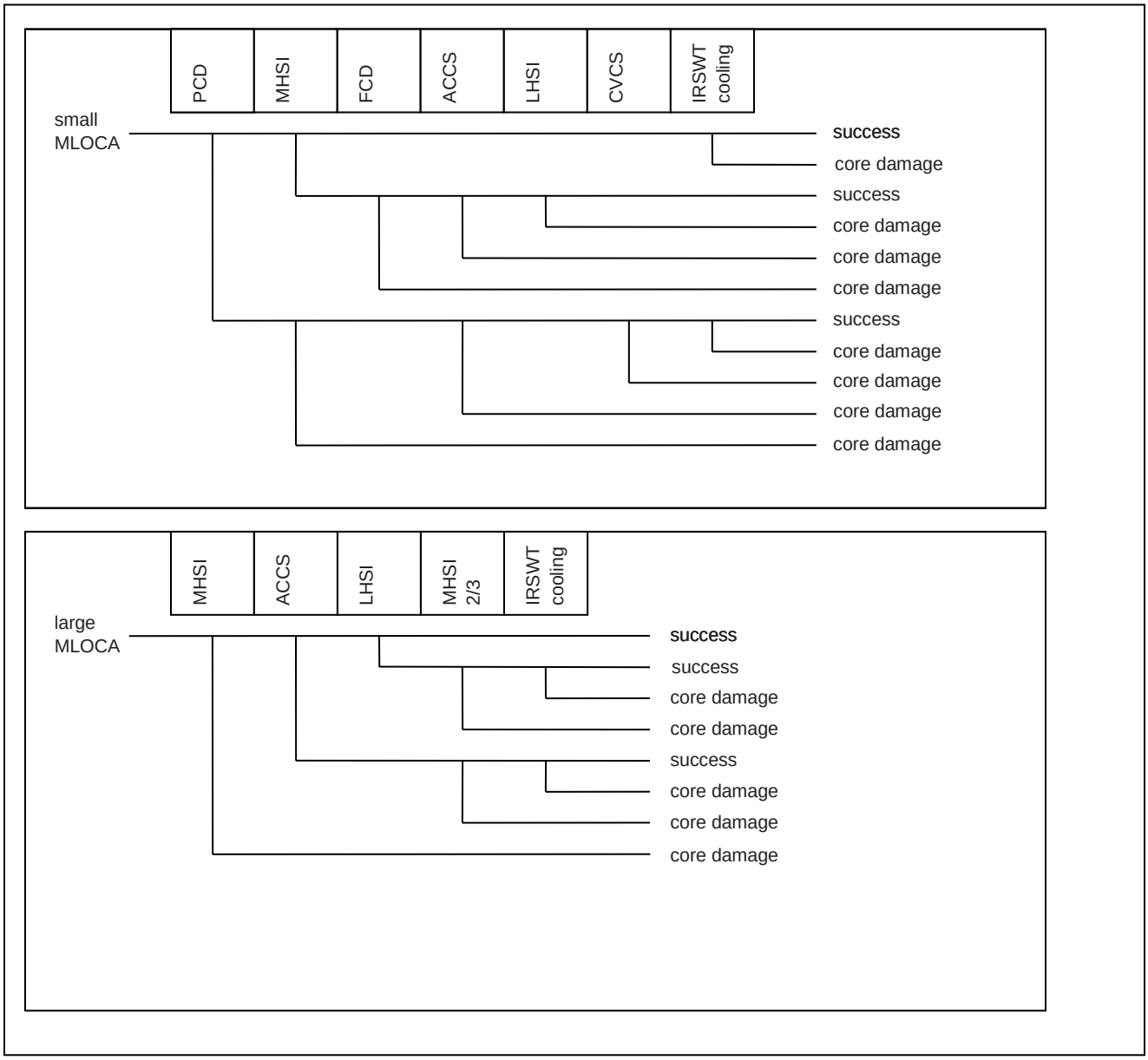

Figure 2. Example of simplified MLOCA event trees

5.3.4 Similarities and differences

Initiating event definition and frequency

The definition of MLOCA, in terms of the range of break sizes, is different between the PSAs, as discussed in Section 5.3.1. 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 vendors, these differences seem to be due to modelling assumptions regarding the break spectrum.

The main differences identified were the assumed MLOCA initiating event 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. Table 8 provides an overview of the initiating event frequencies.

Table 8. Initiating event frequency comparison

	Initiating event frequency/a (break size/cm^2)			
	FA3	**OL3**	**UK EPR**	**U.S. EPR**
Small MLOCA	5.1E-5 (20-45)	1.5E-4 (20-100)	8.0E-6 (45-100)	1.44E-5 (45-180)
Large MLOCA	5.1E-5 (45-120)		8.0E-6 (100-180)	

Success criteria

Since there is a difference in the definition of the initiating event, the scenarios are separated into two cases: small MLOCA (around 45-100 cm^2) and large MLOCA (around 100-180 cm^2). Note that the U.S. EPR PSA model represents both of these LOCA sizes with one event tree, OL3 PSA models only the small size and the UK model represents both (with different event trees). Table 9 and Table 10 provide a summary of the success criteria assumed in each PSA for the small and large medium LOCAs respectively.

Table 9. Small MLOCA success criteria comparison

	Plant Response to IE / Success Criteria /Automatic and manual actions / Timing			
Safety function	**FA3**	**OL3**	**UK EPR**	**U.S. EPR**
Reactor trip (RT)	Included in the event tree, but not analysed this part of the event tree	Present, but not for core damage quantification of this event tree	Included in the event tree, but not analysed this part of the event tree	Not included in the event tree
PCD	1 SG required Via MSB or MSRT, feed from SSS/MFWS/ /EFWS If pressure relief then 1/4 MSRT or 1/8 MSSV	1 SG required Via MSB, feed by MFWS or SSS Via 2/4 MSRT if feed by MFWS, SSS or 1/4 EFWS	1 SG required Via MSRT, feed from SSS/EFWS If only pressure relief 1/4 MSRT or 1/8 MSSV then higher requirements on MHSI (see below)	4/4 MSRT No feed required when all SGs are utilised. *Note: As part of primary bleed function it is required that each SG is*

	Plant Response to IE / Success Criteria /Automatic and manual actions / Timing			
Safety function	**FA3**	**OL3**	**UK EPR**	**U.S. EPR**
				depressurised due to isolated MSIVs
MHSI	1/3 MHSI if PCD successful If PCD fails then 3/3 MHSI (20-45) If PCD fails then 2/3 MHSI (45-125)	1/3 MHSI if PCD successful If PCD fails then 2/3 MHSI (part of MT_PB&F PB-T)	PCD and feed 1/3 MHSI requirement 1 SG without feed, requires 2/3 MHSI	1/4 MHSI
FCD	30 min operator action (20-45) 15 min operator action (45-125) – not accounted for 2/4 EFWS and 2/4 MSRT (2/4 SG)	- SB-LOCA (2-20 cm²): 2400s (incl. diagn. 30 min) - MB-LOCA (20-60 cm²): 1200s (diagn. 10 min) - MB-LOCA (80 cm²): 900s (diagn. 10 min) 2/ 4 MSRT 1/4 EFWS	15 min operator action 2/4 EFWS and 2/4 MSRT (2/4 SG)	30 min operator action 4 / 4 MSRT
Bleed of primary system	Bleed required	Bleed required	No bleed is required (see below)	Bleed required
Feed of primary system	1/3 LHSI 1/3 Accumulator If secondary side RHR fails, then CVCS (2/2) is required until MHSI can be used.	2/3 MHSI 1/2 CVCS 1/3 Accumulator	If PCD incl EFW successful then; 1/3 Accumulator 1/3 LHSI If MSRT successful but no EFW then; 1/3 accumulators 1/2 CVCS IRWST cooling is required 1/2 CHRS or 1/4 LSHI/RHSR	1/4 LHSI 1/4 Accumulator

EFWS (emergency feed water system), FCD (fast secondary cool-down), MFWS (main feed water system), MSB (main steam by-pass), MSRT (main steam relief train), PCD (partial coold-down), SG (steam generator), SSS (start-up and shutdown system)

Table 10. Large MLOCA success criteria comparison

	Plant Response to IE / Success Criteria /Automatic and manual actions / Timing			
Safety function	**FA3**	**OL3**	**UK EPR**	**U.S. EPR**
Reactor trip (RT)	-	-	Included in event tree, but not analysed part of this event tree	Not included in event tree
Partial cooldown (PCD)	-	-	Not required	4 /4 MSRT No feed required *Note: As part of primary bleed function it is required that each SG is depressurised due to isolated MSIVs*
Medium head safety injection (MHSI)	-	-	PCD and feed 1/3 MHSI requirement	1/4 MHSI
Fast cooldown (FCD)	-	-	Not required	30 min operator action 4/4 MSRT
Bleed of primary system	-	-	Not required	Bleed required
Feed of primary system	-	-	1/3 LHSI (including heat removal) OR 2/3 MHSI 1/2 CHRS or 1/4 LHSI/RHR (IRWST cooling)	1/4 LHSI 1/4 Accumulator

Small MLOCA

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 different pressures 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 closed). 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. However, it is noted that, since this comparison was undertaken, the success criteria for the U.S. EPR have been changed. Similarly to the other EPR PSA studies, one steam generator is required; a difference in the U.S. EPR PSA is that no additional feed is required.

Operator action fast secondary cooldown (FCD):

- The FCD is activated by opening the appropriate number of MSRVs (and also feeding the SGs). In the UK EPR PSA, the activation time for FCD is set to 15 minutes. In the U.S. EPR PSA, it is set to 30 minutes.

- In the FA3 PSA, the activation time for FCD is 15 minutes in the case of a 45-125 cm^2 break size, and 30 minutes in the case of a 20-45 cm^2 break size. FCD is not credited for the 45-125 cm^2 case, since it is considered too short a time.

- Discrepancies in grace periods for manual FCD may stem from the differences between the two computing codes (CATHARE and MAAP/RELAP) used for thermal-hydraulic calculations. The differences can also stem from the differences in the break sizes, and the choice of representative scenario.

- It can be noticed that in the UK EPR PSA, there is a sensitivity analysis considering the impact in the UK EPR if the time available for FCD manual actuation is too short. The impact on the results is insignificant.

Bleed function

- In the US, FA3, and OL3 models, there is a requirement on bleed to be able to feed.

- In the UK EPR PSA this is not considered in the event tree. However, on the basis of further information from AREVA it is likely that primary bleed will be necessary between 45 cm^2 and 60 cm^2. This is therefore an optimism in the current UK EPR PSA model, although this is not considered to be significant.

Large MLOCA

The UK and U.S. EPR PSA models cover large MLOCAs. The U.S. model takes into account the possibility to use the secondary side cooling (since it is the same model as the small MLOCA).
If no pressure relief is needed to use LHSI, following successful MHSI and accumulators, then the UK model is more representative.

The FA3 and OL3 models do not cover this size of LOCA in MLOCA analysis (it is included within the large LOCA category).

Data

There are differences in the reliability data and human error probabilities. The impact on the overall medium LOCA results is negligible. However, the impact of these differences on the overall CDF may be more significant, but this was not in the scope of the comparison exercise. The following provide examples of these differences:

- The UK EPR PSA has similar data with the OL3 PSA for the MHSI pump. In US, the unavailability data is about an order of magnitude lower. The FA3 model has pump data and pump motor data separated.
- The operator action failure probabilities in the U.S. EPR PSA are at least an order of magnitude lower than in the UK and OL3 PSAs (the operator action FCD failure probability is also relatively low within the FA3 PSA).
- The check valve data is reasonably similar in the OL3 and U.S. PSAs, but totally different in the UK EPR PSA. This is unknown for the FA3 PSA.
- MSR valve data seems to be significantly higher in U.S. EPR PSA.
- Global (total) common cause failure (CCF) of digital instrumentation and control (I&C) is considered in the OL3 and UK EPR PSAs but not in the US and FA3 PSAs (US and FA3 not evident from cutset list). It should be noticed that in the UK EPR PSA model there are two separate CCFs but no global CCF for all programmable logic.
- Assumptions relating to preventive maintenance are similar.
- Corrective maintenance is not considered in the UK EPR, OL3 and FA3 PSAs. Corrective maintenance is modelled in the U.S. EPR PSA.

Results

Table 11 shows that, notwithstanding the differences in data and initiating event frequencies, the conditional core damage probability is similar in all the PSAs.

Table 11. CDF ad CCDP comparison

	FA3	OL3	UK EPR	U.S. EPR
CDF (Small MLOCA)	2,0E-9 /a (20-45 cm^2)	3,1E-8 /a (20-100 cm^2)	3,2E-9 /a (45 – 100 cm^2)	8,58E-9 /a (45-180 cm^2)
CDF (Large MLOCA)	3,3E-8 (45-120 cm^2)	-	6,0E-9 /a (100-180 cm^2)	-
CDF (Overall MLOCA)	3,6E-8 /a	-	9,2E-9 /a	-
CCDP (Small MLOCA)	3,9E-5 (20-45 cm^2)	2,1E-4	4,0E-4 (45-100 cm^2)	6,0E-4
CCDP (Large MLOCA)	6,5E-4 (45-120 cm^2)	-	7,5E-4 (100-180 cm^2)	-

The dominating minimal cutsets for the MLOCA are described for each PSA models.

Dominating MLOCA minimal cutsets for the UK EPR PSA (45-100 cm^2 and 100-180 cm^2 break sizes) includes failure of the MHSI pumps through combinations of CCF of the pumps, random failure of the pumps and preventative maintenance of a pump. Also included in some cutsets with the MHSI failure is no operator initiation of FCD (MLOCA <100 cm^2). It is noted that in the cutset list both 4 fold and 3 fold CCFs are present. In the case of "CCF of all of the available MHSI", only three trains are considered and therefore both have the same effect. The results are totally dominated by MCSs affecting the MHSI pumps (failure to run of pump, failure to run pump motor). It can be noted that the failure modes for the MHSI pumps are separated in failure to run pump, failure to run pump motor, failure to start pump and failure to start pump motor.

Dominating MLOCA minimal cutsets for the FA3 PSA (20-125 cm^2 break sizes) are similar to those for the UK EPR PSA. The only additional dominating cutset, which differs from the UK PSA, is that one failure of I&C logic is represented: error in logic, loss of condenser and no manual feed and bleed action.

Dominating MLOCA minimal cutsets for the U.S. EPR PSA (45-180 cm^2 break size):

- Failure of one of the 4 MSRs together with operator failure to initiate feed and bleed represents 75% of the top frequency (different causes for unavailability of the MSRs).
- CCF for 4 LHSI/MHSI common check valves will not allow use of LHSI and MHSI and thereby cause core damage.
- Failure of corrective maintenance of SAC0x together with operator failure to recover room cooling
- Failure of SAC0x together with operator failure to recover room cooling

It can be noticed that some of the failures in the cutset list are due to failure of the I&C. Also room cooling is a failure mode of importance, and the possibility to locally recover room cooling. Note: In the UK PSA, room cooling is currently not modelled.

Dominating MLOCA minimal cutsets for the OL3 PSA (20-90 cm^2 break size):

- CCF of all of the available MHSI pumps (including in combination of random failures or preventative maintenance of the pumps) and no operator initiation of FCD
- CCF of TXS hardware (I&C)
- CCF of three check valves (safety injection system isolation valves) and no operator initiation of FCD
- CCF of MSRVs and failure of by-pass condenser and failure of operator to initiate bleed
- CCF of level indication, failure of by-pass condenser, operator fails to initiate PCD and operator fails to initiate primary bleed

It can be noticed that in the cutset list, different types of logic failures are represented together with the obvious failures of the MHSI.

Table 12 compares the significant basic event importances (Fussell-Vesely, FV). The importance for basic events between the different models is significantly different, since the top minimal cutsets are significantly different.

Table 12. Comparison of significant basic event importances (FV greater than 10%)

FA3	OL3	UK EPR	U.S. EPR
• CCF of MHSI pumps (68%) • MHSI pump (~20%, 3*7%)	• Operator fails to initiate FCD (68%) • CCF of MHSI pumps (44%) • Failure by-pass condenser (17%) • Operator fails to initiate PCD (16%) • Operator fails to initiate bleed (14%) • CCF of TXS (~10%)	• Operator fails to initiate FCD (32%) • CCF of MHSI pumps (~80%) several events • Preventive maintenance on cooling chain (RIS/RRI/SEC) (17%)	• Operator fails to initiate feed and bleed (82%) • MSRIVs (~4*10%)

Key insights from the results include:

- CCDP is equivalent across all the PSAs
- There are some differences in the dominant cutsets due to component data assumptions.
- Control and instrumentation differences – there seems to be important differences in the treatment of digital I&C amongst the different models, for example as reflected in the OL3 cutsets. Some of these differences may be due to modelling assumptions, the detailed design information available during the development of the PSA and potential design differences.
- There are significant differences between component importances due to differences in the cutsets.

Summary of differences

In terms of the initiating event definition, differences in this definition may be attributed to different PSA modelling styles or that the studies are in different phases. A conservative approach can be acceptable in a situation where the total impact of such a simplification is negligible. The reason for differences in initiating event definition may be the supporting studies, but they are the same in the UK EPR and OL3, and still, the definitions are not the same; however, this difference can be explained – see Section 5.3.1.

Regarding the data used for the initiating event, there is a significant difference between the OL3/FA3 PSAs and the UK/U.S. EPR PSAs. It is not clear which data are the most representative. However, the differences in design should not affect the initiating event

data (the basis used to estimate the pipe rupture frequencies are not detailed enough to differentiate between minor design differences).

In terms of data for some components, some of these are very different. Data should be discussed for the most important components. However, this should probably be performed on the plant level instead of initiator-by-initiator (otherwise it requires too large an effort). This should preferably be based on the FV estimate for the most important components (say 20) for each plant.

The human error probabilities (HEP) are quite different. In the same way as for data, the HEP should probably be studied from a plant level (total CDF, looking at the most important HEPs).

There seems to be big differences in the treatment of digital I&C amongst the different models. However, the requirements on treatment of digital I&C can be different in different regimes, and therefore, may be relevant as it is. There may also be design differences.

There are differences in the requirements (success criteria) between the studies.

The difference in the total results is, despite the differences identified, not so significant. The CCDP is actually about the same. The differences in the results are due to the initiating event frequency.

5.3.5 Rationale for differences

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

5.3.6 Areas and topics that require further 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 modelling 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 modelling and design.

There will always be differences in the PSA models. However, in a new type of reactor, using mainly the same type of components, using the same basic principles – the data that

are representing the same things should relate relatively closely to each other. From this perspective, the following should be discussed:

- Initiating event frequencies for pipe ruptures – there does not appear to be a good reason that they should not be consistent or the same.
- The main component data should be consistent. There may of course be local deviations because of ensuring consistency with the data from other local plants
- The operator action HEPs. These are very dependent on the assumptions, available instructions etc., but they should be comparable – and the differences should not be due to different experts believing his/hers methods are better than the others.

5.4 Loss of Cooling Chain (LOCC)

5.4.1 Description of Cooling Chain

The following brief description (Chapters 5.4.1.1 and 5.4.1.2) of the cooling chain and its systems is based on OL3 NPP, but the main functions and design details are fairly similar amongst the various EPR designs. The main design difference is the interconnection between common headers (see Figure 3), which is part of UK EPR, U.S. EPR and FA3 design, but not in OL3. This interconnection improves the reliability of RCP thermal barrier cooling and thus plant operability. However, the risk impact of this design difference is negligible.

The Component Cooling Waters System (CCWS) supplies a number of systems and components in the nuclear island with cooling water (see Figure 3). They are themselves cooled by the Essential Service Water System (ESWS). The CCWS encompasses two parts: the safety related part and the process related part.

The safety related part is composed of four safety classified trains each with isolatable connections to CCWS common headers. These trains have the function to transfer the heat load from the safety users as well as from to the CCWS common headers to the heat sink. Further, there are two separate trains of the so-called Dedicated Component Cooling Water System which have the function to transfer the heat load from the Containment Heat Removal System to the heat sink.

The process related part has the function to cool the common users located inside the Fuel Building, Reactor Building, Waste Building and the Nuclear Auxiliary Building.

5.4.1.1 Component Cooling Water System (CCWS, KAA/KAB, RRI)

Safety classified trains 1-4

The Component Cooling Water System (Figure 3) consists of four separated safety classified trains corresponding to the four layout divisions and the four electrical divisions (1, 2, 3 and 4).

Each separated CCWS safety classified train includes:

- A pumping facility fitted with a re-circulation line and a cooling line for the motor of the CCWS pump,
- One heat exchanger which is cooled by the ESWS and fitted downstream with an additional differential pressure control valve, and its bypass line which is fitted with a control valve in order to guide the CCW temperature during the cold seasons,
- One surge tank, concrete structure with steel liner which is connected to the pump suction line and which is located above the highest component cooling water load except the operational chillers which are installed on higher levels. The surge tank is connected to a demineralized water make up to compensate for CCWS normal leaks or component draining water,
- One sampling line, which is connected permanently to a radiation monitor,
- One chemical additive supply line,
- A set of isolation valves which separate the train from the common load set.

Each separated CCWS safety classified train has connection pipes in order to cool the CCWS pumps, the MHSI pump motors, the sealing and motor of LHSI pumps (as a backup for Loss of Ultimate Heat Sink and Total Loss of Cooling Chain the LHSI pump motor of Train 1 and 4 is also cooled by the safety chilled water system), the safeguard building controlled Area Ventilation System and electrical building Main Ventilation System cooling units, and also to cool the SIS/RHR heat exchanger, which belongs to the same division.

The safety functions of the CCWS are the following:

- Residual Heat Removal
  - During normal operation, in case of DBC events, and in complex sequences, the CCWS shall ensure the heat transfer from the Safety Injection Systems to the Essential Service Water System
  - As long as any fuel assembly is in the fuel building spent fuel pool, the CCWS shall ensure the transfer of the decay heat from the FPCS to the ESWS during all operation conditions
  - The CCWS shall ensure the cooling of the thermal barrier of the RCP seals.
  - The CCWS shall transfer heat from the safety chillers of divisions 2 and 3 to the Essential Service Water System
  - During specific complex sequences and design extension conditions, the Dedicated CCWS shall ensure heat removal from the Containment Heat Removal System to the heat sink

- Confinement of radioactive substances
  - The CCWS generally contributes to this function by providing a barrier between various auxiliary systems (potentially carrying activity) and the environmental heat sink and especially in the frame of the containment isolation function

Common headers & loops KAB

The common loads of the CCWS consist of two separate sets of common cooling loads which are referred to common 1 and 2 which are designed to cool the operational component cooling water loads.

Common header 1 is supplied with component cooling water either by train 1 or by train 2 while Common header 2 is supplied with component cooling water either by train 3 or by train 4.

Two separate component cooling water loops, one assigned to common 1, and the other to common 2, are called common 1a and common 2a. Loop 1a is provided to cool the first FPCS train and loop 2a is provided to cool the second FPCS train. They are separated from the other operational loads component cooling water supplies to maintain FPCS cooling capacity during component cooling water common loop maintenance which is performed during plant outage.

The two other component cooling water loops, one assigned to common 1 and the other to common 2 called common 1b and common 2b respectively, are provided to cool the other component cooling water loads.

Each of these four common loops is separated from the associated train by 2 fast closing isolation valves installed in that train (one in the supply, the other in the return line).

The common 1b header is provided to cool mainly the reactor building component cooling water loads via two separate branches. One is dedicated to the component cooling water safety and operational loads, RCP 1/2, thermal barriers of RCP 1/2 and CVCS high pressure cooler 1 (30KAB60). The other one is dedicated to the operational component cooling water loads, HVAC coolers 1/2/3/4 and reactor coolant drain cooler.

The common header 1.b is also designed to cool the reactor boron and water make-up system RBWMS, safety and operational loads in the fuel building, CVCS charging pump 1 motor and oil cooler and nuclear sampling system and in the nuclear auxiliary building, first chiller of both operational chilled water systems and RBWMS.

The common 2b header is provided to cool RBWMS and mainly the operational loads in the nuclear auxiliary building and in the waste building, second chiller of both operational chilled water systems, liquid, waste and coolant treatment users, boron recycle system users.

The common 2b header is also designed to cool component cooling water safety and operational loads in the reactor building, RCP 3/4, thermal barriers of RCP 3/4 and CVCS high pressure cooler 2 and in the fuel building, RBWMS, charging pump 2 motor and oil cooler and nuclear sampling system.

The nuclear auxiliary building non-safety classified component cooling water loads of the two common sets of users can be isolated by fast closing valves in case of an internal or external hazard in the nuclear auxiliary building and/or waste building.

The non-safety classified component cooling water loads located in the reactor building can also be separated from the other safety classified component cooling water loads by isolation valves in case of an internal hazard.

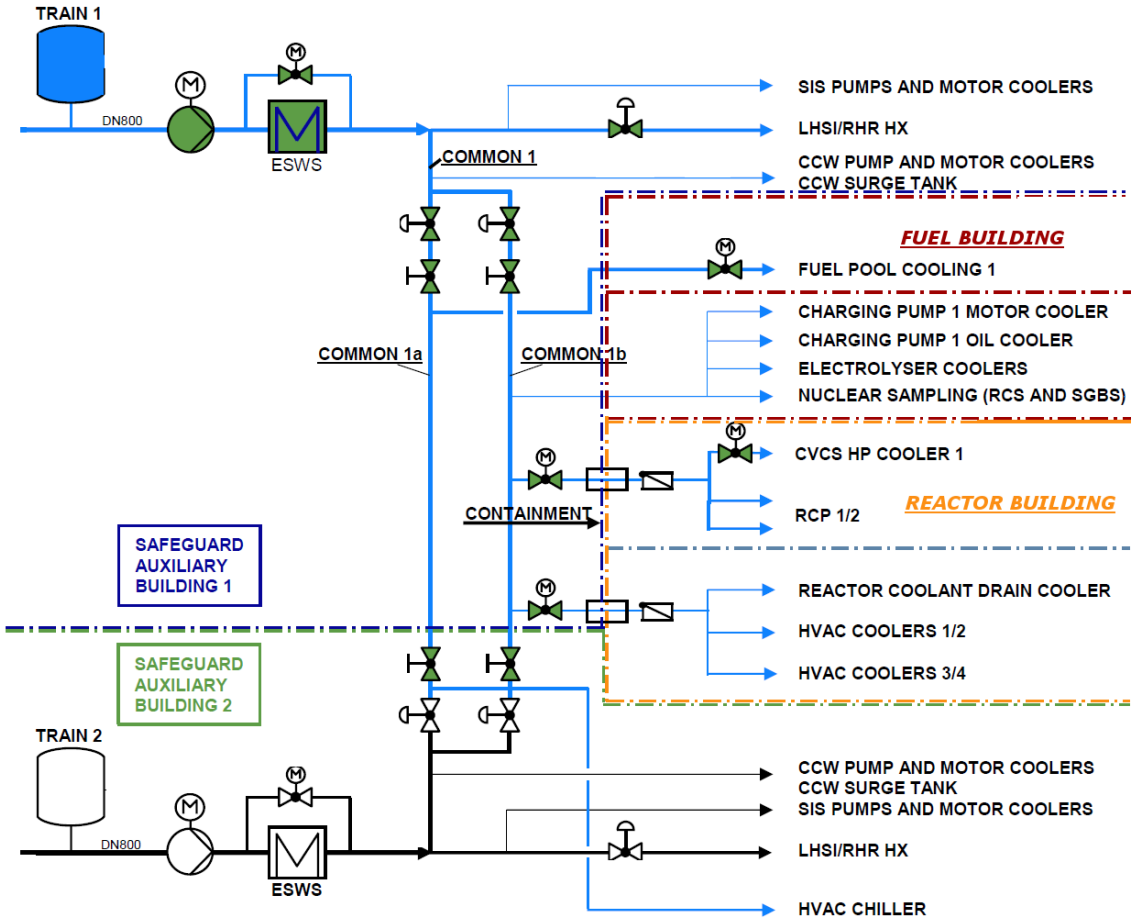

Figure 3. CCWS (KAA) Simplified Diagram [12]

5.4.1.2 Essential Service Water System (ESWS, PE, SEC)

The function of the Essential Service Water System (ESWS) during normal operation is

- to provide the cooling of the Component Cooling Water System (CCWS) heat exchangers with water from the heat sink during all normal plant operating conditions.

The Essential Service Water System, like the main cooling water system, takes suction from the sea.

The Essential Service Water System consists of four separated safety classified trains and of two trains of the dedicated cooling chain (30PEB50/80). The design of ESWS is similar in all EPR designs, except for the interconnection between common user headers (see Table 13).

The safety functions of the Essential Service Water System (ESWS - PEB) are the following:

- Provide capability to transfer the heat (decay heat mainly) from the Component Cooling Water System (CCWS - KAA) following any postulated Design Basis Condition 2 to 4 and DEC events.
- Ensure continued heat transfer from the Fuel Pool Cooling System (FPCS - FAK) via the CCWS as long as any fuel assemblies are in the spent fuel storage pools located outside containment.
- Ensure heat transfer by dedicated ESWS trains 30PEB50/80 via dedicated CCWS trains 30KAA50/80. During complex sequences and severe accidents the pumps 30PEB50/80 AP001 shall ensure the evacuation of the heat from the dedicated cooling chain. Heat removal from containment shall ensure containment integrity.

Table 13. CCWS and ESWS design in EPRs [13]

	FA3	UK	OL3	US
	FSAR 2010	GDA step4 (2011)	pre-OLA (v104)	DC
Current Design				
Design of CCWS	4 independent trains for the safety consumers			
	2 common headers for the operational users			
	2 common headers + interconnection for the RCP-TB		2 common headers for the RCP-TB	2 common headers + interconnection for the RCP-TB
Design of ESWS	4 independent trains			

5.4.2 IE definitions and assumptions

The loss of cooling chain initiating events at power states include several failure modes of CCWS and of ESWS. These failure modes may include e.g.:

- Leaks in CCWS/ESWS train(s)
- Leaks CCWS common header(s)
- Mechanical failures in one or several CCWS/ESWS trains
- Failure of the automatic switchover of the common user header feed to the backup train

Taking into account the failure modes presented above and their possible combinations, potential IEs could are grouped as follows (see Table 14).

- Loss of 1 common user header out of 2
- Loss of the 2 common user headers

Table 14. LOCC IE modelling at power states [13]

	FA3	UK	OL3	US
	FSAR 2010	GDA step4 (2011)	pre-OLA (v104)	DC
AT-POWER: 2 CCWS/ESWS trains in operation				
IE Modelling				
Frequency calc.	Calculated IE frequency			FT modelling
Integr. in PSA	Point estimate / Mean, Lognormal			FT modelling
Loss of one train	YES	NO		
Loss of at least one common header	YES			
CCF	Between trains in operation and between trains in stand-by		All trains operating and stand-by (post accident)	Between trains in operation and between trains in stand-by
Dependencies IE / mitigation				
Dependencies	CCWS/ESWS trains considered unavailable (house events)	Use of specific FTs in the mitigation + I&C modelled in IE	CCWS/ESWS trains considered unavailable (attribute)	Same FT for IE and mitigation

Loss of cooling chain initiating event frequencies and sources for reliability data are presented in Table 15.

Table 15. LOCC IE frequencies

	FA3	UK	OL3*	US**
	FSAR 2010	GDA step4 (2011)	pre-OLA (v104)	DC
IE Frequency at Power (1/a)				
Loss of one train	4.7E-1	***	-	2,7E-3
Loss of one common header	5,8E-3 [2]	***	3,5E-3 [3]	2,0E-1 [1]
Loss of all trains	1,8E-7	***	-	3,6E-8
Reliability database				
Reliability Database	EDF 2009		ZEDB 2007	NUREG

* *Seven IE groups were modelled 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 at the time of comparison*

1 *Spurious openings of safety valves contribute to 93% and leaks contribute to 5%*

2 *Spurious opening of safety valves and leaks contribute each to about 50% (EDF operating experience)*

3 *Includes mechanical failure of one train and failure of switchover to the standby train*

5.4.3 Typical accident sequences and progression

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

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

Loss of one common header leads to 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, which leads to automatic reactor trip and turbine trip,
- two LHSI/RHR trains (but only one LHSI pump due to the diversified cooling of LHSI motors 1 and 4),
- two MHSI trains,
- two EFWS trains.

Loss of Both Common User Headers leads to loss of

- cooling for all RCP (thermal barrier and motor, motor bearing, pump thrust bearing) which leads to an automatic trip of the RCP, which leads to automatic reactor trip and turbine trip,
- all charging pumps (2/2),
- the RCP seal cooling and the thermal barrier of the 4 RCPs,
- four LHSI/RHR trains (but only two LHSI pumps due to the diversified cooling of the LHSI motors 1 and 4),
- four MHSI trains,
- two EFWS trains.

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 main steam by-pass 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.

<u>Automatic actions</u>

- Trip of the 4 RCPs,
- Reactor trip and turbine trip,

- Shutdown of the operating charging pump (CVCS) and automatic startup of the other charging pump,
- Closing of the MFW full load lines.

Manual control of the plant

The following manual actions may influence the accident sequence following the event.

- *Initiating component cooling water train switchover by safety automation system:*

  In case of a failure of the automatic switchover to the CCWS train in standby (failure of Check back signal) the operator performs the switchover manually.

- *Initiating the Partial Secondary Cooldown:*

  Cooling of RCP sealing water and the RCP thermal barrier cooling are not available for two RCPs. The stand still sealing system is qualified for temperatures up to 270°C only. Thus a manual partial secondary cooldown to 60 bar is necessary at 4/4 steam generator to avoid a LOCA via the RCP pump seals.

  In case of RCP seal LOCA, if the automatic actuation of the partial secondary cooldown to Medium head Safety Injection fails, the operator performs it manually.

- *Starting the demineralized water system for Main Feed water:*

  The emergency demineralized water system is started automatically from feed water tank level low signal (process automation system function). If the automatic start fails, the operator starts the demineralized water system supply to the feed water tank manually.

- *Opening of the emergency feed water suction and discharge header:*

  If one or more EFW pumps are not running, the shift team will advise a field operator to open the emergency feed water suction and discharge header. Opening of the suction header is necessary to ensure demineralized water supply for 24h if one EFWS pump is unavailable and the reactor shutdown to cold RHR conditions fails.

- *Refilling EFWS tanks with the demineralized water system*

  In case of a partial failure of emergency feed water system and failure to open the suction header valves, the operator provides refilling of EFWS tanks by the demineralized water system.

- *Need for HVAC cooling recovery in safeguard building electrical and I&C rooms:*

  If frontline system functions are affected by a failure of HVAC cooling in the safeguard building electrical and I&C rooms (e.g. by a Common Cause Failure of safety chillers), the operator will recover the cooling of electrical and I&C equipment.

- *Initiatiing the Fast Secondary Cooldown:*

  In case of a LOCA via the RCP seals and a failure of the Medium Head Safety Injection system the operator performs a fast secondary cooldown to enable injection to the reactor cooling system by the accumulators and low head safety injection system.

- *Initiating the Primary Bleed and Feed:*

  Manual initiation of Primary Feed and Bleed is performed if secondary RHR via the SG is not available, e.g. by a failure of the start-up and shutdown system pump and the EFWS pumps.

- *Initiating the containment heat removal system after primary bleed and feed:*

  If no low head safety injection pump is available for in-containment refuelling water tank (IRWST), the containment heat removal pumps will be actuated in the longer term to ensure a sufficient IRWST temperature.

Table 16 illustrates the summary of safety functions and their success criteria in various failure combinations of loss of cooling chain.

Table 16. LOCC Success Criteria in Power States [14]

Safety function required	Systems used and success criteria related									
	Loss of one common user header							Loss of two common user headers or LUHS		
	Affected RCPs tripped				RCPs not tripped			RCPs tripped		RCPs not tripped
	MSIVs open		MSIVs closed					MSIVs open	MSIVs closed	
Secondary side heat removal:	1/8 MSSV 2/2 EFWS	1/8 MSSV	4/8 MSSV 2/2 EFWS	4/8 MSSV			1/8 MSSV	1/8 MSSV 1/2 EFWS	4/8 MSSV 2/2 EFWS	1/8 MSSV
Primary side heat removal:		1/3 PSV		1/3 PSV						
Partial cooldown:					1/4 MSRT 2/2 EFWS	1/4 MSRT 2/2 EFWS				
Secondary Fast Cooldown: Grace period:						2/4 MSRT 2/2 EFWS 4200s after SI signal				2/4 MSRT 2/2 EFWS 2100s after SI signal
Primary bleed: Criterion:		1/2 PDS[1] RPV level drop to 1.748 m		1/2 PDS[1] RPV level drop to 1.748 m			1/2 PDS[1] 2400s after SI signal			
Safety injection:		2/2 MHSI or 1/2 MHSI 4/4 ACCU		2/2 MHSI or 1/2 MHSI 4/4 ACCU	1/2 MHSI	1/3 LHSI	2/2 MHSI			1/2 LHSI[2]

[1]: 3 PSVs (3*290 t/h) are used in the calculation to bound one PDS (900 t/h) for primary bleed.
[2]: only the divisions 1 and 4 are available for safety injection.

5.4.4 Main Findings and Conclusions

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 and the U.S. EPR, up to seven IE groups 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 use of operating experience (pipe breaks and leaks).

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

According to EPR vendors the modelling of LOCC initiating events started with up to 7 initiators with OL3 PSA model and while the detailed design and PSA modelling evolved, a more realistic modelling led to fewer initiating event groups. Similar evolution may be expected for other EPR PSA models.

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 valves
  - U.S. EPR: CCW common header valves need two divisions (trains) to open/close these valves (division 1 and 2 “OR” divisions 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 according to vendor’s assessment.

Insufficient information was available for a more detailed comparison of LOCC events in EPR PSAs. There are also significant differences in the initiating event grouping and level of modelling maturity in various PSAs. Thus, the detailed comparison of the most important accident sequences, minimal cut sets or basic events was not considered meaningful at this stage.

<u>Areas and topics that require additional information</u>

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 modelling issue is the RCP seal LOCA. Based on the comparison, there are clear differences in the modelling. 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.

5.5 Steam generator Tube Rupture (SGTR)

Following description of steam generator tube rupture modelling in EPR PSAs provides only a general level comparison and summary of typical accident progression. More detailed comparison was unfortunately not possible at this stage.

5.5.1 IE definitions and assumptions

FA 3

The considered initiating event is a Steam Generator Tube Rupture: one tube rupture, two tubes ruptured, multiple ruptures, small leak, and induced rupture (following secondary break), when the reactor is initially at full power operation (state A) and in shut down with secondary-side heat removal (state B).

The following initiating events are considered in the group:

- Steam generator tube small tube rupture in state A and B: SGTRS
- Steam generator tube rupture (1 tube) in state A and B: SGTR1
- Steam generator tube rupture (2 tubes) in state A and B: SGTR2
- Steam generator multiple tube rupture (10 tubes) in state A and B: SGTRM

Induced SGTR

- Steam secondary break (MSRT) opening + SGTR in state A and B: SBST1
- Steam secondary break downstream MSIV + SGTR in state A and B: SBST2
- Steam secondary break upstream MSIV + SGTR in state A and B: SBSTS

OL 3

Two different break events regarding steam generator tubes are analysed (similar to UK EPR):

- Steam Generator Tube Rupture (up to 1 tube): SGTR1_AB
- Steam Generator Tube Rupture (2 tubes): SGTR2_AB

The analyses for the plant states A and B are performed in the same event trees. Differences between state A and B are considered at the fault tree level.

UK EPR

The initiating events considered are Steam Generator Tube Ruptures: one tube rupture and two tubes ruptured, when the reactor is initially at full power operation (state A) and in shut down with secondary-side heat removal (state B).

The following initiating events are considered in the group:

- Steam generator tube rupture (1 tube) in state A and B: SGTR1_AB
- Steam generator tube rupture (2 tubes) in state A and B: SGTR2_AB

Induced steam generator tube rupture is handled as a separate initiator.

U.S. EPR

The mean initiating event frequency for SGTR was estimated as 3.54E-03 /a based on NUREG/CR-6928. Although the U.S. EPR SGs have significantly more SG tubes than the average plant, it is judged that any impact on the SGTR initiating event frequency is offset by material improvements in the U.S. EPR SGs.

Steam Generator Tube Rupture up to 1 tube is analysed.

Steam line break Induced SGTR is analysed as a separate initiator and includes multiple tubes ruptured.

5.5.2 Plant response and automatic signals

FA3

Steam Generator Tube Rupture (SGTR) causes a loss of coolant inventory from the primary to the secondary side of the affected SG. The leak leads to a primary pressure decrease and a level increase in the affected SG.

The leak rate for one tube rupture is around 30 kg/s (initial value for 155 bar), assumed to be covered by the flow rate of 2 CVCS pumps. Consequently the safeguard systems are not automatically initiated.

For a small leak the leak rate is lower, then compensable by CVCS without safeguards systems. The rate is assumed around 20 kg/s, the initial value for the full power state, which stand for a 2 cm^2 break. The small leak is modelled like a particular one tube rupture.

If 2 or more SG tubes are affected, the safeguard systems are automatically initiated. The multiple SGTR is modelled like a 10 tubes rupture on the same SG.

In different states, the main differences are due to different time windows for operator actions. These time windows are defined in support studies or as a result of conservative assumption.

The objective, after reactor trip, is to stop the leak by equalizing the primary and secondary pressures. The principal requirement is the isolation of the affected SG to limit the release outside the containment. This requires actions to limit the filling of the affected SG, and in particular, to avoid the steam relief valves opening under water. The setpoint of the Main

Steam Relief Valves (VDA [MSRV]) is automatically raised to limit the possibility of their actuation.

The transient is terminated when the affected SG is isolated and the main primary parameters are controlled.

For the case of one tube rupture, the Chemical and Volume Control System (RCV [CVCS]) is able to compensate the loss of reactor coolant inventory. Reactor Trip (RT) will occur when a “SG level > MAX1" signal is generated. Partial cooldown is then automatically initiated following a “SG level > MAX2” signal. At the end of the partial cooldown and with a “SG level > MAX2” signal, the affected SG is isolated (MSIV closed), and the (RCV [CVCS]) charging line is closed. If this automatic action is not performed the operator needs to do it in a time window which depend on the number of pumps in service (CVCS and MHSI) and on the success or not of the partial cooldown. Reactor trip can also be actuated on a “pressuriser (PZR) pressure < MIN2” if the primary leak is not compensated. If the volume control system is in service, the Safety Injection System (RIS [SIS]) will not be actuated.

For the case of rupture of two tubes, the Safety Injection System (RIS [SIS]) is required to compensate the loss of reactor coolant inventory. Reactor trip will be actuated following either a “PZR pressure < MIN2" or "SG level> MAX1” signal. The Safety Injection System (RIS [SIS]) will be actuated following a "PZR pressure < MIN3” signal (power states). Partial cooldown will be initiated following a Safety Injection (SI) signal or “SG level > MAX2" signal. At the end of the partial cooldown the affected SG is isolated and the Chemical and Volume Control System (RCV [CVCS]) is shutdown.

For sequences in which isolation fails, but a safe state is reached before the In containment Refueling Water Storage Tank (IRWST) empties, core damage can be prevented.

In the event of an induced SGTR following a secondary steam break (SSB), the support studies for SGTR 2 tubes and SSB are both used.

OL3

An idealized accident sequence following a 2A-rupture of 1 steam generator tube without any equipment failures is presented below for OL3 (in other designs, a reactor trip is not actuated on main steam activity).

The activity in the main steam line increases due to the leak flow rate and a set of specific SGTR related countermeasures is actuated:

- Reactor trip is initiated approx. 15s after the rupture on main steam activity > Max1 (PS).

- Turbine trip and the closure of all feed water full load lines are initiated on reactor trip check-back (protection system and hardwired backup system).
- Actuation of normal and auxiliary pressurizer sprays to decrease the reactor coolant system pressure and the leak flow. In the case the CVCS is in operation, the pressure is kept above the second low pressurizer pressure threshold and the safety injection signal is not reached.
- The reactor control, surveillance and limitation (RCSL) system will compensate the pressurizer level decrease by partial closure of the letdown line and activation of the second CVCS charging pump (after the tube rupture the pressurizer level decreases due to the leak flow from the reactor coolant system to the secondary side: initial flow rate approx. 30 kg/s).
- SGs pressure is controlled at the hot shutdown pressure level by the MSB (90 bar, RCSL, TGI). In case of the MSB is not available, the SGs pressure increases until it reaches the nominal MSRTs pressure set point, inducing the MSRT response signal. Upon the actuation of both high activity in one main steam line and MSRT response signals, a PCD involving the four steam generators is triggered (PS).
- At the end of the automatic partial secondary cooldown, the affected steam generator is isolated (by protection system): the main steam isolation valve is closed, the main steam relief control valve set point and the main steam relief isolation valve opening threshold are increased to 99.5 bar. A lower pressure reached at the end of partial secondary cooldown is set for the unaffected steam generators.
- The pressuriser level set point and the steam generators level set point are decreased.

In case of the RCSL measures given above are effective, the leak flow rate is reduced below 5 kg/s due to the decreased pressure difference between primary and secondary side. Thus the pressurizer target level can be maintained by reactor coolant system feed with one CVCS charging pump. The isolated steam generator can be considered as part of the reactor coolant system afterwards: The leak flow towards the secondary side is stopped as soon as the pressure in the reactor coolant system and the affected steam generator is equalized and a controlled state is reached.

The RCSL will control the steam generator level via the feed water low load control valves and the steam generator feed water supply is performed by the main feed water pumps or the emergency feed water system.

In case of steam generators pressure control by main steam by-pass was available, isolation of the affected steam generator may be performed by the following manual actions:

- The main steam relief train setpoint pressure is increased to 99.5 bar.
- The main steam isolation valve is closed.
- The feed water low load line as well as the EFWS train is isolated.
- The steam generator blowdown line is isolated.

The safe shutdown state is reached once residual heat removal systems is in operation. The following is needed:

- Confirmation of complete isolation of the affected steam generator
- Reactor coolant borating (either automatically by CVCS or operator actuates extra borating system)
- Reactor coolant cool down by main steam by-pass or main steam relief trains of the unaffected steam generators
- Reactor coolant depressurization by means of normal/auxiliary pressurizer sprays or main steam relief train of the affected steam generator only

The following deviations from the idealized sequence may occur:

- In case of the RCSL measures to compensate the leak flow fail (e.g. due to a failure of the CVCS stand-by pump) the primary pressure will decrease during the partial secondary cooldown. Then the controlled state is reached by means of affected steam generator isolation at the end of partial secondary cooldown.
- In case of affected steam generator isolation fails, operator initiates primary depressurization via secondary cooldown or primary feed and bleed.
- In plant state B (hot shutdown) the Max1 threshold of the main steam activity is not reached necessarily. The level in the affected steam generator will increase due to the leak flow until a reactor trip is initiated on SG level >Max1 (PS). An automatic partial secondary cool down via the affected main steam relief train is initiated afterwards. The adjustment of the main steam relief train set point pressure as well as the closure of the main steam isolation valve need to be performed manually in this case (due to main steam activity threshold not reached).

In case of a rupture of 2 tubes (initiating event SGTR2_AB), the plant response is comparable to the case without RCSL mitigation measures as described above. The safety injection signals are initiated on pressuriser pressure < Min3 activating both the MHSI and the LHSI pumps (PS). A partial secondary cooldown via the main steam by-pass is initiated from a decoupled protection system signal (RCSL, TGI). The reactor coolant system is refilled with the medium head safety injection as soon as the partial secondary cool down is finished. The adjustment of the MSRT set point pressure as well as the closure of the MSIV is performed automatically only if the MSB is not available for the partial cool down.

<u>UK EPR</u>

Steam Generator Tube Rupture (SGTR) causes a loss of coolant inventory from the primary to the secondary side of the affected SG. The leak rate for one tube rupture is around 20 kg/s, the initial value for the full power state, and leads to a primary pressure decrease and a level increase in the affected SG.

The mitigation objective, after reactor trip, is to stop the leak by equalising the primary and secondary pressures. The principal requirement is the isolation of the affected SG to limit the release outside the containment. This requires actions to limit the filling of the affected

steam generator and, in particular, to avoid the steam valves opening under water relief. The setpoint of the Main Steam Relief Valves (VDA [MSRV]) is automatically modified to limit the possibility of their actuation.

The transient is terminated when the affected steam generator is isolated and the main primary parameters are controlled.

For the case of one tube rupture, the Chemical and Volume Control System (RCV [CVCS]) is able to match the loss of reactor coolant inventory. Reactor Trip (RT) will occur when a "SG level > MAX1" signal is generated. Partial cooldown is then automatically initiated following a "SG level > MAX2" signal. At the end of the partial cooldown, the affected SG is isolated, and the (RCV [CVCS]) is shutdown. Reactor trip can also be actuated on a "pressuriser (PZR) pressure < MIN2" signal which occurs about 30 minutes after the start of the transient. If the volume control system is in service, the Safety Injection System (RIS [SIS]) will not be actuated.

For the case of rupture of two tubes, the Safety Injection System (RIS [SIS]) is required to compensate for the loss of reactor coolant inventory. RT will be actuated following either a "PZR pressure < MIN2" or "SG level > MAX1" signal. The Safety Injection System (RIS [SIS]) will be actuated following a "PZR pressure <MIN3" signal. Partial cool-down will be initiated following a Safety Injection (SI) signal or "SG level > MAX2" signal. At the end of the partial cooldown, the affected SG is isolated and the Chemical and Volume Control System (RCV [CVCS]) is shutdown.

For sequences in which isolation fails, but a safe state is reached before the In-containment Refuelling Water Storage Tank (IRWST) empties, core damage can be prevented.

Comparison of automatic signals

Analysis of Single SGTR at full power (see Table 17)

FA3, UK:

- Detection on main steam line activity at 15 s,
- Manual Reactor shutdown (on activity detection) at t~RT+30 min
- Manual Partial Cooldown at t~RT+50 min
- Faulted steam generator manually isolated at end of Partial Cooldown at t~60 min

OL3

- Automatic reactor trip and Partial secondary Cooldown on main steam line activity at 15 s,
- Faulted steam generator automatically isolated at end of Partial secondary Cooldown (t<10mn)

US:

- CVCS assumed to operate (offsets break flow)

- Manual reactor trip at 30 min
- Start manual steam generator isolation actions at 40 min
- Pressure equalized between primary and faulted SG at approximately 60 min.

Table 17. SGTR Automatic signals

Action	Signal	FA3	OL3	UK	US
Automatic Reactor Trip (RT) Partial Cooldown	– **PZR-pressure low** – **SG-level high** – **Main steam line activity high**	**X** **X**	**X** **X** **X**	**X** **X**	**X** **X**
SG isolation	– **SG-level high after Partial Cooldown** – **Main steam line activity high** – **SG-level high OR MSL activity high, either after partial cooldown**	**X**	**X** **X**	**X**	**X**

Actions are defined in order to limit SGTR back-flow to the reactor coolant system (concern of heterogeneous dilution)

5.5.3 Main Findings

One and two tube ruptures are modelled in all EPR PSAs, excluding U.S. EPR (one tube SGTR and induced SGTR are modelled). There are significant differences (up to two orders of magnitude) in conditional core damage probabilities (CCDP) and IE specific core damage frequencies (see Tables below). Differences exist as well in the dominant accident sequences.

Low CDF for OL3 SGTR2 is mainly due to low IE frequency. However, the lower CCDP (OL3) for SGTR2 than for SGTR1 is to be reviewed in future PSA update.

Table 18. SGTR IE Frequencies

IE	FA3	OL3	UK EPR	U.S. EPR
SGTR1	9.75E-04	6.0E-03	****	3.5E-03
SGTR2	1.39E-04	1.00E-05*	****	N/A

Table 19. SGTR CDFs

IE	FA3	OL3	UK EPR	U.S. EPR
SGTR1	1.1E-08	2.2E-08	2.2E-10**	2.6E-08
SGTR2	4.4E-09	9.0E-12	4.0E-09	N/A

Table 20. SGTR CCDPs

IE	FA3	OL3	UK EPR	U.S. EPR
SGTR1	1,13E-05	3,67E-06	2,24E-07	7,43E-06

SGTR2	3,17E-05	9,00E-07***	2,04E-05	N/A

* Low frequency is based on German risk study
** Low CDF!
*** Lower than for SGTR1! (assessment ongoing in the context of operating license application review)
**** Commercially sensitive data in EDF/AREVA public report

6 Differences in EPR Designs

6.1 Introduction and summary of design differences

The MDEP EPRWG PSA technical expert subgroup has held joint meetings with EPR vendors exchanging information related to regulatory review findings, modelling 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 modelling or data.

Reasons for differences in design solutions and modelling of EPR PSAs are among others:

- Progress of plant design
  - GDA, DCD, OLA, FSAR…
- project specific customer requirements;
- project specific regulations;
- project specific rules and standards;
- project/customer database;
- project specific site characteristics;
- project specific modelling assumptions/approaches of the PSA teams.

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):

- All EPRs share the same objective to minimize the release to the environment in case of SGTR. Different SGTR management strategies exist. All EPR have faulty steam generator automatically isolated at the end of partial cooldown. If not, all EPR have manual isolation done around 60 minutes post fault. Specifically for OL3, the automatic signal can be initiated by “activity measurements”.
- Differences in system design, e.g. air conditioning and ventilation systems, extra borating system, fuel pool cooling system, EDG size and cooling, fire zoning design, and some of the I&C systems.
- Full rupture (2A LOCA) of reactor coolant systems is not always studied as DBC in all EPR designs although it accounts for the design of the emergency core cooling systems,

- There are differences in reactor coolant system insulation material (mineral vs. glass wool), but this has no impact on the PSA.
- There are design differences related to severe accident management, for example:
  - Fulfilment of single failure criterion in severe accident systems is required in OL3.
  - Diversity between severe accident and design basis accident equipment is required in some EPR designs.
  - Redundancy in severe accident depressurization is required in some EPR designs.
  - Severe accident containment filtered venting is required in some EPR designs.

Main design differences

Some of the information presented in this Section was directly received from EPR vendors. Thus, some details of Taishan NPP (TSN) are also described although it was not included in the EPR PSA comparison.

- Electrical supply
  - Water-cooled EDG (US) vs. air-cooled (OL3, FA3, TSN, UK)
  - SBO diesels not safety classified, automatically started with different alignment (US) vs. safety classified SBO diesel (OL3, FA3, TSN, UK)
  - Gas turbine (OL3 site)
  - Different divisional dependencies for MSRT, CCW Common Header valves and primary depressurization valves
- I&C
  - Non-computerized (OL3 “HBS”, UK “NCSS”, US “DAS”)
  - Hard TXS Kernel (TSN, FA3)
    - *Not modelled in the current FA3 PSA model*
- Essential Service Water
  - ESWS in open loop for OL3, FA3 and UK
  - ESWS in closed loop in reservoir for TSN
  - ESWS in closed loop with cooling tower for US
    - *Make-up possible*
- Diverse heat sinks
  - Deep sea intake (in the outfall structure) for FA3 and UK
  - In reservoir and in the outfall structure for TSN
  - In main heat sink and in the outfall structure for OL3
  - Four “Ultimate Heat Sink” water basins/pools each with a cooling tower, separate from normal heat sink for US
- Core cooling available through SGs in LUHS
  - 2 Air cooled EFWS trains on US and OL3
  - Self-cooled EFWS train on FA3, TSN and UK
- HVAC system design (more details in Section 6.3)
  - OL3, FA3, TSN, UK: Four chillers,

  - *two air cooled,*
  - *two water (CCW) cooled,*
  - *A single chiller cooling one safety division (in LOOP some cross connections are possible [on OL3])*
- U.S.: Four chillers,
  - *two air cooled,*
  - *two water (CCW) cooled,*
  - *a single chiller can cool two safety divisions*

- 1 train of EBS (US) vs. 2 trains (FA3, TSN, UK) and '2+1' trains (OL3)
  - *No difference in risk between OL3 design and FA3,UK,TSN and US*
- EFWS cooling
  - *Cooled by diverse means CCWS/chilled water on OL3/US*
  - *"Self cooled" by EFWS water on FA3, TSN and UK*
- Severe accident (SA) features
  - *1 CHRS train (US) vs. 2 CHRS trains (OL3, FA3, TSN, UK)*
  - *Containment venting (OL3)*
  - *Electrical Supply for Primary Depressurization Valves*
    - **U.S. EPR:** Two MOVs in series are supplied from two different divisions. Risk consequences: (1) a failure of either one "OR" the other division would fail primary depressurization; (2) fire in one division cannot cause a spurious opening of a primary depressurization train (MLOCA).
    - **OL3:** Two MOVs in series are power supplied from the same division. Risk consequences: opening of at least one PDS line is ensured even in case of single failure of one division and to avoid spurious opening of one PDS line due to fire in switchgear rooms of one division, dedicated valves from the same line have their switchgears located in separate divisions.
    - **FA3, UK EPR:** Two MOVs in series are power supplied from the same division. Risk consequences: opening of at least one PDS line is ensured even in case of single failure of one division. Risk of spurious signals (including those due to fires) has been eliminated by the implementation of a manual unlocking in control room (push button guard to validate the opening order).
- Electrical Supply for Main Steam Relief Train (MSRT)
  - **U.S. EPR:** Associated solenoid valves need two divisions to open for partial/fast cooldown. Risk consequence: specific combinations of double failures could fail all 4 MSRTs.
  - **TSN:** The solenoid valves are power supplied from the division the respective SG / Main MSRIV and MSRCV belongs to. Associated solenoid valves need one division to open for partial/fast cooldown. Risk consequence: only the failure of the four divisions could fail all 4 MSRTs. But the same risk as in US exists with regard to depressurization actuated on high SG pressure (PS). In that case (e.g. in case of LOOP), specific combinations of double failures could fail all MSRTs.
  - **FA3=UK:** The solenoid valves are power supplied from the division the respective SG / Main MSRIV and MSRCV belongs to. And they need two I&C divisions to open for partial/fast cooldown. Risk consequence: specific combinations of double failures could fail all 4 MSRTs. (DGs and batteries lost)

- **OL3:** The solenoid valves are power supplied and controlled from the division the respective SG / Main MSRIV and MSRCV belongs to. This design ensures secondary heat removal as long as the power supply of the respective division is available and allows opening and controlling at least two SGs even in case of loss of two PS divisions (one in repair/maintenance, the other one due to single failure). Spuriously opened MSRT is closed with two motorized valves actuated from a neighbouring division in order to ensure closing of the MSRT in case of failure on one PS division. In case of loss of two PS divisions, the closure will be ensured by the manual closure of either the MSRCV or the two motorized valves.

6.2 I&C Architecture and Systems

The main features and differences in I&C architectures and systems in Olkiluoto 3 (OL3), Flamanville 3(FA3) and Hinkley Point C (HPC) EPR units are presented in this Section. Detailed information for U.S. EPR was not available.

FA3 I&C Architecture: Main Features (see Figure 4)

- Bi-directional link PS←→Op I&C with F1 validation command
- CCND (Hard Kernel System) to cope with loss of op I&C
  - TXS
  - Perimeter: DBC2 to 4 + mechanical DEC-A
  - Class: NC
- SAS (Safety Automation System)
  - SPPA-T2000/S5
  - Class: F1B
- PS (Protection System)
  - TXS
  - Class: F1A part (RAU/APU/ALU)
  - Class: F1B part (MSI, PI)
  - Class: F2 part (Gateway)
- PACS
  - Priority management via relay logic in the Switchgears
- SA I&C: CCAG + SAS RRC-B
  - TXS / SPPA-T2000
  - Class: F2

OL3 I&C Architecture: Main Features (see Figure 5)

- Unidirectional link protection system (PS) → operational I&C
- Conventional means to interface PS / SICS & Operating work place
- HBS (Hardwired Backup system) to cope with total loss of computerized I&C
  - TXS family – PLD based
  - Class: SC3
  - Perimeter: DBC2 and frequent DBC3
- SAS (Safety Automation System)
  - SPPA-T2000/S5 (TXP)
  - Class: SC3

- PS (Protection System)
  - TXS
  - Class: SC2 part (RAU/APU/ALU/MSI/PI)
  - Class: SC4 part (Gateway)
- PACS
  - Use of AV42 module
  - Diversity with PC10 module
- SA I&C
  - TXS
  - Class: SC3
  - One system independent from others

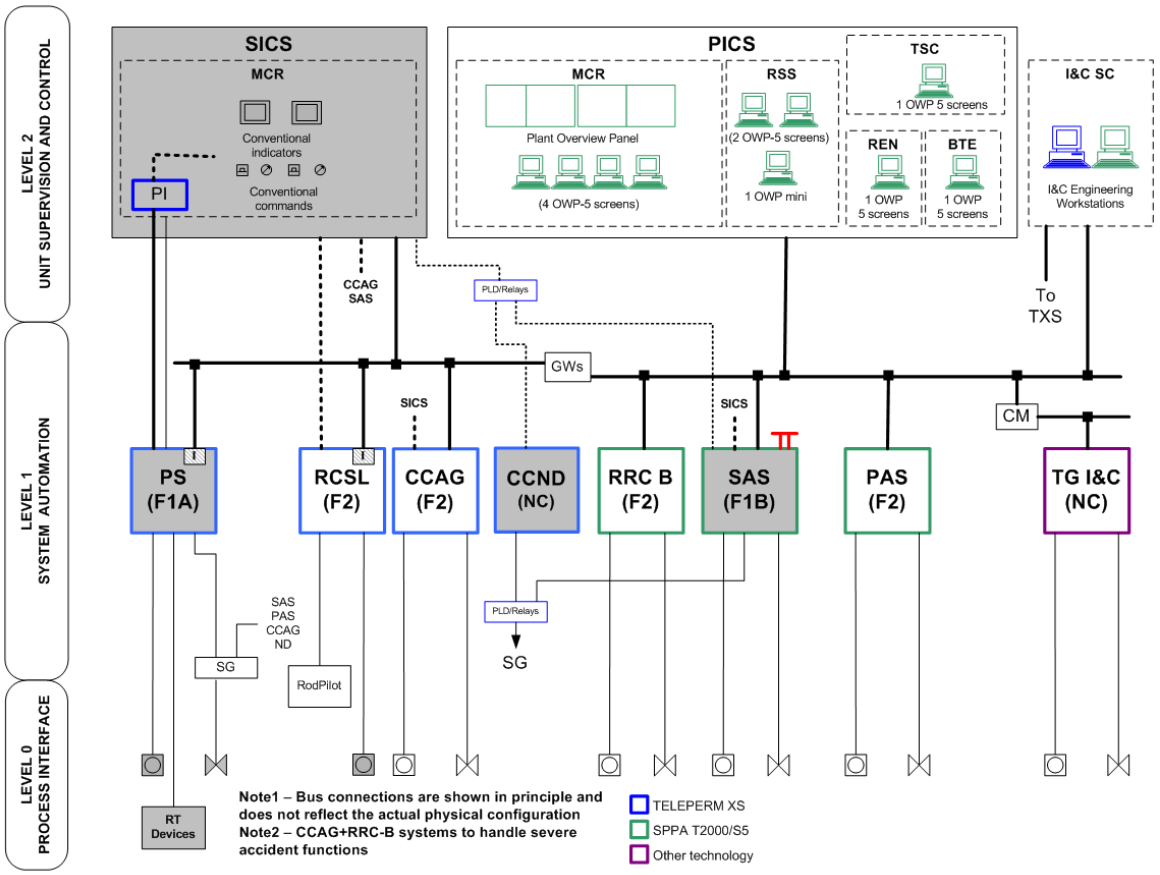

Figure 4. FA3 I&C Architecture [17]

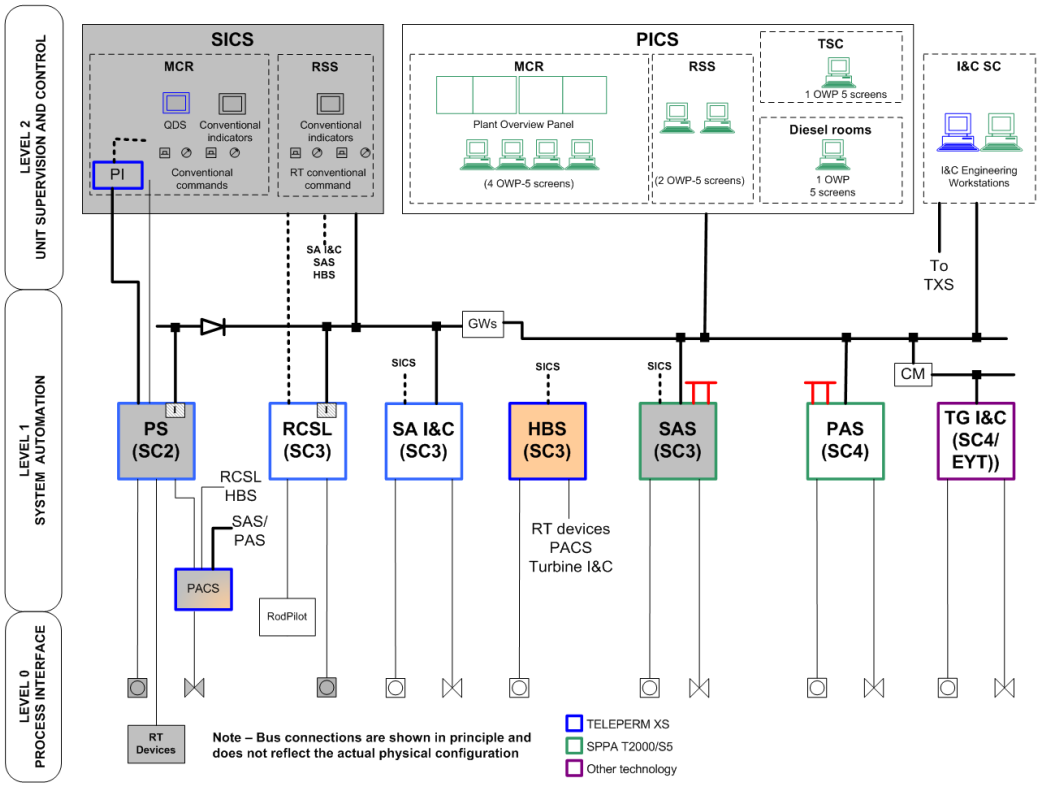

Figure 5. OL3 I&C Architecture [16]

HPC (GDA) I&C Architecture: Main Features (see Figure 6)

- Unidirectional link PS→Op I&C
- Classification of functions/systems changed to cope with UK regulation
- NCSS (Non Computerized Safety System) to cope with total loss of computerized I&C
  - New platform – Analog under development by AREVA-TA
- SAS (Safety Automation System)
  - SPPA-T2000/S7
  - Class 2
- PS (Protection System)
  - TXS
  - Class 1 part (RAU/APU/ALU/MSI/PI)
  - Class 3 part (Gateway)
  - Non-permanent connection of the Protection System Service Unit
  - PSOT (QDS) for class 1 commands and indications for the PS
- PACS
  - Priority management via relay logic in the Switchgears

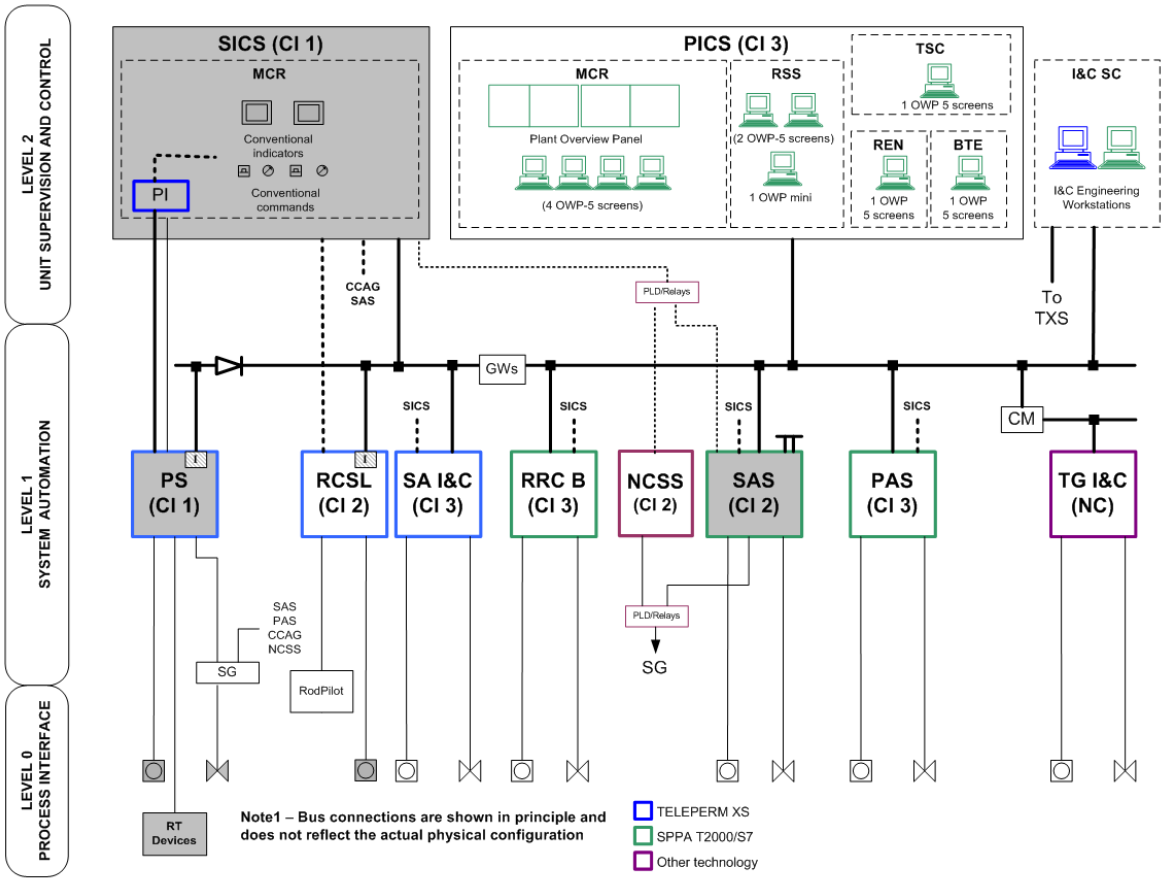

Figure 6. HPC (GDA) I&C Architecture [17]

I&C architectures : main differences

The main difference in OL3, FA3 and HPC EPRs are presented in Table 21. Those differences are directly or indirectly, due to:

- Additional requests (on consideration of total loss of I&C (TLIC), independence of SA I&C or priority modules diversification) in some projects,
- Various classification rules in the different countries,
- Initiation date of the project (for platform choices),
- Designer choices

Table 21. I&C architectures

Feature	FA3	OL3	HPC (GDA)
I&C platforms	Operational I&C platform: • SPPA-T2000/S5 Safety I&C platform: • TXS Non computerized platform: • Not applicable	Operational I&C platform: • SPPA-T2000/S5 Safety I&C platform: • TXS Non computerized platform: • TXS - PLD based	Operational I&C platform: • SPPA-T2000/S7 Safety I&C platform: • TXS Non computerized platform: • UNICORN - Analog
Communication PS←→Op I&C	Bi directional F1 validation of PICS commands	Physical link PS→Op I&C	Physical link PS→Op I&C
Commands to PS	From PICS + F1 validation. Conventional backup from SICS	Conventional from SICS	PSOT (class 1 Qualified Display) Conventional backup from SICS
Total loss of Digital I&C	No – HKS system to cope with loss of op I&C	Yes – HBS to cope with frequent events	Yes – NCSS to cope with frequent events
Priority Actuator Control system	Relay based in switchgears	AV42 module + diversity with PC10	Relay based in switchgears + diversity for NCSS
Main controls classification	NC	SC3 (≈ class 2)	Class 2
Severe Accident I&C	F2 Two sub systems (SPPA-T2000 and TXS)	SC3 Independent from others (TXS based)	Class 3 Two sub systems (SPPA-T2000 and TXS)

6.3 HVAC Systems

Information on HVAC design is presented only for FA3, OL3 and Taishan (TSN). For UK EPR (HPC), the HVAC design specificities are in evolution and, for U.S. EPR, detailed HVAC design information was not available.

Basic Design structure

Table 22. HVAC Systems basic design [17]

DVL	Safety Ventilation	4x100% trains (follows the EPR 4xdivisions concept)
DEL	Safety Chilled Water	4x100% trains (follows the EPR 4xdivisions concept)
DVL (maint)	Operational Ventilation	2x100% trains (for availability/maintenance)
DER	Operational Chilled Water	2x100% trains (for availability/maintenance)

Robustness/ availability	DVL, DVL_{Maint}	Ventilation pipe-work interconnected between div1/2 (resp. 3/4) -> Ventilation/cooling possibly switched to neighbor division
E-supply	Emergency Power supply	Div 1/4 : EDG and SBO-DG Div 2/3 : EDG
Cooling system	DEL/DER Chilled water cooling :	Div 1/4 : Air and CCWS Div 2/3 : CCWS
Diversification	Mechanical equipment:	Chillers, Fans, … as far as necessary
Accidents mitigation	Design Basis Conditions (DBC)	Limiting case “DBC with LOOP + Maintenance + Single Failure”
	Design Extension Conditions (DEC)	Limiting case “SBO or LUHS/TLOCC”

Common Design OL3 / FA3 /TSN

Simplified sketch of the ventilation/cooling of safeguards buildings in OL3 and FA3 designs is presented in Figures and Tables below.

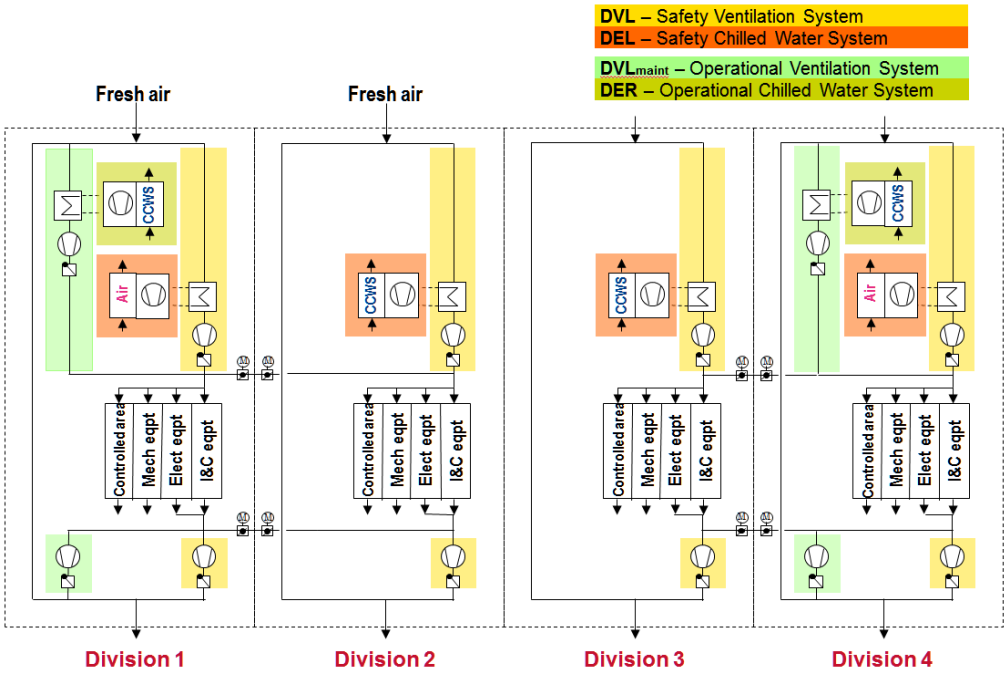

Figure 7. CCWS (KAA) Simplified Diagram 1/2 [18]

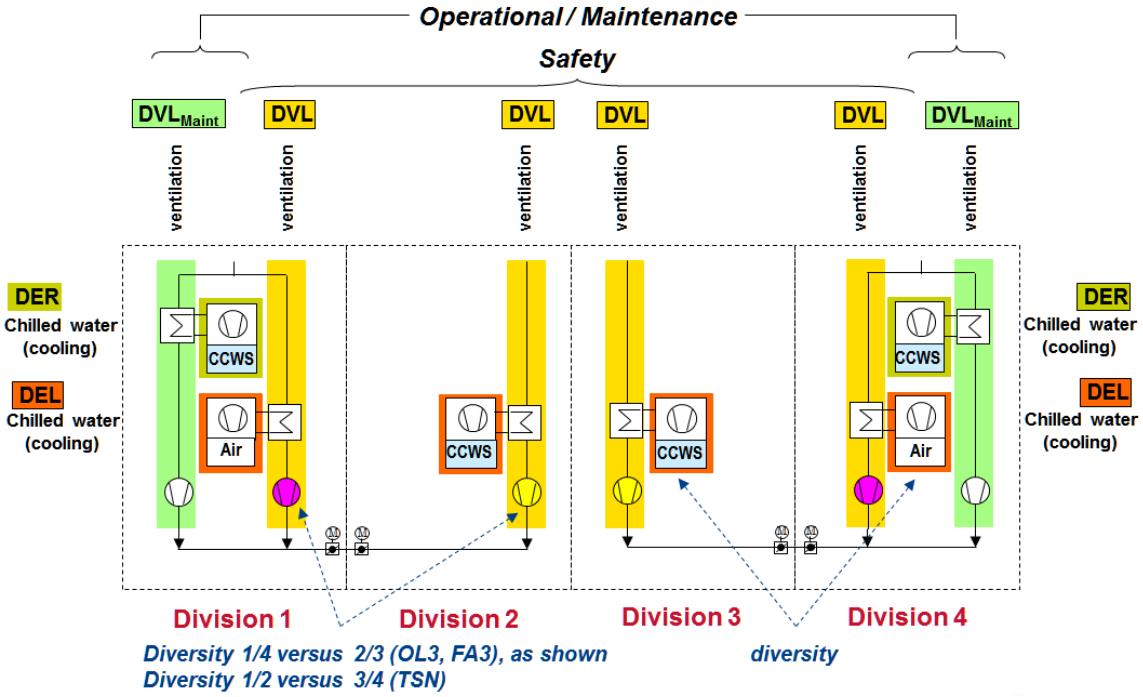

Figure 8. CCWS (KAA) Simplified Diagram 2/2 [18]

Table 23. Common Design of Ventilation/Cooling of Safeguard Buildings [18]

	Division	OL3	FA3	TSN
Safety ventilation DVL Emergency electrical supply Emergency electrical supply	1/2/3/4 1/2/3/4 1/4	4 x 100% 4 EDG 2 SBO-DG		
Safety chilled water DEL Emergency electrical supply Emergency electrical supply	1/2/3/4 1/2/3/4 1/4	4 x 100% 4 EDG 2 SBO-DG		
Operational ventilation DVL_{Maint} Emergency electrical supply	1/4 1/4	2 x 100% /	2 x 100% 2 EDG	
Operational chilled water DER	1/4	2 x 100%		4 x 33% all consumers 4 x 100% essential consumers
Diversity between DVL fans : - within safety trains	1/2/3/4	DVL 1/4 versus 2/3		DVL 1/2 vs 3/4
Diversity between DEL/DER cooling : - within safety trains - between safety/operational trains	1/2/3/4 1/2/3/4	DEL 1/4 (Air) versus DEL 2/3 (CCWS water) DEL 1/4 (Air) versus DER 1/4 (CCWS water)		
Possible switch of Operational trains DVL_{Maint}	1/4	DVL_{Maint} train 1 can supply either div 1 or 2 DVL_{Maint} train 4 can supply either div 4 or 3		

Project specific adaptations in OL3, FA3 and TSN is presented in the Table below. Importance of the chilled water increases with the tropicalization of the site (TSN).

Table 24. Design differences in Ventilation/Cooling of Safeguard Buildings [18]

	OL3	FA3	TSN
Possible simultaneous ventilation of 2 neighbouring div by 1 DVL train	1 DVL (SAC) can supply 2 Elect/I&C div (with reduced flowrate)	No	No
Restriction in Preventive Maintenance of Safety train (DVL and DEL)	No (not needed due to site)	PM allowed only if $T_{air\ outside}$ < threshold (25°C)	PM allowed only if $T_{air\ outside}$ < threshold (30°C)
Safety classification of the 2 DVL_{Maint}-trains	No	Yes	Yes
Start of Operational train (in case of loss of Safety train)	Manual	Automatic	Automatic
Switch of Operational train running from div 2 to 1 (resp. 3 to 4) (in case of loss of safety train 1 or 4)	Manual	Automatic	Manual
Additional diversity or redundancy within DEL trains (DEL 1&4 versus 2&3)	Redundancy on compressors within chiller-unit in div 1&4 (1 safety-classified,1 operational)	No	Diversity (chillers, pumps)

HVAC is an important system to be modelled in PSA because of its significant contribution. Risk insight of HVAC analyses led to some design choices (e.g. DVL diversification). Complete knowledge of the design is necessary to model accurately the HVAC systems. Integrations of HVAC modelling are not at the same level and the outside temperatures differ significantly between various EPR plants. Thus, PSA results cannot be directly compared at this stage.

6.4 Fuel Pool Cooling System

The design features of fuel pool cooling systems in Olkiluoto 3, Flamanville 3, Taishan, Hinkey Point C EPR units are presented in this Section. OL3 NPP is the only EPR unit with 2 spent fuel pools.

OL3

- Spent Fuel Pool (SFP1 and SFP2) :
  - 2 pools : separation of the SFP into two parts (YVL 6.8 requirement)
- Spent Fuel Pool Cooling trains 1&2 (FAK1 and FAK2) :
  - 2 trains in parallel, located in Fuel Building, each one cooling both SFP1 and SFP2
  - Each train with 2x100% pumps in parallel, and 1 Heat Exchanger (cooled by CCWS common)
  - 1 train with 1 pump normally in operation, others in standby (actuated as a back-up) or maintenance

FA3/TSN/HPC

- Spent Fuel Pool (SFP):

  - 1 pool
- Spent Fuel Pool Cooling trains 1&2 (PTR1 and PTR2):
  - 2 trains in parallel, located in Fuel Building
  - Each train with 2x100% pumps in parallel, and 1 heat exchanger (cooled by CCWS common)
  - 1 train with 1 pump normally in operation, others in standby (actuated as a back-up) or maintenance
- Spent Fuel Pool Cooling train 3 (PTR3):
  - 1 train, with 1 pump and 1 Heat Exchanger (cooled by dedicated CHRSi cooling chain-1 and heat sink)
  - In standby, actuated as a back-up or in case of maintenance of trains 1&2

7 Lessons Learned from MDEP Interactions

One of the main objectives for the MDEP EPRWG is to share information, documentation and insights from EPR safety evaluations and PSAs in order to enhance the safety of the design and enable regulators to make timely licensing decisions to ensure safe designs. Another objective is to present and discuss regulatory approaches to risk informed licensing and produce Technical Reports and common positions on selected topics. MDEP co-operation also provides means for the regulators to leverage resources and to focus design reviews on safety issues in areas that are critical to making licensing decisions in member countries.

The establishment of the MDEP EPR PSA TESG is an effective approach to increasing collaboration in the regulatory design & PSA review of the EPR and has supported this goal since the first meeting in 2008. The PSA TESG has held 1-2 meetings per year to share information and experience on regulatory safety and PSA reviews and address many potential issues related to e.g. the scope, assumptions and modelling details in EPR PSAs.

A thorough and detailed comparison of PSAs would require access to practically the entire PSA documentation and PSA models, as well as the main reference documentation. One of the main objectives of MDEP co-operation was to enhance the sharing of information. This goal has been reached only partially, since in all member countries either some or the majority of the PSA related information is categorized as proprietary and/or confidential. Distribution of this kind of sensitive information has proven too difficult even within the MDEP framework and thus limited the scope and details of the EPR PSA comparison, and slowed down the work process. Thus, the PSA subgroup has been able to use only partially the MDEP library for storing and sharing documents related to the PSA comparison.

Successful completion of the PSA comparison effort would not have been possible without the involvement and input from the EPR vendors and customers, which constitutes the

EPR Operators and Owners Group (EPR OOG). PSA TESG had several meetings with the EPR OOG on selected topics and with their approval some of the detailed PSA information could be utilized in the comparison.

Another factor enabling better sharing of information and insights was the co-operation with other EPRWG subgroups. Joint meetings were held with the I&C and severe accidents TESGs. The overall conclusion was very positive and all participants felt that these meetings provided useful insights for the EPR safety reviews.

8 Summary and Conclusions

8.1 Main Insights

The main comparison work was performed a few years ago and therefore the most recent developments in the EPR design and PSA models are not reflected or discussed in this report.

The first overall insight of the PSA comparison is a global agreement on the most important results (total CDF and main contributions) leading to a reasonable confidence in the PSAs. However the more detailed comparison identified several differences which could generally be explained.

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 modelling detail. Some PSAs are so called full scope PSAs in terms of the coverage of operating modes and 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 modelling of IE groups and the accident progression.

The following issues and insights were identified:

- Modelling of digital I&C: the differences in the details and assumptions related to the modelling of I&C systems explain some of the identified differences. The different I&C architecture play also an important role in the difference. In addition, the detailed design of the OL3 I&C system was under development and some changes were foreseen.
- Modelling of ventilations: modelling of HVAC systems is not at the same level in the different PSAs, although the contribution of HVAC can be significantly different due

to site characteristics (tropicalization) and lead to different design choices (e.g. diversification of the safeguard buildings electrical divisions ventilation for OL3).

- RCP seal LOCA management: at the time of the comparison, the assumptions and the level of detail in the seal LOCA modelling appear as rather different and lead to differences in the results.
- Pipe ruptures frequencies: regarding the data used for the LOCA frequencies, there is a significant difference between the OL3/FA3 PSAs and the UK/US EPR PSAs. It is not clear which data is the most representative. However, the differences in design should not affect the initiating event data (the basis used to estimate the pipe rupture frequencies are not detailed enough to differentiate between minor design differences). The choice of applicable data may be driven by the licensee, the vendor or, in some cases, by the regulatory body.
- Success criteria and supporting (thermal-hydraulic) studies: for example the SG success criteria in case of MLOCA or the feed and bleed success criteria are different and can explain different results.
- Reliability data: certain component data are rather different, although the effect on the results remains limited.
- HRA: the human errors probabilities are in some cases quite different, due to different assumptions in modelling and different support calculations concerning the time available for the action.
- CCF: the assumptions relating to CCF are different in some cases (notably for I&C and for batteries) and have a significant contribution to the results.

8.2 Recommendations

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.

The comparison made it possible to identify differences with a potential impact on the results, but generally the information provided is not sufficient for considering that an approach or another is the best practice. So a general recommendation is to review the issues identified by the comparison with a special attention.

In particular it is recommended to review (and improve if possible):

- Modelling of I&C (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 realistic modelling of I&C systems).
- Modelling of HVAC systems.
- Management of RCP seals LOCA.
- Data relating to LOCA frequencies, component failure rates, human errors.
- Supporting calculations (thermal-hydraulics).

- Identification of CCF groups. It has to be noted that even if the assumption is the same for all PSAs (e.g. EDG diesel generators/ SBO diesel generators) the importance of this assumption indicates that the justification is very important.

8.3 Potential Areas for Further Comparison

As mentioned, the sharing of proprietary and confidential information hinders detailed PSA comparison. However, the PSA subgroup has identified areas for which comparison could be continued at least on general level without compromising confidentiality. Examples of such areas include the modelling and quantification of I&C systems and a more complete comparison of human reliability analysis (HRA).

Appendix A: EPR acronyms / EDF coding system

EPR Acronym	EDF Coding System (ECS	AREVA KKS System	Description
ABVS	DWW		Peripheral Room Ventilation System
AVS	EDE	KLB	Annulus Ventilation System
CCVS	EVR	KLA	Containment Cooling Ventilation System
CCWS	RRI	KAA/KAB	Component Cooling Water System
CDS	TEP4	KBG	Coolant Degasification System
CGCS	ETY	JMT	Combustible Gas Control System
CHRS	EVU	JMQ	Containment Heat Removal System
CILWDS	iSEK	KP?	Conventional Island Liquid Waste Discharge System
CPS	TEP2	KBE	Coolant Purification System
CRACS	DCL	SAB	Control Room Air Conditioning System
CRDM	RGL	JDA	Control Rod Drive Mechanism
CSBVS	DWL	KLC	Controlled Safeguard Building Ventilation System
CSS	TEP1	KBB	Coolant Storage And Supply System
CSTS	TEP	KBF	Coolant Storage And Treatment System
CSVS	EBA		Containment Sweep Ventilation System
CTS	TEP3	KBF	Coolant Treatment System
CVCS	RCV	KBA	Chemical And Volume Control System
CWFS	CFI		Circulation Water Filtration System
EBS	RBS	JDH	Extra Boration System
EFWS	ASG	LAR	Emergency Feedwater System
ESWS	SEC	PE	Essential Service Water System
ETBVS	DWQ		Effluent Treatment Building Ventilation System
ExLWDS	TER		Additional Liquid Waste Discharge System
FBVS	DWK	KLL	Fuel Building Ventilation System
FDS	JDT	SGY	Fire Detection System
FPC(P)S	PTR	FAK/FAL	Fuel Pool Cooling (And Purification) System
GWPS	TEG	KPL	Gaseous Waste Processing System
LRMDS	KER		Liquid Radwaste Monitoring And Discharge System
LWPS	TEU	KPF	Liquid Waste Processing System
MFWPS	APA		Motor-Driven Feedwater Pump System
MFWS	ARE	LAB	Main Feedwater System
MSB	GCT	MAN	Main Steam By-Pass
MSIV	VIV	LBA	Main Steam Isolation Valves
MSRT	VDA	LBA	Main Steam Relief Train
MSSS	VVP	LBA	Main Steam Supply System
NABVS	DWN	KLE	Nuclear Auxiliary Building Ventilation System
NIFPS	JPI	SGB	Protection And Distribution Of Ni Fire Fighting System
NIS	RPN	JMY ?	Nuclear Instrumentation System
NSS	REN	KU	Nuclear Sampling System
NVDS	RPE	KT	Nuclear Vent And Drain System
PICS	MCP	CRU	Process Information And Control System
PRMS	KRT	JYK	Plant Radiation Monitoring System
PS	RPR	JR	Protection System
RBWMS	REA	KBC	Reactor Boron And Water Make-Up System
RCPB	CPP		Reactor Coolant Pressure Boundary
RCS	RCP	JA	Reactor Coolant System
RHRS	RRA	JNA	Residual Heat Removal System
SBVSE	DVL		Electrical Divisions Of Safeguard Building Ventilation

EPR Acronym	EDF Coding System (ECS	AREVA KKS System	Description
			System
SCWS	DEL	QKA	Safety Chilled Water System
SGBS	APG	LCQ	Steam Generator Blow Down System
SICS	MCS	CWY	Safety Information And Control System
SIS	RIS	JN	Safety Injection System
SIS/RHRS	RIS/RRA	JNA	Safety Injection System Operating In Residual Heat Removal Mode
SiteLWDS	0SEK		Site Liquid Waste Discharge System
SSS	AAD	LAH/LAJ	Startup And Shutdown Feedwater System
SSSS	DEA	JEW	Standstill Seal System
SWTS	TES		Solid Waste Treatment System
UCWS	SRU		Ultimate Cooling Water System
*	ABP	LCC	Low Pressure Feedwater Heater System
*	CRF	PAB	Circulation Water System
*	DER	QNA	Operational Chilled Water System
*	DFL	SAG	Smoke Confinement System
*	DVD	SAD/SAL	Main Diesel And Sbo Diesel Building Ventilation System
*	JAC	SGB	Fire Fighting Water Supply System
*	JP.	SG	Fire Fighting System
*	KRH	JMU	Hydrogen Detection System
*	RIC	JKS	Incore Instrumentation System
*	SAP	SCA	Compressed Air Production System
*	SAR	SCB	Compressed Air System
*	SAS	DRY	Safety Automation System
*	SDA	GHC	Nuclear Island Demineralised Water Distribution System
PHT			Primary Heat Transport

Appendix B: Abbreviations

AC	alternating current
ALARA	as low as reasonably achievable
ASN	Autorité de sûreté nucléaire (the Nuclear Safety Authority in France)
ATWS	anticipated transient without scram
CCDP	conditional core damage probability
CCF	common cause failure
CCWS	component cooling water system
CDF	core damage frequency
CFR	Code of Federal Regulations (U.S.)
COL	combined license
CVCS	chemical and volume control system
DAC	design acceptance confirmation
DAS	diverse actuation system (U.S.)
DBC	design basis condition
DBE	design-basis event
DBS	diverse backup system
DC	design certification
DC	direct current
DEC	design extension condition
EDF	Électricité de France
EDG	emergency diesel generator
EFWS	emergency feed water system
EPRWG	EPR Working Group (MDEP)
ESF	engineered safety feature
ESFAS	engineered safety feature actuation system
ESWS	essential service water system
EUPS	class 1E uninterruptible power supply
FA3	Flamanville Unit 3
FCD	fast secondary cool-down
FMEA	failure modes and effects analysis
FPCS	fuel pool cooling system
FSAR	final safety analysis report
FV	fussell-vesely importance measure
GDA	generic design assessment
GDC	general design criterion
GL	generic letter (U.S.)
GP	groupe permanent (France) – standing advisory committee
HBS	hardwired backup system (Finland)
HEP	human error probability
HFE	human factors engineering
HKS	hard kernel system (China and France)
HMI	human-machine interface
HPC	Hinkley Point C (NPP unit C)

HSE	Health and Safety Executive (UK)
HVAC	heating, ventilation, and air conditioning
IE	initiating event
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IRSN	Institut de radioprotection et de sûreté nucléaire (the Institute for Radiation Protection and Nuclear Safety in France)
IRWST	in-containment refuelling water storage tank
ISG	interim staff guidance (U.S.)
LC	license condition
LHSI	low head safety injection
LLOCA	large loss of coolant accident
LOCA	loss of coolant accident
LOCC	loss of cooling chain
LOOP	loss of off-site power
LRF	large release frequency
MCR	main control room
MDEP	Multinational Design Evaluation Programme
MFW	main feed water
MHSI	medium head safety injection
MLOCA	medium loss of coolant accident
MSI	monitoring and service interface
MSIV	main steam isolation valve
MSRT	main steam relief train
MSRV	main steam relief valve
MSSV	main steam safety valve
NCSS	non-computerized safety system
NEA	Nuclear Energy Agency
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission (U.S.)
NRSC	Nuclear and Radiation Safety Centre (China)
NSR	non-safety-related
OECD	Organization for Economic Co-operation and Development
OL3	Olkiluoto NPP Unit 3
ONR	Office of Nuclear Regulation (UK)
PACS	priority and actuation control system
PAS	process automation system
PCD	partial (secondary) cool-down
PCSR	pre-construction safety report
PDS	primary depressurization system
PG	policy group
PICS	process information and control system
PIE	postulated initiating event
PLD	programmable logic device
PS	protection system

PWR	pressurized-water reactor
RBWMS	reactor boron and water make-up system
RCP	reactor coolant pump
RCSL	reactor control, surveillance, and limitation
RHR	residual heat removal
RI-ISI	risk informed in-service inspection
RI-IST	risk informed in-service testing
RI-PSI	risk informed pre-service inspection
RI-SC	risk informed safety classification
RI-TS	risk informed technical specifications
RPMS	rod position monitoring system
RPS	reactor protection system
RRC-A/B	risk reduction category-A/B
SA I&C	severe accident instrumentation and control
SAS	safety automation system
SBO	station black-out
SG	steam generator
SGTR	steam generator tube rupture
SICS	safety information and control system
SIS	safety injection system
SLOCA	small loss of coolant accident
SPPA	Teleperm XP a.k.a. TXP
SR	safety-related
SSC	structure, system, and component
SSS	startup and shutdown system
SSSS	stand still sealing system
STUK	Sateilyturvakeskus (the Radiation and Nuclear Safety Authority in Finland)
TESG	Technical Expert Subgroup
TVO	Teollisuuden Voima Oyj (Finland)
TXP	Teleperm XP a.k.a SPPA
TXS	Teleperm XS
VSLOCA	very small loss of coolant accident

Appendix C: List of Reference Documents

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. ONR, Safety Assessment Principles for Nuclear Facilities, 2006 Edition, Revision 1 SAPs, (www.hse.gov.uk/nuclear/saps/saps2006.pdf).
8. 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).
9. Regulatory Guide YVL A.7, “Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant”, Radiation and Nuclear Safety Authority (STUK), 2013.
10. UK EPR pre-construction safety report, Chapter 15, probabilistic safety analysis, 2011, (www.eprreactor.co.uk/scripts/ssmod/publigen/content/templates/show.asp?P=290&L=EN).
11. EPR Vendor’s Presentation: “EPR™ PRA inputs for MDEP Meeting”, MDEP EPRWG meeting, May 17, 2011 (Paris, NEA HQs)
12. OL3 - System Description Component Cooling Water System 30KAA and 30KAB (2012)
13. EPR Vendor’s Presentation: *“Loss of Cooling Chain Initiating Event”*, S. Kahia (AREVA), Oct. 2012, PSA TESG workshop.
14. OL3 PSA Support Studies (AREVA), NEPR-F DC 241, rev. B (2008)
15. EPR Vendor’s Presentation: *“MSRT Design”*, MDEP EPRWG PSA TESG workshop, Oct. 2012 (Paris, NEA HQs)

16. EPR Vendor's Presentations: MDEP EPRWG PSA and Digital I&C TESG meeting, October29th 2015 (Paris, NEA HQs)

17. EPR Vendor's Presentation: *"Internal hazards, HVAC and spent fuel pools"*, PSA meeting, October30th 2015 (Paris, NEA HQs)