RISK-INFORMED EVALUATION OF TECHNICAL SPECIFICATIONS OF LEIBSTADT NPP

Olivier Nusbaumer[1], Devi Kompella[2], Sai Kumar Bulusu[2]

[1] *Safety Compliance & Technical Support, Kernkraftwerk Leibstadt AG, 5325 Leibstadt, Switzerland*
olivier.nusbaumer@kkl.ch

[2] *Risk Management - Nuclear, Lloyd's Register Consulting - Energy Pvt. Ltd., India, 400604*
devi.kompella@lr.org & sai-kumar.bulusu@lr.org

ABSTRACT

Objectives:

Regulatory guideline ENSI-A06 provides requirements for risk-informed applications for Nuclear Power Plants (NPPs) in Switzerland. In particular, probabilistic evaluation of Technical Specifications is mandated as part of PSA submissions towards Periodic Safety Review (PSR). The Technical Specifications of the Leibstadt Nuclear Power Plant (KKL) cover Limiting Conditions of Operations (LCOs) for unavailabilities of (safety) systems and define Allowed Outage Times (AOTs) for each unavailability configuration along with the Surveillance Test Interval (STI) requirements. These important specifications were developed in the 70's, mainly based on expert judgement considering design basis scenarios restricted to transients and LOCAs (e.g. NUREG-1434).

A new state-of-the-art risk-informed (probabilistic) evaluation of AOTs and STIs is performed at KKL based on the plant-specific full scope, all hazards, all levels PSA model. The study applies guidelines ENSI-A06, IAEA-TECDOC-1511[8] as well as NRC Regulatory Guides 1.174 [5], 1.177[10] and NUREG/CR-6141 [9] on "Risk Informed Decision Making" with following objectives: (i) evaluate the completeness and balance of Allowed Outage Times (AOT) and (ii) validate the Surveillance Test Interval (STI) requirements from a risk point of view using PSA.

Methods:

The purpose of the AOT analysis was to perform a probabilistic re-evaluation of all risk significant equipment subjected to LCO based on importance measures like Risk Increase Factor (RIF) and Fussell-Vesely (FV), ensuring they are adequately covered by Technical Specifications. AOTs are said to be "balanced" if risk significant unavailability configurations are assigned shorter AOTs and vice versa. The KKL study involved computation of point-in-time (i.e. instantaneous) risk measures for a given AOT configuration based on CDF/LERF and determination of its maximum duration using a zero maintenance version of the PSA model. System or train related to a particular AOT is set to TRUE (unavailable) using Boundary Condition Set (BCS) and the model is re-quantified to obtain the Conditional Core Damage Frequency (CCDF). The Zero maintenance model is quantified to obtain the Baseline CDF ($CDF_{Baseline}$). The difference between CCDF and $CDF_{Baseline}$ multiplied by the AOT duration gives the Incremental Conditional Core Damage Probability (ICCDP) as defined in ENSI-A06. The PSA based AOT is then estimated using a ICCDP risk budget of 10^{-7}, which is 10% of the current CDF for KKL. This means that the increase in overall annual CDF for a given LCO AOT should always remain lower than this predefined risk budget. 10^{-7} has been selected as the risk budget for the study as opposed to 10^{-6} recommended by international guidance documents like Regulatory Guide RG-1.177[10], mainly because of the low CDF of KKL.

The purpose of PSA based validation of STIs is to evaluate the risk significance of equipment test intervals and optimize the test frequency. As the test interval is closely related to equipment reliability (failure probability) through well-known relations, risk significant STIs can be identified using traditional PSA importance analyses. The duration of these test intervals are evaluated on a case by case basis, assessing the increase in average annual CDF for each case. A Test Interval increase is considered acceptable if ΔCDF remains lower than 10^{-7}/yr.

Results:

The present risk-informed re-evaluation of the Technical Specifications provided interesting and valuable insights from a modern risk perspective. Most remarkably, the study showed that existing Technical Specifications AOTs could be confirmed by the more modern PSA-based analyses. It was also observed that a majority of equipment had AOTs that could potentially be extended, compared to the AOTs that should be shortened, leading to interesting educated discussions and re-considerations.

I. PREAMBLE

Leibstadt Nuclear Power Plant (KKL) is a modern Boiling Water Reactor (BWR) with power output of $3600MW_{th}/1200MW_{e}$, highest among the five operating reactors in Switzerland. The reactor is from the BWR/6 series designed by General Electric (now GEH) and is located in northern part of the country close to the German border beside river Rhine.

Swiss Regulatory Authority (ENSI) follows an Integrated Safety Oversight Approach where Probabilistic Safety Assessment (PSA) is one of the key elements to safety decision making. ENSI developed two guidelines for PSA to standardize the requirements and applications of Swiss PSAs:

- ENSI-A05 – Probabilistic Safety Analysis (PSA): Safety and Scope [1]
- ENSI-A06 – Probabilistic Safety Analysis (PSA): Applications [2]

Probabilistic Evaluation of Technical Specifications is mandated by ENSI-A06 [2] as part of PSA submissions towards Periodic Safety Review (PSR)

To be in line with ENSI requirements and the latest technological evolutions in PSA field, KKL endeavored to upgrade their existing PSA to a state-of-the-art modern full scope PSA. The new KKL PSA is aimed at supporting maintenance planning and other plant specific PSA applications (Technical Specifications Optimisation, Operational Event Analysis etc.) and aid risk-informed operational and safety decisions at KKL. RiskSpectrum® software is used for development of this integrated Level 1 and Level 2 PSA.

Based on this full scope, all hazards PSA model, a state-of-the-art probabilistic re-evaluation of Allowable Outage Times (AOTs) and Surveillance Test Intervals (STIs) is performed at KKL with the following objectives: (i) evaluate the completeness and balance of Allowed Outage Times (AOT) and (ii) evaluate the Surveillance Test Interval (STI) requirements from a risk point of view using PSA.

II. BENEFITS OF PROBABILISTIC EVALUATION OF TECHNICAL SPECIFICATIONS

Technical Specifications are originally based on deterministic design basis accident scenarios (transients and LOCAs) and do not fully consider scenario likelihood and plant risk impact. Past PSA-based Technical Specifications evaluation performed in some NPPs (also in other Swiss NPPs) revealed that not all of the system/train specific AOTs and STIs are proportionate to the risk significance of SSCs.

The benefits of probabilistic evaluation of Technical Specifications related to improvement in safety and plant performance are described below:

- Improve plant capacity factors through avoidance of risk-ineffective forced shutdowns due to technical specification requirements.
- Overall risk reduction by optimizing the plant equipment availabilities.
- Support technical decision making.
- Provide a safety basis on which key maintenance activities could be moved from shutdown to power conditions. This could have a benefit of further reduction in outage duration and quicker return to power following refueling.

III. METHODOLOGY FOR PROBABILISTIC EVALUATION OF AOTs AND STIs

III.A. Technical Adequacy of KKL PSA

The full scope integrated KKL PSA comprises internal events (Transients, LOCAs and Special Initiators), internal hazards (detailed Internal Fire, Internal Flooding and Turbine Missile Events), and External Hazards (Seismic, Aircraft Crashes, High Winds and Tornadoes, External Flooding, Heavy Rains, River Diversion etc.) for all Plant Operating States (full power, low power and shutdown), complying with Swiss regulatory requirements [1]. Latest international guidance, methods and best practices from IAEA [3] [4], USNRC [5] [6] [10], ASME [7], EPRI, NEA/CSNI etc., were referred for the development of various modules of this PSA.

The technical adequacy of KKL PSA for use in risk-informed applications is checked against the important requirements specified in international standard IAEA-TECDOC-1511 [8]. Capability Category II requirements set forth by ASME standard [7] for PSA is the main basis for the development of technical attributes in [8]. Capability category II requirements are representative of currently accepted good industry practices worldwide.

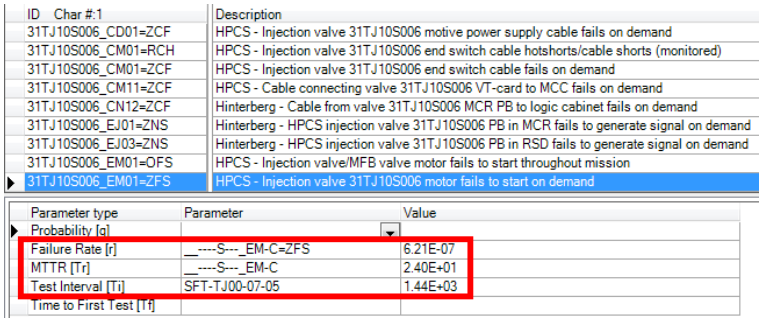
KKL PSA is found to meet all the attributes for probabilistic evaluation of Technical Specifications. Some of these important attributes include:

- Appropriately modelling of maintenance unavailabilities with due respect to mutually exclusive combinations and ability to turn and of the maintenance unavailability basic events;
- Symmetric model development to avoid overestimation of importance of some particular redundant components or trains and underestimation of others;
- Use of time dependent models for standby components as opposed to the demand models;
- Use of parametric models for Common Cause Failure analysis as opposed to simple Beta-factor model and so on.

III.B. Overview of KKL Technical Specifications

Technical Specifications Leibstadt (TSL) stipulates the AOTs and STIs for various systems and components.

Within surveillance testing, there are system function tests (flow tests), instrumentation function tests covering the logic and instrumentation part of the systems. Different components in a system thus can have different test intervals depending on which test they are covered by. For e.g., a trip unit receiving the signals from the transmitters is tested once in a quarter while the system initiation logic is tested once a year. In KKL PSA model, the test procedures are explicitly assigned to basic event reliability model, and these test procedures relate to the Surveillance Test Intervals defined in TSL. Specific Basic Events with different test intervals are used in line with plant practices, as illustrated in the picture below.



ID Char #:1	Description
31TJ10S006_CD01=ZCF	HPCS - Injection valve 31TJ10S006 motive power supply cable fails on demand
31TJ10S006_CM01=RCH	HPCS - Injection valve 31TJ10S006 end switch cable hotshorts/cable shorts (monitored)
31TJ10S006_CM01=ZCF	HPCS - Injection valve 31TJ10S006 end switch cable fails on demand
31TJ10S006_CM11=ZCF	HPCS - Cable connecting valve 31TJ10S006 VT-card to MCC fails on demand
31TJ10S006_CN12=ZCF	Hinterberg - Cable from valve 31TJ10S006 MCR PB to logic cabinet fails on demand
31TJ10S006_EJ01=ZNS	Hinterberg - HPCS injection valve 31TJ10S006 PB in MCR fails to generate signal on demand
31TJ10S006_EJ03=ZNS	Hinterberg - HPCS injection valve 31TJ10S006 PB in RSD fails to generate signal on demand
31TJ10S006_EM01=OFS	HPCS - Injection valve/MFB valve motor fails to start throughout mission
31TJ10S006_EM01=ZFS	HPCS - Injection valve 31TJ10S006 motor fails to start on demand

Parameter type	Parameter	Value
Probability [q]		
Failure Rate [r]	__----S---_EM-C=ZFS	6.21E-07
MTTR [Tr]	__----S---_EM-C	2.40E+01
Test Interval [Ti]	SFT-TJ00-07-05	1.44E+03
Time to First Test [Tf]		

AOTs are addressed in TSL under limiting conditions for operation (LCOs) which are categorized into: (i) LCOs associated with safety or support system unavailability, (ii) LCOs associated with precursors to initiating events (during power operation) and (iii) LCOs associated with precursors to initiating events (during shutdown).

These LCO clauses are studied in detail and segregated as follows:

- LCOs where probabilistic evaluation of associated AOTs is possible (it is verified if the current PSA model has the capability for AOT evaluation or if any model extension is required prior to AOT evaluation).
- LCOs where probabilistic evaluation is not possible. This set includes:
  - Clauses with no AOT specification.
  - Clauses linked with dynamic quantities such as reactivity, neutron flux, specific activity, coolant chemistry etc., which are beyond the scope of PSA.

III.C. Evaluation of Completeness of AOTs:

Completeness of AOTs deals with evaluation of all risk significant Systems, Structures and Components (SSCs) if they are sufficiently covered in TSL.

- All the components with a safety significance criterion of RIF ≥ 2 and FV $\geq 10^{-3}$ are compiled together and mapped to their associated system / train. (Risk Increase Factor – RIF, Fussell-Vesely – FV)

- The completeness of the AOTs is evaluated by verifying if all these risk significant components/trains/systems are covered sufficiently in TSL.

III.D. Evaluation of Balance of AOTs

The balance of AOTs for various systems is evaluated by checking if SSCs of high risk significance have shorter TSL AOTs and vice versa. This is evaluated in following steps:

- $ICCDP_{LCO}$ of an SSC is estimated as:

$$ICCDP_{LCO} = (CCDF_{LCO} - CDF_{Baseline}) \cdot \frac{AOT_{LCO}}{334} \quad (1)$$

Where, $CCDF_{LCO}$ is the Conditional Core Damage Frequency (CCDF) with SSC unavailable and baseline Core Damage Frequency ($CDF_{Baseline}$) is obtained using a zero maintenance model. The value 334 refers to the duration the plant is in full power state (days).

- When the $ICCDP_{LCO}$ for the AOT days is greater than 10^{-7} (10% of the CDF for KKL) for a system/train, this depicts that the TSL AOT is not balanced and the high risk significant system/train is assigned a longer AOT.

III.E. Evaluation of Technical Specifications (AOTs and STIs)

Risk metrics Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) are used for evaluation of TSL AOTs to get a broader perspective. In the present paper, AOT evaluation based on CDF/FDF is presented and a mention is made on the rationale behind the cases that are important to be evaluated by using both CDF and LERF. Also, this paper presents the PSA based evaluation of STIs based on the risk metrics Core Damage Frequency (CDF) for power operation, Fuel Damage Frequency (FDF) for Low Power and shutdown States (LPSD).

PSA based Evaluation of AOTs

While it is possible to evaluate several AOTs using the comprehensive KKL PSA model, bounding cases for some of the LCO clauses were selected in certain cases. For example, in LCO clause of TSL on Reactor Protection System (RPS) Instrumentation, there are 15 trip parameters listed; for each trip parameter, the minimum number of operable channels and their response time are mentioned. It is important to make a rational and pragmatic judgement to choose only typical cases for PSA based AOT evaluation as most of them would not impose any significant risk to the plant due to the redundancy in channels, instrumentation and more importantly most of the initiating events modelled in PSA will have multiple trip parameters. Bounding cases have therefore been selected using expert judgement based on the knowledge of KKL PSA model that incorporates the RPS logic and instrumentation in detail.

As a first step for PSA based evaluation of AOTs, the KKL study involved computation of Baseline CDF ($CDF_{Baseline}$) using a zero maintenance model. As a second step, system or train related to a particular AOT is set to TRUE (unavailable) using Boundary Condition Set (BCS) and the model is re-quantified to obtain the CCDF. With CCDF and baseline CDF available, the PSA based AOT has been estimated using an ICCDP risk budget of 10^{-7} which is 10% of the CDF for KKL and using equation 1 above. The basic idea used here is that the ICCDP for a given PSA based AOT should always remain lower than this predefined ICCDP risk budget of 10^{-7}. Once the PSA based AOT is obtained, it is compared with the TSL AOT. When PSA based AOT is greater than TSL AOT, this means that there is scope for AOT relaxation in TSL AOT. Such cases are important to evaluate using LERF, if such a relaxation can be permitted also from the Level 2 PSA point of view.

The methodology followed for PSA based evaluation of AOTs is presented in the Figure 1 below.

PSA based Evaluation of STIs

KKL Technical Specifications evaluation also involved PSA based evaluation of STIs based on the risk metrics Core Damage Frequency (CDF) for power operation, Fuel Damage Frequency (FDF) for Low Power and shutdown States (LPSD). PSA based evaluation of STIs involved the evaluation of test intervals of equipment that can be (or cannot be) extended. As the test interval is closely related to equipment reliability (failure probability) through well-known relations, risk significant STIs are be identified using importance analyses from the PSA model. All the tests with a safety significance criterion of RIF ≥ 2 are considered as the important. The duration of these test intervals are extended on a case by case basis and PSA model is quantified for CCDF and CFDF (in this case CCDF and CFDF are the annual average increased CDF and FDF respectively as the test interval is assumed to be changed in the base model while calculating these metrics). For each of the test intervals considered $\Delta CDF/\Delta FDF$ is obtained as the difference between CCDF/CFDF and the CDF/FDF respectively.

If both ΔCDF and ΔFDF are lower than 10^{-7}/yr, a comparison of the generic priors for the component failure rates with the plant specific posteriors incorporated into the PSA model has been carried out. The information related to the prior and posterior failure rates is obtained from the component reliability data analysis study carried out for KKL PSA. If the plant specific failure rates of some of the components associated with the test interval in question are greater than the generic failure rates, then ENSI-A06 does not permit extension to the test interval. If the plant specific failure rates for all the components associated with the test interval are less than the generic failure rates then the component failure rate used in the KKLPSA model is doubled and the model is re-quantified to obtain new average CDF/FDF, new CCDF and CFDF for each test interval. ΔCDF and ΔFDF are again calculated and it is verified if the ΔCDF and ΔFDF are less 1% of the original average CDF and FDF respectively. If this criterion is met, test interval can be considered for the extension. The methodology followed for PSA based evaluation of STIs is presented in Figure 2 below.

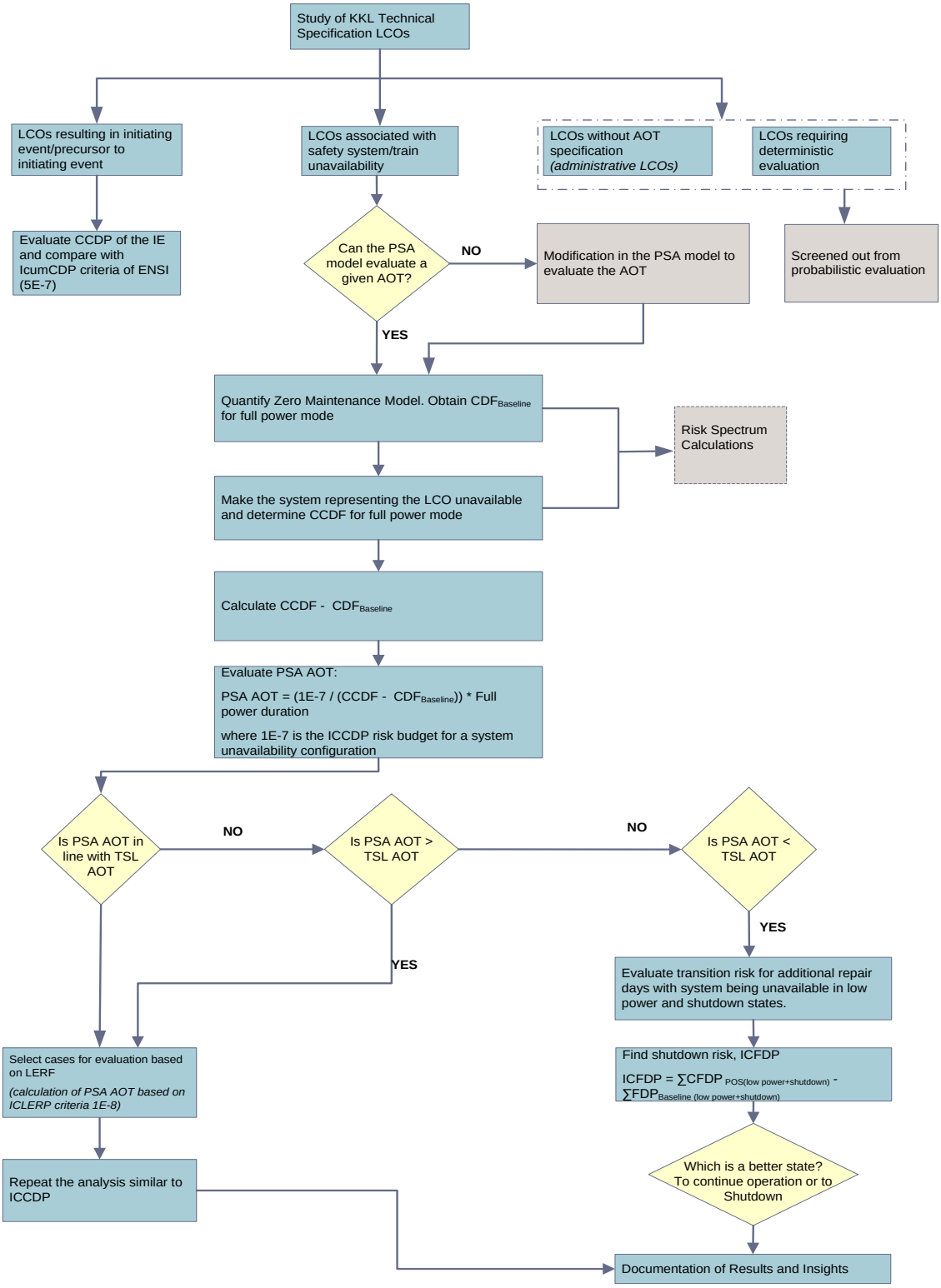


Figure 1 - Workflow for Probabilistic Evaluation of AOTs

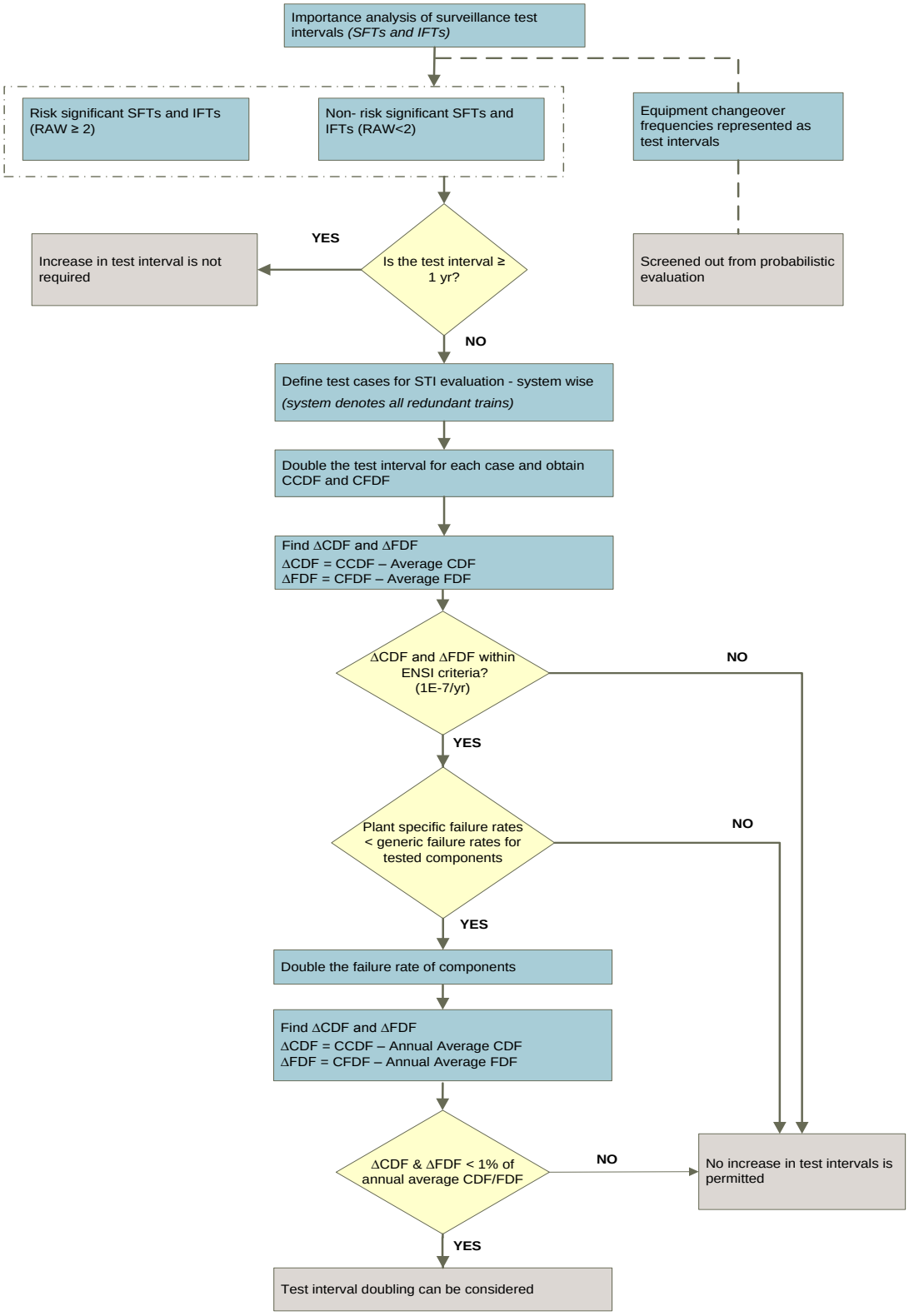
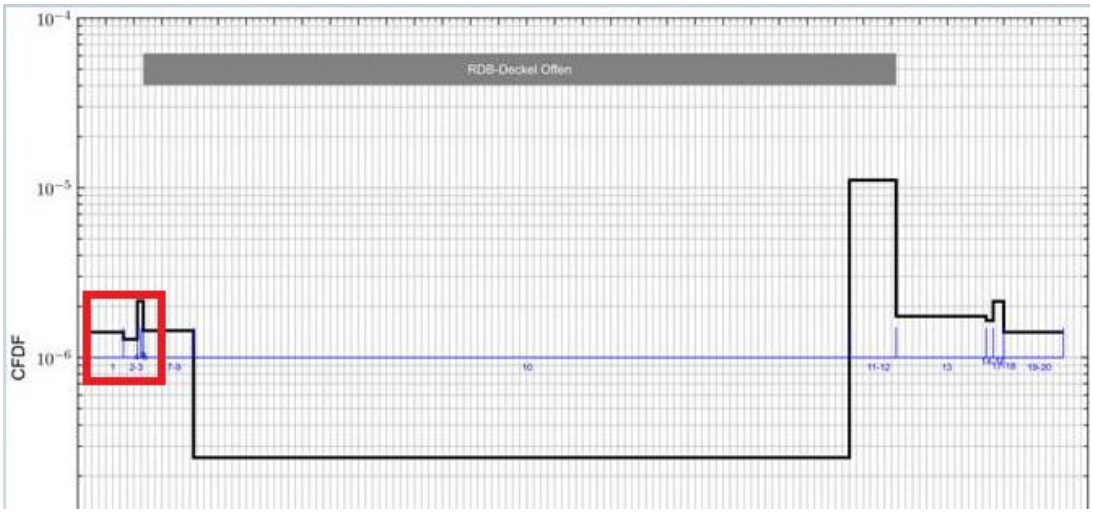


Figure 2 - Workflow for Probabilistic Evaluation of STIs

III.F. Considerations for continuing at full power and going to shutdown

Shutdown risk refers to all of the risk associated with the plant operational modes and Plant Operating States (POSs) involved in the ramping down from full power to cold shutdown and between cold shutdown and full power during ascension. It includes the risk associated with the realignment of a plant from one configuration to another, covering specific operator actions, potential errors of commission, and the potential equipment failures (e.g. pump fails-to-start) involved in transitioning a plant between plant modes, POSs, and configurations, and the possible change in risk level in the new POS.

KKL develops a risk profile for refueling outage each year. The risk profile shows that the risk is generally low in transitioning up to POS-03 with a slight decrease in POS-03 and then increases in POS-04 where RHR is put in service. The peak stays until cold shutdown is reached at the end of POS-06 and then the drops as illustrated in the figure below. Based on these observations, it can be stated that transitioning from full power to cold shutdown state is always associated with some increase in risk.



The consideration of shutdown risk to validation of TSL AOTs is evaluated and concluded as below.

- When PSA based AOTs estimated are longer than current TSL AOTs, the extension can be comfortably permitted as the increase in risk due to the extended time is still within the permissible criteria specified by ENSI. For repairable components, this will provide additional time to bring them back to normal operating condition without the need to enter costly reactor outage.
- When PSA based AOTs estimated are shorter than current TSL AOTs, this indicates that the TSL AOT is not in line with the risk significance of the system. In this case, reactor shutdown is theoretically recommended earlier than the time permitted by TSL. However, early shutdown results in less available time for repair and it may not be possible to complete the repair during this short time. The repair unavailability will continue where its risk significance may be of concern. The important questions that arise at this stage are:
  - Is it better to continue power operation until repair is completed, even if the ICCDP exceeds ENSI acceptance criteria? or
  - Is transition to shutdown state preferable, as the possible risk decrease from power to shutdown may compensate the risk increase when staying at power?

The shutdown risk can be calculated to compare the risk of continuing operation for a given LCO to that of a transition to plant shutdown. Such comparison can be used to decide which option is preferable. Total risk when going to shutdown would be the sum of ENSI's ICCDP acceptance criteria of 10^{-7} for full power and the shutdown ICCDP (ICFDP as known in Switzerland). This when compared with full power ICCDP for the duration required for repair/maintenance gives a good basis to make a decision on whether to continue operation or to go to shutdown.

In the current study, shutdown risk is evaluated for a postulated repair time for the cases when PSA AOT is shorter than TSL AOT.

III.G. LERF and ICLERP Metric Considerations

Using the CDF as a risk metric can only assess safety-level 3 equipment (e.g. frontline and support systems). In order to assess Safety-level 4 equipment (e.g. containment systems), the analysis planned to be extended to the Large Early Release Frequency (LERF) metric. Also, for the cases evaluated using CDF metric, if PSA based AOT obtained is longer than TSL AOT, it is important to evaluate if the system is important from a LERF point of view and if such extension can be permitted from a Level 2 PSA point of view. For Example: Failure of Standby Liquid Control System (SLCS) during ATWS situation results in failure of reactor shutdown. The frequency of the scenario being low does not contribute largely to CDF while the same scenario could result in a containment failure and add to LERF directly thus becoming a more significant contributor in Level 2 PSA. Such cases should be identified based on engineering judgement and evaluated using LERF metric.

At KKL, containment systems and containment responses (Level 1-2 PSA) are fully linked to Level 1 model, allowing for a straightforward quantification of Conditional LERF and ICLERP for each identified LCO using similar approach as presented in III.E. Here, the ICLERP risk budget is 10^{-8}.

IV. RESULTS AND INSIGHTS

Please note that all the results and values presented in this paper are only "indicative" of the actual results and should not be taken as absolute values.

IV.A. Completeness of AOTs - Results and Insights

With regard to completeness of AOTs, it is observed that all the risk significant SSCs are covered within the system/train related LCOs in the TSL.

TABLE I. Completeness based on RIF

Component	RIF	System/ Train	Covered in Tech. Specs?	LCO ID
Control Rod	460	Control Rod Drive	Yes	3.1.C
Pneumatic actuator of SCRAM outlet valve	210			
RPS instrumentation	10	Logics & Instrumentation	Yes	3.3.A
Safety Relief valves	3	Safety Relief Valve	Yes	3.4.E
Minimum Flow Bypass valve, Injection valve	3	High Pressure Core Spray	Yes	3.5.A
Main pump	2			
Motor of Main pump	5	Low Pressure Core Spray	Yes	3.5.A
Main pump	3			
Main pump	3	Reactor Core Isolation Cooling	Yes	3.7.E
Diesel generator components	4	Electrical Power System	Yes	3.8.A
220V DC battery	3	Electrical Power System	Yes	3.8.D
24V DC battery	2	Electrical Power System	Yes	3.8.E

TABLE II. Completeness based on FV

Component	FV	System/ Train	Covered in Tech. Specs?	LCO ID
SCRAM discharge check valve	$3.30 \cdot 10^{-2}$	Control Rod Drive	Yes	3.1.C
Control Rod	$2.20 \cdot 10^{-2}$			

Component	FV	System/ Train	Covered in Tech. Specs?	LCO ID
Safety relief valves	$1.70 \cdot 10^{-2}$	Safety Relief Valve	Yes	3.4.E
Injection line check valve	$2.10 \cdot 10^{-2}$	High Pressure Core Spray	Yes	3.5.A
Main pump	$1.80 \cdot 10^{-2}$			
Minimum Flow Bypass valve, Injection valve	$1.00 \cdot 10^{-2}$			
Injection line check valve	$1.80 \cdot 10^{-2}$	Low Pressure Core Spray	Yes	3.5.A
Main pump	$1.50 \cdot 10^{-2}$			
CB of Main pump	$1.50 \cdot 10^{-3}$			
Main pump	$1.80 \cdot 10^{-2}$	Special Emergency Heat Removal (SEHR) - Train A	Yes	3.5.A
Motor of main pump	$4.90 \cdot 10^{-3}$			
Inlet valve motor, Outlet valve motor	$1.80 \cdot 10^{-3}$	Emergency Service Water - Loop A	Yes	3.7.A
Main pump	$2.20 \cdot 10^{-1}$	Reactor Core Isolation Cooling	Yes	3.7.E
Steam turbine	$7.50 \cdot 10^{-2}$			
Diesel Generator components	$1.10 \cdot 10^{-1}$	Electrical Power System	Yes	3.8.A

There are a few specific cases which call for either:

- Augmentation of existing TSL clauses with additional or more detailed explanation or
- Inclusion of a specific LCO clause to represent a configuration that is observed to be risk relevant but not present in current TSL.

Examples:

- 24V DC cabinets of Div. 31, 51, 61 and SAMG DGs are risk significant from PSA point of view and are good candidates for inclusion in the TSL.
- Some of the risk significant components' unavailability can be bounded by one of the existing clauses within TSL. An example is the restriction orifices YB10F001, YB10F008, YB10F013 and YB10F006 which are risk significant. Concomitant failure of these orifices would result in failure of ATWS signals to initiate Alternate Rod Insertion (ARI). The loss of ATWS instrumentation is bounded by clause 3.3.A (action D) where an immediate shutdown is recommended.
- With respect to fire water system (Hinterberg), LCOs related to maintaining the availability of water in the reservoirs are available in TSL and LCOs that deal with the failure/unavailability of system related components are recommended to be included.

IV.B. Balance of AOTs - Results and Insights

From the analysis on balance of AOTs, although generally there is a good balance between the risk significance of the system/train and the TSL AOT, there are few TSL AOTs that are observed to be not balanced from a risk point of view. Some risk significant SSCs have longer AOTs whereas a few non-risk significant SSCs have shorter AOTs.

TABLE III. Balance of AOTs

LCO ID	System/ Train	TSL AOT	$ICCDP_{LCO}$	Balanced ($ICCDP_{LCO} < 10^{-7}$)?	Comments
3.3.A	Reactor Protection System	Immediate shutdown	$1.80 \cdot 10^{-9}$	Yes	

LCO ID	System/ Train	TSL AOT	$ICCDP_{LCO}$	Balanced ($ICCDP_{LCO} < 10^{-7}$)?	Comments
3.4.E	Safety Relief Valve	1 Year	$4.40 \cdot 10^{-9}$	Yes	Risk Significant System but can have a longer AOT due to multiple redundancy present within the system (1 out of 16 SRVs are enough for pressure relief)
3.5.A	High Pressure Core Spray	30 days	$1.90 \cdot 10^{-7}$	No	Risk Significant System, TSL AOT requires restriction (reduction)
	Special Emergency Heat Removal (Div. 51 & 61)	10 days	$3.20 \cdot 10^{-6}$	No	Risk Significant System, TSL AOT requires restriction (reduction)
3.7.E	Reactor Core Isolation Cooling	30 days	$5.20 \cdot 10^{-8}$	Yes	
3.8.A	6.6 kV Diesel Generator (Div.11)	30 days	$1.10 \cdot 10^{-8}$	Yes	Div. 11 has more alternate power supply alignments compared to Div. 31 and supports low pressure core cooling systems.
3.8.C	6.6 kV Safety related bus bar (Div.31)	30 days	$1.90 \cdot 10^{-7}$	No	Risk Significant System, TSL AOT requires restriction (reduction). Div. 31 support high pressure core spray system.

IV.C. Evaluation of AOTs - Results and Insights

PSA based AOTs are calculated for Reactor Protection System (RPS), Emergency Core Cooling Systems (ECCS), Emergency Diesel Generators (EDG), RPS, ECCS and ADS instrumentation and so on. Bounding cases are selected for instrumentation related AOTs as explained before. The PSA based AOT evaluation is performed using CDF as risk metric. The analysis using LERF as risk metric is underway to obtain more appropriate results from a more holistic risk perspective. Case selection criteria for LERF based AOT evaluation is explained in section III.G above.

TABLE IV. PSA based Evaluation of AOT (some examples)

System	LCO ID	Description	TSL - AOT	PSA – AOT (using CDF)	LERF evaluation required?
Reactivity Control System	3.1.I	SLCS unavailable	24 hrs.	90 Days	Yes
Instrumentation	3.3.G	SEHR - ADS initiation unavailable	72 hrs.	24 hrs.	-
	3.3.P	Failure of ARI initiation through RPV high pressure instrumentation	Immediate shutdown	180 Days	Yes
Reactor Coolant System	3.4.E	8 Safety Relief Valves inoperable (in open condition)	Immediate shutdown	1 Day	-
Emergency Core Cooling and Special Emergency Heat Removal	3.5.A	HPCS unavailable	30 Days	15 Days	-
		All LP ECC systems except SEHR unavailable	1 Day	10 Days	Yes
		One train of SEHR unavailable	30 Days	30 Days	-
		SEHR unavailable	10 Days	1 Day	-
		ADS function unavailable	Immediate shutdown	10 Minutes	-
Containment Systems	3.6	Failure of one pair of containment isolation valves	Immediate shutdown	-	Yes

System	LCO ID	Description	TSL - AOT	PSA – AOT (using CDF)	LERF evaluation required?
		Failure of suppression pool makeup function	72 hrs.	-	Yes
		Failure of Filtered Containment Venting System (FCVS)	10 Days	-	Yes
Plant Systems	3.7.E	RCIC unavailable	30 Days	60 Days	Yes
	3.7.J	Fire Water System unavailable	3 Days	180 Days	Yes
Electrical Power Systems	3.8.A	Div. 31 DG unavailable	30 Days	30 Days	-
		Div. 51 DG unavailable	30 Days	60 Days	Yes
		Div.31, 51 & 61 DG unavailable	1 Day	5 hrs.	-
	3.8.D	220V busbars 11ES and ET unavailable	30 Days	20 Days	-

PSA AOT > TSL AOT

PSA AOT < TSL AOT

PSA AOT and TSL AOT match

KKL PSA has proved to be quite efficient and robust in calculating the risk based AOTs for different systems. This can be attributed to the following key features of KKL PSA:

- The detailed modelling of safety systems and their support systems in line with the systems design and operational aspects without conservative assumptions,
- Modelling of symmetrical/redundant configurations of safety and support systems in line with the plant operational practices and
- Inclusion of secondary systems modelling wherever their credit is taken for safety functions.

The robust model made it possible to derive important insights and to provide logical explanations for questions like:

- Why some systems are risk significant and the TSL AOTs for these systems need a re-evaluation and reduction (HPCS, SEHR)?
- Why some redundant trains of the same system have different risk significance and different PSA AOTs (E.g., SEHR trains A and B)?
- Is it better to continue power operation until repair is completed or is it advisable to go for a costly outage for completion of maintenance?

PSA based AOT evaluation revealed the following interesting insights:

- **Most of the PSA based AOTs and TSL AOTs match well**

  Most of the PSA based AOTs match with TSL AOTs for safety systems and trains and no AOT change is required to be reviewed, confirming the sound deterministic analysis done in the 70's (e.g.: NUREG-1434)

  Examples:

  PSA based AOTs of one train of SEHR, complete ADS function failure, Div. 31 DG, 220V DC batteries of Div.31 and 51, 24V buses of Div.11 and 21 are observed to match the TSL AOTs.

- **Some of the PSA based AOTs are higher than their corresponding TSL AOTs indicating possibility of AOT extension for systems of either lower risk significance or when there is high redundancy between safety systems**

  There are candidate systems/trains where AOT extension can be reviewed by plant operators as their PSA based AOT is much longer than TSL AOT.

Examples:

- The TSL AOTs defined for simultaneous unavailability of two trains of LP ECCS other than SEHR are found to be restrictive. As there are multiple redundant trains of LP ECCS, PSA based evaluation shows longer AOTs and hence there is a scope for relaxation of TSL AOTs for LPCS and LPCI Systems
- RPS instrumentation (redundant trip parameters are available in case of any initiating event) and SLCS are found to have much longer PSA AOTs as compared to their TSL AOT. These however need to be evaluated using LERF as sequences with ATWS and failure of SLCS have low contribution to CDF but are important from LERF point of view as ATWS followed by failure of SLCS directly results in LERF due to the postulated containment failure

❖ **A few PSA based AOTs for some systems/ trains are lower than their corresponding TSL AOTs and these represent the risk significant systems important for TSL AOT re-consideration (reduction)**

Examples:

- HPCS and SEHR are highly important and have shorter PSA AOTs compared to TSL AOTs. The PSA AOT of HPCS is about 15 days as against its TSL AOT of 30 days while the PSA AOT of SEHR is 1 day as against the 10 days specified in TSL.
- Risk Significance of HPCS originates mainly from Large LOCA best-estimate scenarios for which HPCS alone by design can provide sufficient cooling to the core. External events like seismic events also contribute to the high importance of HPCS. The external events induce extended TLOOP (24 hours). APRM channels (sensing the reactor power) lose their normal power supply on TLOOP, the normal supply is backed by batteries with a capacity of 12 hours after depletion of which the APRMs fail high (the normal supply is not backed up currently by a DG). APRMs failing high (indicative of ATWS) leads to ADS inhibit by some complex mechanisms. KKL is endeavoring to replace the existing analog APRM system (from where the ADS inhibit signal gets generated on loss of power supply to APRMs) with digital PRNM system which is backed by a separate set of battery banks lasting for 24 hours. A SAMG Diesel Generator is installed to provide the first line of back up.
- SEHR is of critical importance in seismic events and airplane crash events. Seismic events of higher accelerations fail the 220V and 24V DC switchgears associated with Div.11, 21 and 31 systems. SEHR is the only makeup system available during these scenarios through div 51 and 61 without which the scenarios directly result in core damage. Also SEHR has high importance in case of some fire events.
- PSA AOTs for some of the systems are shorter due to the conservative assumptions made in the model either because of complexity of systems (CRD system with 149 control rods) or due to software limitations (e.g., using the 4-factor alpha factor model for a population of 8 SRVs)

❖ **For clauses associated with precursor events, a qualitative study is performed by comparing the CCDPs of IEs that the precursors may cause against ENSI cumulative CCDP criteria ($5 \cdot 10^{-7}$).**

For high CCDP events, it is checked if the corresponding LCO recommends an immediate shutdown. For instance, recirculation flow controller related failures, KKL Technical Specification warrants immediate reactor shutdown following this event which is also supported by PSA based evaluation of CCDP of the probable IE that can be caused by this precursor event.

Full Power vs Shutdown Risk

The results of shutdown risk evaluation for selected AOT cases concur with the observations of outage risk profile presented in section III.F and show that it is either less or equal risk to continue operating in full power (and avoiding costly outage) than entering shutdown for some of the safety system unavailability configurations. Some examples:

❖ PSA based AOT for HPCS unavailability is 15 days. Assuming an average repair time of 20 days for the system, Transition risk evaluation for the additional 5 days shows that risk of entering shutdown and risk of being in full power is almost comparable when HPCS is unavailable.

❖ The risk of entering shutdown is higher than being in full power when both SEHR and HPCS become inoperable.

❖ PSA based AOT for HPCS and RCIC unavailability is 7 days while TSL AOT is 10 days for this combination. Transition risk evaluation shows that risk does not vary when the plant is allowed to operate for 10 days or shutdown after 7 days, with 3 days in shutdown state.

IV.D. Extension of STIs - Results and Insights

Interesting observations are made from the PSA based evaluation of test intervals associated with system function tests and instrumentation function tests.

As an example, it has been observed that no test interval extension can be permitted for group of DGs (Div. 11, 21, 31, 51 and 61) and systems like HPCS and RCIC. On the other hand, test interval extension can be considered for instrumentation function tests of Emergency Service Water (ESW), RCIC and HPCS. Finally, a vast majority of non-PSA relevant tests could potentially also be extended.

REFERENCES

1. ENSI-A05 – Probabilistic Safety Analysis (PSA): Safety and Scope
2. ENSI-A06 – Probabilistic Safety Analysis (PSA): Applications
3. INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, IAEA, Vienna (2010).
5. Regulatory Guide 1.174, "An approach for using probabilistic risk assessment in risk-informed decisions on plant specific changes to the licensing basis," U.S. Nuclear Regulatory Commission, Washington, DC
6. Requirements for monitoring the effectiveness of maintenance at nuclear power plants, 10 CFR 50.65.
7. Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants, ASME/ANS RA-S-1.4-2013
8. INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA TECDOC Series No. 1511, IAEA, Vienna (2006).
9. Handbook of methods for risk-based analyses of Technical Specifications, NUREG/CR - 6141
10. Regulatory Guide 1.177, "An approach for plant-specific, risk-informed decision making: technical specification," U.S. Nuclear Regulatory Commission, Washington, DC