Development of state-of-the-art full scope integrated PSA model for Leibstadt NPP

Devi Kompella
Lloyd's Register Consulting, India

Olivier Nusbaumer
Kernkraftwerk Leibstadt, Switzerland

1. BACKGROUND

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

Swiss regulator 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:

1. To define the requirements on scope and quality of Swiss PSAs (ENSI-A05); and
2. To define the risk-informed applications for which the PSA is intended to be used (ENSI-A06).

The aim of these guidelines is to have standardized high quality Swiss PSAs and to use them effectively in plant specific applications.

Also in the recent past, international PSA standards and guides like ANSI/ASME RA-S-2009 [1], IAEA SSG-3 [2], and SSG-4 [3] etc. were published with the goal of promoting high quality PSA and encourage its use in risk-informed decision making.

As a consequence of these new national and international technological evolutions in PSA field, KKL decided to initiate a major consolidation and upgrade of its existing PSA to a state-of-the-art modern PSA, that can be used extensively to support maintenance planning and risk-informed operational and safety decisions at KKL.

2. OBJECTIVES AND SCOPE OF KKL PSA

The objectives of KKL PSA are:

- To develop full scope PSA model in line with Swiss PSA guidelines and international best practices
- To have high level of detailing for I&C, Electrical Power Supply and Secondary Systems
- To establish a clear connection between PSA and plant specific information
- To have a high quality and detailed PSA model for plant specific risk informed applications (evaluation of risk impact of plant modifications, operational event analysis, technical specifications optimization, etc.)

KKL PSA was developed as a full scope Level 1 and Level 2 ANS/ASME PRA Capability Category–II PSA model (with detailed internal events, external and internal hazards) for full power, low power and

shutdown states of the plant by adhering primarily to ENSI guidelines and taking help of several other latest international PSA guidelines.

The benefits of using a single integrated model are:

- To ensure consistency of modelling between different modes of plant operation.
- To reduce the degree of repetition within the modelling and to simplify the PSA model maintenance and future development.

3. GENERAL OVERVIEW OF KKL PSA MODEL

RiskSpectrum® PSA was used **to develop the multistate full scope Level 1 and 2 PSA model**; and quantify various Risk metrics like Core Damage Frequency (CDF), Large Early Release Frequency (LERF), Large Release Frequency (LRF) etc.

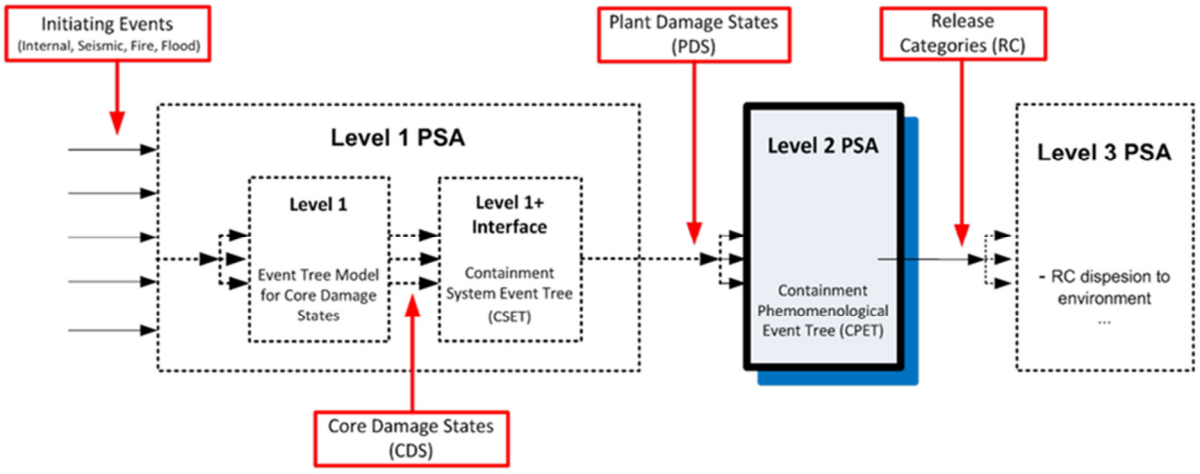

Figure 1 - Integrated PSA model structure

The event sequence progression in Level 1 Event Trees (ETs) can either lead to successful termination of the IE or can lead to Core Damage/Fuel Damage (CD/FD). All the frontline systems performing reactivity control, high pressure and low pressure make up, pressure control and decay heat removal are modelled by Fault Trees and integrated with the ETs.

Post CD/FD severe accident progression is modelled in a two-stage process. In the first stage which is called Level 1+, containment systems are modelled whose functions are to restrict the radioactive release to outside containment or environment. The Containment System Event Trees (CSETs) model all these functionalities using containment system fault trees and by taking Level 1 consequences as input. This linked event tree approach takes care of the functional dependencies between Level 1 and Level 1+ CSET modelled systems.

Each sequence of CSETs is assigned with a consequence called Plant Damage State (PDS). Since, all PDSs do not have a high frequency of occurrence and vary in severity, PDSs are condensed to a few significant Key Plant Damage States (KPDS).

These KPDS Consequences are used as input to the next or the final stage modelling, the Level 2 model that models the possible Containment physical phenomena occurring during a severe accident progression. Level 2 Containment Phenomena Event Trees (CPETs) model various possible Containment phenomena and their probabilities of occurrence.

Each of the CPET sequences is assigned a Consequence called Release Category (RC). The radioactivity release data from MELSIM_KKL provides the information about the Sequences and release categories contributing to Large Early Release Frequency (LERF) and Large Release Category (LRF).

4. INITIATING EVENTS AND PLANT OPERATING STATES

The major initiating events modelled in the KKL PSA are given in the table below.

Event Type	Number of events modelled (over all Plant Operating States)
Internal events	
Loss of Coolant Accidents (LOCAs)	62
Transients	25
Special initiators	19
Internal Plant Hazards	
Internal fires	66
Internal flooding	25
Turbine missiles	1
External Plant Hazards	
Earthquakes	26
Lightning strikes	1
Sun storms	1
Aircraft crashes	3
Extreme winds	3
Tornadoes	3
Heavy rains	1
Service water intake plugging	1
River diversion (weir Doggern failure)	1
Total	**238**

The above initiating events are spread over 12 different plant operating states (POS).

Full power operation, Power reduction, Hot shutdown, Reactor cooling and depressurization (2 states), Reactor vessel opening, Refueling, Reactor vessel closure, RPV leak test, Reactor heat up
Criticality and power increase (2 states)

5. INTERNAL EVENTS

5.1 *Initiating Event Analysis*

A comprehensive list of internal events was developed by different approaches

- Starting with the “List of Transients and Accidents for Leibstadt (KKL Störfall-Liste)”.
- Failure Modes and Effect Analysis (FMEA) of plant systems, evaluation of KKL operating experience and
- Comparison with national and international guidelines and references such as IAEA SSG-3 [2], ENSI-A05 [5], NUREG/CR-3862 [6], NUREG/CR-6928 [9], NUREG/CR-6890 [7], and NUREG/CR-6143[8].

- Comprehensive system interaction analysis and a critical review of the test and maintenance practices with the help of plant operations group to see whether any of the failure modes of the system could directly or in combination with other failures lead to an IE.

Other highlights of the internal event analysis includes,

- Grouping of IEs are based on similarity of plant response and success criteria of systems and the possibility of occurrence of the IE in same POS.
- Consideration of partial system failures resulting in Select Rod Insertion (SRI) for power reduction either automatically or manually.
- Detailed evaluation and inclusion of shutdown specific IEs also including LOCAs caused due to flow diversions (H-LOCA) and test and maintenance induced LOCAs (K-LOCA).
- Identification and segregation of Loss of Coolant Accidents (LOCAs) based on release medium (steam/liquid), size of the break and location of the break in all systems connected to RPV which lead to unavailability of the system (e.g. LOCA in HPCS injection line) and with respect to the Containment considering the possibility of isolation of the LOCA site.
- Excessive LOCA (RPV bottom vessel rupture) and interfacing system LOCAs (e.g LOCAs when the boundary between primary systems or high pressure system and low pressure systems is breached)

5.2 *System Modelling: Special Aspects*

30 system models were developed that include 12 frontline systems, 07 secondary systems, 07 support systems and 04 containment systems. FMEA of the system was carried out to ascertain the failure modes of system components that lead to unavailability of the system.

5.2.1 Modelling Rules and Modelling Templates

In order to keep the modelling approaches consistent among different modelers 50+ modelling rules were developed. For example: Rules to be taken when failures are indicated/announced/monitored, modelling of train changeover, circular logic, limiting modelling of multiple random spurious actuations etc.

In order to bring uniformity in modelling for PSA components for a specific failure mode across all systems, Object Oriented Programming (OOP) concept of computer coding was used to develop “Object Oriented Modelling Templates (OOMTs)”. These modelling templates were replicated for similar components modelled across all systems, which helped the modeler to standardize the basic event coding, description, reliability model type, parameter code etc. globally. Altogether, 24 OOMTs were developed for 07 different components. (MOVs, CBs, DGs, SOVs etc)

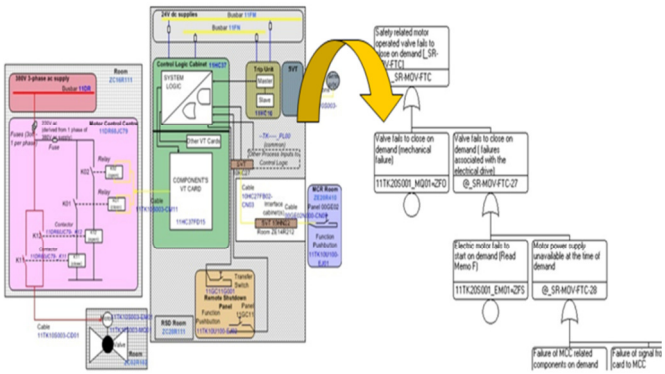

Figure 2 - Object Oriented Modelling Template (OOMT) of Motor Operated Valve (MOV)

5.2.2 *Symmetric modelling*

Asymmetries arise within PSA models when one set of equipment (train or component) out of a set of redundant similar equipment is deliberately chosen to be modelled as the one in normal operation, with other(s) in standby. This results in the train chosen as normally operating having a higher risk contribution than the others. In reality (with standard procedures of equipment changeover) the risk contribution would be expected to be equally distributed among redundant trains. Such asymmetries are typical in LOCA modelling, shutdown cooling system operation and operation of non-standby systems (e.g. feedwater).

Keeping a distant view on the usage of the PSA model for risk monitoring applications, KKL PSA model was developed by adopting a symmetric modelling approach, thereby modelling all possible operational configurations of plant operating systems.

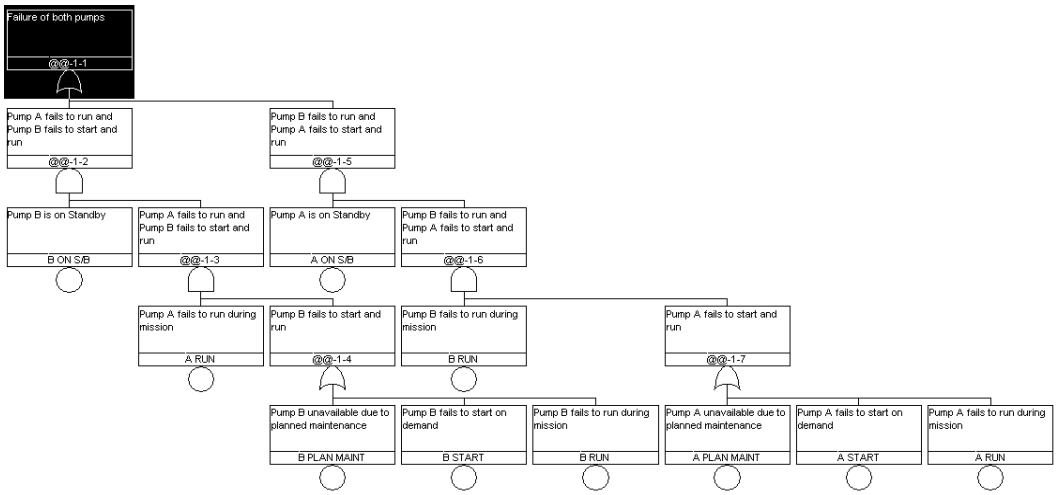

Figure 3 - Illustration of Avoiding Asymmetry

5.2.3 *Electrical Power Supply (EPS) System*

EPS was modelled in great detail including alternate alignments, circuit breaker interlocks and logics. Altogether there are 800+ Fault Tree pages comprising 3340 Basic Events for EPS alone. Loss Of Offsite Power (LOOP) is modelled as grid centered (recoverable in less than 30mins, 2hrs, 10hrs and 24hours), plant centered (non-recoverable less than 24hrs) and external event induced LOOP (non-recoverable in 24hrs). Diesel Generators are modelled with varying mission times for different durations of grid centered LOOP.

5.2.4 *Cycling Components*

Cycling components, which are required to change state during the mission period, have been modelled with a separate failure mode than their first time change of state failure mode. For example, the HPCS injection valve (31TJ10S006) that is required to open to permit HPCS injection closes on reactor high water level, and then re-opens on low water level, with the process repeating throughout the mission period. Safety Relief Valves (SRVs), HPCS system valves and Reactor Core Isolation Cooling (RCIC) system components are modelled as cycling components. Usually, the failure rates / failure probabilities of components during cycling are higher.

5.2.5 *Instrumentation & Control System*

A major feature in the KKL PSA model is the detailed modelling of the instrumentation & control system. The major components modelled in this system are: Sensors, Trip units, Logic cards & cabinet, Instrumentation cables, VT cards, Manual actuation using push buttons in MCR and RSD, Cables and Cable routing (using attributes). This detailing is important for the analysis of Internal Plant Hazards (fires, floods) and also for incorporating some plant modifications or checking design options for modifications.

5.2.6 *Component Reliability Data*

A detailed study of the following generic data sources was carried out for selecting appropriate generic failure rate value: NUREG/CR-6928 [**Error! Reference source not found.**9], ZEDB [10], IAEATECDOC-478 [11], EGG-SSRE-8875 [12] and WASH-1400 [13] and a cross-comparison database table was generated. A thorough comparison between all applicable generic data sources has been conducted and documented.

Similarity in the type of component (rating for pumps and circuit breakers etc.), careful consideration of a matching component boundary between KKL PSA components and those mentioned in generic data source; and use of more latest and BWR related component failure data sources are some of the factors considered while adopting a generic failure rate.

Generic failure rate values are then Bayesian updated with KKL plant specific failure data and posterior failure rates thus obtained are used as the reliability parameters in component unavailability computations.

5.2.7 *Intra and inter system Common Cause Failures (CCF)*

Functional dependences are explicitly covered within the detailed fault tree models of systems. Non-functional dependencies or the so called common cause failures are modelled using parametric models.

Various international documents like NUREG/CR-5497 [14] and NUREG/CR-5485 [15] were used to identify the components that are generally analyzed for CCFs in PSAs. Considering ENSI-A05 [5] recommendation, following CCF modelling strategies are adopted:

- Intra system CCF groups are modelled using alpha factor model that is inbuilt in the RiskSpectrum®;
- Inter system CCF is modelled using a single probability basic event whose probability is calculated assuming a beta factor model;

5.3 ***KKL PSA Alignment with Plant Specific Environment***

As the KKL PSA is to be used for practical applications, a key objective of this improvement and enhancement is to improve the correlation between the PSA model and the KKL plant to make the PSA easy and comprehendible for explaining to the operators when it is used for plant specific applications like allowed outage time/surveillance test interval optimization, maintenance optimization, operational event analysis and so on.

- Component Basic Events have a many-to-one relation to their real plant ID (AKZ);
- A room and a fire-zone (identified by AKZ) are associated to each modeled component;
- Initiating Events have a one-to-one relation to the KKL deterministic accident list (“Störfallliste”) and related supporting thermal hydraulic analyses;
- Plant Operating States (POS) definitions are matched and related to the POS defined in the KKL Technical Specifications (VO/262);

- Where potential repair times are affected by identified Limited Conditions of Operation (LCO), these are mapped with a one-to-one relation to the corresponding LCO rule of the KKL Technical Specification;
- Tested components have their associated test procedure code assigned as a test interval parameter in the basic event reliability model (about 110 test procedures are related);
- Operator error specific basic event probabilities have a one-to-one relation to the corresponding Emergency Operating Procedure (EOP) actions.

5.4 *Success Criteria*

An integrated set of success criteria was developed addressing overall accident success criteria. This was developed into success criteria for individual function events, and then individual systems success criteria. About 300 success criteria cases were analyzed using MELSIM KKL (MELCOR with GUI). These analysis results along with Design Basis Document (DBD) and KKL-based thermal-hydraulic analyses were used to finalize the success criteria for the overall PSA model development.

5.5 *Human Reliability Analysis*

PSA model includes following types of human errors,

- Category A; Pre-trip (or other demand) human errors that may degrade the availability of the system/train (THERP method)
- Category B; Human errors leading to an initiating event
- Category C: Post-trip (or other demand) human errors (SLIM and anchor points by THERP)
- Actions are divided into 4 calibration groups
  - Easy actions from MCR
  - Complex actions from MCR
  - Local/RSD actions
  - SAMG actions

6. INTERNAL HAZARDS

6.1 *Internal Fire*

Based on the experience of the fire PSA analysis team, a few simplifications were adopted while largely following the NUREG/CR-6850 [16] guidance for KKL internal fire PSA. Figure-3 provides the comparison of fire PSA methodology of KKL vis-a-vis NUREG/CR-6850 [16].

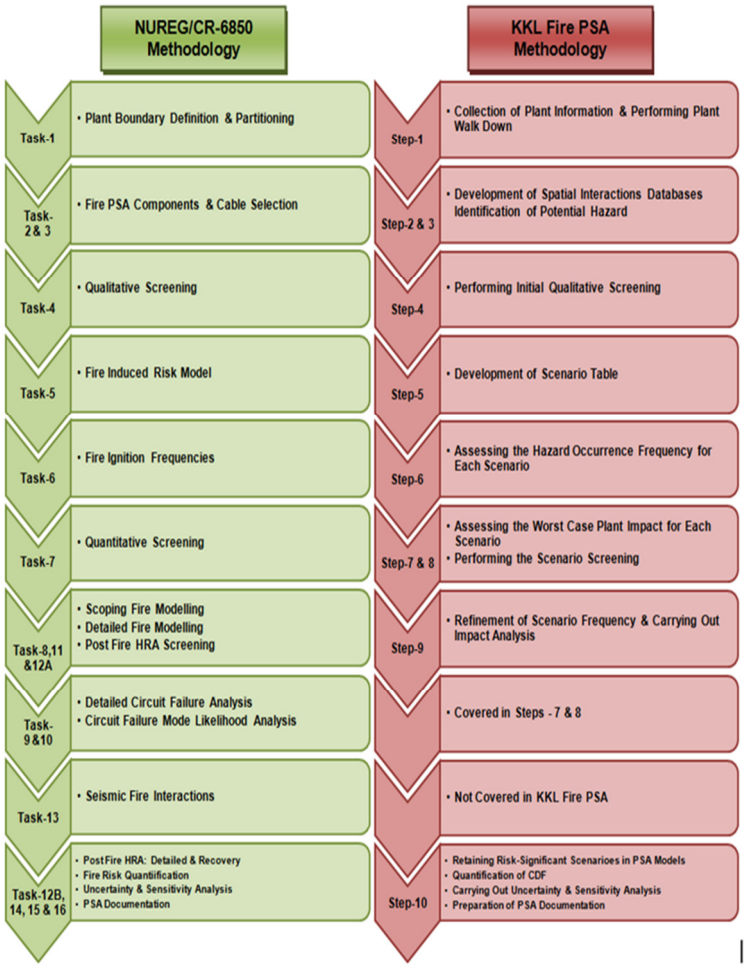

Figure 4 - KKL PSA Fire PSA methodology vis-à-vis NUREG/CR-6850 methodology

The highlights of the fire PSA are presented below.

- A total of 718 zones in the entire plant buildings were initially selected for the plant walk down.
- Plant walk down was performed by 3 to 4 specialists covering a total of 20 buildings.
- Spatial Interactions Database was developed that contains:
  - Fire zones within the facility;
  - Location of fire sources;
  - Location of all PSA equipment and related cables;
  - Susceptibility of equipment to fire;
  - Basic events in the PSA model for the affected equipment;
  - Fire Hazard associated with equipment.

Using the data collected, a qualitative screening was done and 349 zones were retained for quantitative screening analysis. Plant specific data was also gathered on equipment related fire events for a 20-year period based on KKL's experience. Bayesian update was carried out for all 37 fire categories of NUREG/CR-6850 [16] to obtain KKL specific fire frequencies. Fire hazard frequency was developed for each of the 349 retained zones. The worst case impact for each zone (no detection and suppression) was assumed for evaluation of Conditional Core Damage Frequency (CCDF). A cut off criterion of a cumulative CDF of less than 5E-10/yr was used and 305 fire zones were screened out. Only 44 zones were retained for detailed fire analysis.

The Fire Scenarios were refined by modelling the fire zones and their propagation using CFAST and FDS. The detection and suppression (auto and manual) for each zone were considered during the analysis. Fire induced "cable hot shorts" and spurious actuations too were considered during the impact evaluation. Based on the respective zone fire event tree, all possible scenarios were modeled and CDF quantified. 54 scenarios were retained with a cut-off criterion of 5.0E-10 /yr.

For fire event analysis during shutdown, following details are obtained:

- Shutdown specific activities like welding and cutting;
- Transient fire loads and;
- Increased number of people during shutdown.

Using this information, shutdown specific fire ignition frequency for each of the 37 fire categories was obtained. Correspondingly, shutdown specific fire ignition frequency was estimated for each zone. Fire impacts were reassessed to study the impact of fire and the IE caused due to fire during shutdown. Altogether, 66 fire scenarios were modeled covering all Plant Operating States.

6.2 *Internal Flood*

A spatial interaction database for flooding events was developed to

- Identify flood areas, properties and flood sources
- Identify equipment which might be affected by internal floods
- Identify flooding pathways to other areas.

To simplify the analysis, leaks of pipes with <1" dia were eliminated from analysis due to their insignificance. For those flood sources that have been retained, flooding frequencies were estimated. Subsequently, component vulnerability due to internal flood event was determined.

The flow and capacity for the various flood sources were estimated and flood scenarios were developed. For each identified flood scenario a complete range of effects were assumed which include:

- Submergence
- Water sprays
- Steam or steam-water leaks

In total, 44 flood scenarios are developed and out of these 30 scenarios were screened out due to insignificant contribution <5.0E-10/yr. During shutdown states, the frequencies of flood may be increased for certain areas due to the increased activities during this period. To reflect the increase of human induced flooding events in these areas, based on judgement, a factor of 2 was used for shutdown POSs.

7. EXTERNAL HAZARDS

7.1 *Seismic hazards*

For PSA modelling of seismic event, two hazards curves were used, one for near field (<25km) hazards and another for far field (>25km) hazards. The whole hazard spectrum was divided into 13 discrete Peak Ground Acceleration (PGA) bins. Therefore, 26 (13 each for near field and far field) seismic initiating events are part of the seismic PSA model. KKL also developed two sets of fragilities (far field and near

field) for all the equipment groups, structures for use in the seismic PSA. Seismic correlations, seismic HRA, relay chatter analysis are other important aspects modelled in detail.

7.2 *Aircraft Crash , High Winds and Tornadoes*

The effect of crash of any of the three types of aircrafts on the nuclear power plant site was studied. The three types of aircraft are commercial aircraft, light aircraft and military aircraft. Both direct and indirect effects of aircraft crash were studied. The direct effects included mechanical impact such as wall penetration, perforation, scabbing and displacement. The functional failures of Structure, Systems & Components (SSC) due to shock and vibration from impact were also studied. The indirect effects studied include fire/explosion effects. High Winds and Tornadoes were modelled in detail considering the fragility of structures,

8. LEVEL 1+ AND LEVEL 2 PSA

8.1 *Level 1+ PSA*

The accident progression following Core Damage/Fuel Damage (CD/FD) is modelled in Level 1+ Event Trees which are called Containment Systems Event Trees (CSETs). The Transition Codes based on dry/wet drywell condition and RPV pressure assigned to the CD/FD Sequences are used as input to CSETs. The following figure presents the post-CD/FD response of containment systems that aims to minimize the release of radioactivity outside the containment.

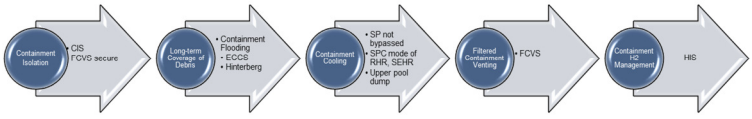

Figure 5 - Containment system response post CD/FD for KKL reactor

In the first stage which is called Level 1+, containment systems are modelled whose functions are to restrict the radioactive release to outside containment or environment; to provide debris cooling; to limit containment pressure below the gross failure pressure; to burn H2 and other combustible gases so that severe deflagration and detonation is prevented; and to scrub the released radioactivity as much as possible.

Each of the Sequence in CSET represents a Plant Damage State (PDS). The PDS characterization factors include the initiating event type (i.e. transient or LOCA, etc.), RPV pressure at the time of core damage and drywell status (wet or dry), status of frontline systems, containment isolation status, sequences that result in containment bypass, status of containment systems for heat removal or pressure reduction, debris cooling status, suppression pool status, FCVS status and possibility of H2 burning by igniters. Since, all the assigned PDSs vary in severity and not all of them have a high frequency of occurrence, PDSs are condensed to a few significant Key Plant Damage States (KPDS).

8.2 *Level 2 Containment Phenomena Modelling*

Corresponding to each KPDS, there is a Containment Phenomenon Event Tree (CPET) that models the Containment phenomena occurring during severe accident progression post CD/FD. Each of the Top

Event in the CPET represents a physical phenomenon that has significant impact on Containment integrity and radioactivity release. Each of the CPET Top Event has multiple alternatives that model the uncertainty associated with the possible physical phenomena during the severe accident progression. Each such alternative is assigned a probability value called "Split Fraction (SF)".

For the evaluation of SFs, all KPDS accident scenarios were simulated using the MELSIM_KKL code. This code is the KKL accident analysis code that uses the calculation engine of MELCOR version 1.8.6. MELSIM_KKL is the complete model of KKL plant; and can perform various thermal-hydraulic analyses to simulate transients and other accidents including severe accident scenarios. The output of the code provides the chronology of the severe accident progression along with the release data of various important radionuclides; and hydrogen and carbon monoxide distribution inside modelled Control Volumes (CVs) of the Containment and other buildings. These output data are used to estimate the Split Fractions (SFs) for each KPDS. For all the sequences in a CPET, a consequence called Release Category (RC) is assigned. The radioactivity release data from MELSIM_KKL provides the information about the Sequences contributing to Large Early Release Frequency (LERF) and Large Release Category (LRF).

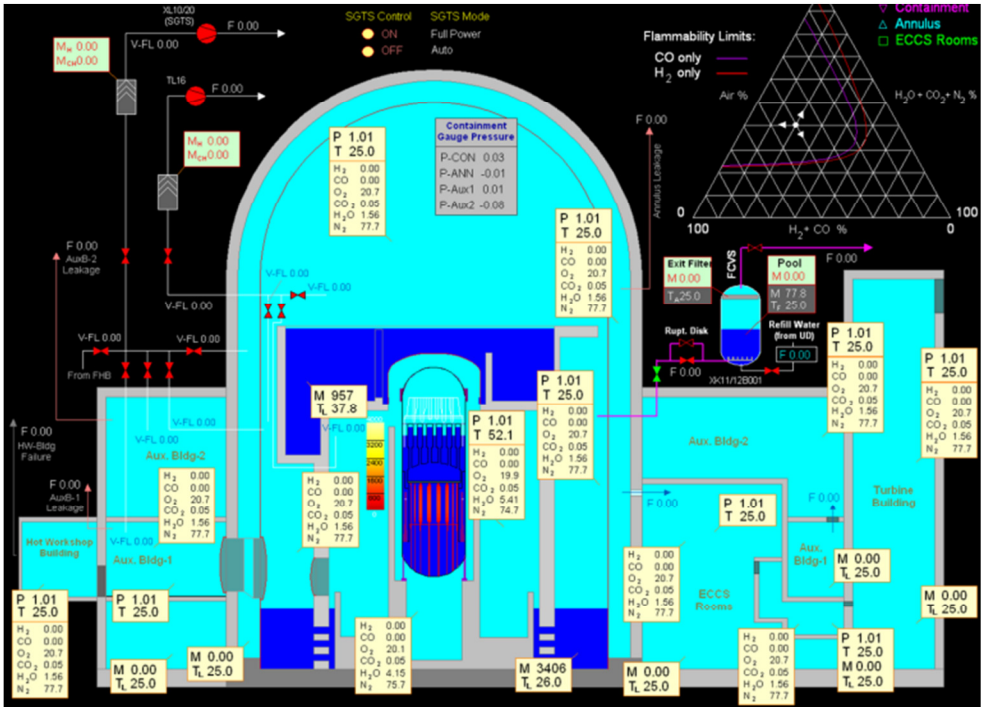

Figure 6 - A typical on screen output of MELSIM_KKL

9. IAEA IPSART REVIEW OF KKL PSA

During November 2014, the International Probabilistic Safety Assessment Review Team (IPSART) was at Leibstadt to conduct review of the Level 1 & 2 PSA model. The team comprised of 8 international experts led by International Atomic Energy Agency (IAEA).

The IPSART experts appreciated the strong commitment and effort of the PSA team to develop a high quality and a comprehensive scope Level 1 and Level 2 PSA to support safe operation of the plant. They recognized that the PSA not only uses state-of-the-art guidance and methodologies but also through many new and innovative approaches, it has gone beyond the state-of-the-art in certain areas of PSA.

10. REFERENCES

1. "Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications includes Addenda RA-Sa-2009 and Errata", ANSI/ASME RA-S-2008, ASME International (2009).
2. "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants" IAEA-SSG-3, International Atomic Energy Agency (2010).
3. "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants" IAEA-SSG-4, International Atomic Energy Agency (2010).
4. "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, United States Nuclear Regulatory Commission (1983).
5. "Probabilistic Safety Analysis (PSA): Quality and Scope", ENSI-A05, Swiss Federal Nuclear Safety Inspectorate (ENSI) (2009).
6. "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments", NUREG/CR-3862, United States Nuclear Regulatory Commission (1985)
7. "Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004", NUREG/CR-6890-Volume 1, United States Nuclear Regulatory Commission (2005)
8. "Evaluation of Potential Severe Accidents during Low Power and Shut down Operations at Grand Gulf, Unit-1", NUREG/CR-6143, United States Nuclear Regulatory Commission (1995).
9. "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants", NUREG/CR-6928, United States Nuclear Regulatory Commission (2007).
10. "Centralized Reliability and Events Database – Reliability Data for Nuclear Power Plant Components", VGB-TW805e-11, VGB PowerTech e.V. (2010)
11. "Component Reliability Data for use in Probabilistic Safety Assessment", IAEA-TECDOC-478, International Atomic Energy Agency (1988).
12. "Generic, Component Failure Data Base for Light Water and, Liquid Sodium Reactor PRAs", EGG-SSRE-8875, 1990.
13. "Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014), United States Nuclear Regulatory Commission (1975).
14. "Common Cause Failure Parameter Estimation", NUREG/CR-5497, United States Nuclear Regulatory Commission (1998).
15. "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment", NUREG/CR-5485, United States Nuclear Regulatory Commission (1998).
16. "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities", NUREG/CR-6850, U.S. Nuclear Regulatory Commission and Electric Power Research Institute (2005).