IAEA
International Atomic Energy Agency
Atoms for Peace and Development

P11. Use of PSA for Design Evaluation

Workshop on Application of Level 1 Probabilistic Safety Assessment

Bangkok, Thailand
5-9 September 2022

Mikhail Lankin

Safety Assessment Section
Division of Nuclear Installation Safety
Department of Nuclear Safety and Security
International Atomic Energy Agency

Highlights of the Presentation

Application of PSA to Support Decisions Made During the NPP Design (Plant Under Design) IAEA-TECDOC-1804

- Licensing of design
- Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard-induced fires and floods
- Establishment of equipment reliability targets for manufactories
- Development operator procedures and training programmes and support for human factors engineering
- Identification of R&D which are necessary to support the design

Application of PSA to Support Decisions Made During the NPP Design (Plant Under Design)

Application of PSA to Support Decisions Made During the NPP Design (1/3)

- At design stage it is easier to optimise the facility rather than when the facility is in operation => the aim of this application is to optimize the design of a new plant in terms of risk metrics and cost
- **The design process typically start from initial design which is based on prototypes**
  - Where certain features aimed to either improve safety or reduce cost of the plant construction and operation are introduced
  - Contradictory tasks: reduced cost generally means that less efforts are involved in safety features of the facility
- **The main focus of the application:**
  - Identification of weaknesses in the initial design and effective areas for improvement in view of plant risk
  - The improvements considered can include the provision of additional or diverse protective systems and features for mitigating the consequences of a severe accident
- **Assessment may include:**
  - Investigation of variants and exploratory design options
  - Sufficiency in systems' redundancy and diversity
  - Effectiveness in emergency and accident management measures, as well as
  - Development of reliability and availability targets for SSCs to meet safety goals

Application of PSA to Support Decisions Made During the NPP Design (2/3)

- **Risk metrics used: CDF/FDF_{AVE}, $LERF_{AVE}$, CDP, LERP, QHOs, $\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$,** Risk importance measures of affected SSCs and HEs (e.g. **FV, RAW**), other PSA insights
- **The major difference with Safety Assessment of the operating NPP are that:**
  - Additional assumptions are needed in lieu of lack of design and operational details
  - For design change evaluations, the level of detail of the PSA model in the areas affected by the design changes must be sufficient to catch the impact of the change
  - Uncertainties in risk estimates are correspondingly larger than for as-built plant
- **Typical outputs of the PSA at the design stage**
  - Selection of the design options that provides high level of safety and at the same time are cost-effective
  - Justification of technical specifications (AOTs, scheduled maintenance, etc.)
  - Modification of the list of design basic accidents
  - Classification of safety related SSCs and establishing of SSC reliability and availability targets
  - Suggestions for the list of accidents scenarios for which accident management guidelines must be developed

Application of PSA to Support Decisions Made During the NPP Design (3/3)

Detailed design information on plant systems might not or only partially be available. This missing information can be bridged by related assumptions for PSA purposes.

- Detailed operating procedures are not available
- No or only generic operational experience is available
- Completeness of initiating events is difficult to ascertain
- Limited information on HMI and on training of operating staff is available
- Limited information on maintenance practices and procedures. Equipment/cable/piping location information is limited or missing (important for internal hazards analysis, CCF modelling and modelling of secondary effects).
- Details on Tech Spec are missing or limited.

Licensing of Design

Licensing of design

- The assessment of the overall plant safety is necessary for applying for operational licence and usually requires a full scope Level 1 and Level 2 PSAs
  - A comparison of the results against safety goals or quantitative health objectives is performed
    - Typically, safety goals are used as safety targets
    - A safety evaluation for applying a pre-construction licence may involve a limited scope of the PSA with additional assessments
- This application provides also input to public relation activity in the pre-licensing process aimed to obtain public acceptance for the NPP construction and operation
- Risk metrics used: **$\Delta CDF/FDF_{AVE}$, $\Delta LERF_{AVE}$, CDF/FDF_{AVE}, $LERF_{AVE}$, QHOs**, risk importance measures of all SSCs and HEs, primary contributors to risk
- Licensing of the design would likely involve an all modes of operation, full scope PSA and all sources of radioactivity

Optimization of protection against hazard events (e.g. fires, floods) and common cause failures, including consideration of correlated site hazards and hazard-induced fires and floods

Optimization of protection against hazard events (1/2)

- Carrying out internal and external hazards PSA from the very beginning of the design development can give the benefit of modifying plant design easily to mitigate impact of the hazard on the NPP
  - A thorough analysis can provide a cost-effective approach to hazard protection optimization at the design stage. Such a benefit is impossible when performing an assessment for operating plants
- Risk metrics - **ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHO**s, risk importance measures of all SSCs and HEs, primary contributors to risk
- The use of PSA at the design phase for optimization of protection against hazard events as supported by PSA has the following goals
  - To establish requirements for the fragilities of the SSCs, including containment (based on the results of seismic PSA and aircraft crash)
  - To define requirements for equipment separation, cable tracing, and plant layout (based on the results of fire/flood PSA)
  - Separation of systems trains/cables
  - Location of flood or fire rated barriers and doors
  - Location of high impact sources, such as large pipes or large fire sources
  - Location and elevation of the rooms housing the important equipment (based on flood PSA), etc.

Optimization of protection against hazard events (2/2)

- Helps to define requirements for internal hazards protective features (Fire/flood PSA)
  - Drainage system
  - Fire detection/mitigation
  - Flood detection
  - Flood isolation
  - Isolation of the compartments, etc.
- To identify and reduce maintenance activities that can lead to fire/floods events
- Specific features of internal/external hazards PSA at the design stage
  - Numerous uncertainties related to the aspects important for internal and external hazards PSA development (e.g. detailed cable tracing, fire and flood barriers, anchorage of the SSCs, location and orientation of the components, etc.).
  - Also lack of operating and emergency procedures introduces additional uncertainties
    - These uncertainties need to be always taken into account

Establishment of Equipment Reliability Targets for Manufactories

Establishment of Equipment Reliability Targets for Manufactories (1/2)

- When the design PSA confirms the satisfaction of safety goals / targets
  - The failure rates of all SSCs in the PSA are used as reliability targets for SSCs
    - Higher safety class is assigned to SSCs with high RAW (RIF)
- **Reliability targets for SSCs** are established considering one or more of the following
  - **Risk**: Contribution to the plant risk, such as core/fuel damage, release, or potential dose to workers or the public
  - **Availability**: Contribution to the plant availability or power generation
  - **Cost**: Replacement cost may be considered, especially for SSCs requiring significant investment
  - **Other Factors**: These may include components not directly impacting the above items, but are important for other reasons such as personnel safety, environmental protection, plant security, or other factors
- Area for **IRIDM** process

Establishment of Equipment Reliability Targets for Manufactories (2/2)

- The risk input is generally focused on ensuring that reliability of SSCs maintains the PSA results at or below the estimated **CDF/FDF** or **LRF**
  - The failure rates are typically based on the already achieved reliability level for the SSCs
    - Proved to be achievable by the industry
    - **Starting point** for the manufacturing reliability goals:
      - High reliability goal for high or medium important SSCs
      - May be relaxed (in limited cases) for low importance SSCs
- PSA models can also be used to analyse the overall plant availability through development of a generation risk assessment (**GRA**)
  - The **GRA** includes modelling of all major causes of a plant shutdown combined with the expected down time for the plant as a result of the failure
  - PSA models might include most of the balance of plant equipment impacting availability and some of the mean time to repair estimates
  - The SSC reliability goals are then established to ensure an overall plant availability is below the availability goal (e.g. 92% availability)

Development operator procedures and training programmes and support for human factors engineering

Development of Operator Procedures and Training programmes

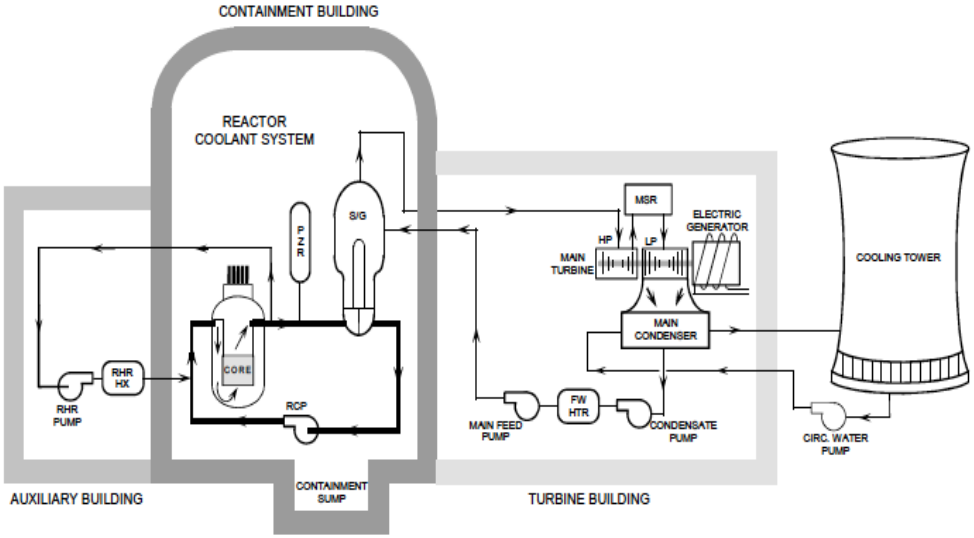
- PSA is used to enhance the training, procedures, and human machine interface for operator responses associated with high or medium importance HFEs
- Risk Metrics: **CDF/FDF_{AVE}, $\Delta LERF_{AVE}$, CDF/FDF_{AVE}, $LERF_{AVE}$**, risk importance measures of all HEPs, assumptions and uncertainties affecting the PSA
- The PSA importance measures include a list of HEPs that are used as an input to programmes involving operator training and procedures development
- The modelling of operator responses which may not be included in the base PSA model due to assumptions and simplifications is a part of the PSA process
- Specific features of HRA at design stage
  - Conservatism need to be removed
    - The best estimate HEPs can be used assuming the best procedures are in place
    - The time window achievable in the design is used in the HEPs assessment
    - The indicators for human interactions are defined that allows action to be timely performed
  - IMPORTANT
    - The above assumptions are provided to the designers to ensure that estimated HEPs are realistic
  - HFEs dependencies and dependent HEPs are defined realistically
    - Typical limitation on dependent HEP (**10^{-5}**) is not applied

Identification of R&D which are necessary to support NPP design

Identification of R&D which are necessary to support the design

- R&D for plants in the design phase, may include new components, systems or uses of components not included in previous plants in operation (or with limited use)
  - R&D relates to SSCs rather than to PSA techniques
  - that potentially impact the risk results, accounting for the uPSA is used to focus R&D on those areas ncertainty
- Risk Metric: **ΔCDF/FDF$_{AVE}$, ΔLERF$_{AVE}$, CDF/FDF$_{AVE}$, LERF$_{AVE}$, QHOs**, risk importance measures of all SSCs, assumptions and uncertainties affecting the PSA
- Typical examples for advanced plants
  - Use of passive SSCs
    - For passive components, such as passive containment cooling, or for components such as explosive valves, the industry experience is limited
    - The reliability is not expected to be as big a concern as either the efficiency or the impact due to non-condensable gases generated during an accident condition
  - Digital I&C, Use of software for controls and actuation

An Example (1/4)



During the design stage of a new NPP, the design review indicated that the risk of Residual Heat Removal (RHR) shutdown line isolation valve leakage would not meet the Design Safety Guideline (DSG) target. Leakage of the RHR motor operated valves at full or reduced power could lead to overpressurisation and possible failure of the RHR system.

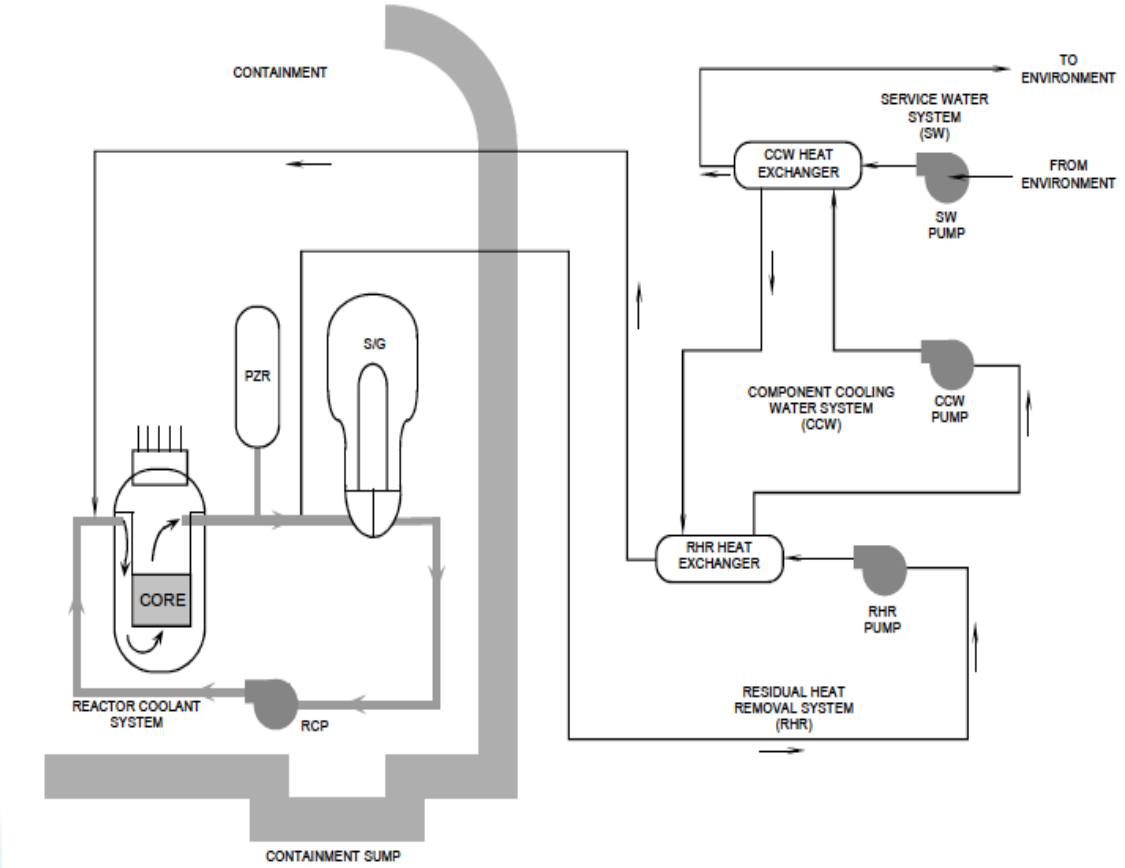
Non-isolable relief or rupture of the RHR effectively bypasses the containment and would be classed as ILOCA. Failure to meet the DSG targets could result in the design CDF and/or LERF not being met and the possibility that the plant would not be licensed.

Various options were proposed to ensure that the RHR Suction Line Isolation reliability would meet the DSG target.

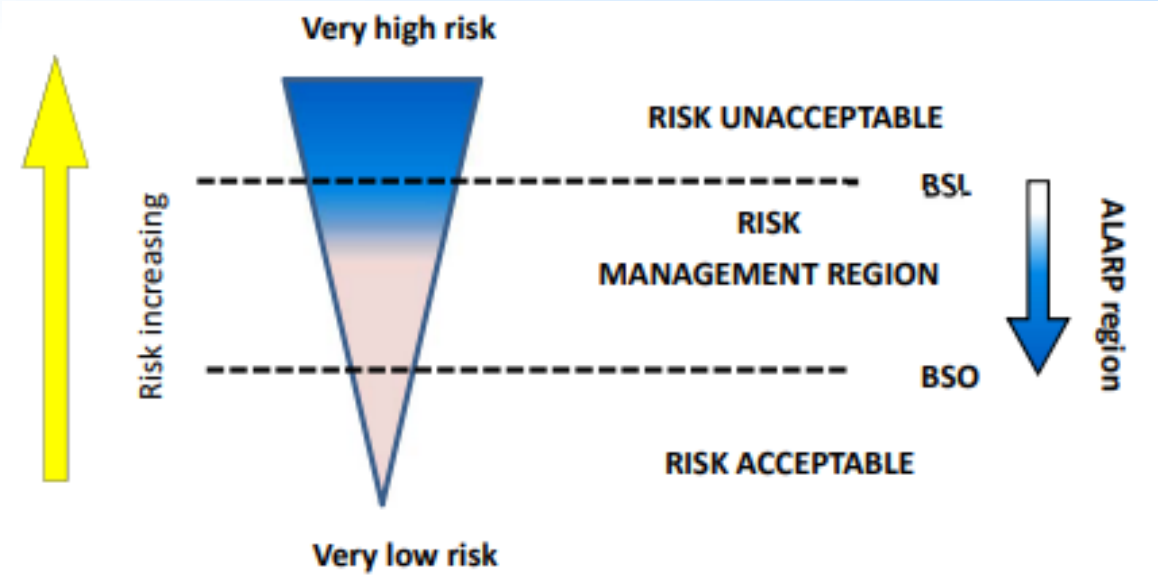
MOV leakage failure rate data used in the preliminary design PSA was based on generic data.

An Example (2/4)

The initial design of residual heat removal system (RHR)



An Example (3/4)



The design safety guideline set by the utility and the design body for all safety systems was that:

- ✓ No single accident sequence contributes more than 10^{-8}/y to CDF or LERF. This goal was defined based on the following considerations:
- ✓ Design goal target for the NPP was to achieve a CDF of 10^{-5}/y, or as near as possible, to meet the Basic Safety Objective (BSO);
- ✓ As there are thousands/tens of thousands of sequences which make up the CDF, it was specified that no individual sequence contributes more than 10^{-8}/y.

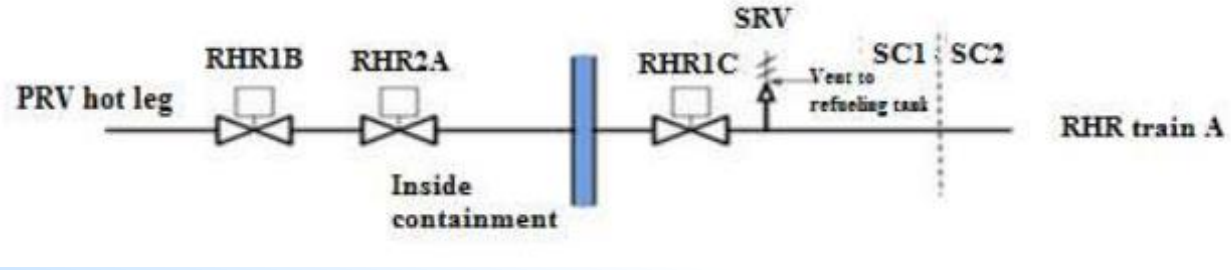
Overall legal requirement is that risks must be reduced:

- ✓ As Low as Reasonably Practicable (ALARP)
- ✓ Measures need to be taken to avert risks unless their cost (in terms of money, time, trouble) is grossly disproportionate to risk averted

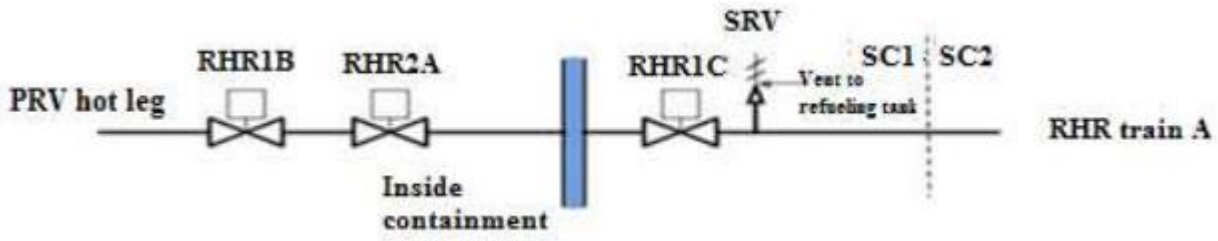
An Example (3/4)

The main reasons for the need to consider change of the design were as follow:

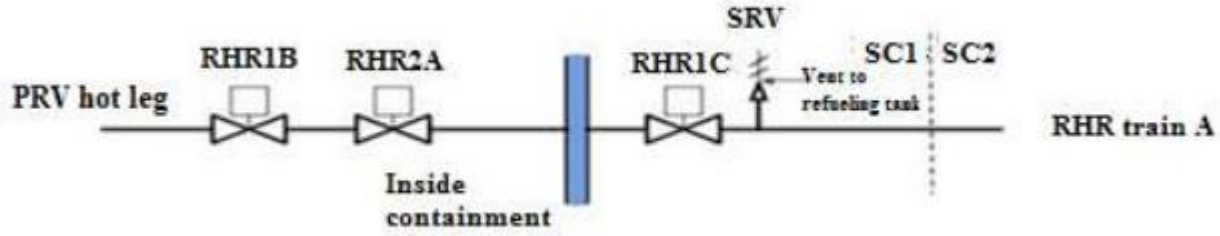
- ✓ The newly developed PSA used MOV leakage failure rate that was based mainly on plants specific information. The derived failure rate appears to be higher than the failure rate based on generic data that was used in previous licencing submissions
- ✓ Leakage of the RHR motorized isolation valves RHR1B, RHR2A and RHR1C could lead to overpressurization and possible failure of the RHR system. A pressure operated Safety Relief Valve (SRV) is provided on the RHR suction line outside of the containment to reduce the probability of failure by relieving to a relief tank. Such external relief or rupture of the RHR effectively bypasses the containment and would be classed ILOCA. Valve reliability indicates the design goal CDF or LERF would not be achievable
- ✓ In addition, the suction line of RHR system outside of the containment and downstream of Relief Safety Valve is not designed to withstanding full power reactor pressures and temperatures
- ✓ The PSA indicated that the risk of RHR suction line leakage is unacceptable
- ✓ There is a legal requirement to demonstrate that the design goal is ALARP



Residual Heat Removal System line drawings

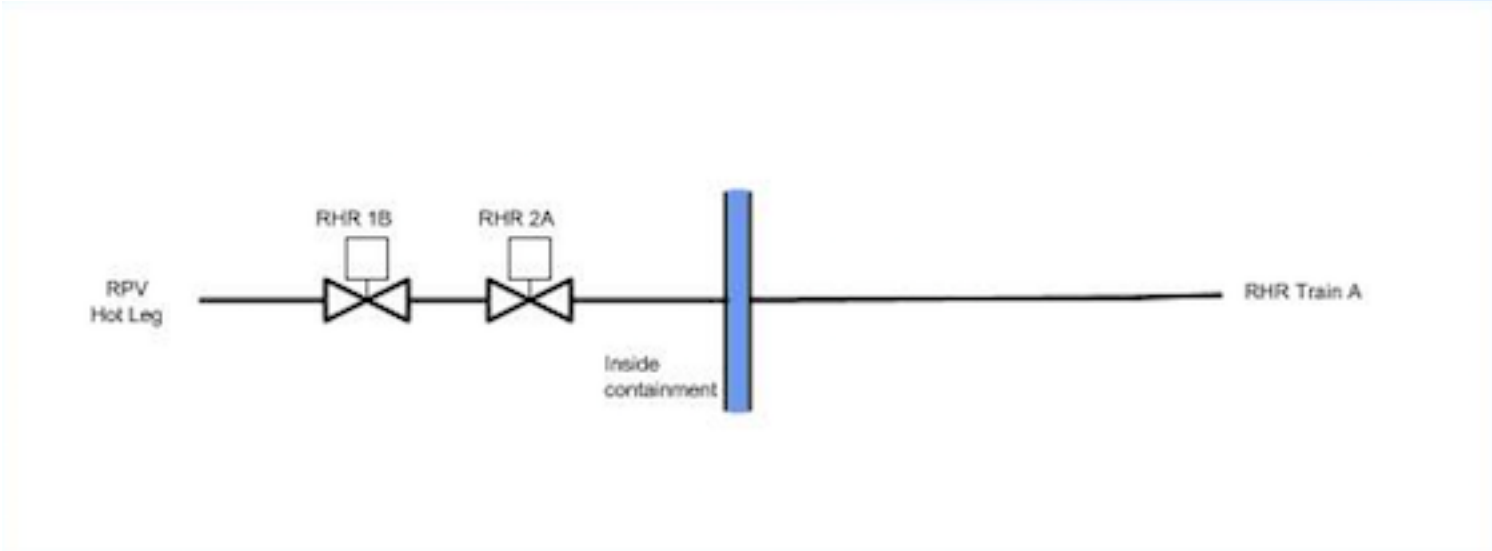


Option 1



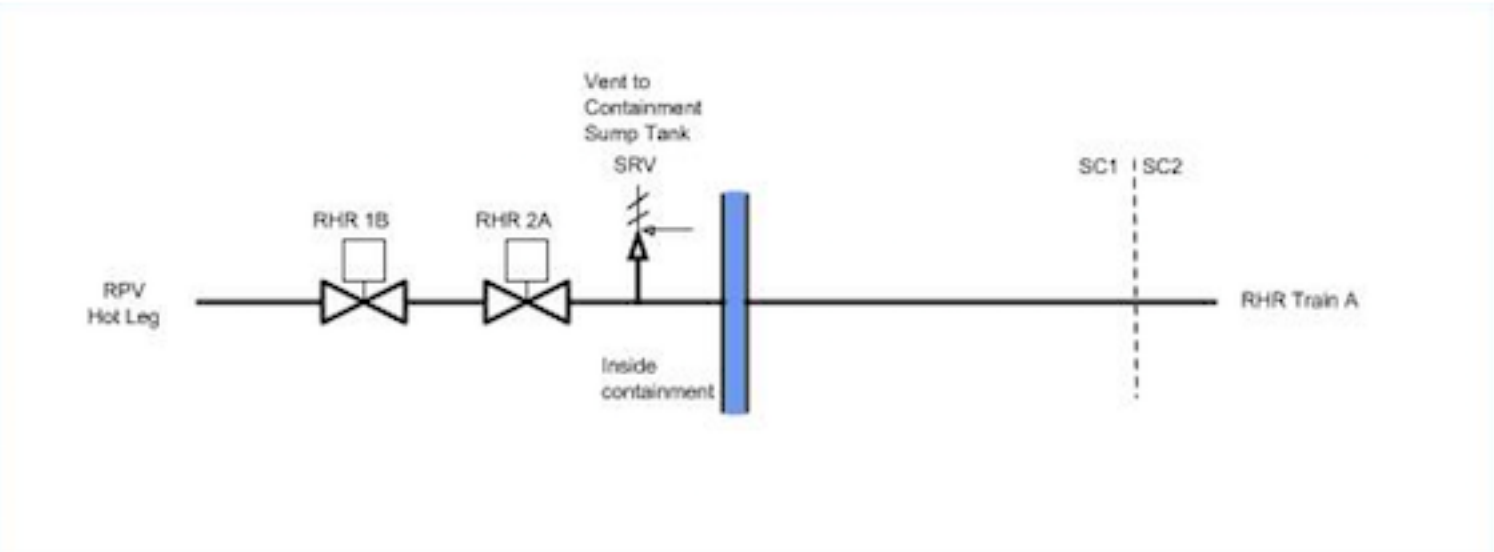
- Design remains unchanged, generic data used to justify safety

Option 2



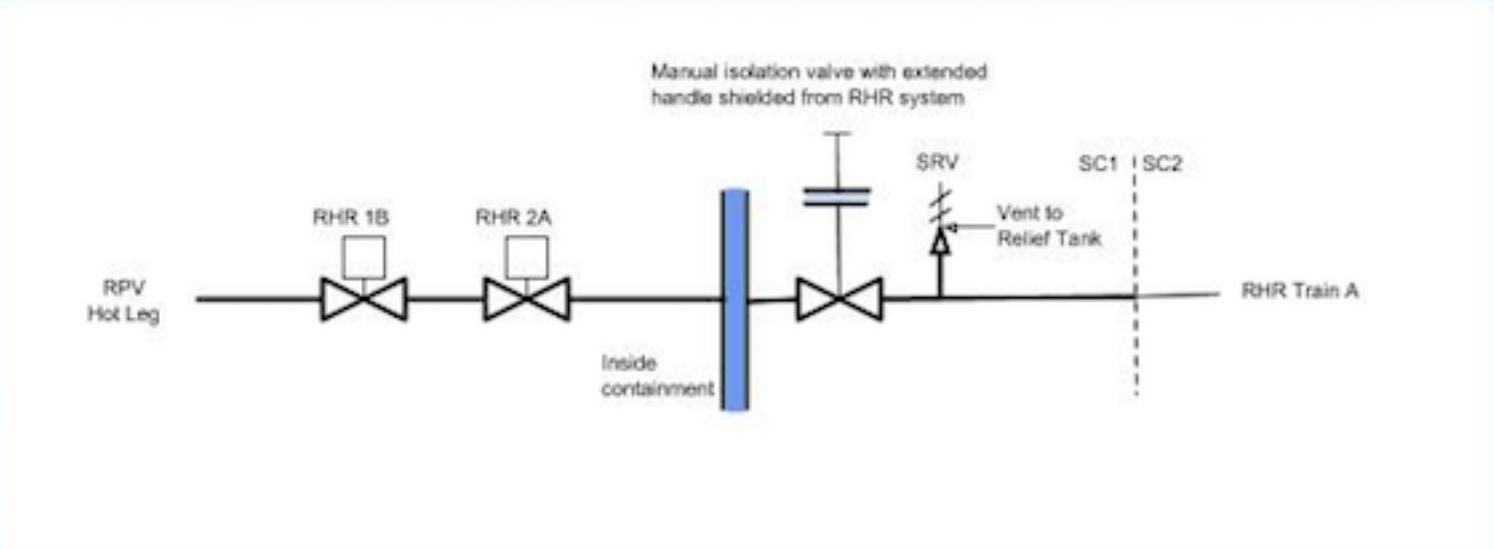
- Upgrade complete RHR system to withstand primary pressure and temperature
- Note: Safety Relief Valve and Relief Tank no longer required to protect lower class components and pipework

Option 3



- Relocate Safety Relief Valve inside containment, valve discharges to containment sump

Option 4



- Install qualified manually operated isolation valve outside containment with hand wheel shielded from RHR system

IRIDM: RHR Isolation Concern (1/7)

3. Inputs to RIDM

- Applicable mandatory requirements and criteria
  - **Affected mandatory requirements:**
    - The probabilistic results based on component specific feedback data are likely to fall between the basic safety level (BSL) and the basic safety objective (BSO), which requires an As Low As Reasonably Practicable (ALARP) justification to be made as to why it is impractical to improve the design.
  - **Other requirements and criteria**
    - No effect on other mandatory requirements and criteria was determined
    - A non-mandatory requirement is that the reactor design must be licensable in the country of origin.

IRIDM: RHR Isolation Concern (2/7)

3. Inputs to RIDM (Cont.)

- Insights from deterministic analysis
  - **Defence-in-depth**
    - ✓ Compliance with the defence-in-depth concept was justified for all options under consideration.
  - **Safety margins**
    - ✓ No change to the safety margins for all options
  - **Other deterministic criteria**
    - ✓ No other deterministic criteria are violated (fail-safe design, single failure criteria, redundancy, diversity, etc.) Note: the two motorised valves are powered by different electrical supplies

IRIDM: RHR Isolation Concern (3/7)

3. Inputs to RIDM (Cont.)

- Insights from the probabilistic analysis
  - Quantitative insights
    - ✓ **For Option 1** the PSA showed that the use of RHR MOV leakage data based on data derived from actual experience would result in a higher ILOCA frequency which in turn would not allow the design CDF and LERF to be met
    - ✓ **For Option 2** the ILOCA frequency was reduced such that the design CDF and LERF would be met
    - ✓ **For Option 3** the ILOCA frequency was slightly reduced as the SRV discharge would no longer outside of the containment. The possibility of other RHR component leakage still remains, however the design CDF and LERF might be met
    - ✓ **For Option 4** the ILOCA frequency remains unchanged, however the leakage would be detectable and the leak can be isolated and the VLOCA terminated. The design CDF and LERF would be met
  - **PSA Quality**
    - ✓ Internal review accepted the quality and level of detail of the PSA and the supporting data to be sufficient for the decision

IRIDM: RHR Isolation Concern (4/7)

3. Inputs to RIDM (Cont.)

- Other factors that have been considered and have been estimated
  - **Equipment qualification**
    - ✓ **Option 1:** No changes to the periodicity of preventive maintenance of equipment
    - ✓ **Option 2:** Increase in preventive maintenance and inspection due to change to SC1
    - ✓ **Option 3:** SRV maintenance could only be perform during outage when containment is open
    - ✓ **Option 4:** Increased maintenance due to additional isolation valve
  - **Electricity production**
    - ✓ **Option 1:** No change to electrical production
    - ✓ **Option 2:** Longer outage time due to increased maintenance of SC1, slight decrease in electrical production
    - ✓ **Option 3:** Slightly longer outage time due to SRV maintenance inside containment, electrical production unlikely to be effected
    - ✓ **Option 4:** Slightly longer outage time due to additional valve maintenance, electrical production unlikely to be effected
  - **Maintenance costs**
    - ✓ **Option 1:** No change to maintenance costs
    - ✓ **Option 2:** Large increase in maintenance cost due to complete RHR now being a SC1 system
    - ✓ **Option 3:** Small increase in maintenance cost due to SRV maintenance inside containment
    - ✓ **Option 4:** Small increase in maintenance cost due to additional valve maintenance
  - **Radiation doses for workers**
    - ✓ **Option 1:** No change to radiation dose
    - ✓ **Option 2:** Large increase in radiation dose due to greater maintenance and testing requirements of a SC1 system
    - ✓ **Option 3:** Small increase in radiation dose due to increased work inside containment
    - ✓ **Option 4:** Small increase in radiation dose due to additional valve maintenance

IRIDM: RHR Isolation Concern (5/7)

3. Inputs to RIDM (Cont.)

- Other factors that have been considered and have been estimated
  - **Regulatory Acceptance**
    - ✓ **Option 1:** Unlikely to be accepted by regulator, cost of modifying design to met regulatory approval likely to be significant
    - ✓ **Option 2:** Most likely to be accepted by regulator
    - ✓ **Option 3:** Unlikely to be accepted by regulator, cost of modifying design to met regulatory approval likely to be significant
    - ✓ **Option 4:** Likely to be accepted by regulator
  - **Equipment and installation costs**
    - ✓ **Option 1:** No change to equipment and installation costs
    - ✓ **Option 2:** Significant increase in equipment and installation costs due to complete RHR now being a SC1 system
    - ✓ **Option 3:** Small increase in installation costs due to SRV now inside containment, cost offset as SRV relief tank no longer needed
    - ✓ **Option 4:** Small increase in equipment and installation costs due to additional valve and shielding

IRIDM: RHR Isolation Concern (6/7)

4. Weighting the inputs from the assessments carried out

- Weighting the inputs from the evaluations
  - The IRIDM team then defined weighting factors for the above inputs based on expert judgment:
    - **Weights from 0 to 10 assigned based on importance perceived by IRIDM team**
    - **Impacts were assigned 1 to 7 with 4 being no change, 1-3 – negative impact, 5-7 positive impact.**
- The lists of factors and their weights are shown for each Option on next slide

IRIDM: RHR Isolation Concern (7/7)

The list of factors and their weights (for Option 1)		
Factor	**Weight (W) (0-10)**	**Impact (I) (1-7, 4 – no change from existing case i.e. Option 4)**
Mandatory requirements	**High (10)**	**4**
Defence-in-depth	**High (10)**	**4**
Safety Margins	**Medium (3)**	**3**
Risk changes	**Medium (3)**	**5**
Equipment qualification	**Medium (3)**	**4**
Electricity production.	**High (10)**	**5**
Maintenance costs	**Low (1)**	**2**
Radiation doses for workers	**Medium (3)**	**3**
Overall score = Sum (W*I)	**177 Normalized: 1.03**	

References

- Development and Application of Level-1 PSA, IAEA Safety Standards Series, SSG-3, IAEA Vienna (2010).
- Development and Application of Level-2 PSA, IAEA Safety Standards Series, SSG-4, IAEA Vienna (2010).
- Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants , IAEA-TECDOC-1804, IAEA, Vienna (2016)


Thank you for your attention
Questions?