Vysus Group

An Approach to Assessment of Reliability of Passive Safety Systems

Ingenuity.
Imagination.
Insight.

Sergey Galushin[1*], Graeme Trundle[2], Manorma Kumar[1], Anders Olsson[1]
[1]Vysus Group,
[2]Royal Institute of Technology (KTH)

Context

Passive Safety Systems Reliability is Hard to Quantify

Advanced reactor designs increasingly rely on passive safety systems - but their small, physics-driven forces make performance sensitive to uncertainty, and there is no industry-standard method to quantify their reliability.

Low-Magnitude Driving Forces
Natural circulation, gravity, and pressure differentials replace pumps and active control - increasing sensitivity to boundary conditions.

No Established Data Pool
Active components draw on decades of operational reliability data. No passive analog exists, so assessment must be design- and scenario-specific.

Three Open Challenges
Uncertainty, parameter dependencies, and non-binary success/failure states all complicate integration into standard PSA models.

Four Categories of Passivity (IAEA-TECDOC-1752)

Passive components are classified into four categories based on their level of passivity and internal complexity [IAEA TECDOC-1752]:

A. Fully Static. No signal, no power, no moving parts, no moving fluid.

B. Moving Fluid Only. No mechanical parts but working fluid moves once activated by thermal-hydraulic conditions.

C. Moving Mechanical Parts. Internal imbalances (e.g., static or hydrostatic pressure) drive mechanical motion.

D. Intermediate Zone. Passive execution as above, but without internal intelligence to initiate the process.

Categories B, C, and D rely on physical processes such as natural circulation, pressure-driven flows, or internal mechanical responses.

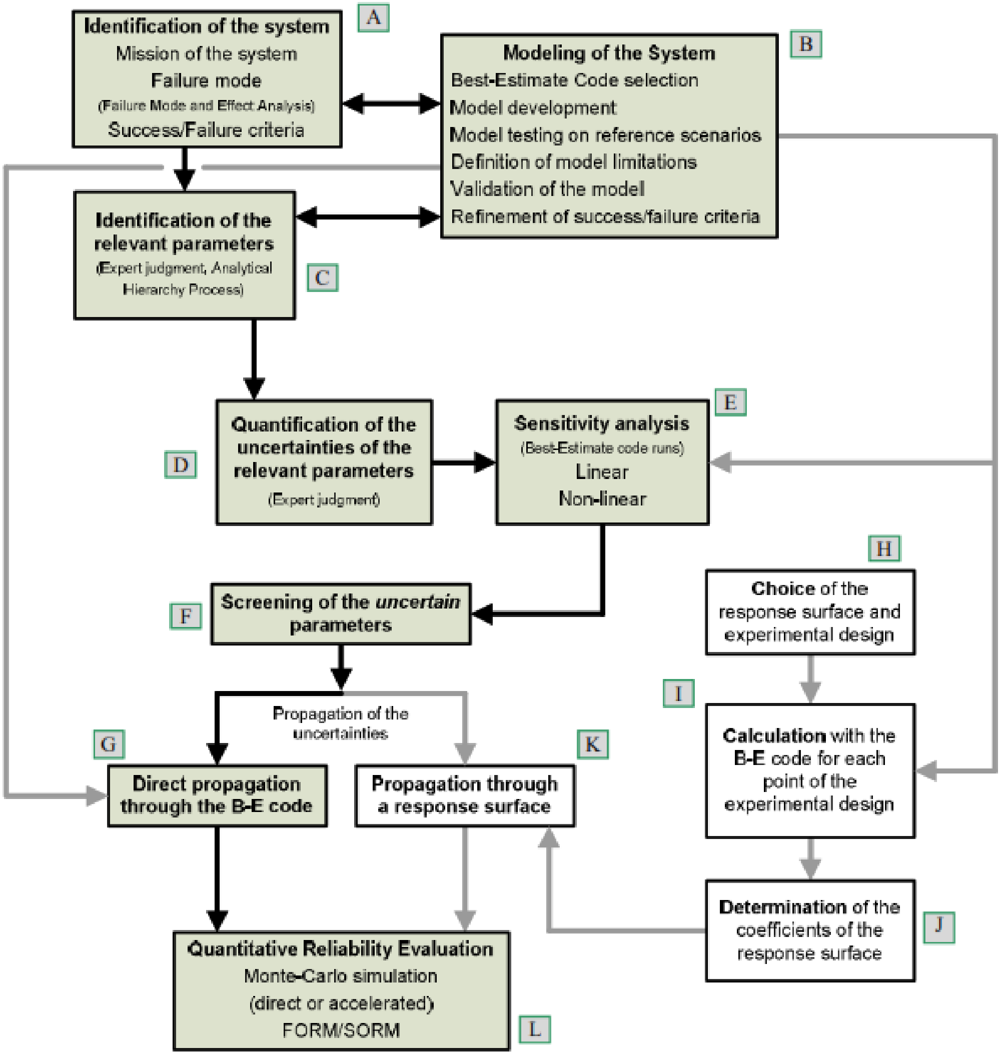
Three Open Issues in Passive System Reliability

- Uncertainties
  - Reliability is difficult to quantify due to uncertainty in the thermal-hydraulic phenomena driving the system.
- Dependencies
  - Critical parameters influencing natural driving forces may not be statistically independent - treating them as such may overestimate the reliability.
- Integration
  - Behavior often does not conform to binary success/failure logic, complicating integration into traditional event/fault tree PSA models.

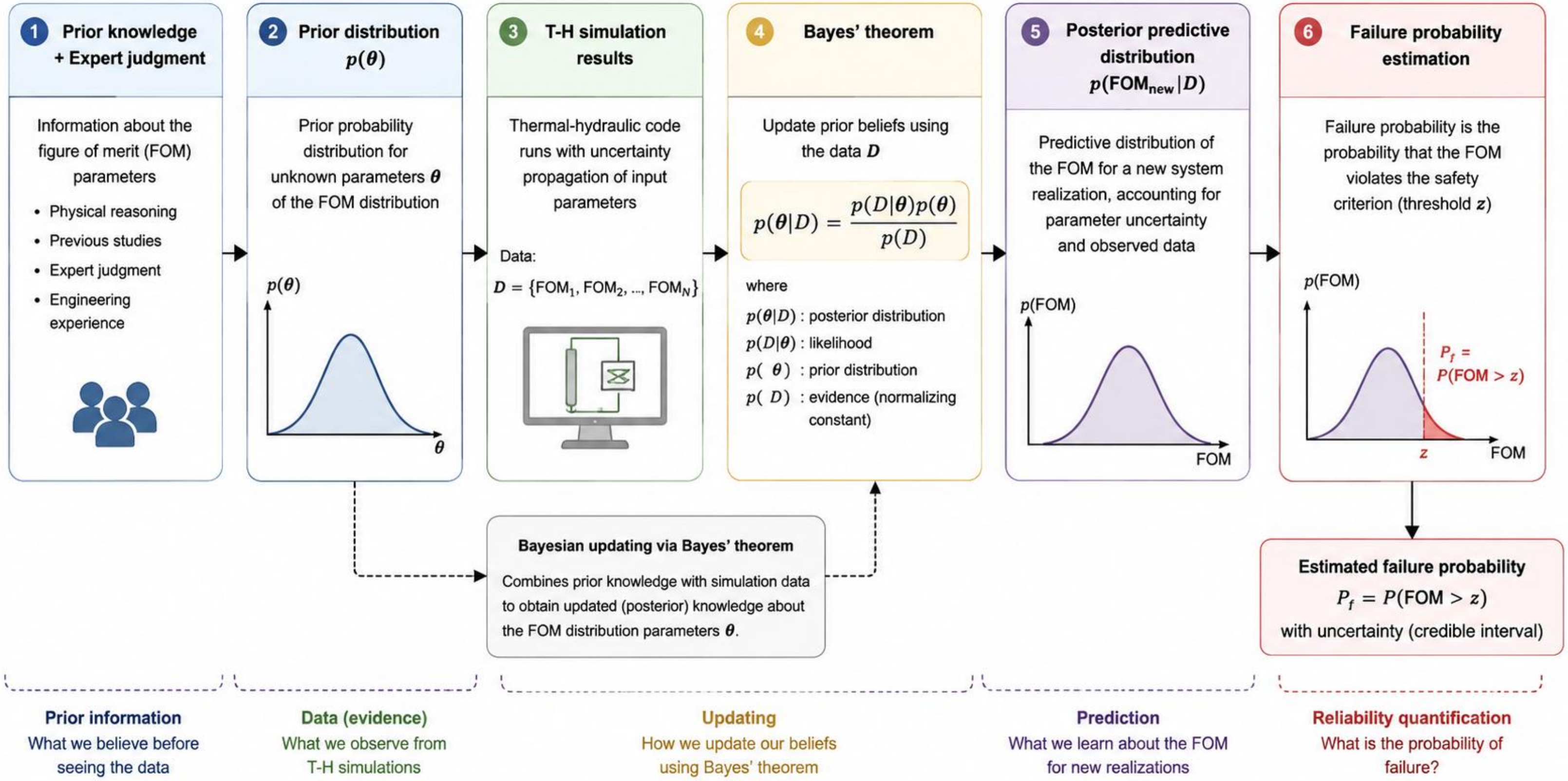
RMPS Methodology

RMPS Steps:

- Accident scenario definition
- System characterization
- System modeling and identification of uncertainties
- Uncertainty characterization
- Sensitivity analysis
- Reliability evaluation
    - MC Simulation
    - FORM/SORM
    - Surrogate Models
    - Bayesian Estimation



Bayesian Estimation

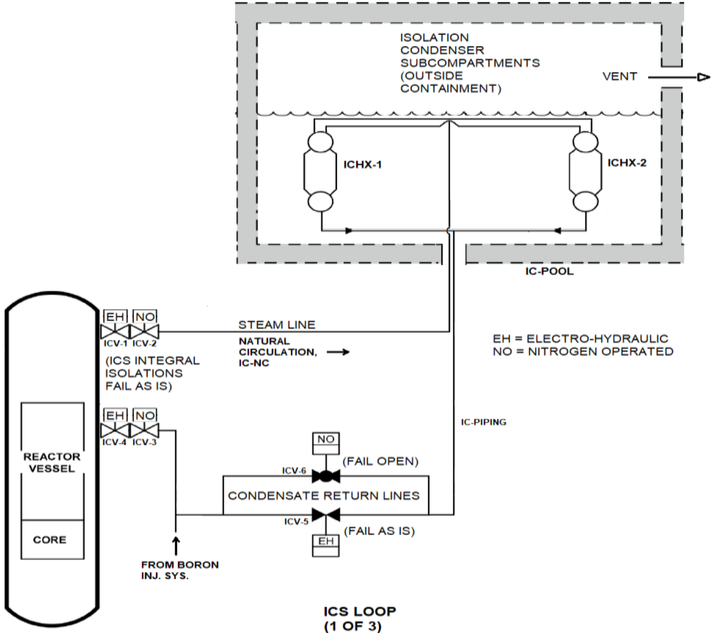


Demonstrating the Approach: the BWRX-300 ICS

The methodology is applied to the Isolation Condenser System (ICS) of the BWRX-300 small modular reactor - a passive system providing decay heat removal and RPV over-pressure protection.

- Safety Function: Decay heat removal on loss of normal heat sink, and RPV isolation, plus over-pressure protection.

- Redundancy: Three identical loops; success requires only one of three (1-of-3) loops to operate.



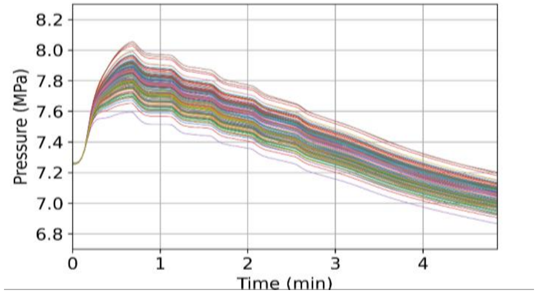
Thermal-Hydraulic Simulations

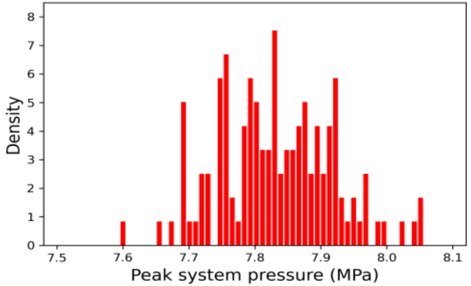
- A TRACE model of the BWRX-300 was developed to simulate a transient that leads to a reactor trip with ICS actuation.
  - 130 iterations were run (Wilks' method (DAKOTA) for 95% tolerance/99% confidence)
- Acceptance Criteria:
  - RPV pressure remains below 150% of the design pressure, 15.45 MPa.
  - Peak cladding temperature is maintained below 1204 C.

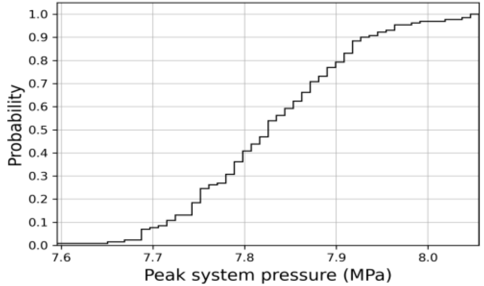
Parameter	**Distribution**
Gas gap thermal conductivity	Normal ($\mu = 1.0$, $\sigma = 0.102043$), scaling factor
Fuel thermal conductivity	
Cladding thermal conductivity	
Fuel specific heat capacity	
Cladding specific heat capacity	

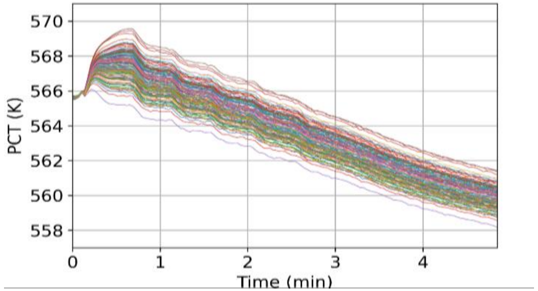
Results

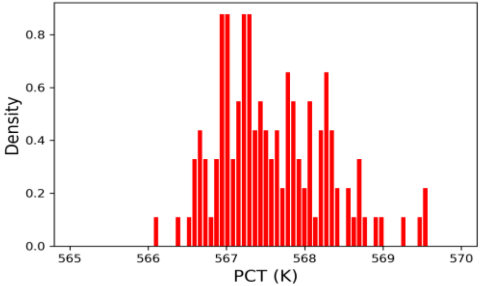
Parameter	Normal Dist. Parameters (μ, σ)
Peak system pressure	(7.8328 MPa, 87.5 kPa)
Peak cladding temperature	(567.59 K, 0.70 K)

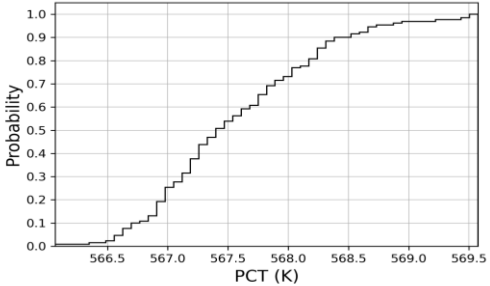






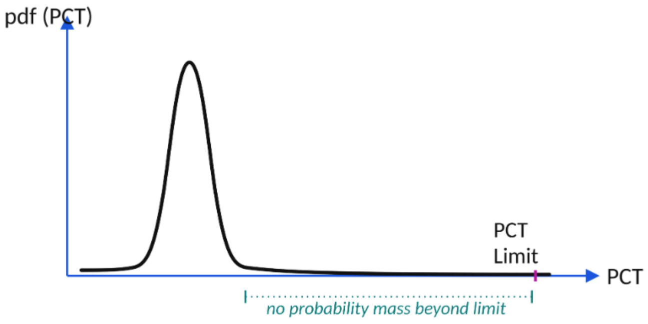






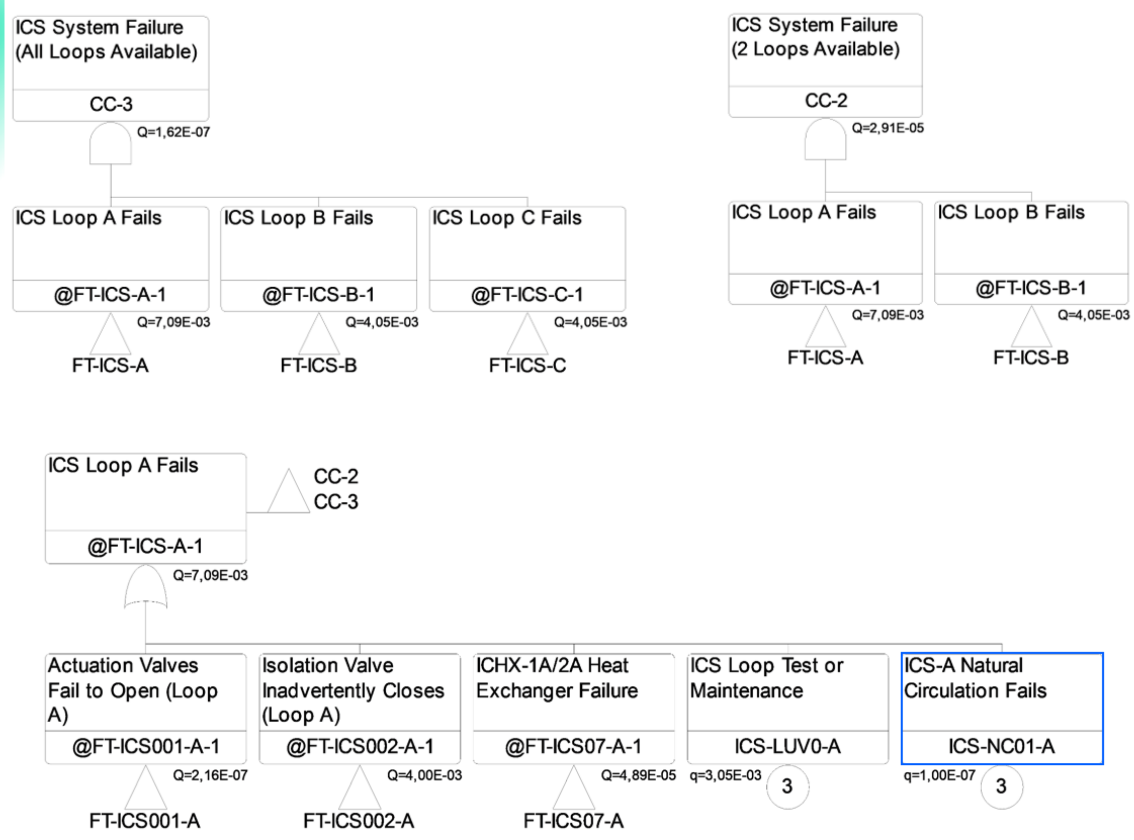
Quantifying Natural Circulation Failure Probability

- Six model variants (Normal, Log-Normal, and Gamma distributions, each with non-informative and weakly-informative priors) were fit via MCMC
  - In every case, the estimated failure probability was effectively zero.



- The complexity of natural circulation, together with the limited scope of parameters considered, means residual uncertainty in natural circulation cannot be ignored.
- As a result, assigning a probability of exactly zero to natural circulation as a failure mode is not appropriate.
- To account for residual uncertainty a failure probability of 1.0E-07 is therefore adopted.

Isolation Condenser System Unavailability



Loops Available	Unavailability, Q
CC-3	1.62E-07
CC-2	2.91E-05

- Natural circulation unavailability was integrated into an ICS fault tree as a basic event using Failure Mode & Effect Analysis (FMEA) with RiskSpectrum software.
- System unavailability was calculated for case where all three loops are available (CC-3) as well as when only two loops are available (CC-2).
- CC-2 used exclusively for event tree analysis of ICS Line Break initiating event in accompanying PSA.
- All three loops considered identical, except only Loop A contains 'ICS Loop Test or Maintenance' basic event.

Isolation Condenser System Unavailability

- For ESBWR ICS (broadly equivalent design), $Q = 2.13\text{E-}03$.
- ESBWR requires 2 of 4 loops operational for success, vice BWRX-300s 1 of 3.
- Unavailability due to 'Loop test or maintenance' basic event has decreased from 3.84E-02 to 3.05E-03 (NUREG/CR-6928 2020 Update)

Loops Available	Unavailability, $\boldsymbol{Q}$
CC-3	1.62E-07
CC-2	2.91E-05

	Cutset	Contribution (%)
CC-3	Common cause failure of all heat exchangers	34.75
	Spurious isolation of all loops due to isolation valve signal failure	34.56
	Spurious isolation of two loops due to isolation valve signal failure with remaining loop in test or maintenance	26.08
CC-2	Spurious isolation of both loops due to isolation valve signal failure	54.88
	Spurious isolation of a loop due to isolation valve signal failure with remaining loop in test or maintenance	41.88

CC-3: Three loops available
CC-2: Two loops available

Core Damage Frequency Analysis

- Level 1 PSA performed, involving analysis of initiating events, event tree analysis, and FMEA of safety systems
- Credit only taken for passive safety features (no human action, no connection to electrical grid)
- **Final Result:** CDF = 1.23E-07 yr^{-1}
- Simplified sensitivity analysis shows that a 100-fold increase of natural circulation failure probability increases CDF by only 0.41%

Initiating Event	Component Failures	Frequency (yr^{-1})	Contribution (%)	# of Cutsets
Transient	CCF of All ICS HXs	4.23E-08	34.45	1
Transient	Spurious isolation of all ICS loops due to isolation valve signal failure	4.17E-08	33.98	64
Transient	Spurious isolation of 2 ICS loops due to signal failure, remaining ICS loop in test or maintenance	3.18E-08	25.92	16
Transient	CCF of HXs in 2 ICS loops, remaining ICS loop in test or maintenance	7.16E-10	0.58	4
Transient	CCF of HXs in 2 ICS loops, spurious isolation of remaining ICS loop due to isolation valve signal failure	4.70E-10	0.38	8
Transient	ATWS with BIS check valve failure	2.60E-10	0.21	2
LOCA	Mechanical failure of RPVIVs	1.68E-10	0.14	2
Transient	ATWS with spurious closure of BIS AOVs	1.21E-10	0.10	2
RPVR	Vessel rupture	1.00E-10	0.08	1

Conclusions

Key Findings

- **RMPS** successfully quantified the reliability of the passive Isolation Condenser System and enabled its integration into a **Level-1 PSA**.
- The **BWRX-300 ICS** demonstrated robust passive performance, with a conservative natural circulation failure probability of **1.0×10^{-7}**.
- **TRACE constitutive correlation uncertainties** had only a marginal impact on ICS performance, and overall plant risk was weakly sensitive to passive natural circulation uncertainty.
- The proposed methodology provides a practical framework for reliability assessment of **future SMRs and advanced passive reactor designs**.

Lessons Learned

- Numerical stability remains challenging for simulations involving **large naturally convecting volumes**, wide uncertainty ranges, and long transient analyses.
- Accurate **heat transfer boundary conditions** are critical for predicting the transition between short- and long-term passive cooling performance.

Manorma Kumar

Principal Consultant | Operations Manager – Nuclear USA,

M: +1 (630) 300 8926 |

E: manorma.kumar@vysusgroup.com

Thank you