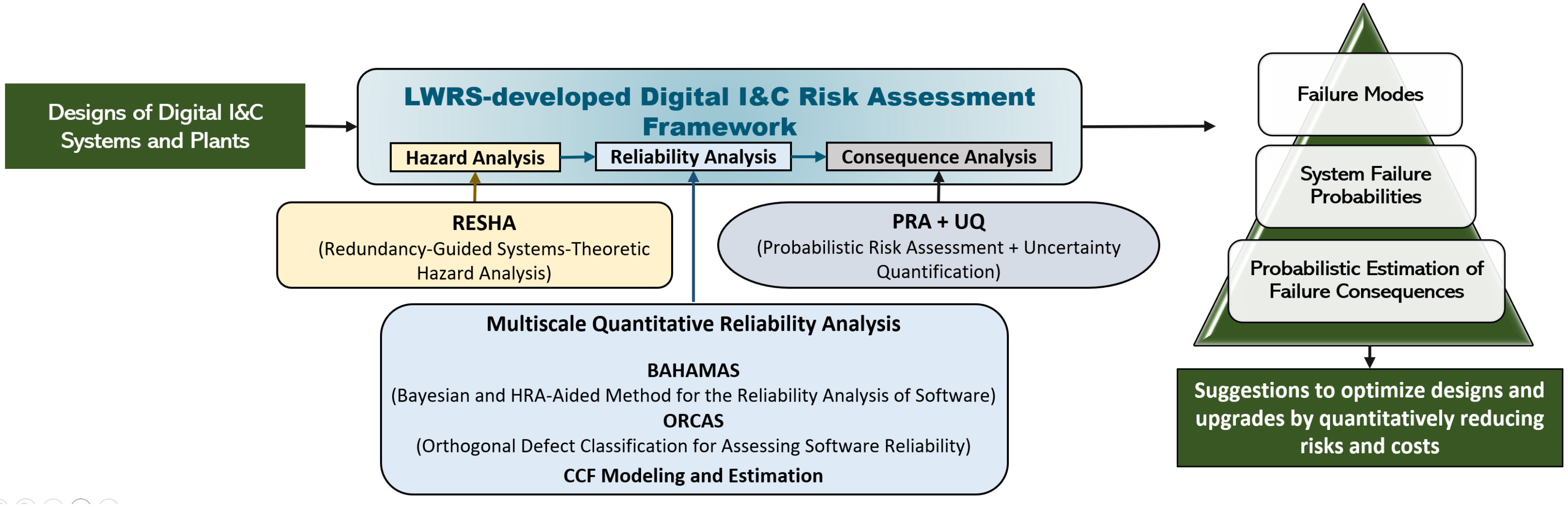
Assessing Digital Human-System Interfaces Based on RESHA and Human Reliability Analysis

Jooyoung Park

11/13/2024

1. Introduction

- **Digital I & C Risk Assessment Project**
  - Supported by the Risk Informed Systems Analysis (RISA) Pathway of the Department of Energy (DOE) Light Water Reactor Sustainability (LWRS) program
  - Offer a capability of design architecture evaluation of various digital I&C (DI&C) systems to support system design decisions on diversity and redundancy applications
  - Develop systematic and risk-informed tools to address common cause failures (CCFs) and quantify corresponding failure probabilities for DI&C technologies
  - Support and supplement existing risk-informed DI&C design guides by providing quantitative risk-informed and performance-based evidence
  - Reduce uncertainty in risk/cost and support integration of DI&C systems at nuclear power plants



1. Introduction

- **Goal**
  - Development of An Advanced Risk Analysis Method Especially for Human-System Interface (HSI) of DI&C Systems

- **Contents**
  - Evaluation of HSIs in risk assessment
  - Approach to evaluating HSI for DI&C systems
  - Feasibility of the approach based on the APR1400 DI&C systems and a reactor trip system (RTS) fault tree of generic pressurized water reactor (GPWR) probabilistic risk assessment (PRA) model

2. Evaluation of HSIs in Risk Assessment

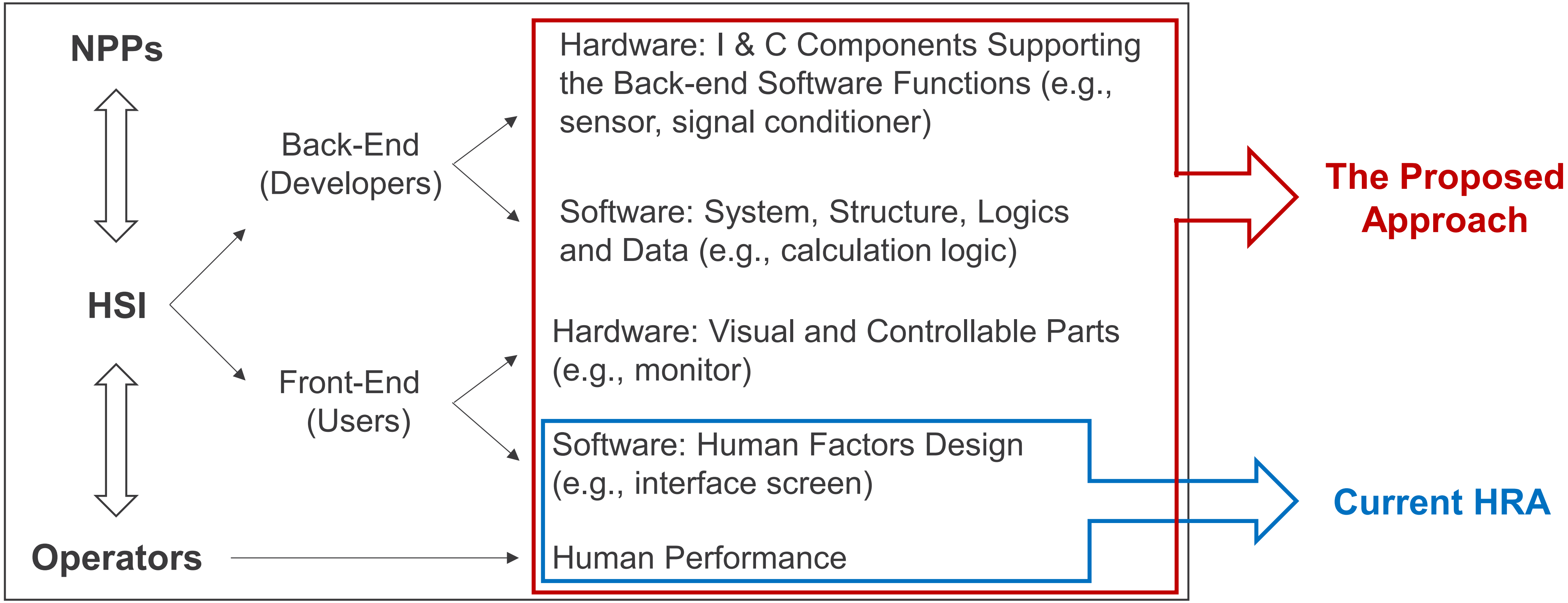
- **HSI Evaluation in Human Reliability Analysis (HRA)**
  - Use of performance shaping factor (PSF) concept
    - Any factors that influence human performance such as HSI, experience, or complexity
    - Used for highlighting error contributors and adjusting human error probabilities (HEPs) in HRA

HRA Method	PSF	PSF Level	PSF Multiplier
Standardized Plant Analysis Risk HRA (SPAR-H)	Ergonomics/HSI	Missing/misleading	50
		Poor	10
		Nominal	1
		Good	0.5

- **Current Status of HSI Evaluation in HRA**
  - The current HSI evaluation in HRA only concentrates on the relationship between HSI designs and human performance.
  - It rarely reflects the unique characteristics of HSI systems, but instead mainly focuses on the specific or overall qualities of the HSIs themselves.
  - HSI failure or degradation due to software/hardware issues during scenarios have not considered when conducting HRA.

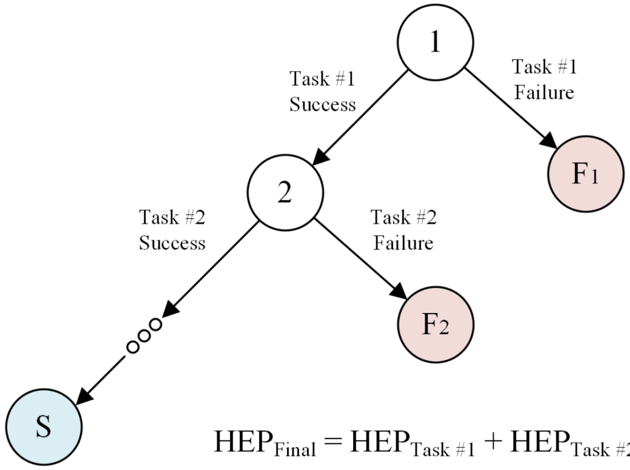
3. Approach to Evaluating HSI for DI&C Systems

- **Extension of HSI Evaluation Categories**

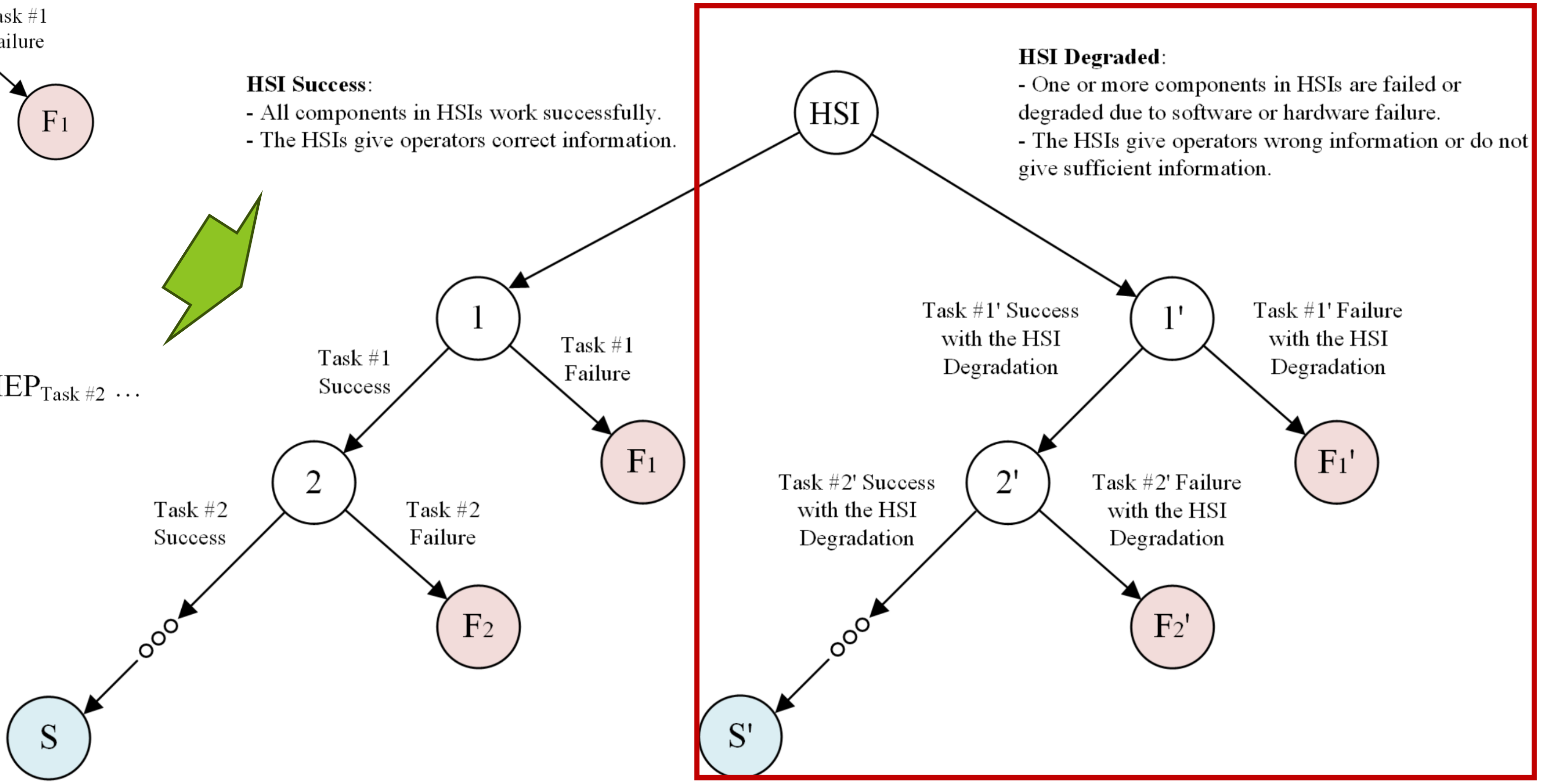


3. Approach to Evaluating HSI for DI&C Systems

- **Extension of HRA Event Tree**



$$HEP_{Final} = HEP_{Task\ \#1} + HEP_{Task\ \#2} \dots$$



$$HEP_{Final} = HEP_{HSI\_Success} + P_{HSI\_Degraded} \cdot HEP_{HSI\_Degraded}$$

$$HEP_{HSI\_Success} = HEP_{Task\ \#1} + HEP_{Task\ \#2} \dots$$

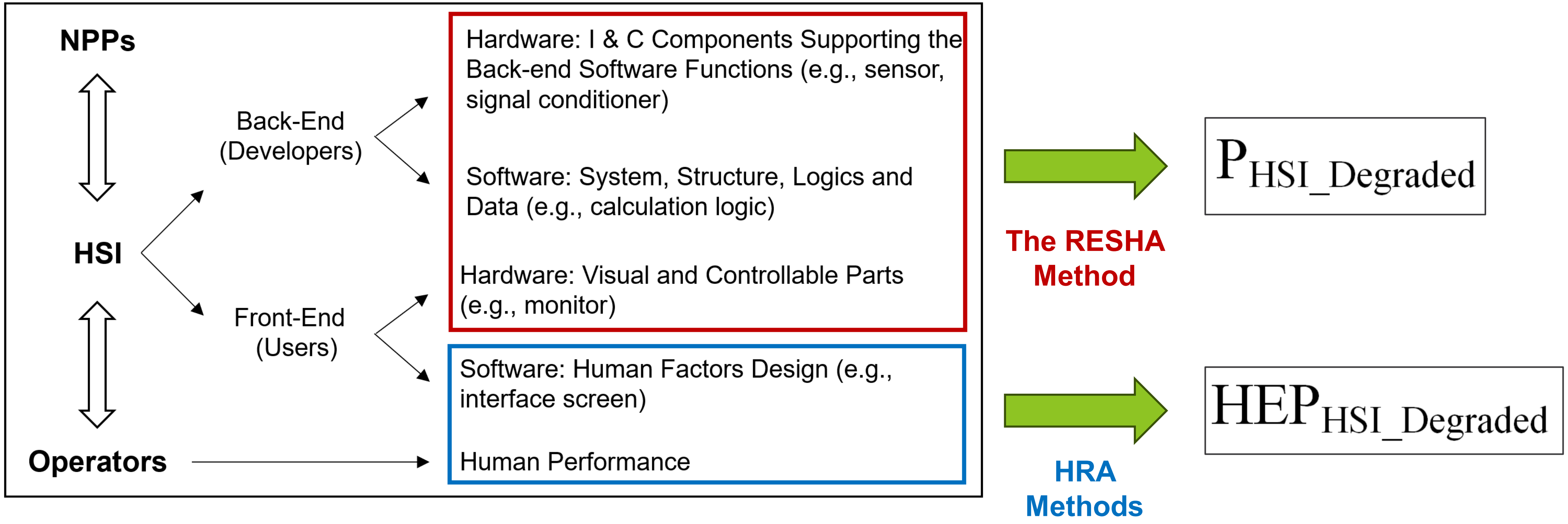
$$HEP_{HSI\_Degraded} = HEP_{Task\ \#1'} + HEP_{Task\ \#2'} \dots$$

LWRS LIGHT WATER REACTOR SUSTAINABILITY

3. Approach to Evaluating HSI for DI&C Systems

- **The Proposed Method**

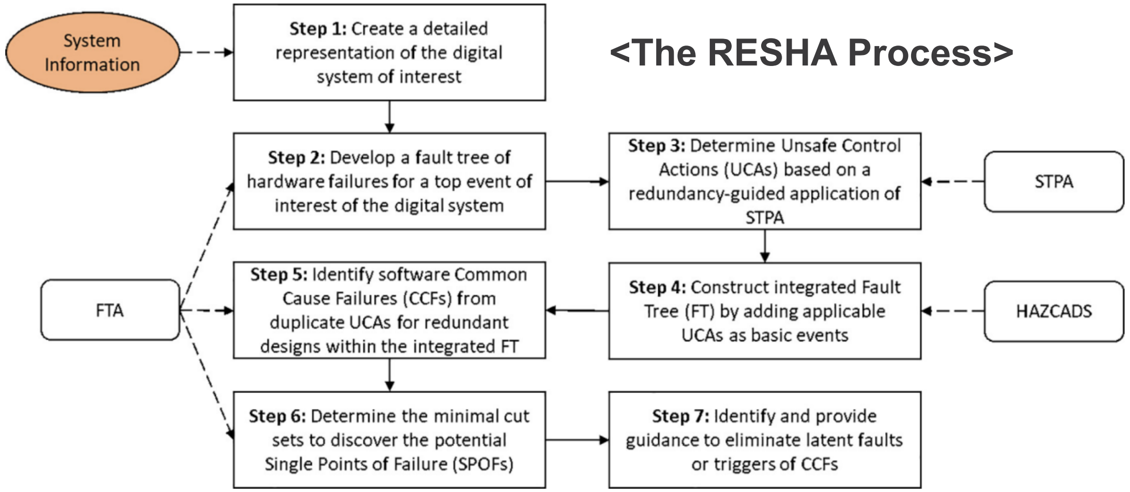
$$P_{HSI\_Failure} = P_{HSI\_Degraded} \cdot HEP_{HSI\_Degraded}$$



3. Approach to Evaluating HSI for DI&C Systems

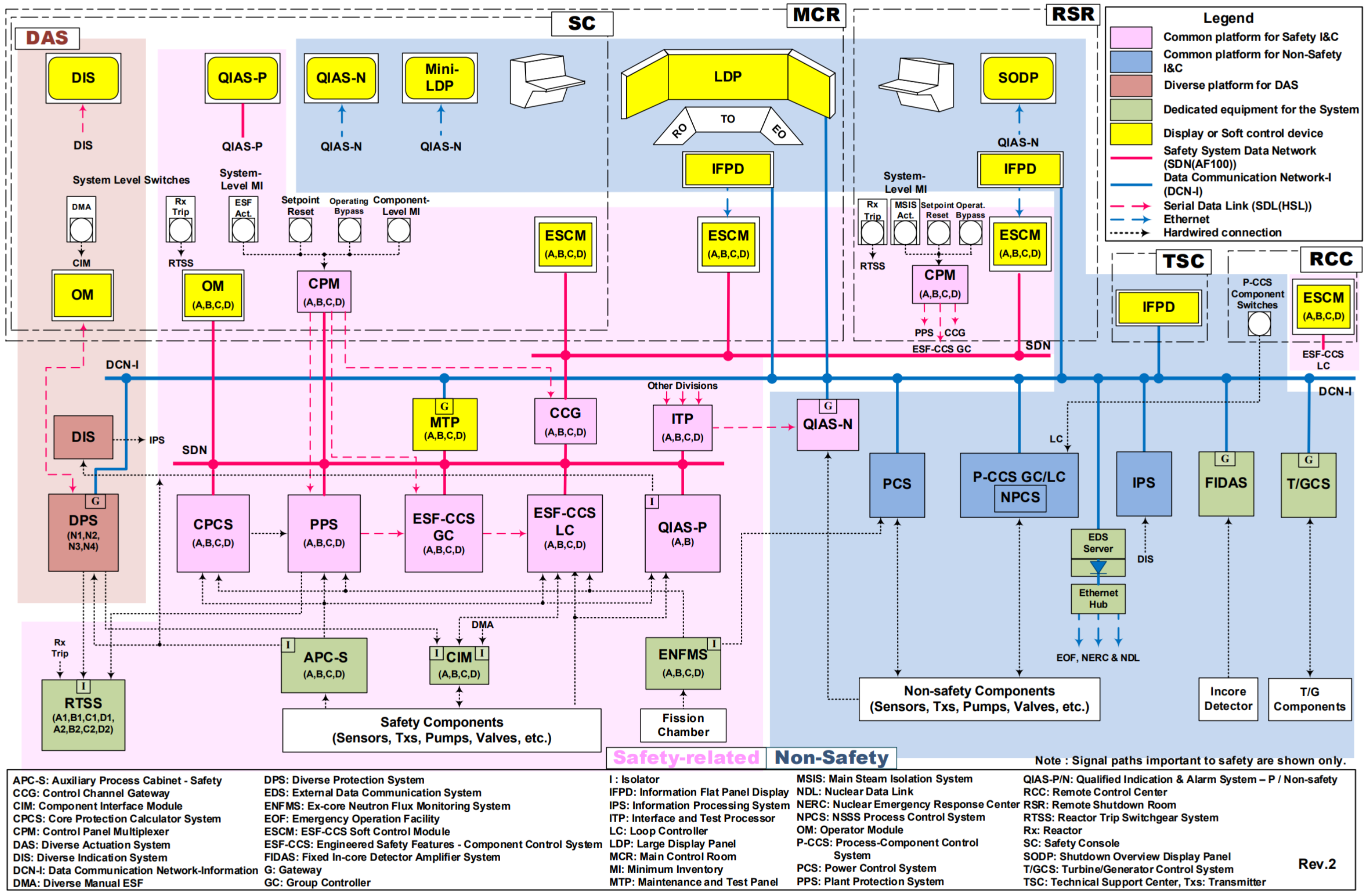
- **The Proposed Method**
  - **Step #1: Development of HSI fault trees based on the Redundancy-guided Systems-theoretic Hazard Analysis (RESHA) method**
    - The RESHA method
      - A method for analyzing DI&C systems with redundancy features
      - Technically developed based on the Fault Tree Analysis (FTA) and Systems-Theoretic Process Analysis (STPA)
  - **Step #2: HRA analysis for human actions under HSI Degradation**
    - Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA)
      - The latest HRA method developed by U.S. NRC
      - Providing many options for specifically evaluating human actions under HSI degradation
  - **Step #3: Integration into PRA models**

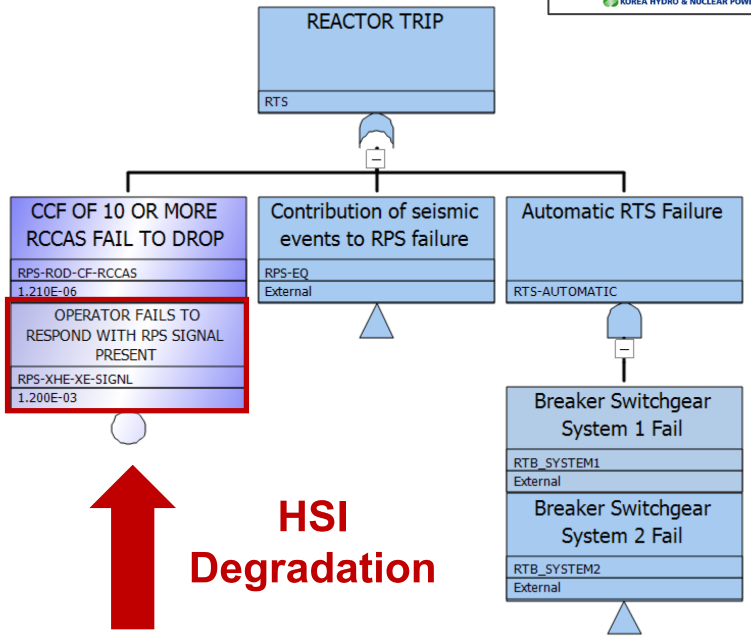
<The RESHA Process>



4. Feasibility of the Approach

- **Assumption**
  - APR1400 DI&C systems prepared for the design certification application to U.S. NRC
  - A RTS fault tree of GPWR PRA model



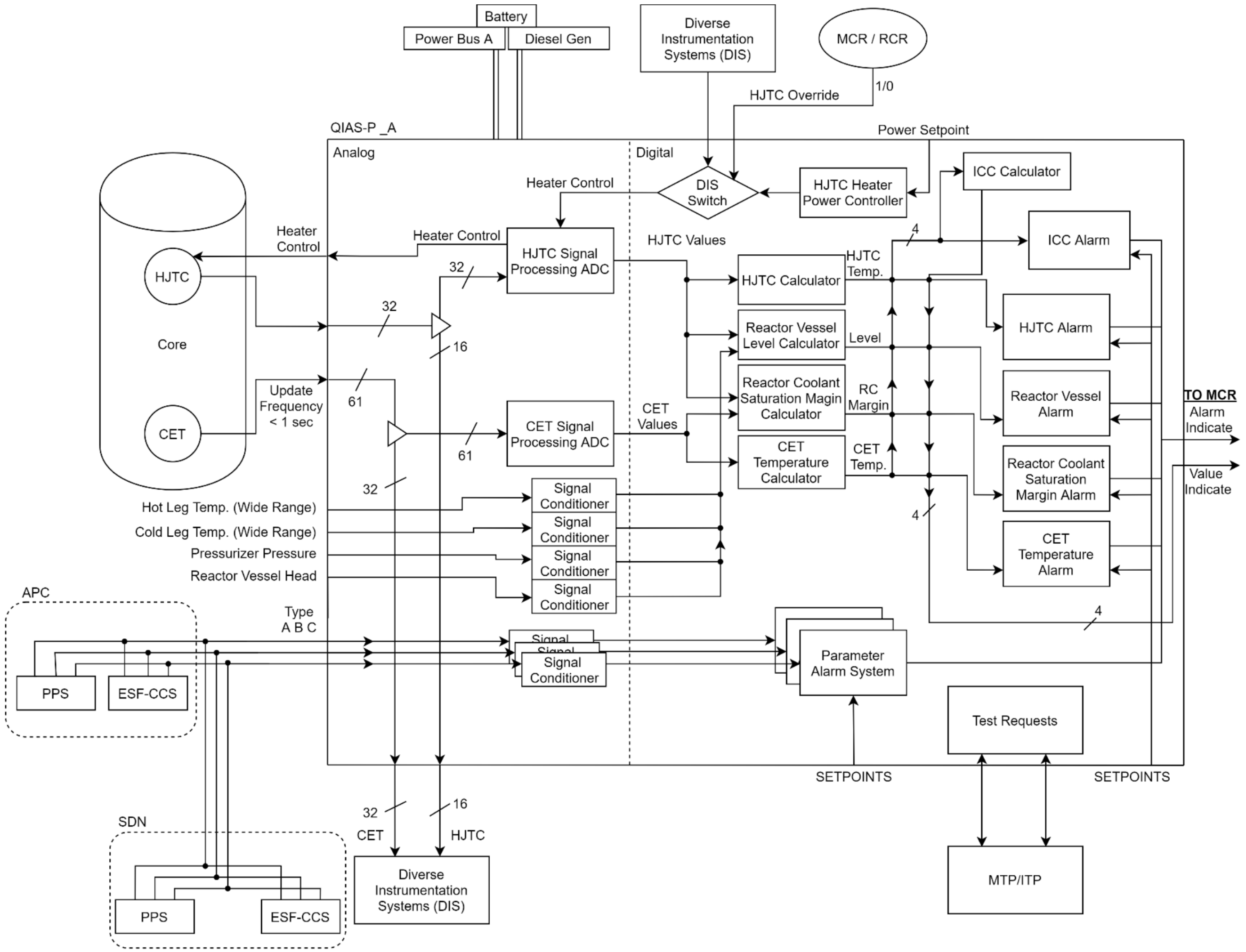


HSI Degradation

- QIAS-P (safety-graded)
- QIAS-N (non-safety-graded)
- IPS (non-safety-graded)

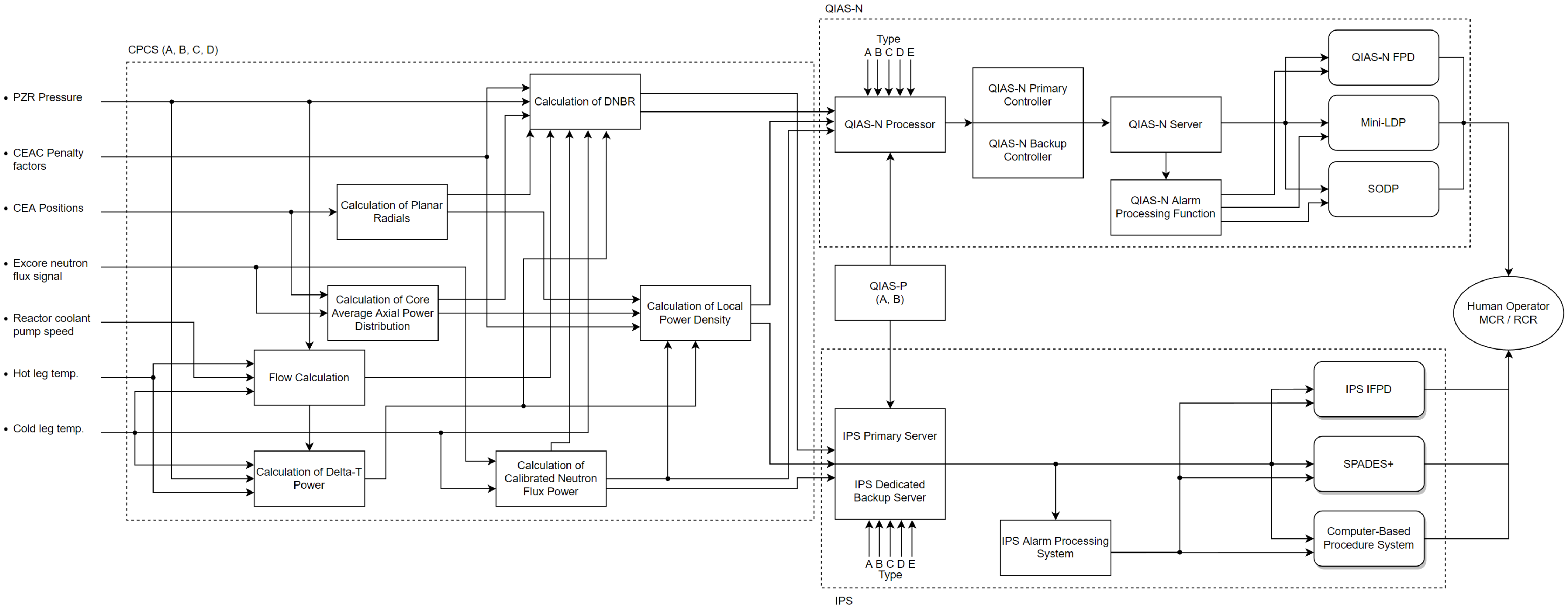
4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - Piping and Instrumentation Diagram (P&ID) for QIAS-P, IPS, and QIAS-N



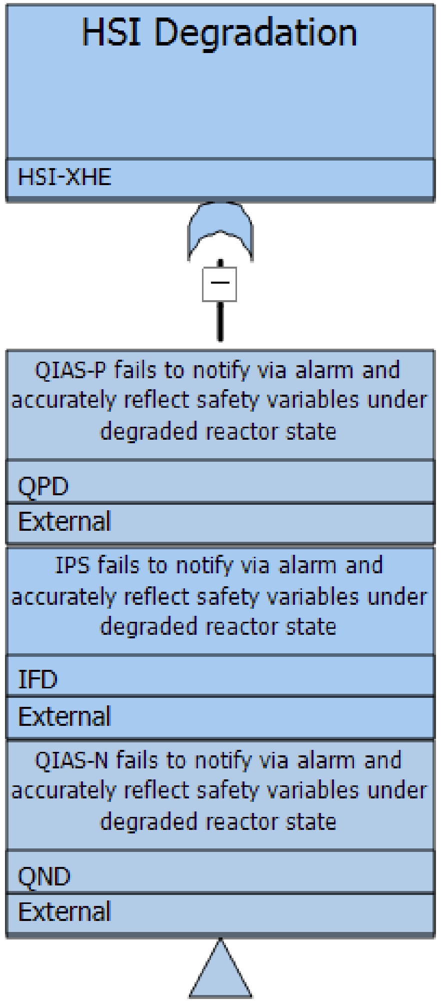
4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - Piping and Instrumentation Diagram (P&ID) for QIAS-P, IPS, and QIAS-N



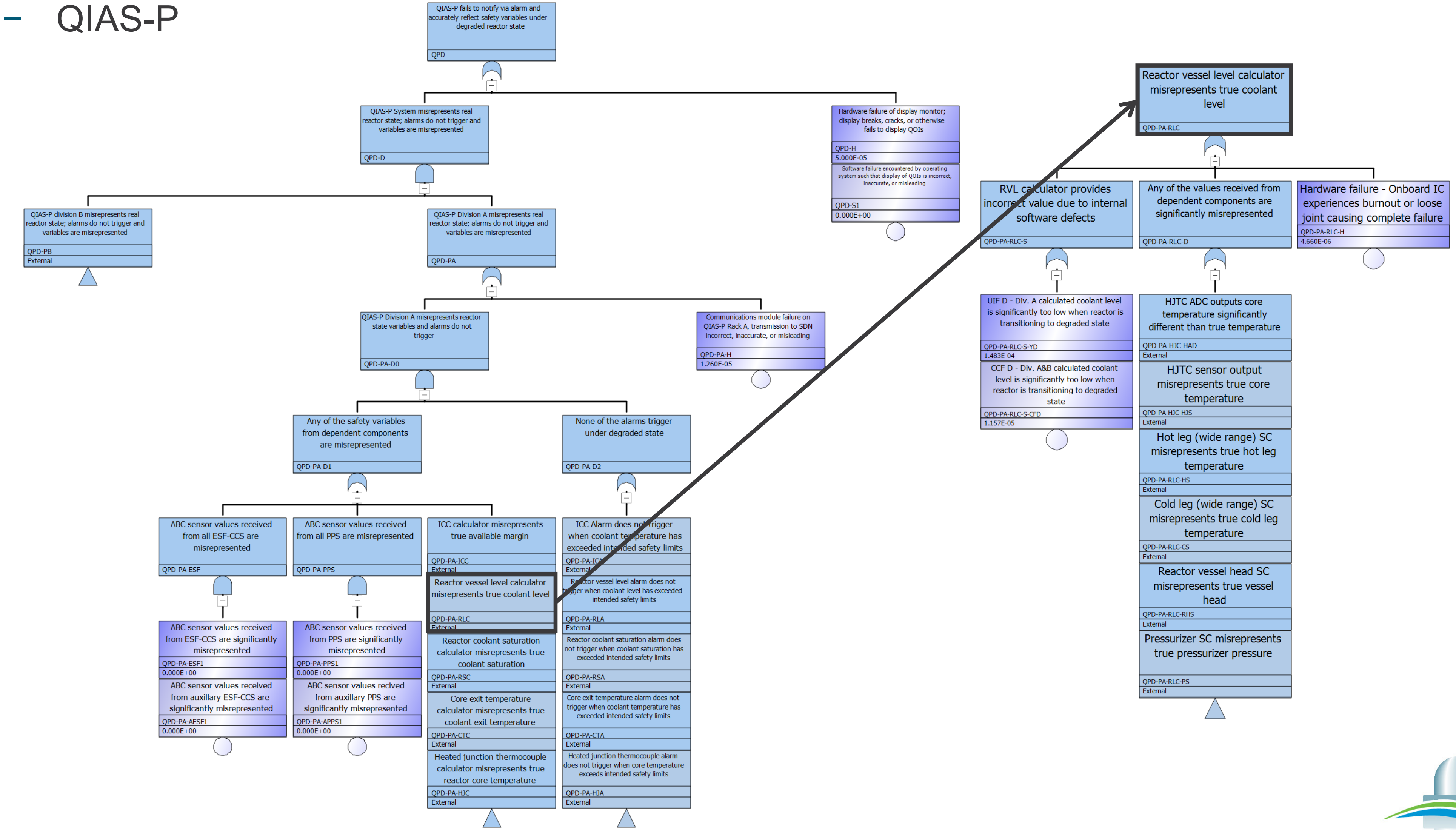
4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - Top Event



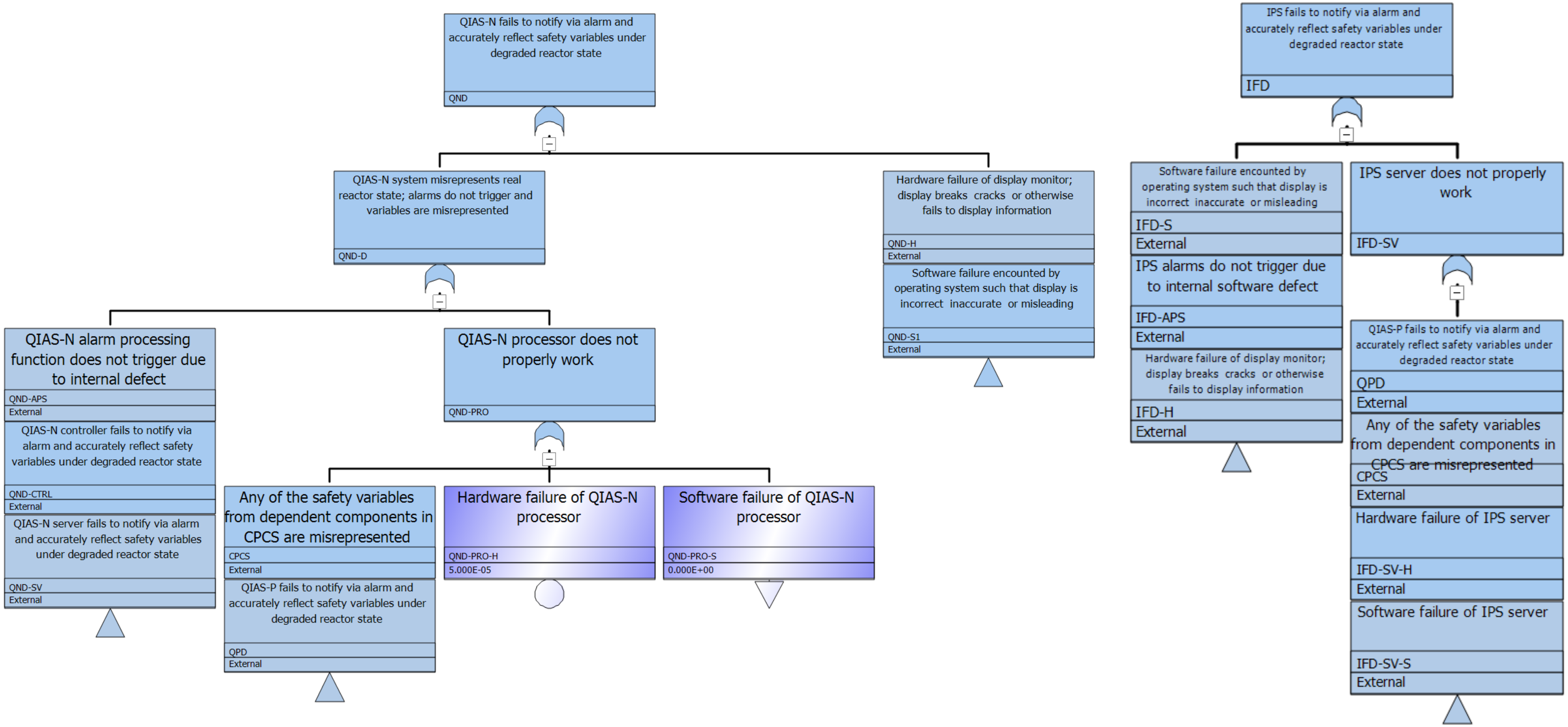
4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - QIAS-P



4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - QIAS-N & IPS



LWRS LIGHT WATER REACTOR SUSTAINABILITY

4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - Hardware failure probabilities
  - Software failure probabilities
  - Common cause failure probabilities

Table 31. Single failure probabilities for UCAs/UIFs for all QIAS-P components.

Component	UCA/UIF	Single Failure Probability
HJTC Controller	UCA A	$2.372 \cdot 10^{-4}$
	UCA F	$1.483 \cdot 10^{-4}$
	UCA G	$1.483 \cdot 10^{-4}$
HJTC Calculator	UIF A	$2.372 \cdot 10^{-4}$
	UIF F	$1.483 \cdot 10^{-4}$
	UIF G	$1.483 \cdot 10^{-4}$
HJTC Alarm	UIF A	$2.372 \cdot 10^{-4}$
	UIF B	$1.483 \cdot 10^{-4}$
ICC Calculator	UIF A	$2.372 \cdot 10^{-4}$
	UIF F	$1.483 \cdot 10^{-4}$
	UIF G	$1.483 \cdot 10^{-4}$
ICC Alarm	UIF A	$2.372 \cdot 10^{-4}$
	UIF B	$1.483 \cdot 10^{-4}$
RVL Calculator	UIF A	$2.372 \cdot 10^{-4}$
	UIF F	$1.483 \cdot 10^{-4}$
	UIF G	$1.483 \cdot 10^{-4}$
RVL Alarm	UIF A	$2.372 \cdot 10^{-4}$
	UIF B	$1.483 \cdot 10^{-4}$
RCS Calculator	UIF A	$2.372 \cdot 10^{-4}$
	UIF F	$1.483 \cdot 10^{-4}$
	UIF G	$1.483 \cdot 10^{-4}$
RCS Alarm	UIF A	$2.372 \cdot 10^{-4}$
	UIF B	$1.483 \cdot 10^{-4}$
CET Calculator	UIF A	$2.372 \cdot 10^{-4}$
	UIF F	$1.483 \cdot 10^{-4}$
	UIF G	$1.483 \cdot 10^{-4}$
CET Alarm	UIF A	$2.372 \cdot 10^{-4}$
	UIF B	$1.483 \cdot 10^{-4}$

Table 33. CCF rates for all QIAS-P components.

Component	CCF	CCF Probability
HJTC Controller	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
HJTC Calculator	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
HJTC Alarm	CCF A	$1.851 \cdot 10^{-5}$
	CCF B	$1.157 \cdot 10^{-5}$
ICC Calculator	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
ICC Alarm	CCF A	$1.851 \cdot 10^{-5}$
	CCF B	$1.157 \cdot 10^{-5}$
RVL Calculator	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
RVL Alarm	CCF A	$1.851 \cdot 10^{-5}$
	CCF B	$1.157 \cdot 10^{-5}$
RCS Calculator	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
RCS Alarm	CCF A	$1.851 \cdot 10^{-5}$
	CCF B	$1.157 \cdot 10^{-5}$
CET Calculator	CCF A	$1.851 \cdot 10^{-5}$
	CCF F	$1.157 \cdot 10^{-5}$
	CCF G	$1.157 \cdot 10^{-5}$
CET Alarm	CCF A	$1.851 \cdot 10^{-5}$
	CCF B	$1.157 \cdot 10^{-5}$

Table 23. Hardware total failure probability for QIAS-P digital components.

Hardware Name	**Failure Probability**
Heated-junction thermocouple sensor	1.05E-07
Heated-junction thermocouple sensor controller	2.21E-06
Core exit thermocouple	1.05E-07
Signal conditioner	1.00E-06
Analog to digital converter	7.13E-06
Parameter calculator	2.21E-06
Parameter alarm	2.21E-06

- Bao, H., Zhang, H., Shorthill, T., & Chen, E. (2021). *Quantitative Risk Analysis of High Safety Significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology* (No. INL/EXT-21-64039-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).
- Bao, H., Lawrence, S., Park, J., Ban, H., Chen, E., Dinh, N., ... & Shorthill, T. (2022). *An Integrated Framework for Risk Assessment of High Safety Significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants: Methodology and Demonstration* (No. INL/RPT-22-68656-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).

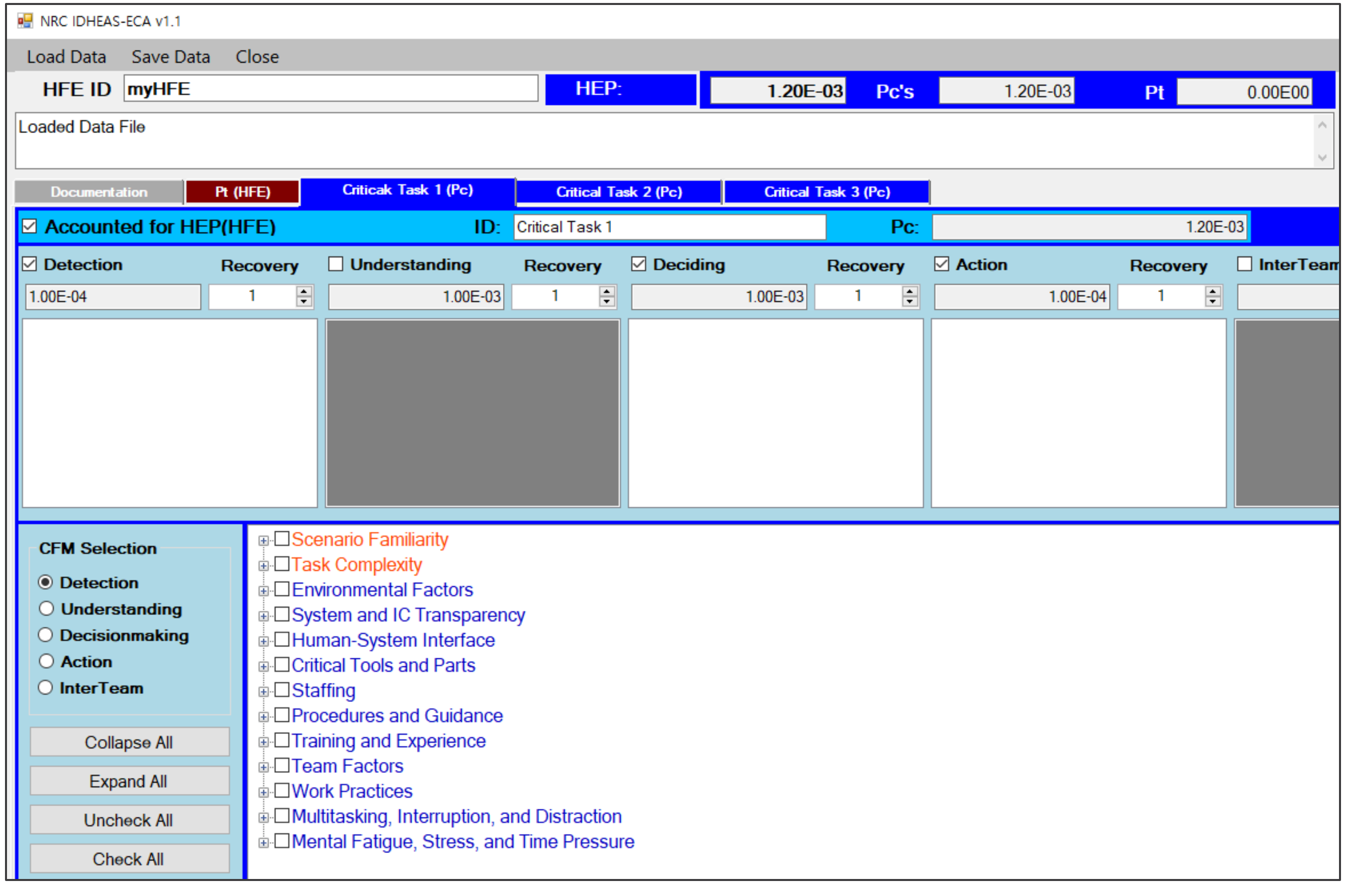
4. Feasibility of the Approach

- **Step #1: Development of HSI fault trees based on the RESHA method**
  - Cutoff: 1.0e-12
  - $\mathbf{P_{HSI\_Degraded} = 9.21e\text{-}4}$

ID	Description	Probability	# of Cutsets
HSI-XHE (Top Event)	HSI degradation	**9.21e-4**	394
QPD	QIAS-P fails to notify via alarm and accurately reflect safety variables under degraded reactor state.	9.66e-5	383
IFD	IPS fails to notify via alarm and accurately reflect safety variables under degraded reactor state.	5.34e-4	389
QND	QIAS-N fails to notify via alarm and accurately reflect safety variables under degraded reactor state.	4.84e-4	388

4. Feasibility of the Approach

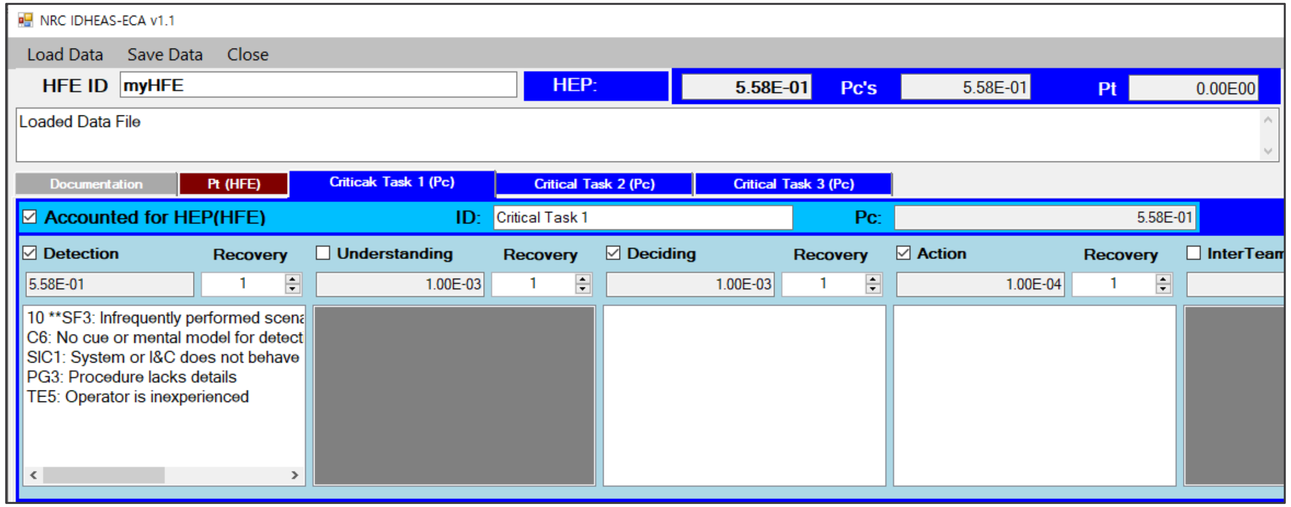
- **Step #2: HRA analysis for human actions under HSI Degradation**
  - Human action: Operator fails to respond with RPS signal present.
  - **$HEP_{HSI\_Success}$ = 1.20e-3**

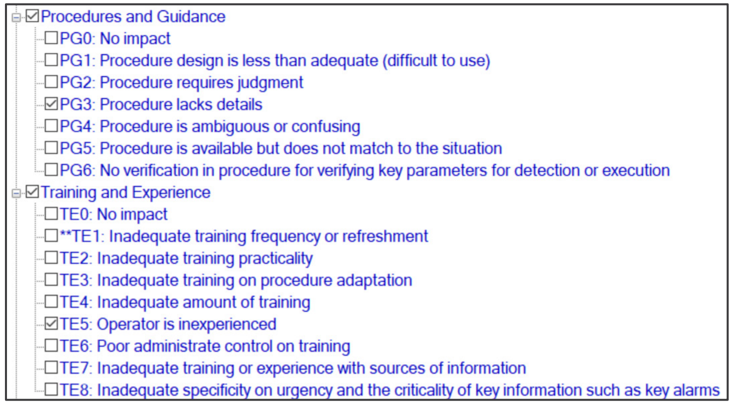


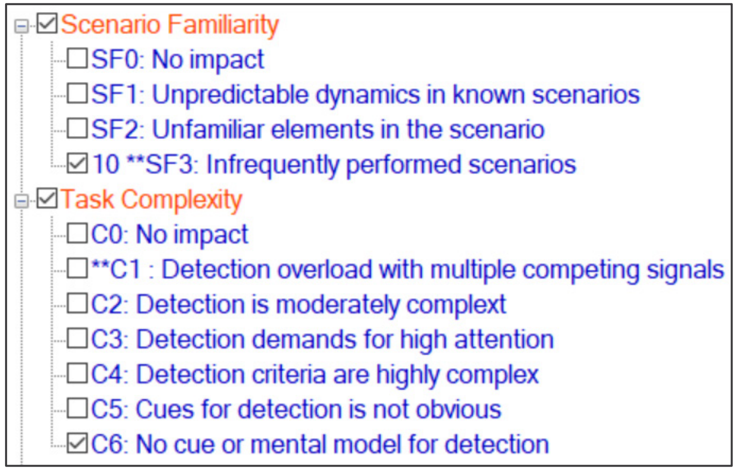
LWRS LIGHT WATER REACTOR SUSTAINABILITY

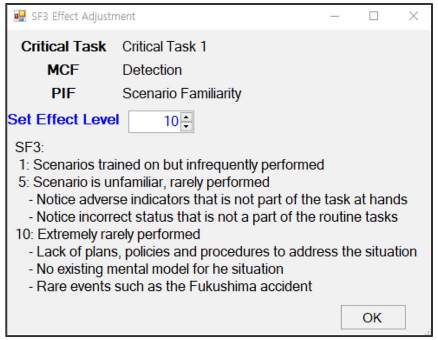
4. Feasibility of the Approach

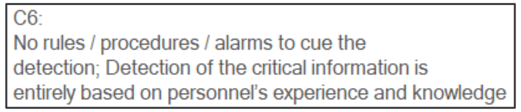
- **Step #2: HRA analysis for human actions under HSI Degradation**
  - $HEP_{HSI\_Degraded} = 5.58e\text{-}1$

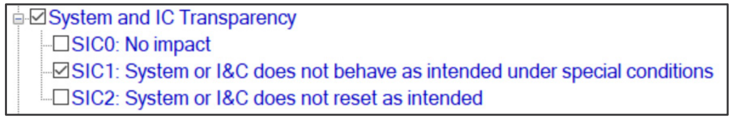


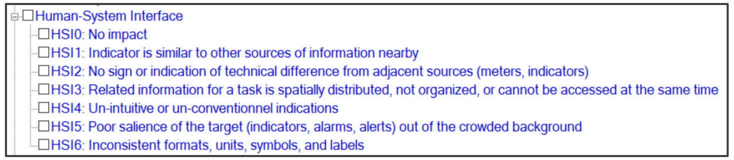












LWRS LIGHT WATER REACTOR SUSTAINABILITY

4. Feasibility of the Approach

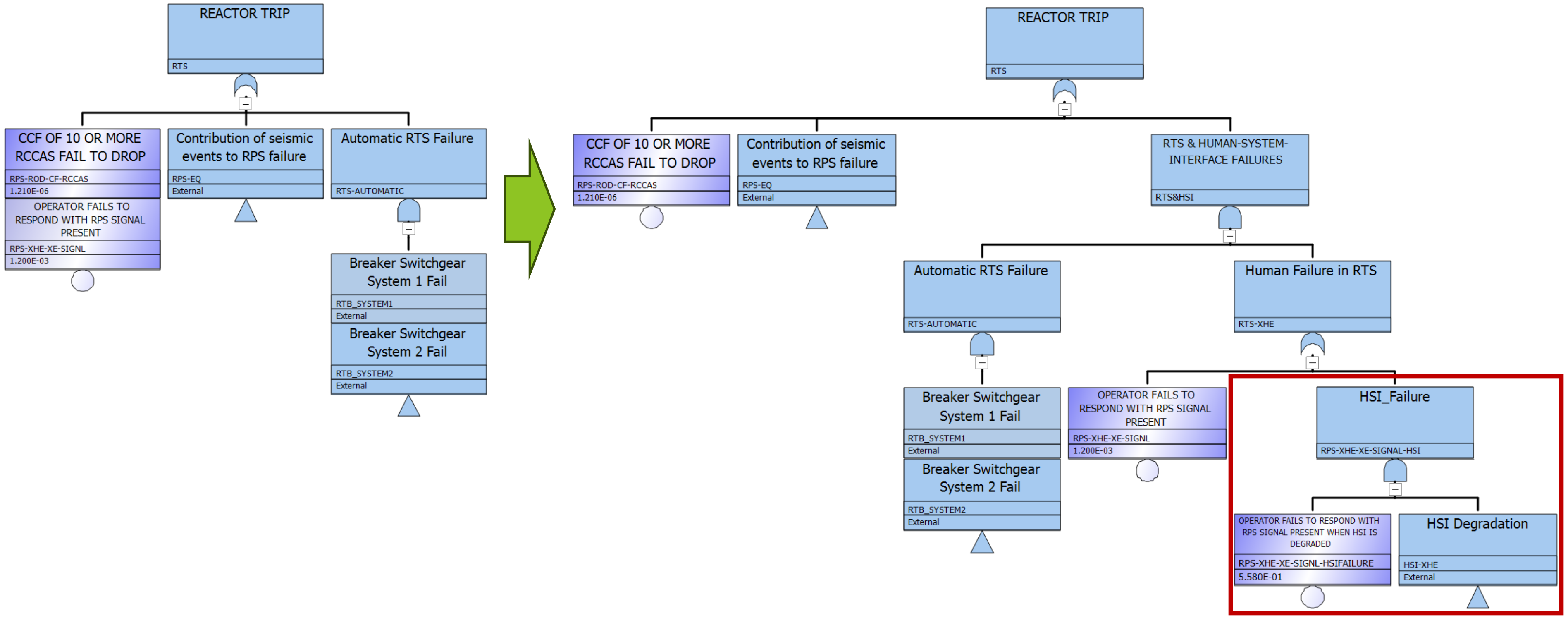
- **Step #3: Integration into PRA models**

$P_{HSI\_Degraded}$	9.21e-4
$HEP_{HSI\_Degraded}$	5.58e-1

$$P_{HSI\_Failure} = P_{HSI\_Degraded} \times HEP_{HSI\_Degraded}$$

$$= 9.21e\text{-}4 \times 5.58e\text{-}1$$

$$= 5.14e\text{-}4$$



LWRS
LIGHT WATER REACTOR SUSTAINABILITY

4. Feasibility of the Approach

- **Step #3: Integration into PRA models**
  - Probability change: 9% Increase

Cutsets Ranking	RTS before adding the HSI failure	RTS after adding the HSI failure
1	RPS-ROD-CF-RCCAS	RPS-ROD-CF-RCCAS
2	LC-LP-SF-CCF-TA,RPS-XHE-XE-SIGNL	LC-LP-SF-CCF-TA,RPS-XHE-XE-SIGNL
3	LC-BP-UCA-A-CCF,RPS-XHE-XE-SIGNL	LC-BP-UCA-A-CCF,RPS-XHE-XE-SIGNL
4	RPS-XHE-XE-SIGNL,RTB-UV-HD-CCF	RPS-XHE-XE-SIGNL,RTB-UV-HD-CCF
5	LP-HW-CCF,RPS-XHE-XE-SIGNL	**IFD-APS-UIFA**,LC-LP-SF-CCF-TA,**RPS-XHE-XE-SIGNL-HSIFAILURE**
6	LC-BP-HW-CCF,RPS-XHE-XE-SIGNL	LC-LP-SF-CCF-TA,**QND-APS-UIFA**,**RPS-XHE-XE-SIGNL-HSIFAILURE**

4. Feasibility of the Approach

- **Step #3: Integration into PRA models**
  - Importance analysis on RTS

Ranking No.	Name	FV
1	RPS-ROD-CF-RCCAS	8.231e-1
2	LC-LP-SF-CCF-TA	1.214e-1
3	RPS-XHE-XE-SIGNAL	1.169e-1
4	RPS-XHE-XE-SIGNAL-HSIFAILURE	6.005e-2
5	LC-BP-UCA-A-CCF	3.074e-2
6	RTB-UV-HD-CCF	1.815e-2
7	IFD-APS-UIFA	1.547e-2
8	QND-APS-UIFA	1.547e-2
9	LP-HW-CCF	4.079e-3
10	IFD-APS-H	3.260e-3

5. Conclusion

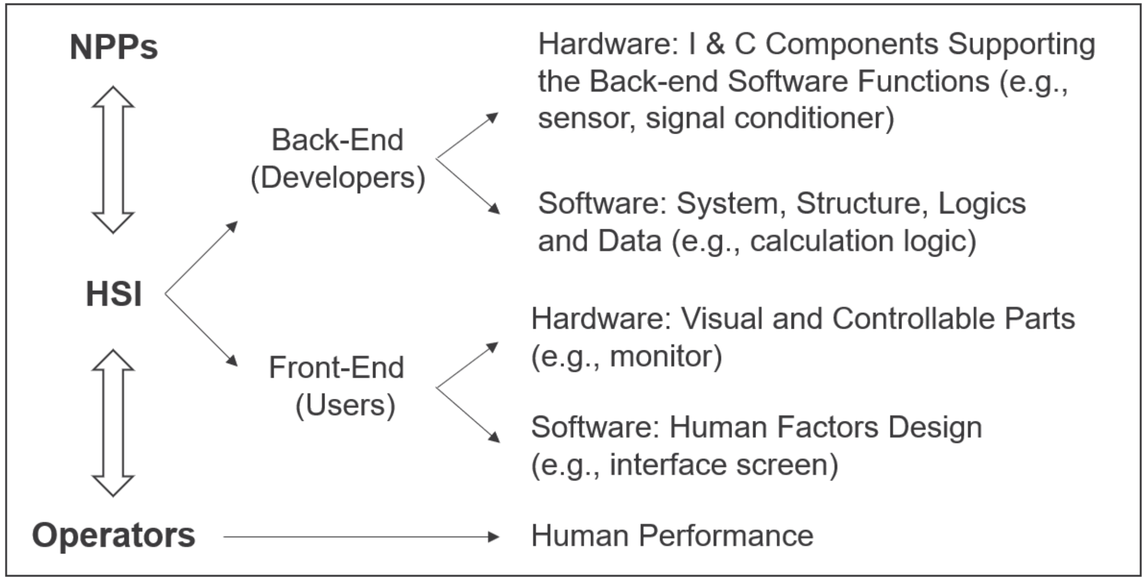
- **Summary**
  - Development of An Advanced Risk Analysis Method Especially for Evaluating HSIs of DI&C Systems
    - Extension from HSI evaluation in HRA
    - Use of the RESHA and IDHEAS-ECA methods
    - Based on the APR1400 DI&C systems and a RTS fault tree of GPWR PRA model
    - Considering potential risk oriented from HSIs of DI&C systems

- **Benefit**
  - This approach quantifies failure probabilities of HSIs by considering both risk from HSIs and the influence of HSIs on human operators.
    - New HSI system does not always contribute to human performance improvement.
      - Secondary tasks in digital main control rooms have the potential to increase the likelihood of human errors when the interfaces are poorly designed.

U.S. NRC, 2002. The effects of interface management tasks on crew performance and safety in complex, computer-based systems: overview and main findings. NUREG/CR-6690.

5. Conclusion

- **Future Work**
  - Additionally investigating on (1) how failure cases for back-end hardware and software contribute to HSI failure and (2) how HSI errors or degradations influence human performance to support HRA part in the method
  - Generalizing the method and making it easier with the step-by-step guidance
    - RTS only → A variety of safety systems
    - A human action for manual reactor trip only → A variety of human actions



LWRS LIGHT WATER REACTOR SUSTAINABILITY

Sustaining National Nuclear Assets

Point of Contact:

- Jooyoung Park <Jooyoung.Park@inl.gov>
- Congjian Wang <Congjian.Wang@inl.gov>