

From Human Error Probabilities to Unsafe Control Actions: Rethinking HRA in Automated Nuclear Power Plants

26 March 2026

Sung-Min Shin, Yochan Kim



Korea Atomic Energy
Research Institute



Risk Assessment
Research Division

This presentation in one sentence...

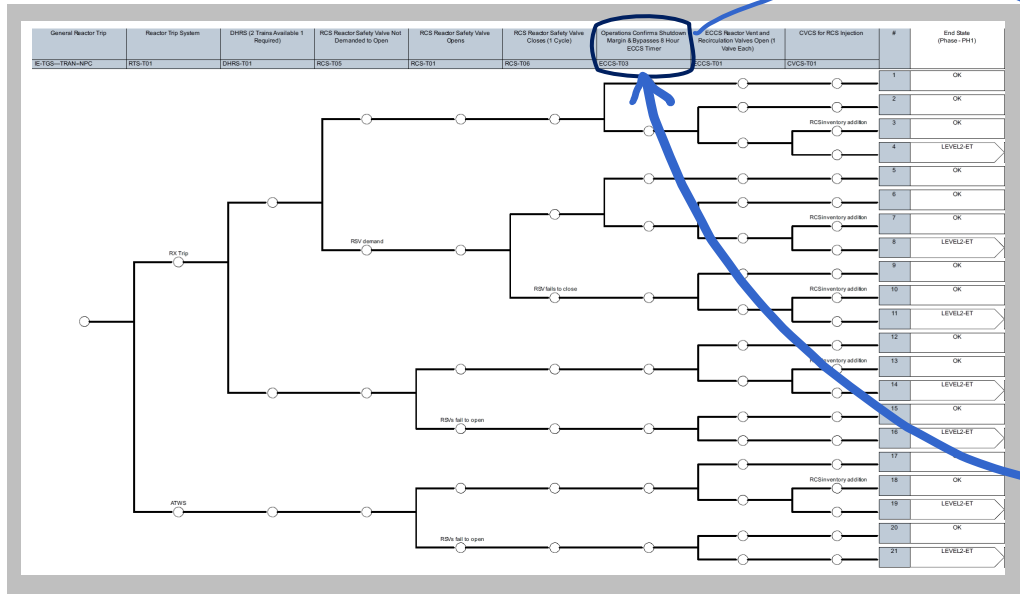
Why a transition from HEP (Human Error Probability) **quantification** in HRA (Human Reliability Analysis) **to UCA identification** based on the STAMP framework **is necessary;**

It reviews how human operator risk in nuclear power plants has traditionally been analyzed, discusses the limitations of these approaches, in the context of increasing automation

PRA (Probabilistic Risk Assessment) – HRA (Human Error Analysis) Framework

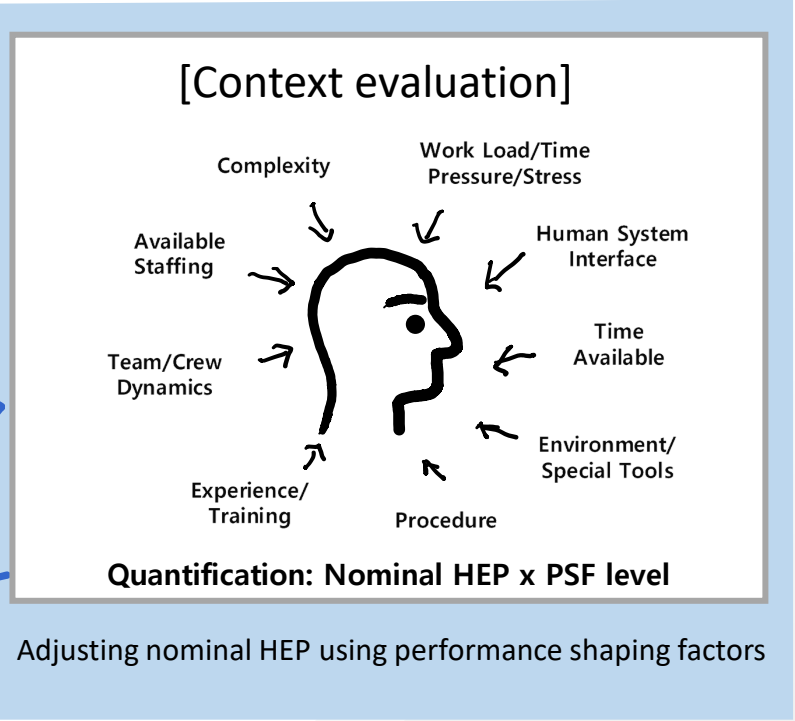
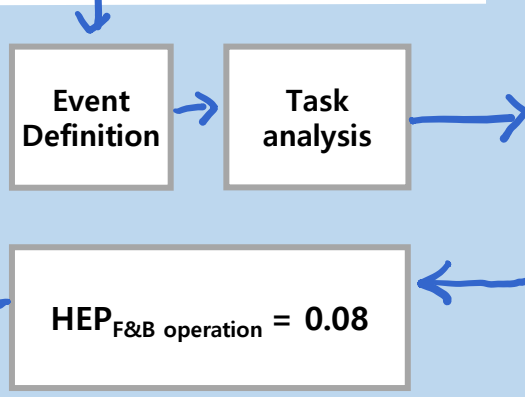
- PRA identifies a critical human action in a “predefined scenario”
- HRA quantifies its failure likelihood, human error probability (HEP)

PRA models (Event tree)



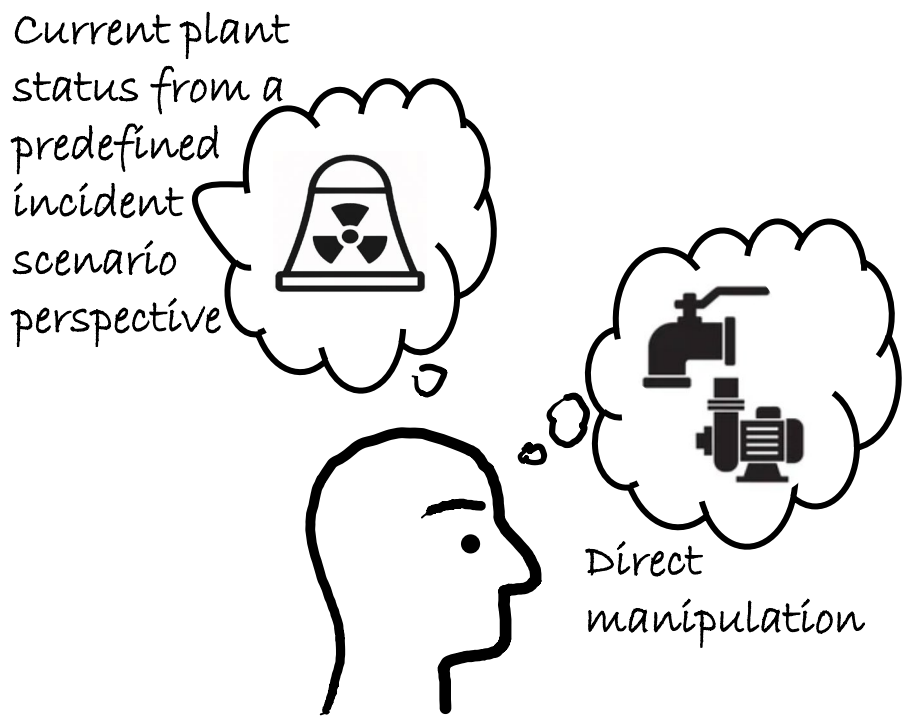
Critical human action

HRA Process

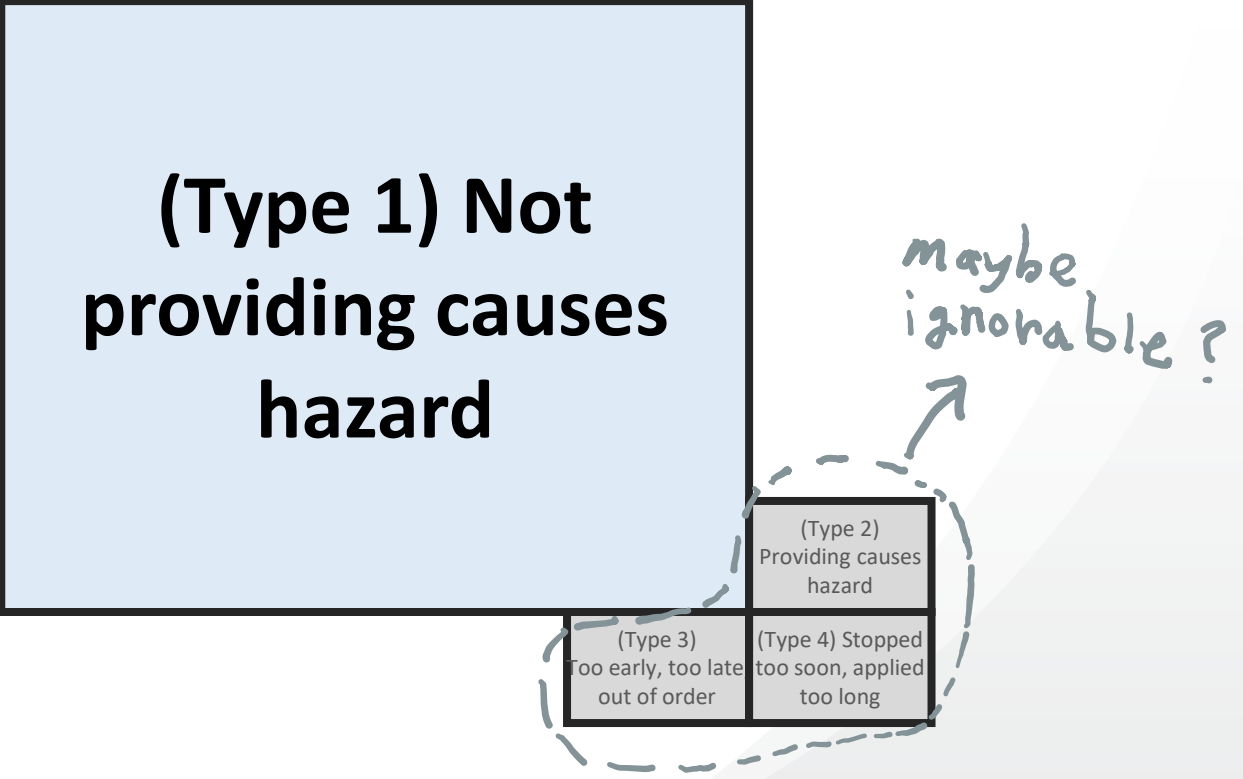


Applicability of the Framework in the Past

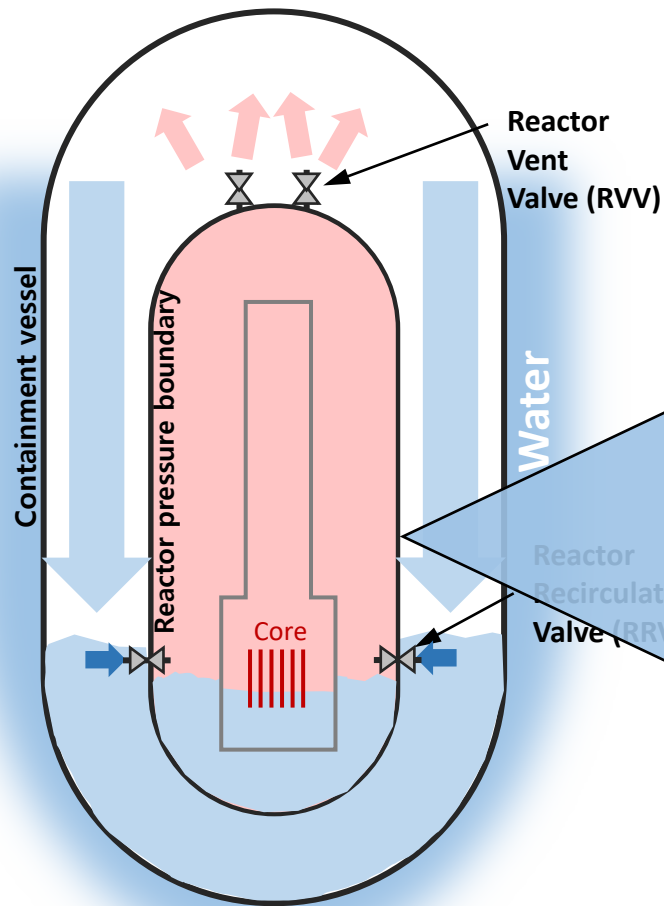
- PRA–HRA framework, for quantification, was well-suited for operators who directly manipulated plant equipment within predefined accident scenarios.



[Probable hazardous scenarios]



An Automation of a Safety System in NPP



Emergency Core Cooling System (ECCS)

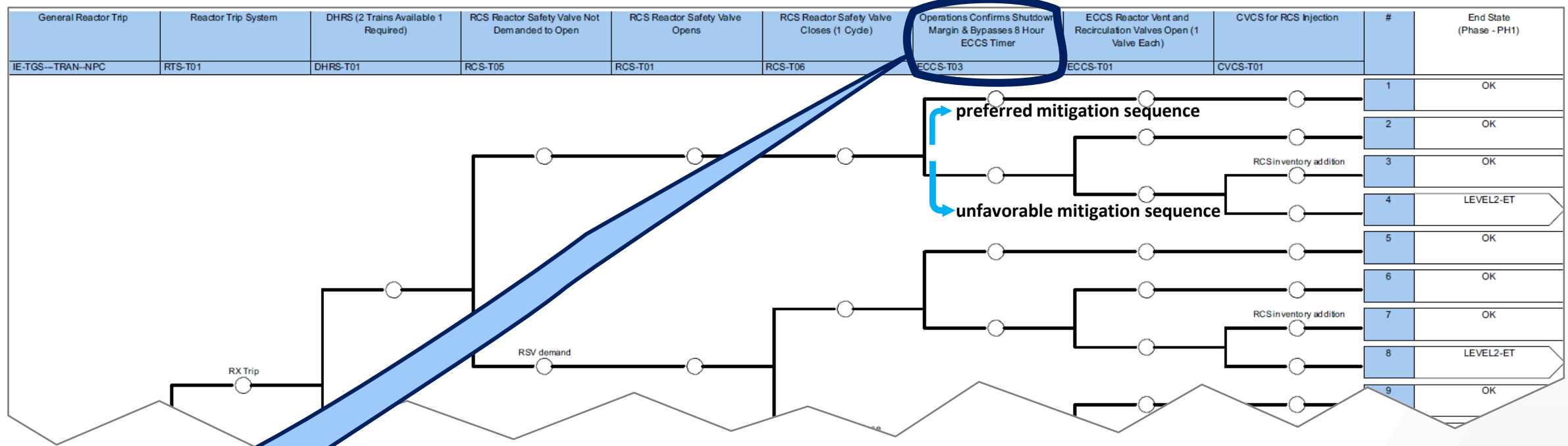
- **Operating sequence**
 - Opens specific valves to initiate a gravity-driven cooling loop
- **8-Hour Timer (Safety priority logic)**
 - A timer begins to count down after the reactor trip
 - 8 hours later, **the timer initiates ECCS automatically**

Unless a loss of primary coolant loss accident has already occurred, mitigation actions that **unnecessarily discharge primary coolant as the first step of mitigation mean should be avoided**, as it lead to significant downtime by increasing restoration efforts.

- **Operator Intervention (An critical human action)**
 - During the 8-hour window, the **human operator may issue a manual Block(bypass the auto-actuation of ECCS) or Release the block command.**

An Automation of a Safety System in NPP

NuScale Final Safety Analysis Report, Ch19 Rev.0 2022



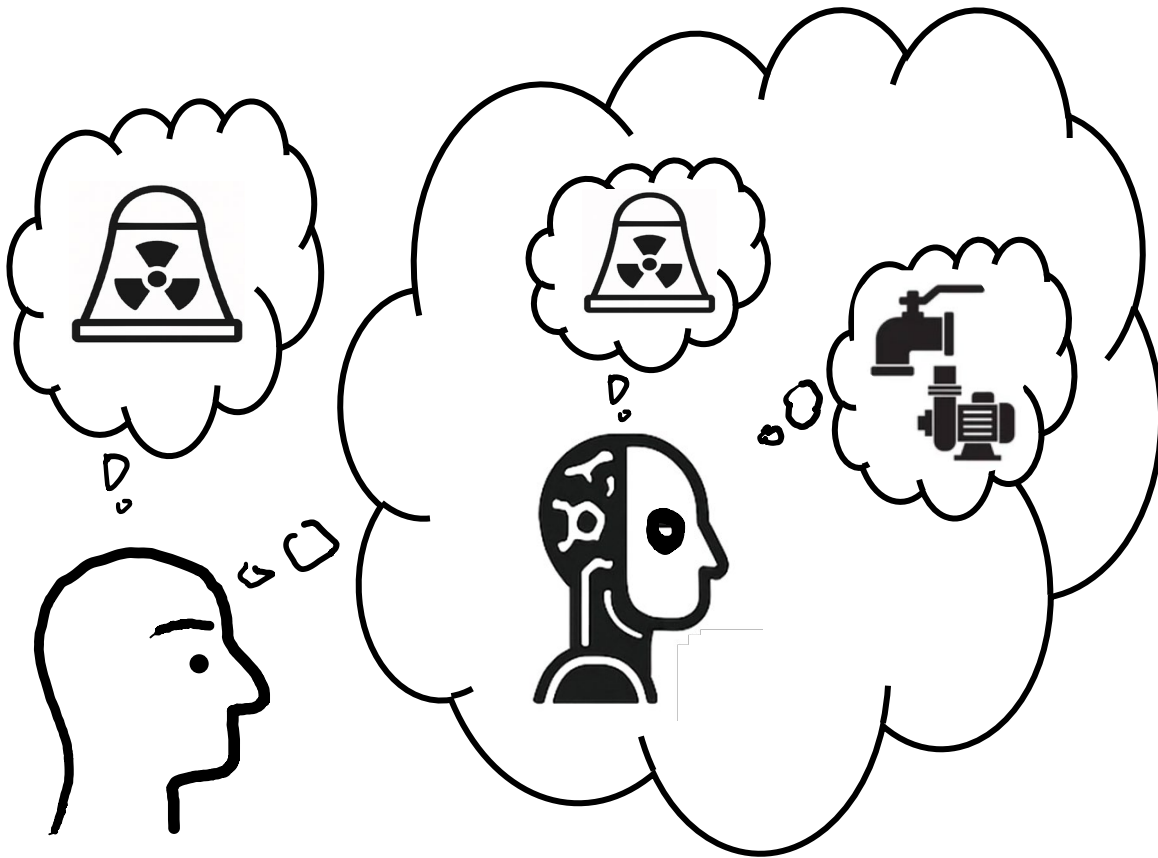
Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer

ECCS-T03

At the moment condition	Operator intervention	ECCS operation at 8 hours after trip
Not Blocked	X	YES
	O (Enable blocking)	NO
Blocked	X	NO
	O (Enable releasing)	YES

Automation changes operator role

- Operators increasingly act as supervisors of automation
- Decision-making on automation and situation awareness become more important



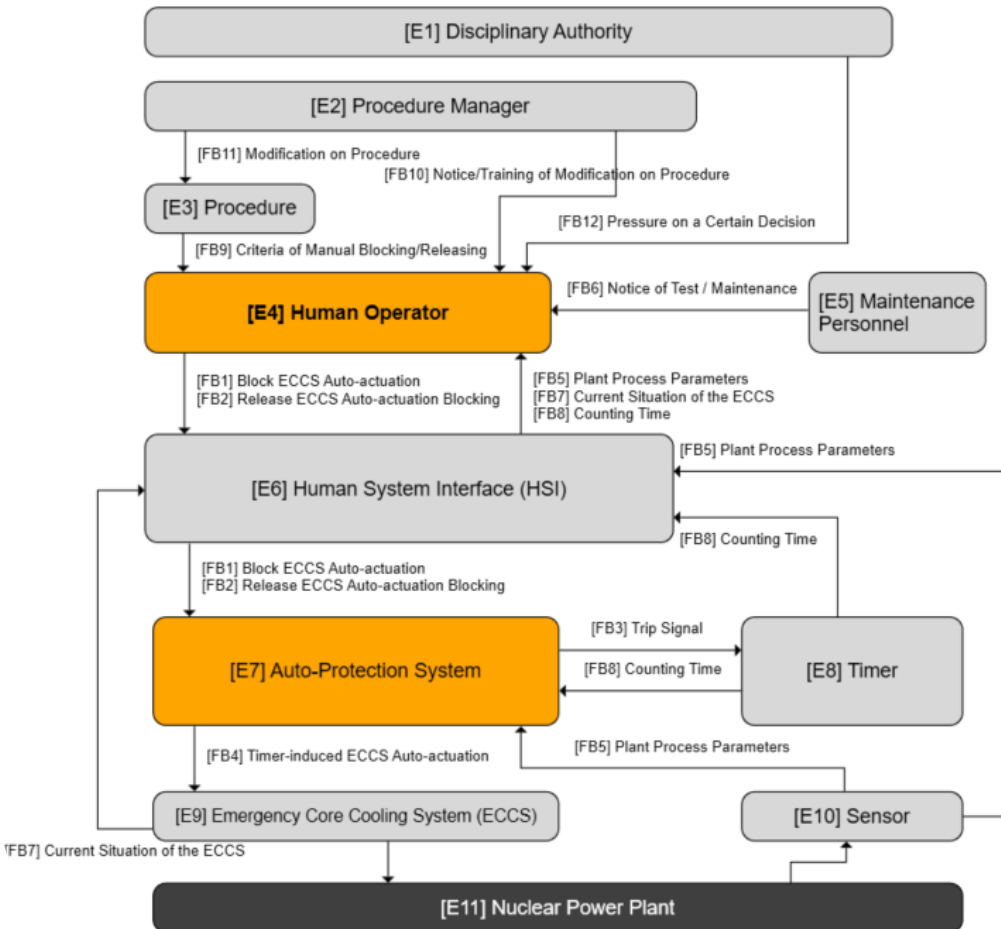
[Probable hazardous scenarios]

<p>(Type 1) Not providing causes hazard</p>	<p>(Type 2) Providing causes hazard</p>
<p>(Type 3) Too early, too late, out of order</p>	<p>(Type 4) Stopped too soon, applied too long</p>

A Pilot Study

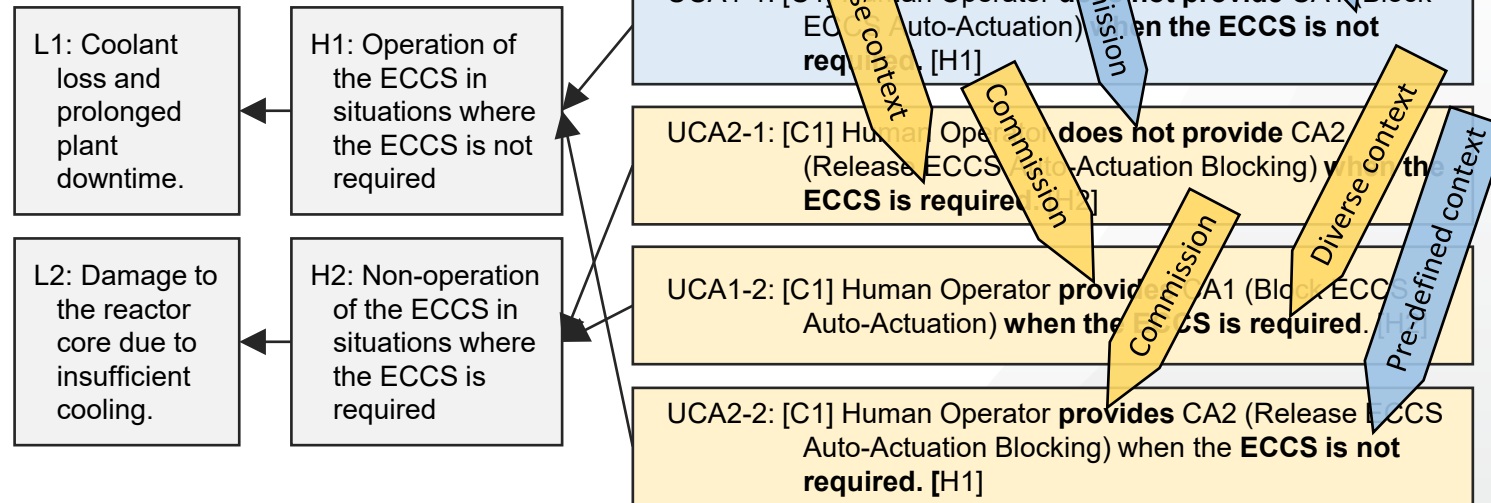
System entities

- **Procedure and Procedure Manager:** Provides guidance to the operator, including conditions under which ECCS blocking/releasing is permissible.
- **Sensors:** Monitor plant parameters such as reactor pressure, temperature, neutron flux, and coolant levels, supplying real-time status information.
- **Automatic Protection System:** Detects abnormal conditions and initiates a reactor trip based on sensor inputs, and it also triggers automatic ECCS actuation after 8 hours if no manual intervention occurs
- **Timer:** Initiated upon a reactor trip, this component counters the elapsed time.
- **Emergency Core Cooling System(ECCS):** A gravity-driven reactor cooling system.
- **Human-System Interface(HSI):** Aggregates and displays information from various subsystems to support operator situational awareness and decision-making.
- **Maintenance Personnel:** Ensure the operational readiness of ECCS and other supporting components, potentially influencing system availability.
- **Disciplinary Authority:** Organizational or regulatory agent that may influence operator decision-making either directly or indirectly, under certain conditions.



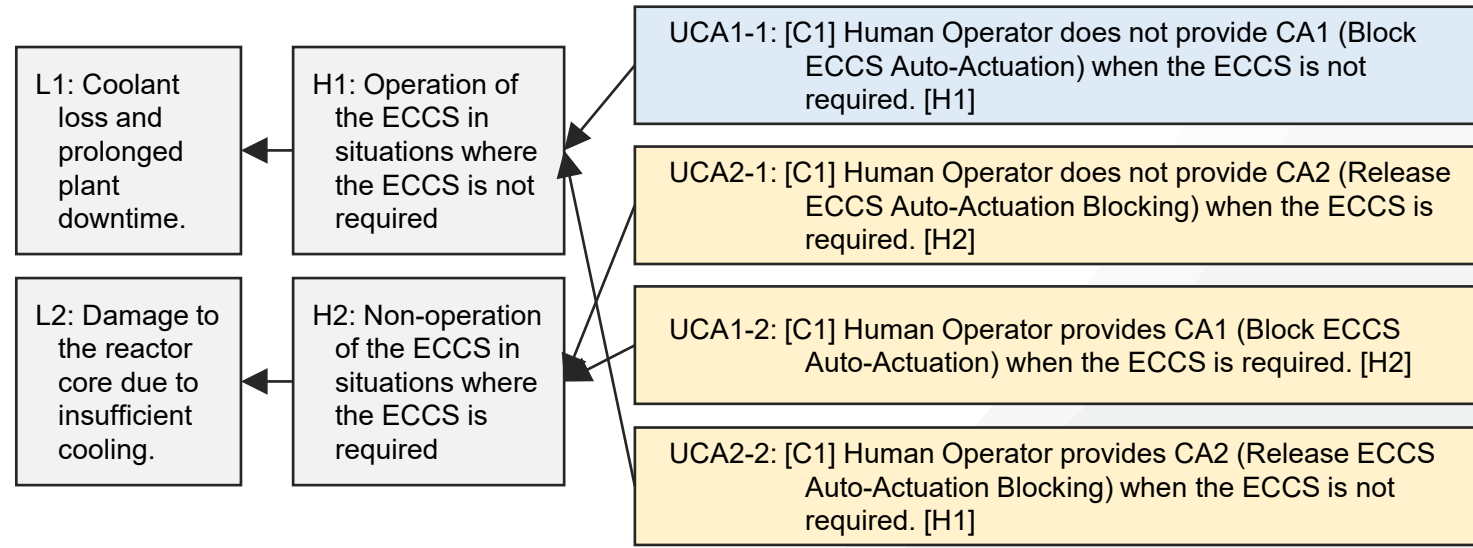
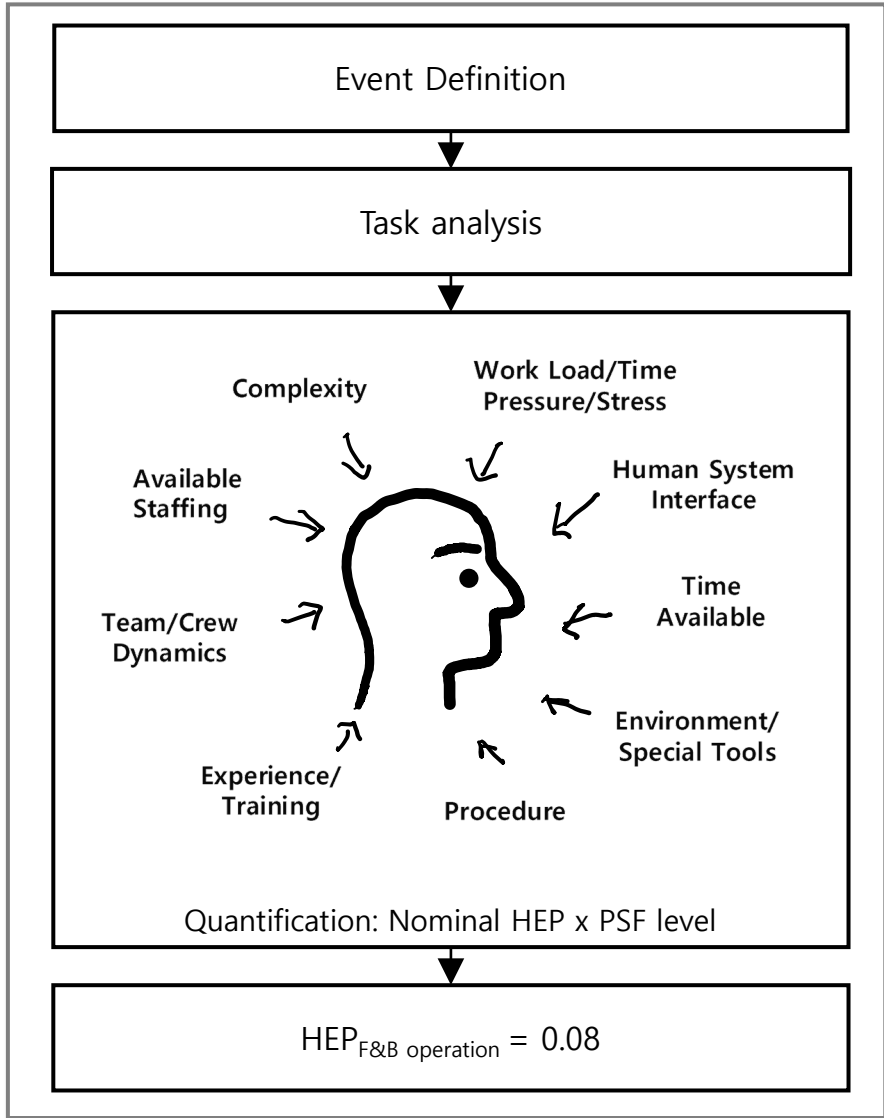
CA01 Block ECCS Auto-actuation

CA02 Release ECCS Auto-actuation Blocking



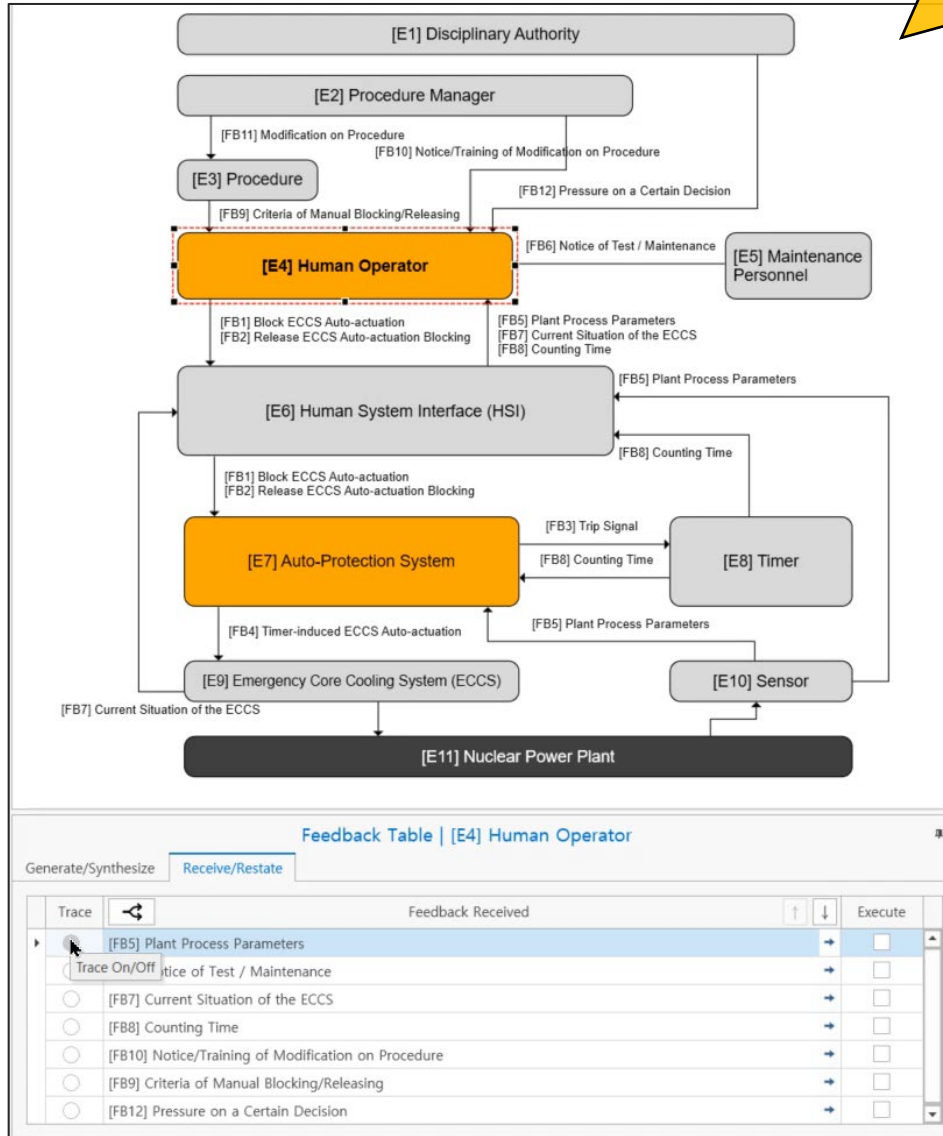
- UCA1-1: [C1] Human Operator **does not provide** CA1 (Block ECCS Auto-Actuation) **when the ECCS is not required.** [H1]
- UCA2-1: [C1] Human Operator **does not provide** CA2 (Release ECCS Auto-Actuation Blocking) **when the ECCS is required.** [H1]
- UCA1-2: [C1] Human Operator **provides** CA1 (Block ECCS Auto-Actuation) **when the ECCS is required.** [H1]
- UCA2-2: [C1] Human Operator **provides** CA2 (Release ECCS Auto-Actuation Blocking) **when the ECCS is not required.** [H1]

HRA based Approach



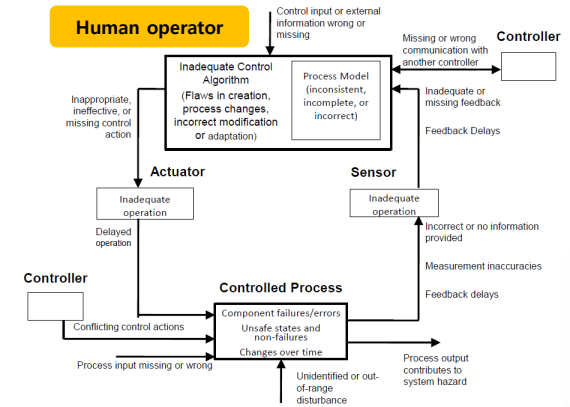
STAMP based Approach

Developed by TRACEIT



Potential feedbacks required for Human Operator's decision-making

- Plant Process Parameters
- Notice of Test/Maintenance
- Current Situation of the ECCS
- Counting Time
- Notice/Training of Modification on Procedure
- Criteria on Manual Blocking/Releasing
- Pressure on a Certain Decision



L1: Coolant loss and prolonged plant downtime.

H1: Operation of the ECCS in situations where the ECCS is not required

UCA1-1: [C1] Human Operator does not provide CA1 (Block ECCS Auto-Actuation) when the ECCS is not required. [H1]

UCA2-1: [C1] Human Operator does not provide CA2 (Release ECCS Auto-Actuation Blocking) when the ECCS is required. [H2]

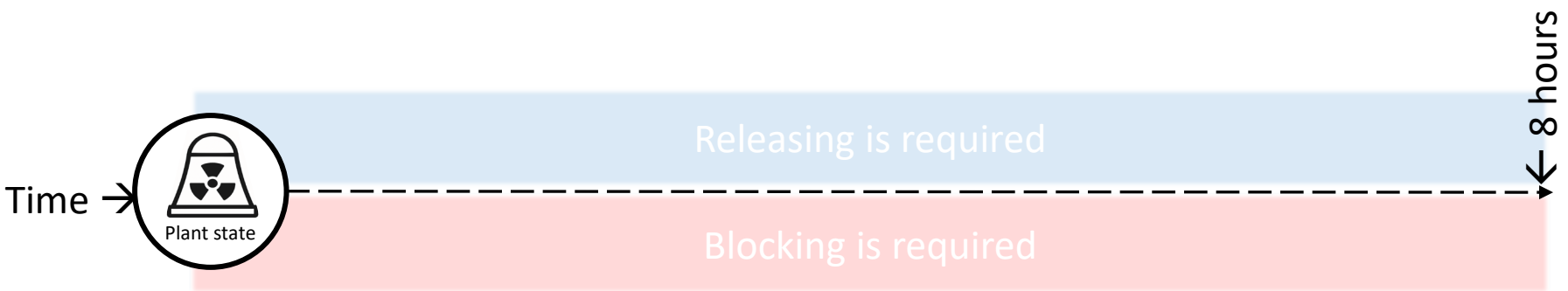
L2: Damage to the reactor core due to insufficient cooling.

H2: Non-operation of the ECCS in situations where the ECCS is required

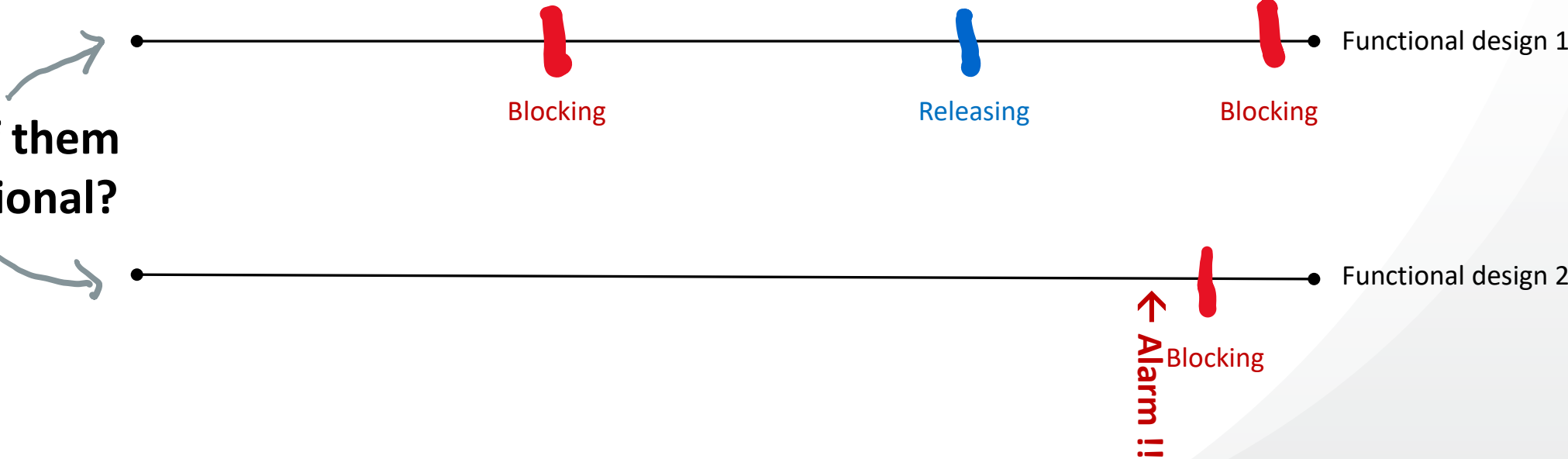
UCA1-2: [C1] Human Operator provides CA1 (Block ECCS Auto-Actuation) when the ECCS is required. [H2]

UCA2-2: [C1] Human Operator provides CA2 (Release ECCS Auto-Actuation Blocking) when the ECCS is not required. [H1]

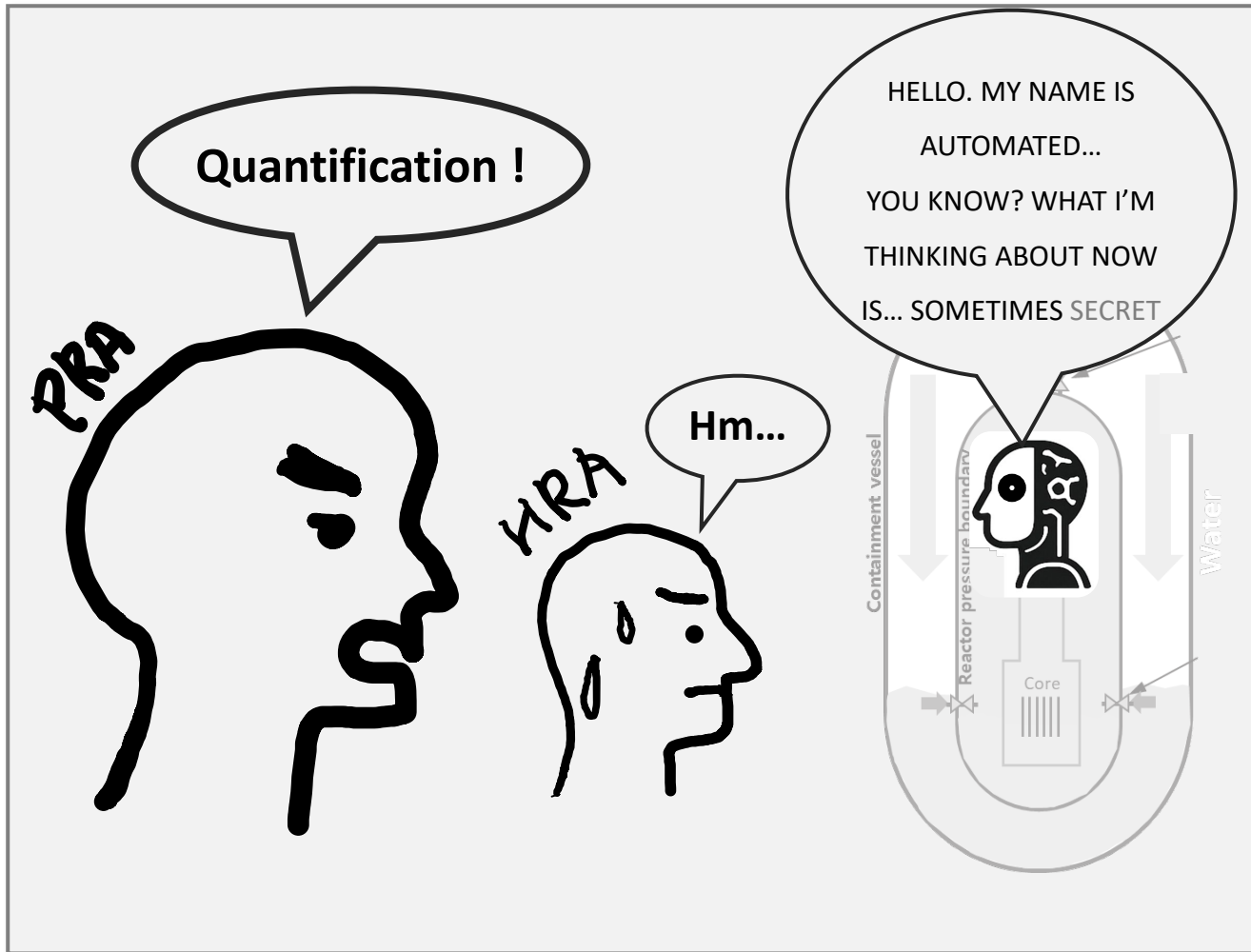
One interesting finding is...



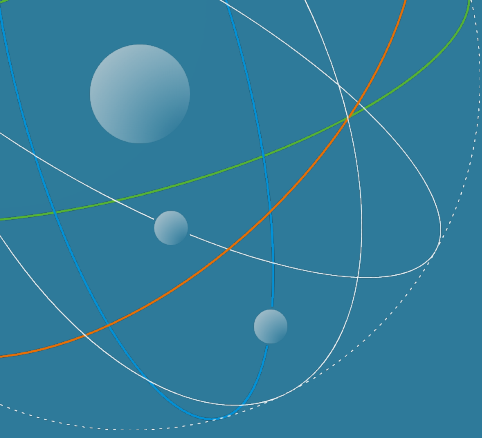
One of them
or **Optional?**



Concluding Remarks



- The HRA field clearly recognizes the importance of analyzing why and how operators may perform unnecessary actions and is seeking appropriate analytical frameworks.
- Nevertheless, because it remains embedded in the conventional PRA structure that emphasizes quantitative results, there is an inherent conflict between multi-perspective safety analysis and the need for quantification, which seems to hinder the application of STPA in HRA.



I am planning a one-year research sabbatical in Brisbane, Australia, starting in January 2027. If anyone is interested in potential collaboration, please feel free to reach out. (smshin@kaeri.re.kr)

Acknowledgement

- This work was supported by an Innovative Small Modular Reactor Development Agency grant funded by the Korean Government (MSIT) (No. RS-2023-00258118).

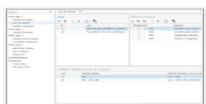
TRACEIT: STPA Tool with Full Traceability

(Version 2.0 Released Jan 2026)



- TRACEIT is a system-theoretic safety analysis tool developed by KAERI for modeling computerized control structures through signal interactions among system components. Its data-driven representation simplifies traditional control-structure modeling and enables comprehensive trace functions across the STPA process, supporting the analysis of complex systems with overlapping control loops.

Key Features



End-to-End STPA Workflow Integration (Steps 1 to 4): Supports the full range of steps in STPA: defining losses & hazards, constructing the control structure, conducting UCA analysis, and drafting loss scenarios.



Computerized Control-Structure: Instead of using a visual diagram, TRACEIT models signal interconnections among system components in data form.



Control-Structure Completeness Checking: It checks the completeness and consistency of the control structure, using standard inspection rules (e.g. verifying that generated signals are referenced in process models).



Automated Fault Impact Assessment (Bridging the gap between PSA and STPA): Simulates fault impact analysis by assuming unavailability of individual or multiple system components, or by manipulating shared property values (e.g. platform, location).



Comprehensive Trace Information Throughout the STPA Process: Throughout the STPA process, TRACEIT provides various trace views (highlighting, abstract views, etc.) to support model review, confirmation, and UCA cause analysis.



Flexible Model Editing and Expansion: Supports incremental modification, supplementation, and extension of existing computerized control-structure data without needing to rewrite the structure from scratch.



Management of Causes & Countermeasures: For each loss scenario (Cause – UCA – Hazard – Loss), TRACEIT helps users develop, organize, and manage associated causes and countermeasures.



Trace View of Analysis Results: Enables trace-based display of the entire analysis and specific items according to user settings, facilitating review, communication, and system improvement.