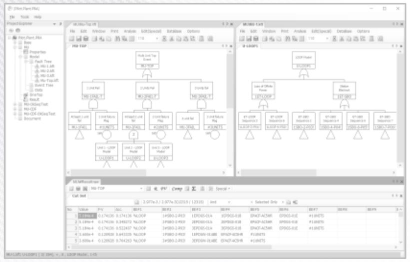
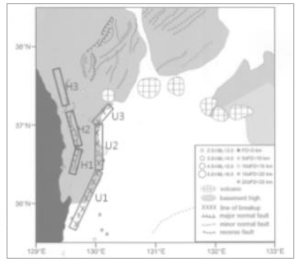
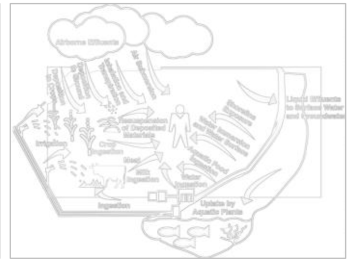
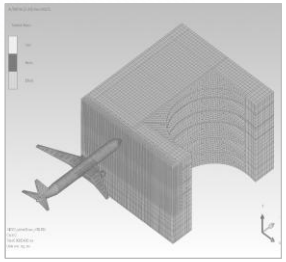
www.kaeri.re.kr

Proposal to Modify Types of the Unsafe Control Actions in the STPA for the Detailed Sub-task Analysis of the Human Reliability Analysis

Seong Woo Kang, Jaewhan Kim, Jinkyun Park, Sung-Min Shin, Ho-Gon Lim

Korea Atomic Energy Research Institute (KAERI)

Risk Assessment Research Division

Presentation for KNS Spring Conference

2025. 5. 22.

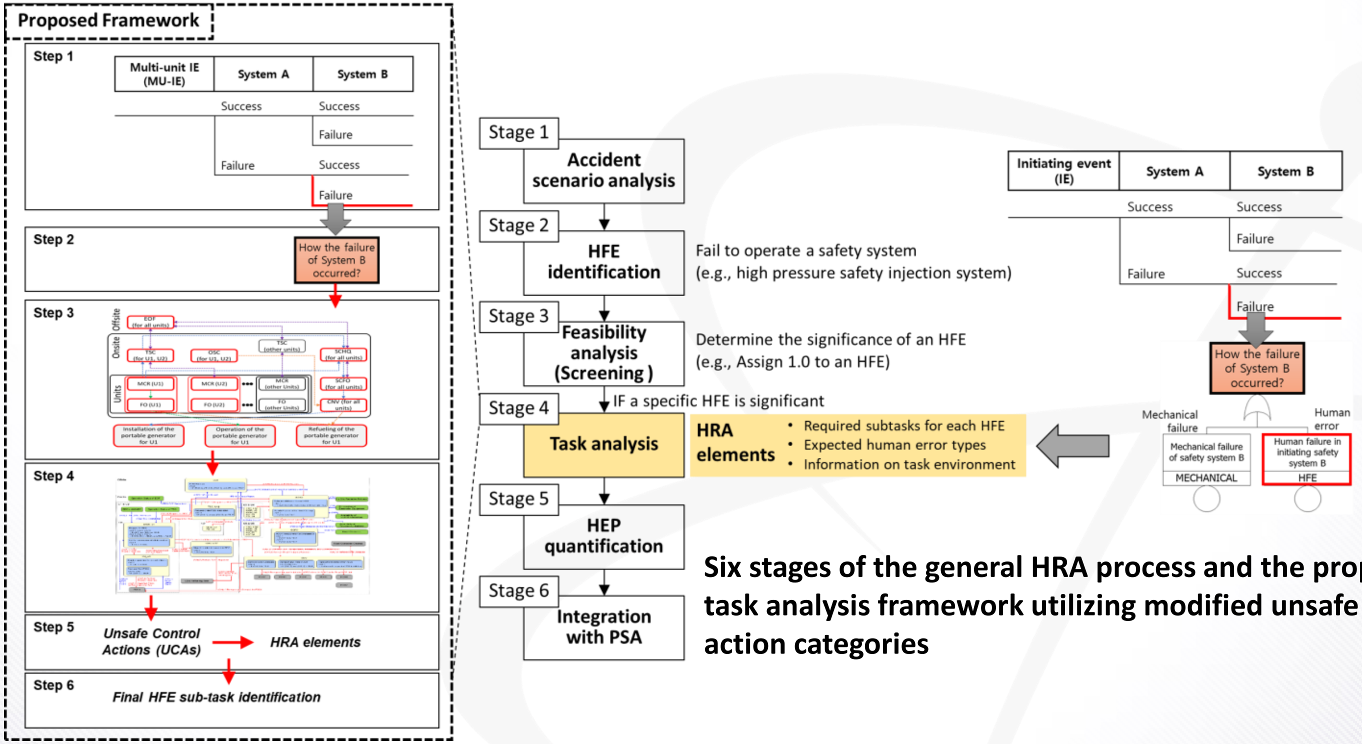
CONTENTS

1. Background

Human Reliability Analysis, HRA

- HRA is generally defined as a structured approach to identify potential human failure events (HFEs) to ultimately estimate the human error probabilities (HEPs) of those errors using data, models, or expert judgement

- A general HRA process can be divided into 6 stages:



Six stages of the general HRA process and the proposed HFE task analysis framework utilizing modified unsafe control action categories

- HRA is needed to assess the human-operated portion of the probabilistic safety assessment (PSA) models

Limitations of typical HRA methods

- **HRA methods have inherent flaws dealing with uncertainties**
  - Even using same HRA methods (e.g. THERP, SPAR-H, K-HRA, etc.) by different experts may result in different HRA results due to subjectivity and conservatism (due to lack of data)
- **Traditional HRA methods are developed based mainly on a single-unit basis**
  - Traditional methods assume no need to transfer and/or share the equipment with other units for the accident management
  - Also, they assume human operators working in the main control room (MCR) are mainly responsible for the manipulation of the equipment
  - To be utilized in the MU-PSA, MU-HRA must better assess the inter-organizational interactions (e.g. between organizations and portable equipment)

Examples of varying HEP results

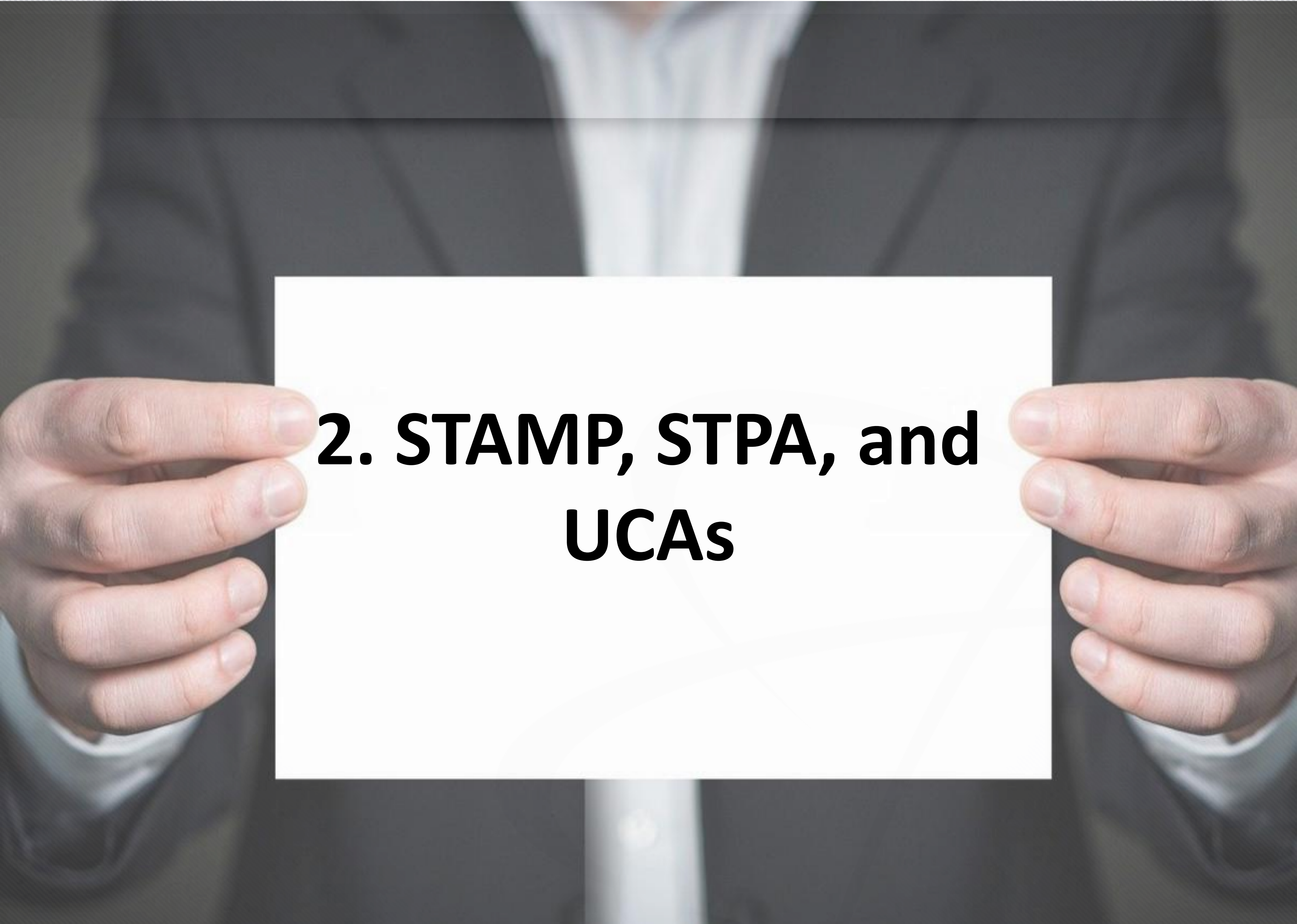
- Averaged values for [1st, 50th, 99th percentile] from NRC RIL 2020-13, "Vol.1 Applying HRA to FLEX – Expert Elicitation"

SBO Scenario		Internal Event			External Hazard		
Equipment	Percentile	1st	50th	99th	1st	50th	99th
FLEX generator	Transport	0.023	0.057	0.27	0.038	0.14	0.52
	Connect	0.027	0.088	0.31	0.046	0.16	0.41
	Operate	0.024	0.052	0.22	0.036	0.12	0.44
FLEX pump	Transport	0.016	0.06	0.33	0.023	0.12	0.47
	Connect	0.019	0.078	0.27	0.036	0.13	0.45
	Operate	0.017	0.05	0.21	0.043	0.14	0.44

- Note that above results do not include interorganizational interactions and inter-unit dependencies

Improving the MU-HRA Processes

- **To conduct the more realistic MU-HRA for the MU-PSA approach, important tasks reflecting interorganizational characteristics that arises from the deployment of these portable equipment must be properly identified**
  - More data through simulations
  - More structured approach/framework to identify HFE subtasks for complex multi-unit events without missing critical subtasks
- **A structured guideline for the HRA experts to follow during HFE subtask analysis may help**
  - STPA (Systems-Theoretic Process Analysis) technique provides specific, proactive, and easy-to-follow analysis guideline to analyze the potential cause of accidents that may arise from complex interactions of the components and emerging properties from those interactions



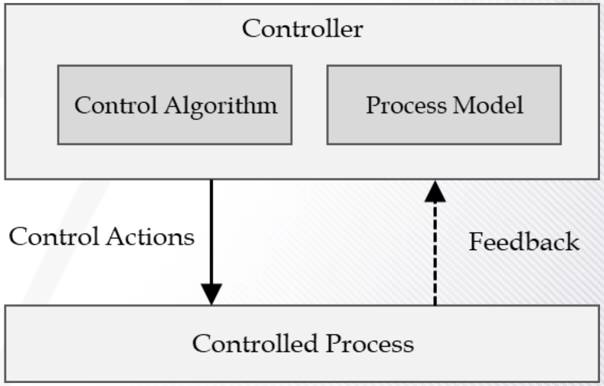
2. STAMP, STPA, and UCAs

Overview of STAMP

- **STPA is developed based on STAMP (Systems-Theoretic Accident Model and Processes)**
- **STAMP visually models a target system using connections between many control loops**
  - Control loops are composed of a controller that provides control actions for a controlled process through a control algorithm, which may give feedback to the controller to update a process model.

Key elements included in a STAMP control loop

Element	Description
Controlled process	Object to be controlled
Feedback (FB)	Information indicating the status of the controlled process
Controller	Subject determines whether a CA is generated or not. • Control algorithm: The controller's decision-making procedures or logic • Process model: Status of the controlled process understood by the controller (internal belief)
Control action (CA)	Control commands issued by the controller

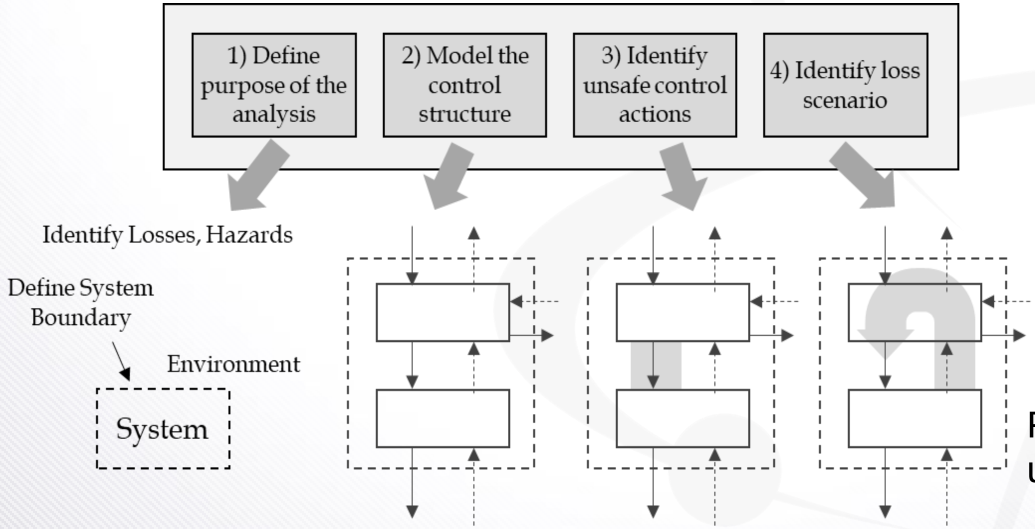


Typical control loop configuration of STAMP

Overview of STPA

- **STPA is a four-phase hazard analysis technique**
  - First phase: catalog of undesired losses and hazards are defined
  - Second phase: causal factors and control flaws are identified through development of a control structure

  STAMP
  - Third phase: among the control actions developed in the second phase, a catalog of UCAs(unsafe control actions) is identified
    - Detailed analysis for the MU-HFE subtasks performed in this step
  - Fourth phase: the causes of the UCAs are analyzed



Four phases of STPA utilizing STAMP

Unsafe Control Actions

- **Unsafe control actions (UCAs) are the control actions by the controller that may result in hazard on the examined system**

Representative UCA types in STPA

UCA type		Description format
1	Not providing causes hazard	Hazard occurs because <Controller> does not provide <Control Action>
2	Providing causes hazard	Hazard occurs because <Controller> provides <Control Action>
3	Providing too early, too late, out of order causes hazard	Hazard occurs because <Controller> provides <Control Action> too early, too late, or in the wrong order
4	Providing too long or stopping too soon causes hazard	Hazard occurs because <Controller> provides <Control Action> for too long or too short

Proposed Modification of UCAs for HRA

- **Utilizing traditional STPA for the purpose of HRA may allow catching critical sub-tasks but also may require large amount of resources which may burden the HRA practitioners**
  - i.e., too much resources and too detailed results
- **To be better utilized in the field of MU-HRA, this study proposes simplification/modification of the standard STPA technique**
  - More specifically, modified types of the UCAs

Proposed Modification of UCAs for HRA

UCA type	Description format
Not providing causes hazard	Hazard occurs because “controller” does not provide “control action”
Providing causes hazard	Hazard occurs because “controller” provides “control action”
Providing too early, too late, out of order causes hazard	Hazard occurs because “controller” provides “control action” too early, too late, or in the wrong order
Providing too long or stopping too soon causes hazard	Hazard occurs because “controller” provides “control action” for too long or too short

Modified UCA types	Guideline	Additional details for the HRA practices
Not providing / providing too late causes hazard	(<UCA number>) [<hazard number>] <Controller> fails or provides too late <Control Action>	after/when <prerequisite Control Action and/or Feedbacks, if any> when/during <other situational/environmental conditions>
Providing out of order causes hazard	(<UCA number>) [<hazard number>] <Controller> provides <Control Action> out of order	
Stopping too soon causes hazard	(<UCA number>) [<hazard number>] <Controller> provides <Control Action> too short	

3. Case Study Results

Case Study: Portable Generator Failure

- **A case study is carried out with respect to an HFE "failure of starting and running a PDG (portable diesel generator)"**
- **Scenario: multi-unit ELAP (extended loss of AC power) due to a beyond design-basis external event**
- **Some assumptions:**
  - Recovery using the AAC-DG failed
  - There are 6 units at the site, with multiple EROs that interact for starting and running the PDG
  - MCR and field operators for each unit are available on-site, but others are to be convocated (i.e. called and summoned) from offsite for the multi-unit accident
  - One TSC is assigned to manage twin units, and EOF makes decisions on a site level

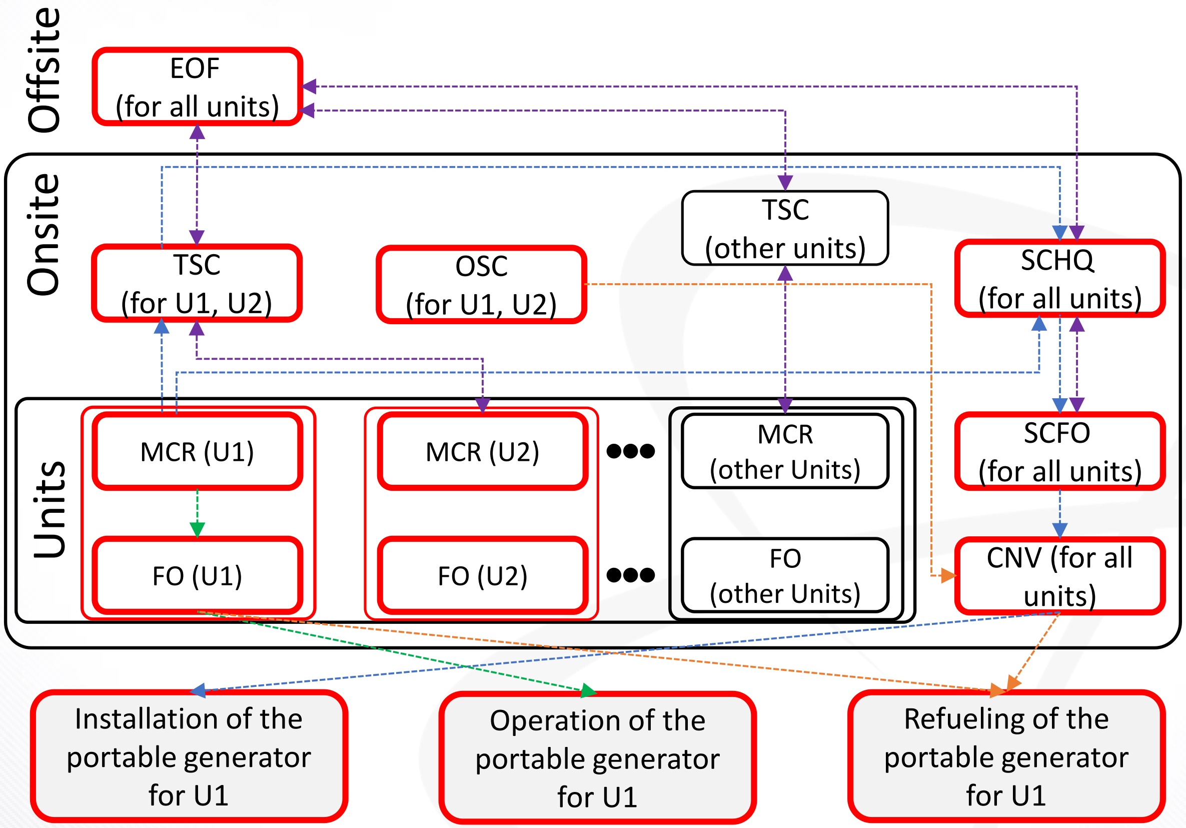
Case Study: Organizational Assumptions

Assumed EROs and their roles during a general multi-unit accident management

Organization	Roles
TSC (technical support center)	• It is activated with its facility onsite • In a twin-unit level, TSC is responsible for plant management and providing technical support to MCR operators when a beyond design basis accident (BDBA), severe accident, BDBEE, or multi-unit accident occurs • It makes decisions regarding the priority of deploying any portable equipment shared by twin units in a single site
OSC (operational support center)	• It is activated with its facility onsite • OSC provides engineering support for the operation of chemical, electrical, mechanical, and instrumentation and control systems • It performs maintenance, firefighting, and rescue activities if necessary • It performs cable alignment before the required mobile equipment arrive, to reduce the accident progression time
EOF (emergency operating facility)	• It is activated and mobilized off-site • In a site-level, EOF is responsible for plant management of the overall emergency response • EOF provides technical support to both the TSC and MCR operators during the progression of a BDBA, severe accident, or multi-unit accident • It makes important top-level decisions regarding the course of action in situations when two or more units are involved • It makes the final decision regarding the priority of deploying portable equipment, especially when two or more TSCs request same portable equipment simultaneously • It coordinates radiological and environmental assessment as well as response activities with federal/state/local agencies
SCHQ (safety center head quarters)	• On-site portable equipment is generally stationed and deployed from here • It prepares/maintains essential equipment performances (pre-HFE) • It orders correct portable equipment to be installed on the requested site
SCFO (safety center field operators)	• The field workers from the safety center (SC) oversees CNV for transporting, installing, and connecting the portable equipment • The field workers also oversee removal of road debris
CNV (convocated workers)	• They are field workers who transports, installs, and connects the portable equipment • They also connect the refueling line of the portable equipment to the EDG refueling tank

Case Study: Identifying HRA elements

- **From the perspective of unit #1 (U1), organizations and interactions involved in the identified HFE are defined**

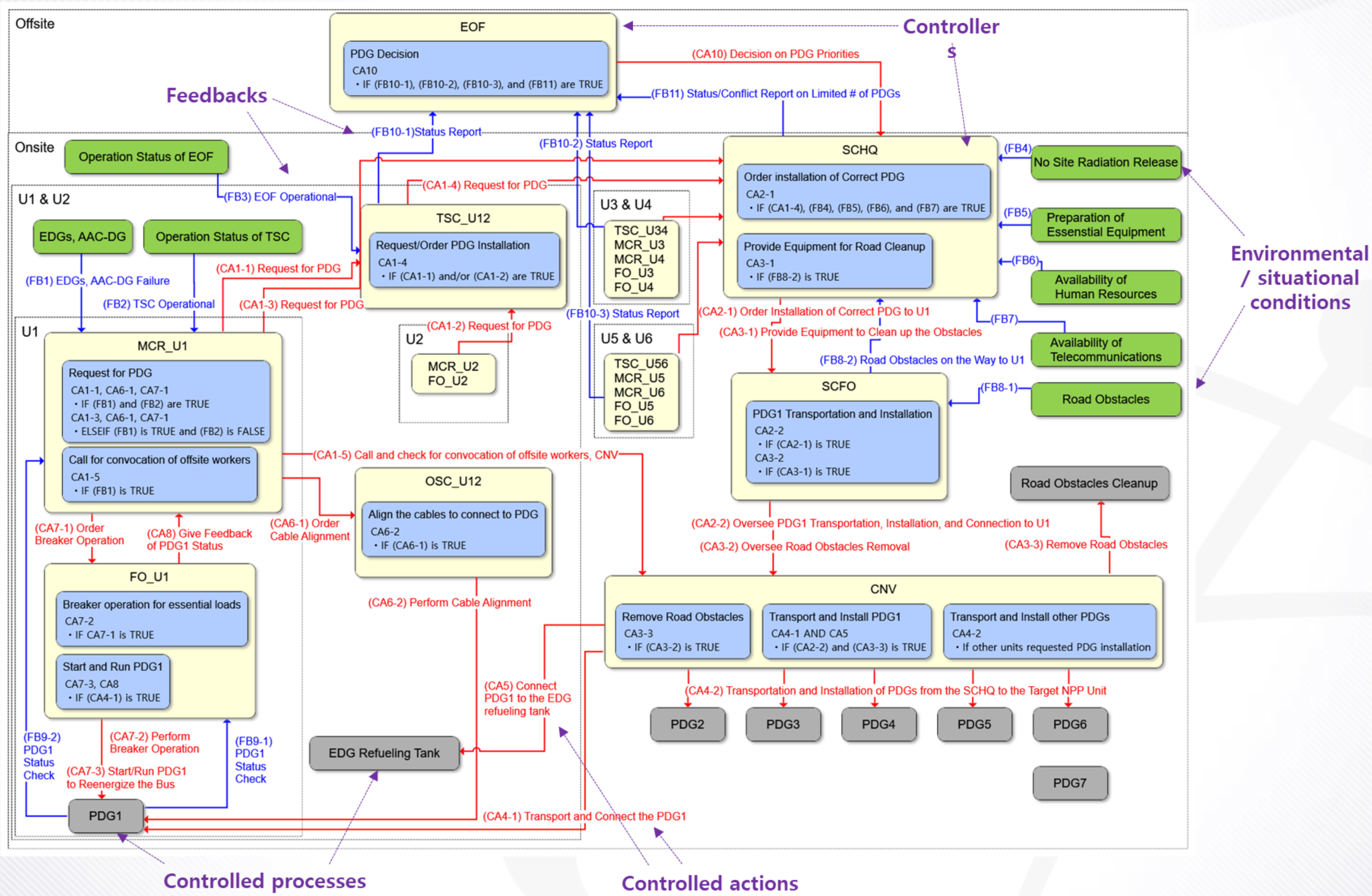


Schematic of the organizations involved in the successful start and run of the portable generator in the perspective of the unit #1 (highlighted in red). Dotted lines related to installation, operation, refueling, and additional decision-making of the portable equipment are colored in blue, green, orange, and purple, respectively

Case Study: Defining Loss & Hazard

- **Loss**
  - Failure of starting and running the portable diesel generator (PDG)
- **Hazards**
  - Fail to install the PDG [H-1]
  - Too late to install the PDG [H-2]
  - Fail to maintain operation of the PDG [H-3]

Results: Developing a STAMP Model



Developed STAMP model for successful utilization of the portable generator in perspective of U1

Results: Identification of UCAs for the HRA

- **Through traditional STPA, a total of 38 UCAs were identified in the case study**
- **Through the proposed modified STPA, 25 UCAs were identified**
  - In general, most UCAs for multi-unit accident management occurred when corresponding organizations do not take required actions or take actions too late
- **These may further be grouped on the similarities of the control actions for the final HFE-subtask analysis**
  - See "Kang et al., *A Framework to Identify the Catalog of Important Tasks Reflecting Interorganizational Characteristics Regarding the Deployment of Portable Equipment*, IEEE Access, 2025"

4 STPA UCA types
(2 mainly used)
→ 38 UCAs defined

Control Action From -> To	UCA Type 1: Not providing causes hazard	UCA Type 2: Providing causes hazard	UCA Type 3: Providing too early, too late, out of order causes hazard	UCA Type 4: Providing too long or stopping too soon causes hazard
(CA1-1) Request for PDG MCR_U1 -> TSC_U12	(UCA-1) MCR_U1 fails to request for PDG during ELAP when TSC_U12 is functional [H-1]		(UCA-2) MCR_U1 is too late to request for PDG during ELAP when TSC_U12 is functional [H-2]	
(CA1-3) Request for PDG MCR_U1 -> SCHQ	(UCA-3) MCR_U1 fails to request for PDG during ELAP when TSC_U12 is not functional [H-1]		(UCA-4) MCR_U1 is too late to request for PDG during ELAP when TSC_U12 is not functional [H-2]	
(CA1-4) Request for PDG TSC_U12 -> SCHQ	(UCA-5) TSC_U12 fails to request PDG from SCHQ after receiving request of PDG from MCR_U1 [H-1]		(UCA-6) TSC_U12 is too late to request PDG from SCHQ after receiving request of PDG from MCR_U1 [H-2]	
(CA1-5) Call and check for convocation of offsite workers, CNV MCR_U1 -> CNV	(UCA-7) MCR_U1 fails to call for convocation of offsite workers during ELAP [H-1]		(UCA-8) MCR_U1 is too late to call for convocation of offsite workers during ELAP [H-2]	
(CA2-1) Order Installation of Correct PDG to U1 SCHQ -> SCFO	(UCA-9) SCHQ fails to order installation of correct PDG to U1 after receiving request for PDG from MCR_U1 or TSC_U12 when there is no radiation release, essential equipment/components are prepared, human resources are available due to successful convocation, and telecommunication methods are available [H-1]		(UCA-10) SCHQ is too late to order installation of correct PDG to U1 after receiving request for PDG from MCR_U1 or TSC_U12 when there is no radiation release, essential equipment/components are prepared, human resources are available due to successful convocation, and telecommunication methods are available [H-2]	
(CA2-2) Oversee PDG1 Transportation, Installation, and Connection to U1 SCFO -> CNV	(UCA-11) SCFO fails to oversee the transportation and installation of PDG1 after SCHQ orders installation of correct PDG to U1 [H-1]		(UCA-12) SCFO is too late to oversee the transportation and installation of PDG1 after SCHQ orders installation of correct PDG to U1 [H-2]	
(CA3-1) Provide Equipment to Clean up the Obstacles SCHQ -> SCFO	(UCA-13) SCHQ fails to provide equipment to clean up the obstacles on the road when there are road obstacles [H-1]		(UCA-14) SCHQ is too late to provide equipment to clean up the obstacles on the road when there are road obstacles [H-2]	
(CA3-2) Oversee Road Obstacles Removal SCFO -> CNV	(UCA-15) SCFO fails to oversee the removal of road obstacles after necessary equipment for obstacle removal are provided [H-1]		(UCA-16) SCFO is too late to oversee the removal of road obstacles after necessary equipment for obstacle removal are provided	
(CA3-3) Remove Road Obstacles CNV -> Road Obstacles Cleanup	(UCA-17) CNV fails to remove road obstacles when SCFO oversees the obstacle removal with necessary equipment from SCHQ [H-1]		(UCA-18) CNV is too late to remove road obstacles when SCFO oversees the obstacle removal with necessary equipment from SCHQ [H-2]	
(CA4-1) Transport and Connect the PDG1 CNV -> PDG1	(UCA-19) CNV fails to transport, install, and connect the PDG1 [H-1]		(UCA-20) CNV is too late to transport, install, and connect the PDG1 [H-2]	
(CA5) Connect PDG1 to the EDG refueling tank CNV -> EDG Refueling Tank	(UCA-21) CNV fails to connect PDG1 to the EDG refueling tank connection point after PDG1 has been installed [H-3]		(UCA-22) CNV is too late to connect PDG1 to the EDG refueling tank connection point after PDG1 has been installed [H-3]	(UCA-27) Refueling through the EDG refueling tank stops too soon after being

3 proposed new
UCA types
(3 mainly used)
→ 25 UCAs defined

Base control action from the STAMP model From → To	Not providing / providing too late causes hazard	Providing out of order causes hazard	Stopping too soon causes hazard
(CA4-1) Transport and Connect the PDG1 CNV → PDG1	(UCA-10) [H-1] CNV fails or is too late to transport, and connect the PDG1 when SCFO oversees PDG1 transportation / installation / connection to U1, road obstacles are removed, and there are enough staff left if other units requested PDG installation	(UCA-11) [H-1] CNV connect the PDG1 out of order when SCFO oversees PDG1 transportation / installation / connection to U1, road obstacles are removed, and there are enough staff left if other units requested PDG installation	
(CA5) Connect PDG1 to the EDG refueling tank CNV → EDG Refueling Tank	(UCA-12) [H-3] CNV fails or is too late to connect PDG1 to the EDG refueling tank connection point when SCFO oversees PDG1 transportation / installation / connection to U1, road obstacles are removed, and there are enough staff left if other units requested PDG installation	(UCA-13) [H-3] CNV connect PDG1 to the EDG refueling tank connection point out of order when SCFO oversees PDG1 transportation / installation / connection to U1, road obstacles are removed, and there are enough staff left if other units requested PDG installation	(UCA-14) [H-3] CNV stops refueling through the EDG refueling tank too soon after being connected to the PDG1
) Order Alignment R_U1 → SC_U12	(UCA-15) [H-1] MCR_U1 fails or is too late to order cable alignment to the OSC_U12 when there is EDG and AAC-DG failure		
(CA6-2) Perform Cable Alignment OSC_U12 → PDG1	(UCA-16) [H-1] OSC_U12 fails or is too late to align cables for PDG1 after MCR_U1 orders cable alignment	(UCA-17) [H-1] OSC_U12 align cables for PDG1 out of order after MCR_U1 orders cable alignment	
(CA7-1) Order Breaker Operation MCR_U1 → FO_U1	(UCA-18) [H-1] MCR_U1 fails or is too late to order breaker operation to FO_U1 when there is EDG and AAC-DG failure		
(CA7-2) Perform Breaker Operation FO_U1 → PDG1	(UCA-19) [H-1] FO_U1 fails or is too late to perform breaker operation correctly with PDG1 after MCR_U1 orders breaker operation	(UCA-20) [H-1] FO_U1 perform breaker operation out of order with PDG1 after MCR_U1 orders breaker operation	
(CA7-3) Start/Run PDG1 to Reenergize the Bus FO_U1 → PDG1	(UCA-21) [H-1] FO_U1 fails or is too late to start and run PDG1 to reenergize the bus after CNV transports and connect the PDG1	(UCA-22) [H-1] FO_U1 start and run PDG1 out of order to reenergize the bus after CNV transports and connect the PDG1	(UCA-23) [H-3] FO_U1 stops PDG1 too soon after PDG1 started and the bus is reenergized
(CA8) Give	(UCA-24) [H-3]		

4. Discussions

Discussions

- **There are limitations in using the traditional STPA method**
  - Large amount of resources may be required to explicitly visualize diverse and complicated interactions STAMP models via control loops
    - Solution: develop a tool (TRACEIT)
  - After control loops are successfully created, HRA practitioners also have to spend a huge amount of resources on identifying the catalog of UCAs based on STPA
    - Solution: simplify/modify STPA to fit the HRA purposes
- **The UCAs may be screened or combined afterward for final HFE subtask analysis**
- **Proposed methodology can be utilized for the multi-unit HFE subtask analysis, allowing the HRA experts to use easy and repetitive systematic approach for the MU-HRA**

THANK YOU