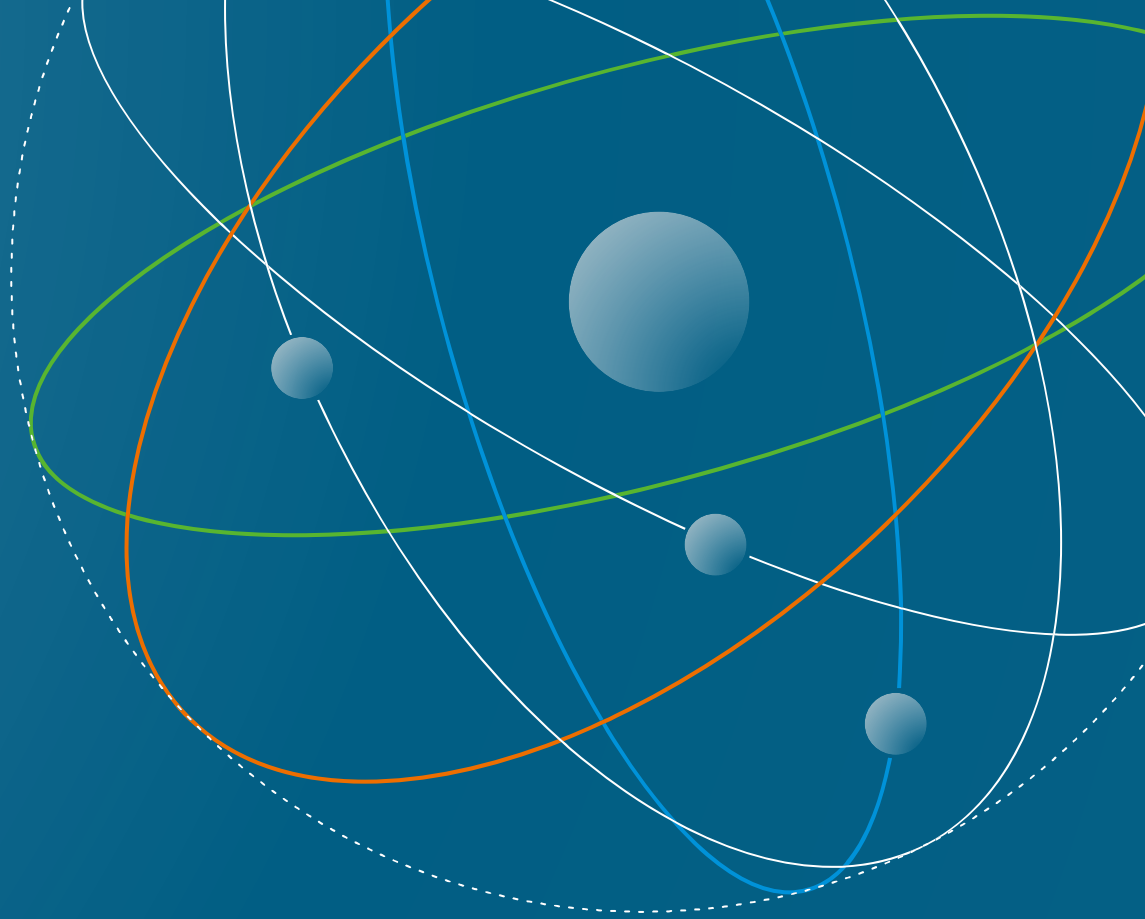
2023 KNS Spring / Workshop (F)



STAMP/STPA-based Research on the Application of the Domestic Nuclear Industry

2023 / 05 / 17(Wed.)

Shin Sung-Min

KAERI Korea Atomic Energy Research Institute / Risk Assessment Research Division

A hazard situation(loss scenario)

in modern complex safety control systems **can be caused by**

- **interactions** between system components or between system components and the environment

- **not only** combinations of the **failures** of system components

CONTENTS

1 HANARO: high-performing multipurpose research reactor designed and built independently by kaeri with a thermal power capacity of 30 mw
2 MACST: Multiple Barrier Accident Coping Strategy

Part 1

Pilot studies applying STPA

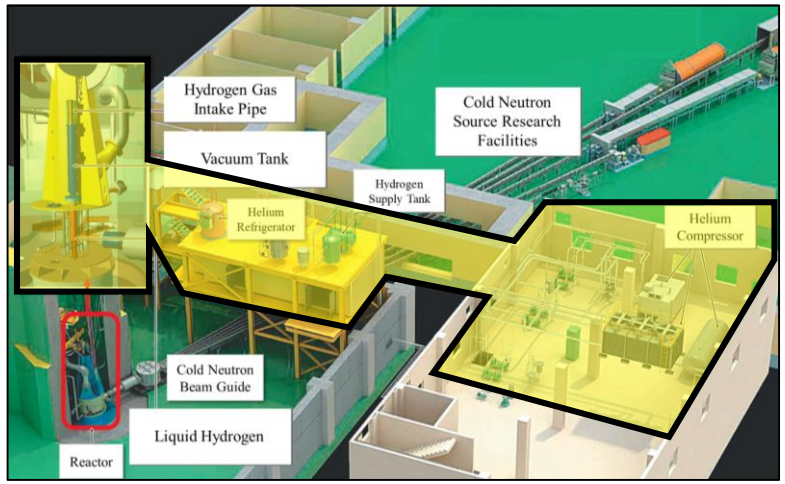
Research background

Year	RRS auto trip	Manual trip	RPS auto trip	Main cause
2005	0	0	1	Instantaneous outages(1)
2006	0	0	1	Instantaneous outages(1)
2007	2	0	1	Error in trip setpoint setup(1), Control rod(1), Instantaneous outages(1)
2008	1	0	0	Control rod(1), Delayed neutron(1)
2009	6	0	0	CNS(3), FTL(3)
2010	9	0	0	CNS Bubbling (4), I&C(1), Control rod(2), Pump oil(1), Reflector
2011	0	0	1	Bath high radiation(1)
2012	1	0	1	Bath high radiation(1), Human error in CNS(1)
2013	1	0	0	CNS hydrogen pressure(1)
2014	0	1	0	Bio-D power terminal burnout(1)
2015	Seismic retrofitting (2016.05 - 2017.04)			
2016				
2017	0	1	0	Bath high temperature(1)
2018	1	1	0	Control rod(1), CNS hydrogen pressure(1)
2019	1	0	0	CNS hydrogen pressure(1), Human error(1)

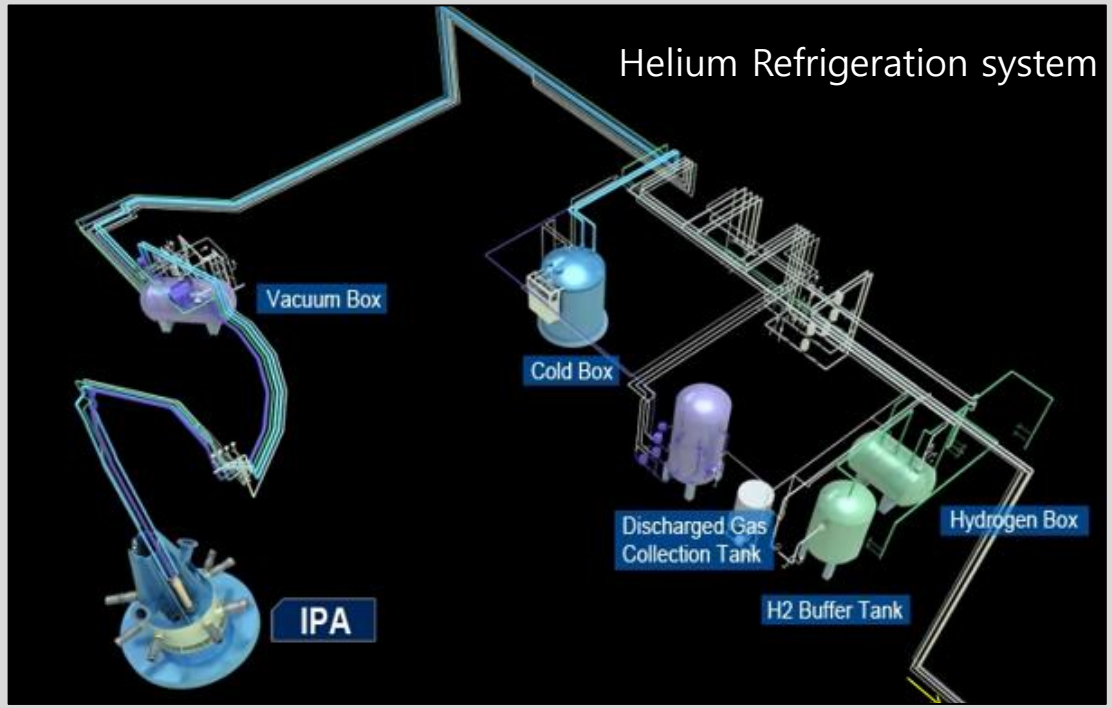
HANARO unplanned-trip by year

➔ In 2020, as part of a comprehensive plan to increase the utilisation of the research reactor HANARO, STPA was piloted on the CNS(Cold Neutron Source) system **to identify hidden problems between operations** in addition to equipment aging or failure.

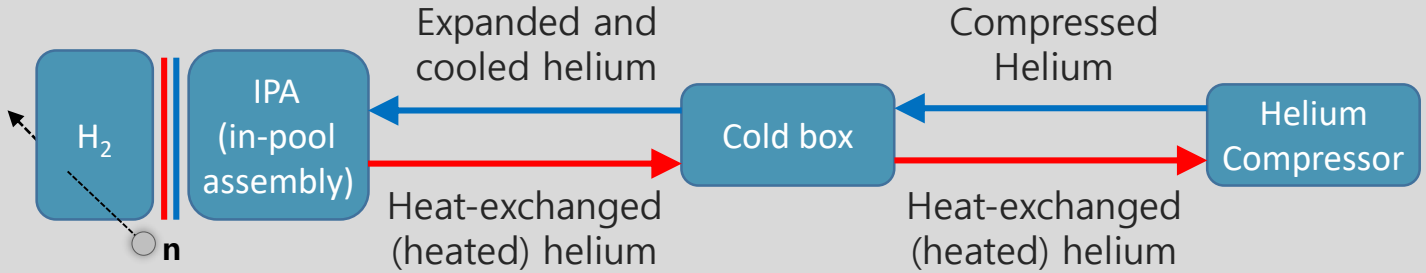
Overview of the target system



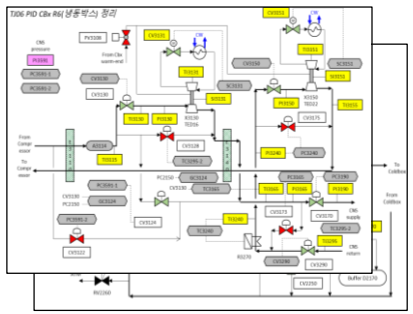
Overview of CNS system



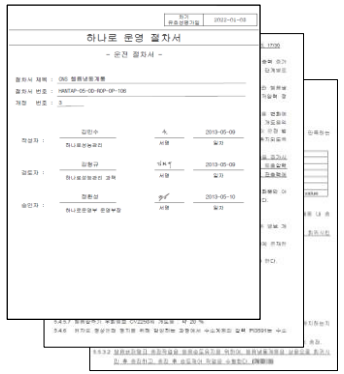
Helium refrigeration system	
Key Features	Removes heat from the hydrogen system
Key components	Cold box, Helium compressor
Linked systems	Hydrogen system, Chilled water system, Compressed air supply system, Electricity supply system, Control systems



Perform STPA (1/2)



System configuration



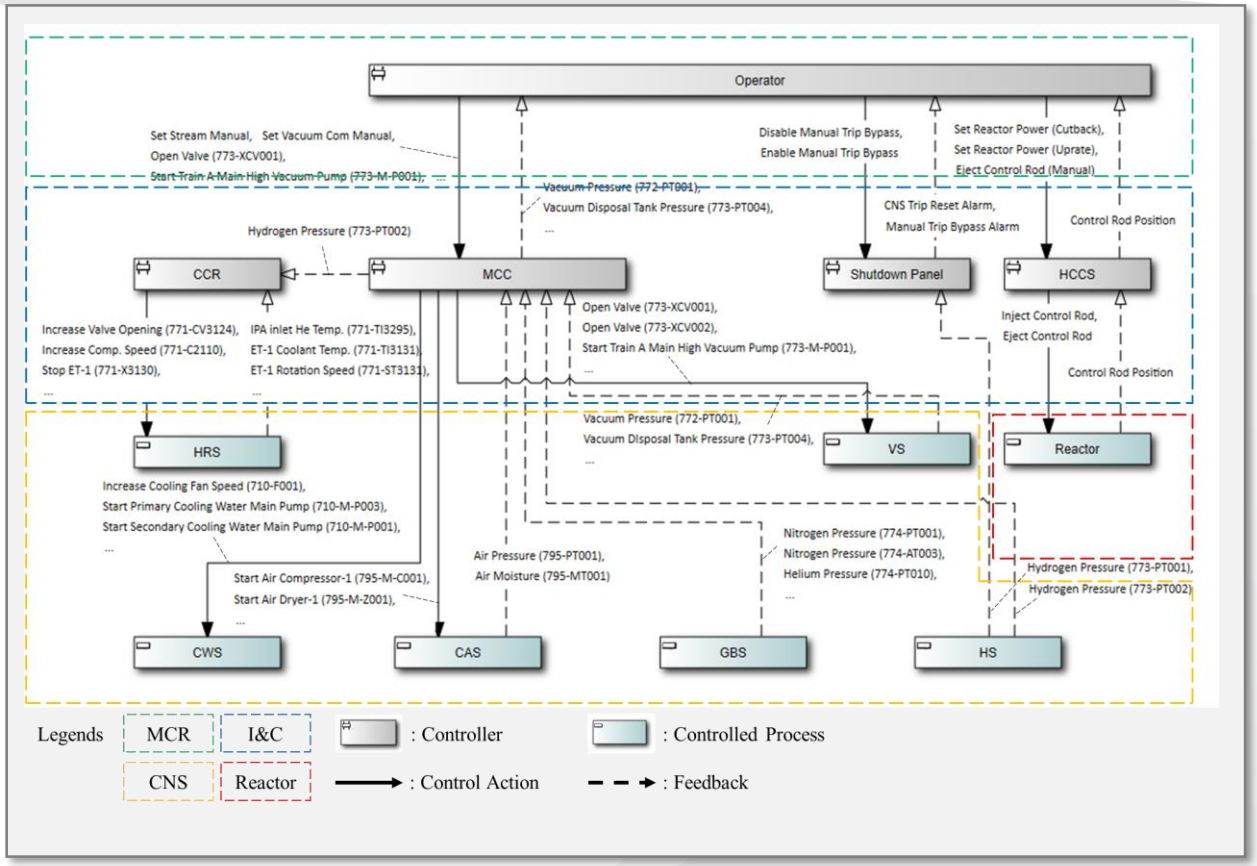
System operation procedure

Configuration and operations of Helium refrigeration system

1) Define purpose of the analysis → 2) Model the control structure → 3) Identify unsafe control actions ····· 4) Identify loss scenario

Loss	
L-1	RRS generates spurious trip signal due to CNS hydrogen high pressure (> 200 kPa)
L-2	RRS generates spurious trip signal due to CNS hydrogen low pressure (< 120 kPa)

Hazard	
H-1	HRS does not maintain hydrogen thermosiphon (L-1, L-2)
H-2	VS does not maintain vacuum in vacuum box of IPA (L-1)
H-3	CWS does not provide enough cooling water to heat exchanger tube in HRS (L-1, L-2)
H-4	GBS does not provide enough air to air operated valves in VS (L-1)
H-5	Operator or I&C system provide abnormal power uprate/cutback operation (L-1, L-2)
H-6	CAS does not provide enough air to air operated valves in HRS (L-1, L-2)



Control structure
(5 controllers, 7 controlled processes, 103 CAs and 122 FBs)

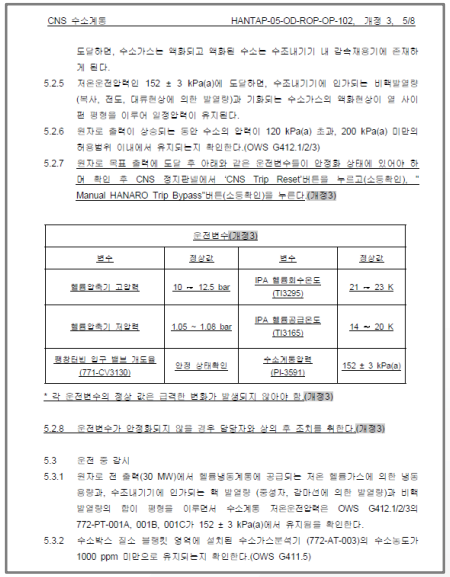
HRS: Helium Refrigeration System VS: Vacuum System CWS: Cooling Water System
GBS: Bas Blanket system CAS: Compressed Air System HS: Hydrogen System

Perform STPA (2/2)

1) Define purpose of the analysis → 2) Model the control structure → **3) Identify unsafe control actions** ⋯ 4) Identify loss scenario

127 UCAs

Control Action	UCA Types					
	(a) Provided, but not needed and unsafe	(b) Provided, but the intensity is too much or little	(c) Provided, but executed in incorrect order	(d) Provided, but the duration is too long or short	(e) Provided, but the starting time is too soon or late	(f) Not provided, when needed to maintain safety
Open Valve (773-XCV001)	N/A	N/A	N/A	N/A	(UCA-60) Valve 773-XCV001 is opened too late when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]	(UCA-61) Valve 773-XCV001 is not opened when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]
Disable Manual Trip Bypass	N/A	N/A	(UCA-57) Operator manipulated 'Manual HANARO Trip Bypass' button, before 'CNS Trip Reset' button during OP-102 5.2.7 [H-5]	N/A	(UCA-58) Operator manipulated trip bypass buttons, before checking the stability of process parameter during OP-102 5.2.7 [H-5]	N/A
Enable Manual Trip Bypass	N/A	N/A	N/A	N/A	N/A	(UCA-112) Operator does not press 'Manual HANARO Trip Bypass' button before reactor power cutback during OP-01 5.2.1.1
Set Reactor Power (Cutback)	N/A	(UCA-8) Operator sets reactor power level too low via OWS in shutdown phase during OP-01 5.2 [H-5]	N/A	N/A	(UCA-9) Operator sets reactor power too soon via OWS before target power level is reached during OP-01 5.2 [H-5]	N/A
Start Train B Low Vacuum Pump (773-M-P004)	(UCA-62) Low vacuum pump M-P004 runs when VDT pressure PT-004 is high resulting in pump rupture during OP-103 5.1.5 [H-2]	N/A	N/A	(UCA-63) Low vacuum pump M-P004 stopped too soon while running when VDT pressure PT-004 is high during OP-103 5.1.5 [H-2]	(UCA-64) Low vacuum pump M-P004 started too late when VDT pressure PT-004 is high during OP-103 5.1.5 [H-2]	(UCA-65) Low vacuum pump M-P004 does not start running when VDT pressure PT-004 is high during OP-103 5.1.5 [H-2]
Start Train A Low Vacuum Pump (773-M-P003)	N/A	N/A	N/A	N/A	N/A	(UCA-107) Operator does not start low vacuum pump M-P003 via OWS when VS is in manual mode during OP-103 5.2.2 [H-2]


CNS 수소계통 HANTAP-05-OD-ROP-OP-102, 개정 3, 5/8

도달하면, 수소가스는 역화되고 역화된 수소는 수조내기기 내 압축재공기에 존재하게 된다.

5.2.5 저온운전압력인 152 ± 3 kPa(a)에 도달하면, 수조내기기에 인가되는 비핵발열량(복사, 전도, 대류현상에 의한 발열량)과 기화되는 수소가스의 역화현상이 열 사이클 평형을 이루어 일정압력이 유지된다.

5.2.6 원자로 출력이 상승되는 동안 수소의 압력이 120 kPa(a) 초과, 200 kPa(a) 미만의 허용범위 이내에서 유지되는지 확인한다.(OWS G412.1/2/3)

5.2.7 원자로 목표 출력에 도달 후 아래와 같은 운전변수들이 안정화 상태에 있어야 하며 확인 후 CNS 정지판넬에서 "CNS Trip Reset"버튼을 누르고(소등확인), "Manual HANARO Trip Bypass"버튼(소등확인)을 누른다.(개정3)

운전변수(개정3)

변수	정상값	변수	정상값
헬륨압축기 고압력	10 ~ 12.5 bar	IPA 헬륨입구온도 (TI3295)	21 ~ 23 K
헬륨압축기 저압력	1.05 ~ 1.08 bar	IPA 헬륨공급온도 (TI3165)	14 ~ 20 K
평형터빈 입구 헬륨 가도율 (771-CV3130)	안정 상태확인	수소계통압력 (PI-3591)	152 ± 3 kPa(a)

* 각 운전변수의 정상 값은 급격한 변화가 발생되지 않아야 함.(개정3)

5.2.8 운전변수가 안정화되지 않을 경우 담당자와 상의 후 조치를 취한다.(개정3)

5.3 운전 중 감시

5.3.1 원자로 전 출력(30 MW)에서 헬륨냉동계통에 공급되는 저온 헬륨가스에 의한 냉동용량과, 수조내기기에 인가되는 핵 발열량 (중성자, 감마선에 의한 발열량)과 비핵발열량의 합이 평형을 이루면서 수소계통 저온운전압력은 OWS G412.1/2/3와 772-PT-001A, 001B, 001C가 152 ± 3 kPa(a)에서 유지됨을 확인한다.

5.3.2 수소방출 감시 불평형 영역에 설치된 수소가스분석기 (772-AT-003)의 수소농도가 1000 ppm 이만으로 유지되는지 확인한다.(OWS G411.5)

Expert review on UCAs of HANARO CNS system

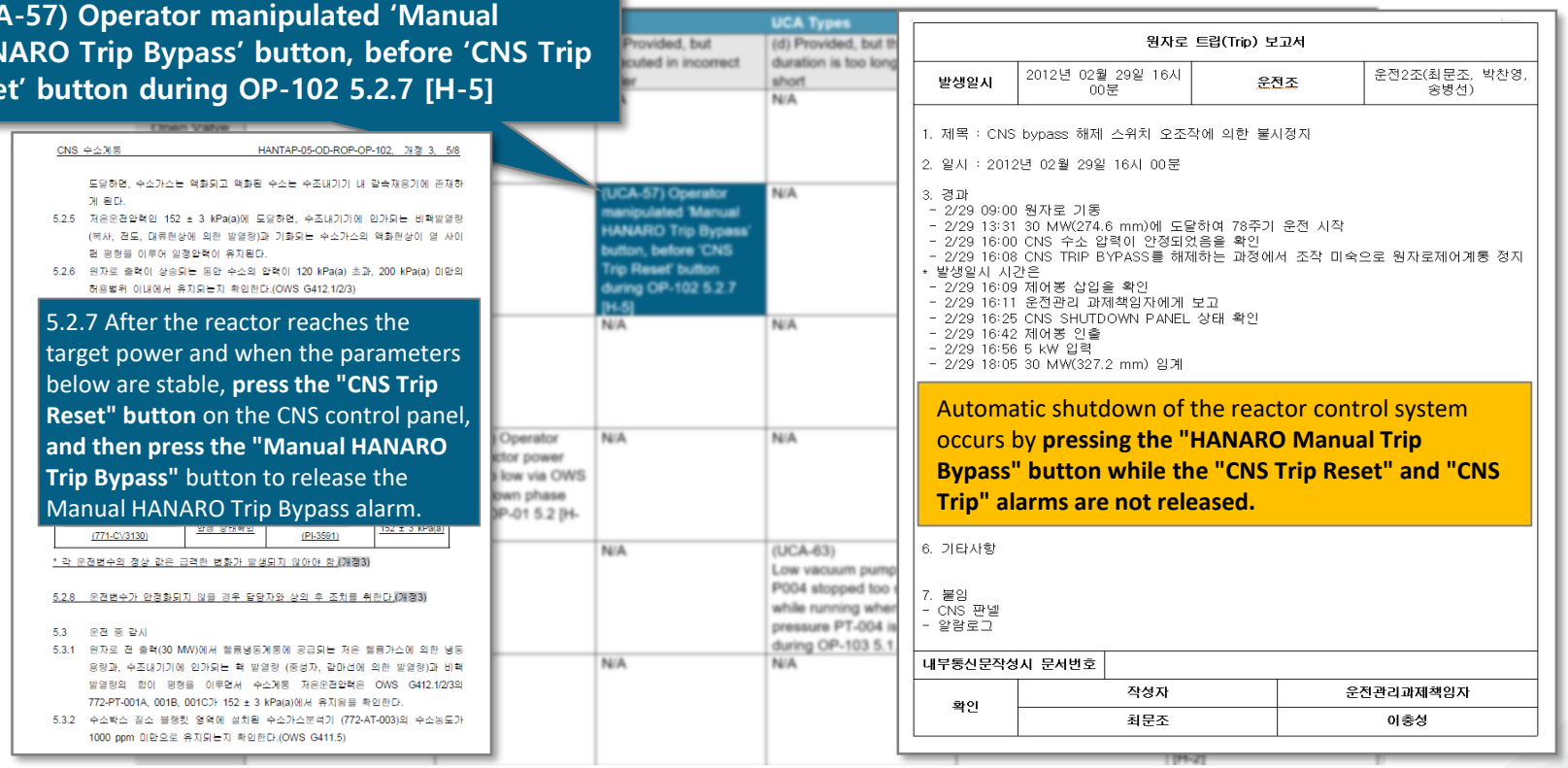
Insights

- It is crucial to change the way(expand our thinking) about safety-related question.

What happens if it is unavailable/failed?

(If there is an order to it),
What happens if the order is reversed?

(UCA-57) Operator manipulated 'Manual HANARO Trip Bypass' button, before 'CNS Trip Reset' button during OP-102 5.2.7 [H-5]



CNS 수소계통 HANTAP-05-OD-ROP-OP-102, 개정 3, 5/8

도달하면, 수소가스는 액화되고 액화된 수소는 수소내기기 내 감속재용기에 존재하게 된다.

5.2.5 저온운전압력인 152 ± 3 kPa(a)에 도달하면, 수소내기기에 인가되는 비핵발열량(복사, 전도, 대류현상에 의한 발열량)과 기화되는 수소가스의 액화현상이 열 사이펌 평형을 이루어 일정압력이 유지된다.

5.2.6 원자로 출력이 상승되는 동안 수소의 압력이 120 kPa(a) 초과, 200 kPa(a) 미만의 허용범위 이내에서 유지되는지 확인한다.(OWS G412.1/2/3)

5.2.7 After the reactor reaches the target power and when the parameters below are stable, **press the "CNS Trip Reset" button** on the CNS control panel, **and then press the "Manual HANARO Trip Bypass"** button to release the Manual HANARO Trip Bypass alarm.

(771-CV3130) (PI-3591) 152 ± 3 kPa(a)

* 각 운전변수의 정상 값은 급격한 변화가 발생되지 않아야 함.(개정3)

5.2.8 운전변수가 안정화되지 않을 경우 담당자와 상의 후 조치를 취한다.(개정3)

5.3 운전 중 감시

5.3.1 원자로 전 출력(30 MW)에서 헬륨냉동계통에 공급되는 저온 헬륨가스에 의한 냉동용량과, 수소내기기에 인가되는 핵 발열량 (중성자, 감마선에 의한 발열량)과 비핵발열량의 합이 평형을 이루면서 수소계통 저온운전압력은 OWS G412.1/2/3의 772-PT-001A, 001B, 001C가 152 ± 3 kPa(a)에서 유지됨을 확인한다.

5.3.2 수소탱크 질소 블랭킷 영역에 설치된 수소가스분석기 (772-AT-003)의 수소농도가 1000 ppm 미만으로 유지되는지 확인한다.(OWS G411.5)

UCA Types

(d) Provided, but duration is too long / short

N/A

(UCA-57) Operator manipulated 'Manual HANARO Trip Bypass' button, before 'CNS Trip Reset' button during OP-102 5.2.7 [H-5]

(UCA-63) Low vacuum pump P004 stopped too ... while running ... pressure PT-004 ... during OP-103 5.1

Operation procedure

원자로 트립(Trip) 보고서

발생일시	2012년 02월 29일 16시 00분	운전조	운전2조(최문조, 박찬영, 송병선)

1. 제목 : CNS bypass 해제 스위치 오조작에 의한 불시정지

2. 일시 : 2012년 02월 29일 16시 00분

3. 경과
- 2/29 09:00 원자로 기동
- 2/29 13:31 30 MW(274.6 mm)에 도달하여 78주기 운전 시작
- 2/29 16:00 CNS 수소 압력이 안정되었음을 확인
- 2/29 16:08 CNS TRIP BYPASS를 해제하는 과정에서 조작 미숙으로 원자로제어계통 정지

* 발생일시 시간은
- 2/29 16:09 제어봉 삽입을 확인
- 2/29 16:11 운전관리 과제책임자에게 보고
- 2/29 16:25 CNS SHUTDOWN PANEL 상태 확인
- 2/29 16:42 제어봉 인출
- 2/29 16:56 5 kW 임력
- 2/29 18:05 30 MW(327.2 mm) 임계

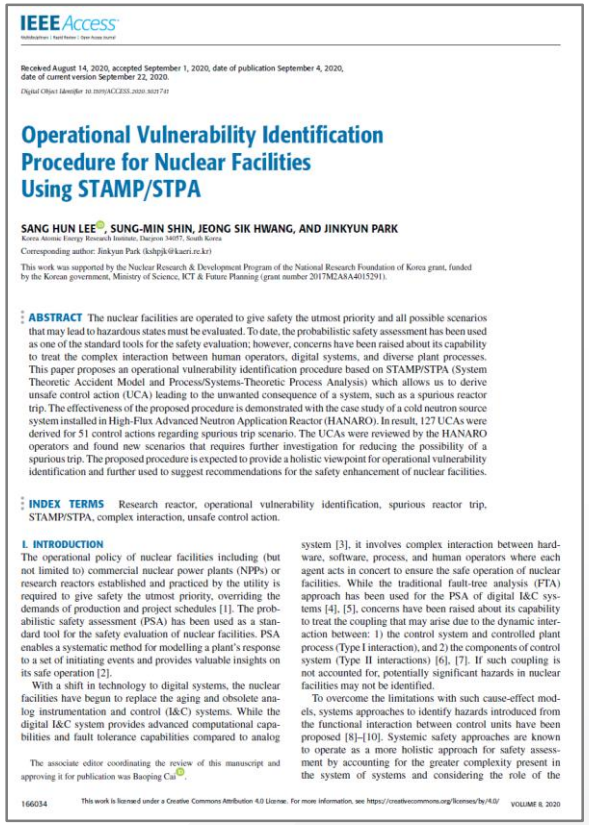
Automatic shutdown of the reactor control system occurs by **pressing the "HANARO Manual Trip Bypass" button while the "CNS Trip Reset" and "CNS Trip" alarms are not released.**

6. 기타사항

7. 불임
- CNS 판넬
- 알람로그

내부통신문작성시 문서번호		
확인	작성자	운전관리과제책임자
	최문조	이충성

Reactor trip report



IEEE Access

Received August 14, 2020, accepted September 1, 2020, date of publication September 4, 2020, date of current version September 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3021741

Operational Vulnerability Identification Procedure for Nuclear Facilities Using STAMP/STPA

SANG HUN LEE, SUNG-MIN SHIN, JEONG SIK HWANG, AND JINKYUN PARK

Korea Atomic Energy Research Institute, Daejeon 34057, South Korea

Corresponding author: Jinkyun Park (kshpjk@kaeri.re.kr)

This work was supported by the Nuclear Research & Development Program of the National Research Foundation of Korea grant, funded by the Korean government, Ministry of Science, ICT & Future Planning (grant number 2017M2A8A4015291).

ABSTRACT The nuclear facilities are operated to give safety the utmost priority and all possible scenarios that may lead to hazardous states must be evaluated. To date, the probabilistic safety assessment has been used as one of the standard tools for the safety evaluation; however, concerns have been raised about its capability to treat the complex interaction between human operators, digital systems, and diverse plant processes. This paper proposes an operational vulnerability identification procedure based on STAMP/STPA (System Theoretic Accident Model and Process/Systems-Theoretic Process Analysis) which allows us to derive unsafe control action (UCA) leading to the unwanted consequence of a system, such as a spurious reactor trip. The effectiveness of the proposed procedure is demonstrated with the case study of a cold neutron source system installed in High-Flux Advanced Neutron Application Reactor (HANARO). In result, 127 UCAs were derived for 51 control actions regarding spurious trip scenario. The UCAs were reviewed by the HANARO operators and found new scenarios that requires further investigation for reducing the possibility of a spurious trip. The proposed procedure is expected to provide a holistic viewpoint for operational vulnerability identification and further used to suggest recommendations for the safety enhancement of nuclear facilities.

INDEX TERMS Research reactor, operational vulnerability identification, spurious reactor trip, STAMP/STPA, complex interaction, unsafe control action.

I. INTRODUCTION

The operational policy of nuclear facilities including (but not limited to) commercial nuclear power plants (NPPs) or research reactors established and practiced by the utility is required to give safety the utmost priority, overriding the demands of production and project schedules [1]. The probabilistic safety assessment (PSA) has been used as a standard tool for the safety evaluation of nuclear facilities. PSA enables a systematic method for modelling a plant's response to a set of initiating events and provides valuable insights on its safe operation [2].

With a shift in technology to digital systems, the nuclear facilities have begun to replace the aging and obsolete analog instrumentation and control (I&C) systems. While the digital I&C system provides advanced computational capabilities and fault tolerance capabilities compared to analog system [3], it involves complex interaction between hardware, software, process, and human operators where each agent acts in concert to ensure the safe operation of nuclear facilities. While the traditional fault-tree analysis (FTA) approach has been used for the PSA of digital I&C systems [4], [5], concerns have been raised about its capability to treat the coupling that may arise due to the dynamic interaction between: 1) the control system and controlled plant process (Type I interaction), and 2) the components of control system (Type II interactions) [6], [7]. If such coupling is not accounted for, potentially significant hazards in nuclear facilities may not be identified.

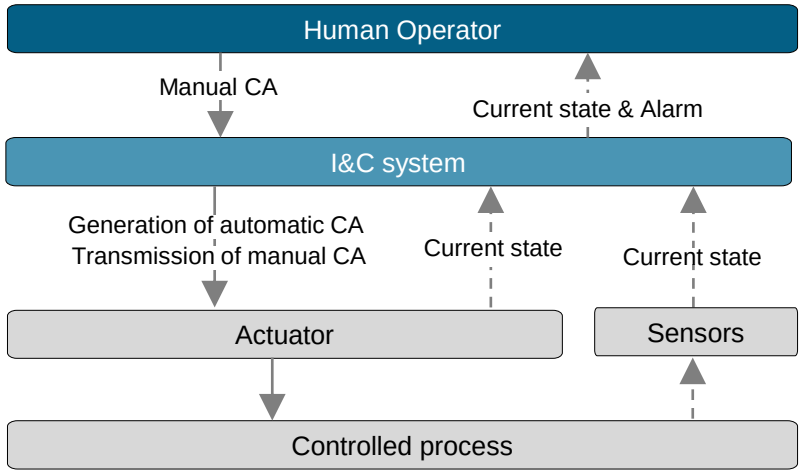
To overcome the limitations with such cause-effect models, systems approaches to identify hazards introduced from the functional interaction between control units have been proposed [8]–[10]. Systemic safety approaches are known to operate as a more holistic approach for safety assessment by accounting for the greater complexity present in the system of systems and considering the role of the

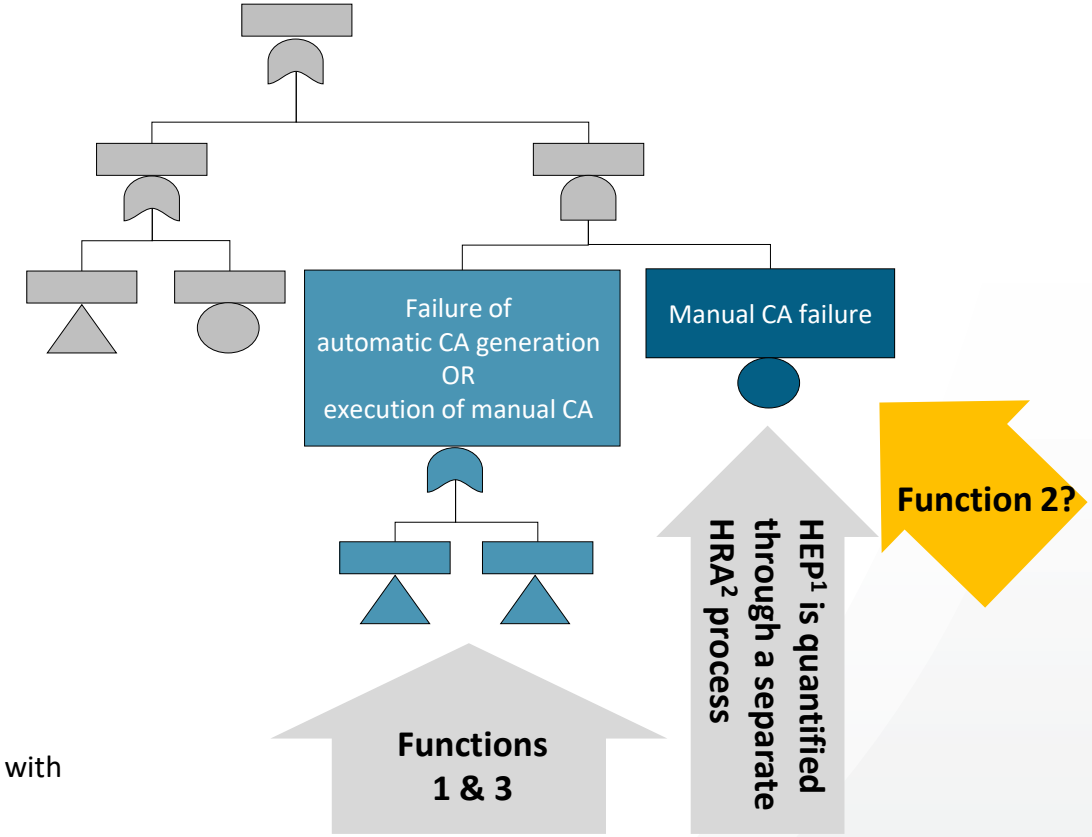
The associate editor coordinating the review of this manuscript and approving it for publication was Baoping Cai.

166034 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/ VOLUME 8, 2020

Operational vulnerability identification procedure for nuclear facilities using STAMP/STPA, SH Lee, SM Shin, JS Hwang, J Park, IEEE access 8, 166034-166046, 2020

Research background





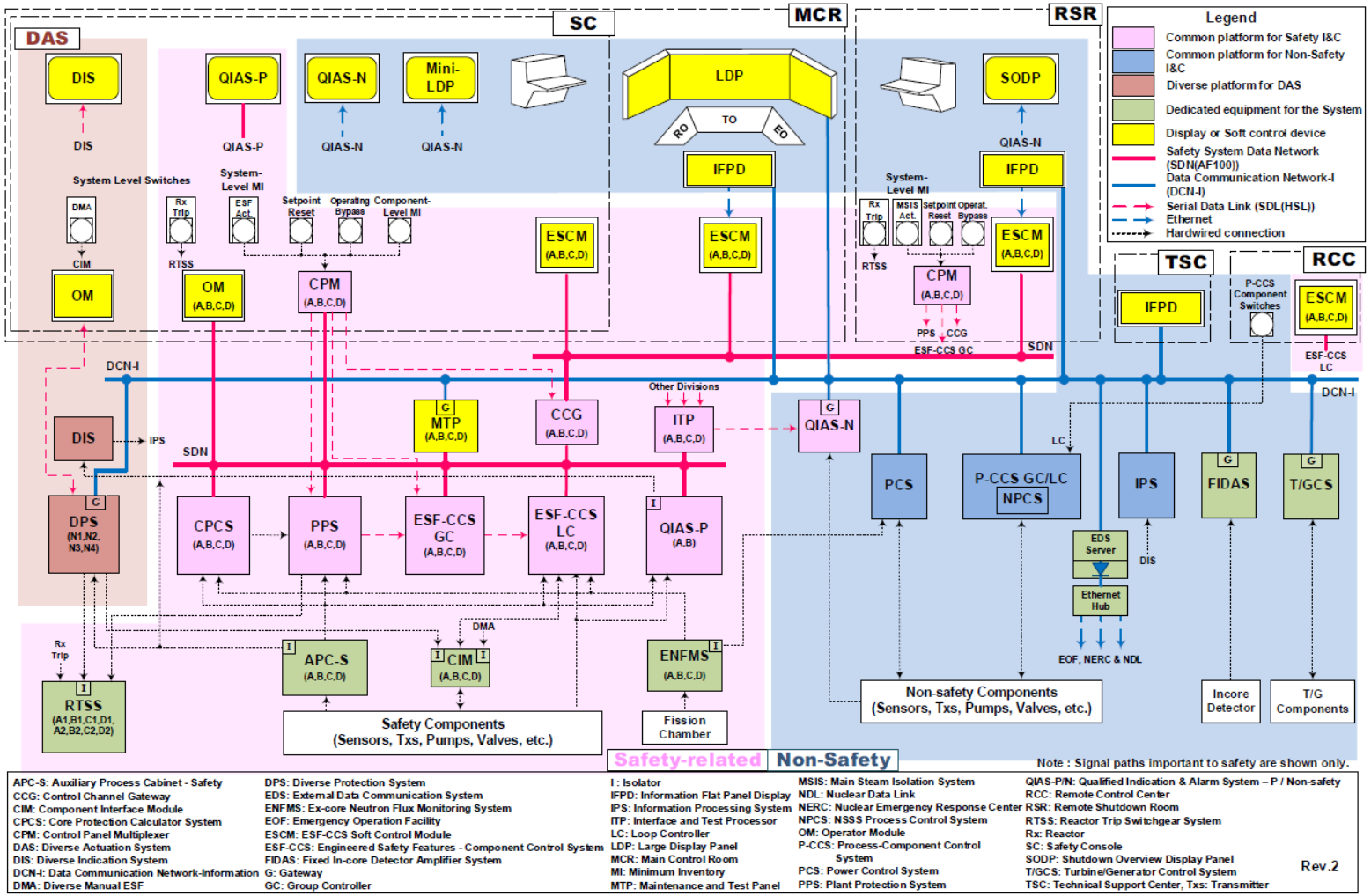
Function-1)
Obtaining the current state of the controlled process through sensors, generating an automatic control action (CA) based on it, and transmitting it to the actuator.

Function-2)
Obtaining the current states of the controlled process and actuator and transmitting them with relevant alarms to the human operator.

Function-3)
Receiving the manual CA from the human operator and transmitting it to the actuator.

1 HEP: Human error probability
2 HRA: Human reliability assessment

Overview of the target system



Advanced Power Reactor(APR) 1400 I&C system overview architecture[1]

Assumptions

Assuming a situation causing pressurizer low pressure (Only the following FBs are assumed to be available):

For automatic trip by PPS
- WR PZR PR (wide range PZR. Pressure)

For manual trip by human operator
- WR PZR PR (wide range PZR. Pressure)
- NR PZR PR (narrow range PZR. Pressure)
- PZR Low PR ALM (PZR low pressure alarm)
- PZR LV (PZR level)
- PZR Low LV ALM (PZR (low level alarm)
- Log PWR (Log power)
- Linear PWR (Linear power)
- RPS trip STAT (RPS trip status)
- CH trip STAT (Channel trip status)

* It should be noted that the pilot study has been conducted under conservative assumptions as some diversity & redundancy features are excluded

1 KEPCO and KHNP "ARP1400 design control document tier2: chapter 7 instrumentation and controls", APR1400-K-FS-1400-NP Rev 3. Aug. 2018.

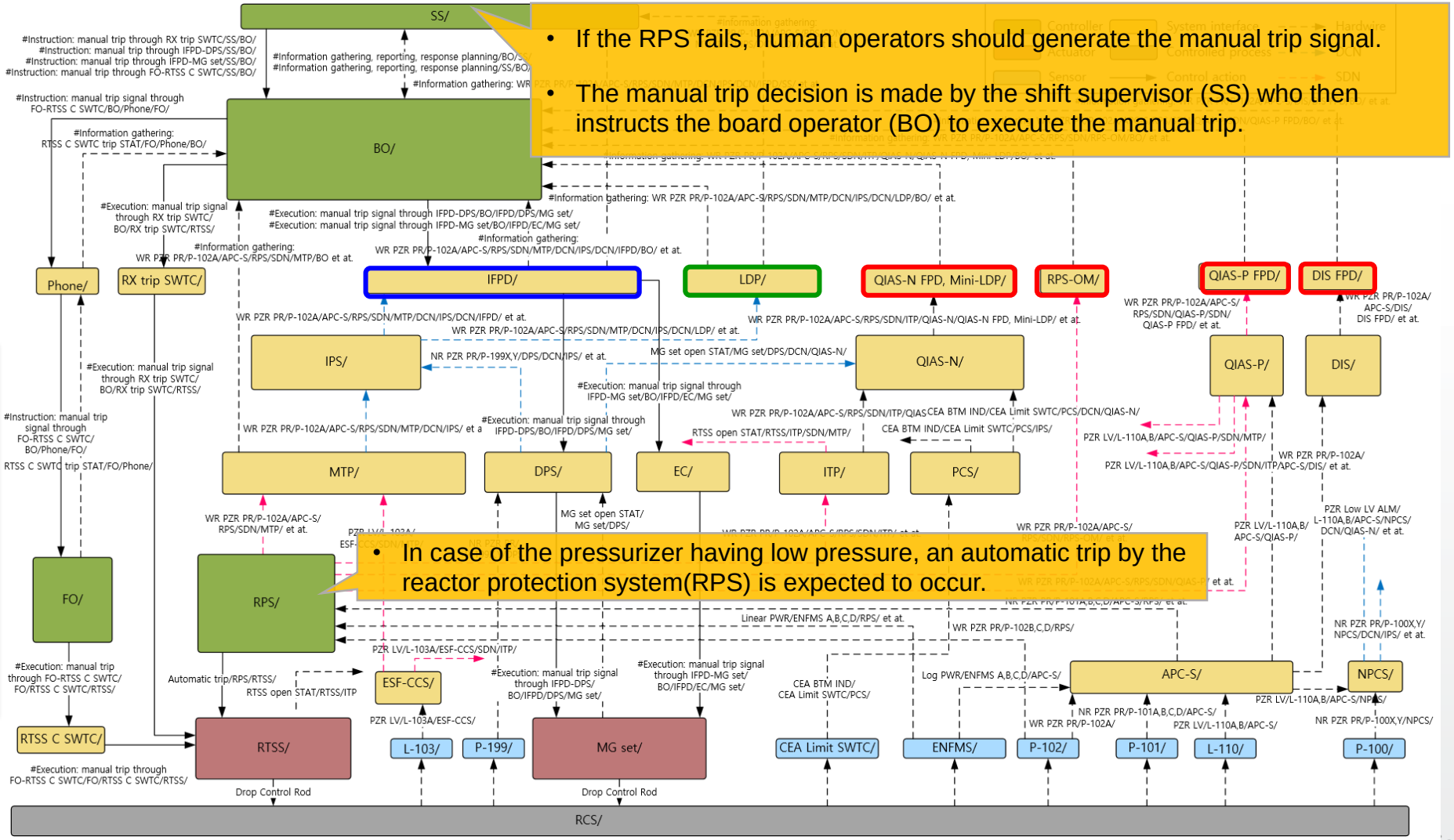
Perform STPA (1/2)

1) Define purpose of the analysis — **2) Model the control structure** — **3) Identify unsafe control actions** — **4) Identify loss scenario**

Loss	
L-1	Reactor fuel is damaged

Hazard	
H-1	Failure of automatic trip through RPS (L-1)
H-2	Failure of manual trip by human operators (L-1)

FBs to the human operators (SS and BO)		
(1) WR PZR PR	(4) PZR LV	(7) Linear PWR
(2) NR PZR PR	(5) PZR Low LV ALM	(8) RPS trip STAT
(3) PZR Low PR ALM	(6) Log PWR	(9) CH trip STAT



Perform STPA (2/2)

1) Define purpose of the analysis — 2) Model the control structure — **3) Identify unsafe control actions** — **4) Identify loss scenario**

➔ UCA: SS does not instruct the manual trip when RPS fails.

➔ How does a failure of any component (cause) that causes the RPS to fail affect the soundness of FBs referenced in the manual trip decision?

#	FBs and their transmission paths			Components that cause RPS failure & Soundness of FB transmission		
	FBs	HSI[1]	Transmission paths	P-102(WR PZR PR sensor)	APC-S	RPS
1	WR PZR PR (Ch. A)	IFPD	WR PZR PR(Ch. A)P-102→APC-S(P)→RPS→SDN→MTP→DCN→IPS→DCN→IFPD	X	X	X
2	WR PZR PR (Ch. B,C,D)		WR PZR PR(Ch. B,C,D)P-102→RPS→SDN→MTP→DCN→IPS→DCN→IFPD	X		X
3	NR PZR PR (Ch. A,B,C,D)		NR PZR PR(Ch. A,B,C,D)P-101→APC-S(P)→RPS→SDN→MTP→DCN→IPS→DCN→IFPD		X	X
4	NR PZR PR (Ch. X,Y)		NR PZR PR(Ch. X,Y)P-199→DPS→DCN→IPS→DCN→IFPD			
5	Linear power (Ch. A,B,C,D)		Linear power(Ch. A,B,C,D)ENFMS→RPS→SDN→MTP→DCN→IPS→DCN→IFPD			X
6	Log power (Ch. A,B,C,D)		Log power(Ch. A,B,C,D)ENFMS→RPS→SDN→MTP→DCN→IPS→DCN→IFPD			X
7	CH trip status		CH trip status→RPS→SDN→MTP→DCN→IPS→DCN→IFPD			X
8	RPS trip status		RPS trip status→RPS→SDN→MTP→DCN→IPS→DCN→IFPD			X
9	MG set open status		MG set open status→MG set→DPS→DCN→IPS→DCN→IFPD			
10	RTSS open status		RTSS open status→RTSS→ITP→SDN→MTP→DCN→IPS→DCN→IFPD			
11	WR PZR PR	LDP	WR PZR PR→P-102→APC-S(P)→RPS→SDN→MTP→DCN→IPS→DCN→LDP	X	X	X
12	WR PZR PR (Ch. B,C,D)		WR PZR PR(Ch. B,C,D)P-102→RPS→SDN→MTP→DCN→IPS→DCN→LDP	X		X
13	Linear power (Ch. A,B,C,D)		Linear power(Ch. A,B,C,D)ENFMS→RPS→SDN→MTP→DCN→IPS→DCN→LDP			X
14	Log power (Ch. A,B,C,D)		Log power(Ch. A,B,C,D)ENFMS→RPS→SDN→MTP→DCN→IPS→DCN→LDP			X
15	RPS trip status		RPS trip status→RPS→SDN→MTP→DCN→IPS→DCN→LDP			X
16	MG set open status		MG set open status→MG set→DPS→DCN→IPS→DCN→LDP			
17	RTSS open status		RTSS open status→RTSS→ITP→SDN→MTP→DCN→IPS→DCN→LDP			
18	WR PZR PR (Ch. A)	QIAS-N FPD, Mini-LDP	WR PZR PR(Ch. A)P-102→APC-S(P)→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP	X	X	X
19	WR PZR PR (Ch. B,C,D)		WR PZR PR(Ch. B,C,D)P-102→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP	X		X
20	NR PZR PR (Ch. A,B,C,D)		NR PZR PR(Ch. A,B,C,D)P-101→APC-S(P)→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP		X	X
21	Linear power (Ch. A,B,C,D)		Linear power(Ch. A,B,C,D)ENFMS→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP			X
22	Log power (Ch. A,B,C,D)		Log power(Ch. A,B,C,D)ENFMS→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP			X
23	CH trip status		CH trip status→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP			X
24	RPS trip status		RPS trip status→RPS→SDN→ITP→QIAS-N→QIAS-N FPD, Mini-LDP			X
25	MG set open status		MG set open status→MG set→DPS→DCN→QIAS-N→QIAS-N FPD, Mini-LDP			
26	CEA floor indicator		CEA floor indicator→CEA Limit SWTC→PCS→DCN→QIAS-N→QIAS-N FPD, Mini-LDP			
27	WR PZR PR (Ch. A)	RPS-OM	WR PZR PR(Ch. A)P-102→APC-S(P)→RPS→SDN→RPS-OM	X	X	X
28	WR PZR PR (Ch. B,C,D)		WR PZR PR(Ch. B,C,D)P-102→RPS→SDN→RPS-OM	X		X
29	CH trip status		CH trip status→RPS→SDN→RPS-OM			X
30	RPS trip status		RPS trip status→RPS→SDN→RPS-OM			X
31	WR PZR PR (Ch. A)	QIAS-P FPD	WR PZR PR(Ch. A)P-102→APC-S(P)→RPS→SDN→QIAS-P→SDN→QIAS-P FPD	X	X	X
32	WR PZR PR (Ch. B)		WR PZR PR(Ch. B)P-102→RPS→SDN→QIAS-P→SDN→QIAS-P FPD	X		X
33	Log power (Ch. A,B)		Log power(Ch. A,B)ENFMS→RPS→SDN→QIAS-P→SDN→QIAS-P FPD			X
34	WR PZR PR (Ch. A)	DIS FPD	WR PZR PR(Ch. A)P-102→APC-S(P)→DIS→DIS FPD	X	X	
35	Log power (Ch. A,B,C,D)		Log power(Ch. A,B,C,D)ENFMS→APC-S(NF)→DIS→DIS FPD		X	

1 HIS: Human System Interface

Insights

- **STAMP/STPA is well suited to consider hazards resulting from the interaction of nuclear I&C system with human operators**, as it provides a basis for representing any type of controller, mechanical or human, in a single control structure and for examining shared feedbacks or transition paths.

- Human errors are symptom of system error; **It is possible to derive the realistic failure conditions of the DI&C system to be confirmed** whether it can be handled well by human operators.

Reliability Engineering and System Safety 213 (2021) 107698

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

STPA-Based Hazard and Importance Analysis on NPP Safety I&C Systems Focusing on Human–System Interactions

SUNG-MIN SHIN *, SANG HUN LEE, SEUNG KI SHIN, INSEOK JANG, JINKYUN PARK

Korea Atomic Energy Research Institute, 111 Daedeok-daero, 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057

ARTICLE INFO

KEYWORDS:
STPA
I&C
NPP
Human-system Interaction

ABSTRACT

To ensure system safety, conducting required control actions (CAs) in time at the right place is essential. Among the CAs, safety critical ones such as reactor trip signals in a nuclear power plant are preferentially and automatically generated by the instrumentation and control (I&C) system. If necessary, however, they can also be generated manually by human operators. Even for manual CAs, though, the I&C system is still needed to convey relevant feedback to the human operators. It is therefore indispensable to analyze the risk associated with the transmission of feedback to the human operators in terms of the condition of the I&C system. In this context, System-Theoretic Process Analysis (STPA) can provide a framework to link the conditions of the I&C system with the feedback transmission for manual CA generation. Based on STPA, this study proposes a method to analyze I&C system hazards and assess the relative importance of system components in terms of human–system interactions, or more specifically, feedback transmission for manual CA generation. As a feasibility study, the method is applied to an example case requiring reactor trip signal generation in the Advanced Power Reactor 1400 (APR-1400).

1. INTRODUCTION

Instrumentation and control (I&C) systems in nuclear power plants (NPPs) play a vital role in that they initiate safety functions by automatically generating control actions (CAs). In addition to the I&C system, there is, of course, another means to initiate safety functions: human operators. Currently, the reliability assessment process for human behavior during manual CA generation is conducted through the so-called human reliability analysis (HRA), which estimates the likelihood of failures in generating manual CAs by considering diverse performance shaping factors (PSFs) such as stress level and workload [1,2]. As a result of HRA, human error probability is derived. In addition to the PSFs currently applied in HRA, the condition of the I&C system itself at the moment of interaction with operators also needs to be considered because it affects not only the correctness of the relevant information required to make decisions but also the acquisition and transmission of manually generated CAs.

Figure 1 outlines the interactions when an I&C system and human operator are associated together in generating a CA. Based on Figure 1, the overall functions of the I&C system can be summarised as follows:

Function-1) Obtaining the current state of the controlled process, generating an automatic CA based on it, and transmitting the CA to the actuator.
Function-2) Obtaining the current states of the controlled process and actuator, and transmitting them with relevant alarms to the human operator.

Abbreviation: APC-S, Auxiliary Process Cabinet; BO, Board Operator; CEA, Control Element Assembly; CEA Limit SWTC, Control Element Assembly Limit Switch; DCN, Data Communication Network; D&C, Digital I&C; DIS, Diverse Indication System; DPS, Diverse Protection System; EC, Electrical System; ENFMS, Ex-core Neutron Flux Monitoring System; ESF-CCS, Engineered Safety Feature-Component Control System; FO, Field Operator; FPD, Flat Panel Display; HRA, Human Reliability Analysis; HSI, Human–System Interface; IPFD, Information Flat Panel Display; IM, Importance Measure; IPS, Information Processing System; ITP, Interface and Test Processor; LDP, Large Display Panel; LOCA, Loss Of Coolant Accident; MCS, Minimal Cut Sets; MCR, Main Control Room; MG set, Motor Generator set; MTP, Maintenance and Test Panel; NPCS, Nuclear steam supply system Process Control System; PCS, Power Control System; PSF, Performance Shaping Factor; QIAS-N, Qualified Indication and Alarm System-N (Non safety); QIAS-P, Qualified Indication and Alarm System-P (Safety); RCS, Reactor Coolant System; RPS, Reactor Protection System; RPS-OM, RPS Operator Module; RTSS, Reactor Trip Switchgear System; SDN, Safety Data Network; SS, Shift Supervisor.

* Corresponding author.
E-mail address: smshin@kaeri.re.kr (S.-M. SHIN).

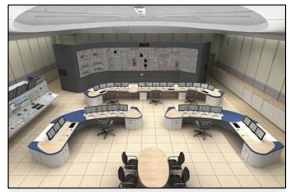
https://doi.org/10.1016/j.ress.2021.107698
Received 25 November 2020; Received in revised form 7 April 2021; Accepted 11 April 2021
Available online 15 April 2021
0951-8320/

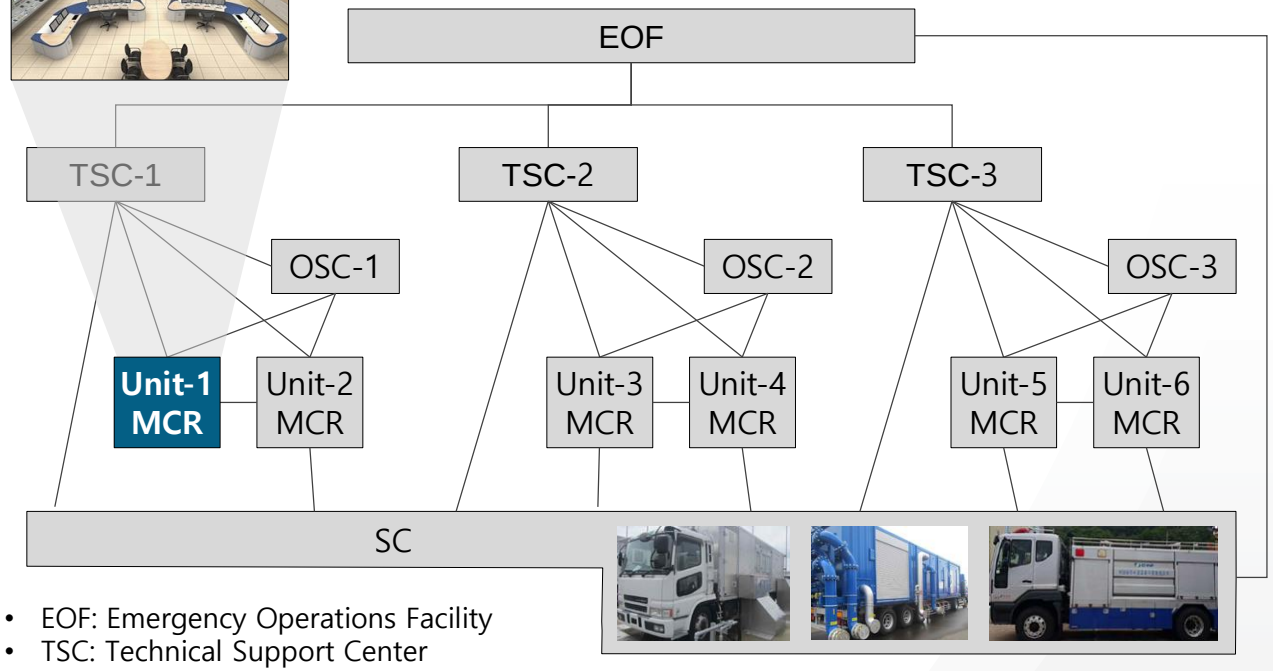
STPA-based hazard and importance analysis on NPP safety I&C systems focusing on human–system interactions, SM Shin, SH Lee, SK Shin, I Jang, J Park, Reliability Engineering & System Safety 213, 107698, 2021

Research background

General process of an HRA[1]

1. (Accident) scenario analysis
2. Identification and definition of HRA elements
3. Feasibility analysis of HRA elements
4. Quantification of human error probabilities(HEP)
5. Integration of HEPs to the PSA





MACST (Multi-barrier Accident Strategies) Equipment

- EOF: Emergency Operations Facility
- TSC: Technical Support Center
- OSC: Operational Support Center
- SC: Safety Center
- MCR: Main Control Room

➔ The question is… **"How are we able to identify HRA elements** (e.g., HFEs, potential subtasks, human error modes and the associated PSFs) **in multi-unit accidents"**

1 Xing, J., et., al. 2017. An integrated human event analysis system (IDHEAS) for nuclear power plant internal events at-power application, Volume 1, NUREG-2199.

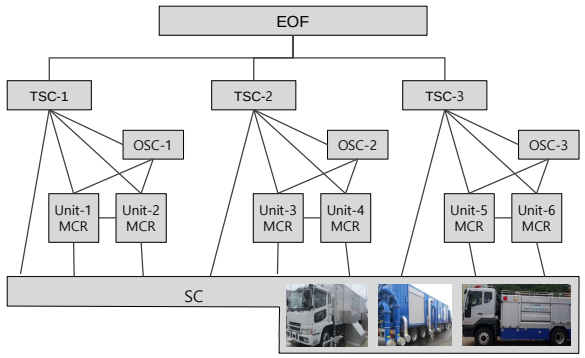
Overview of the target system

$$S_x = f(Task_i, Org_j)$$

- S_x = A specific STAMP x
- $Task_i$ = Required task i
- Org_j = Configuration of responsive organizations j

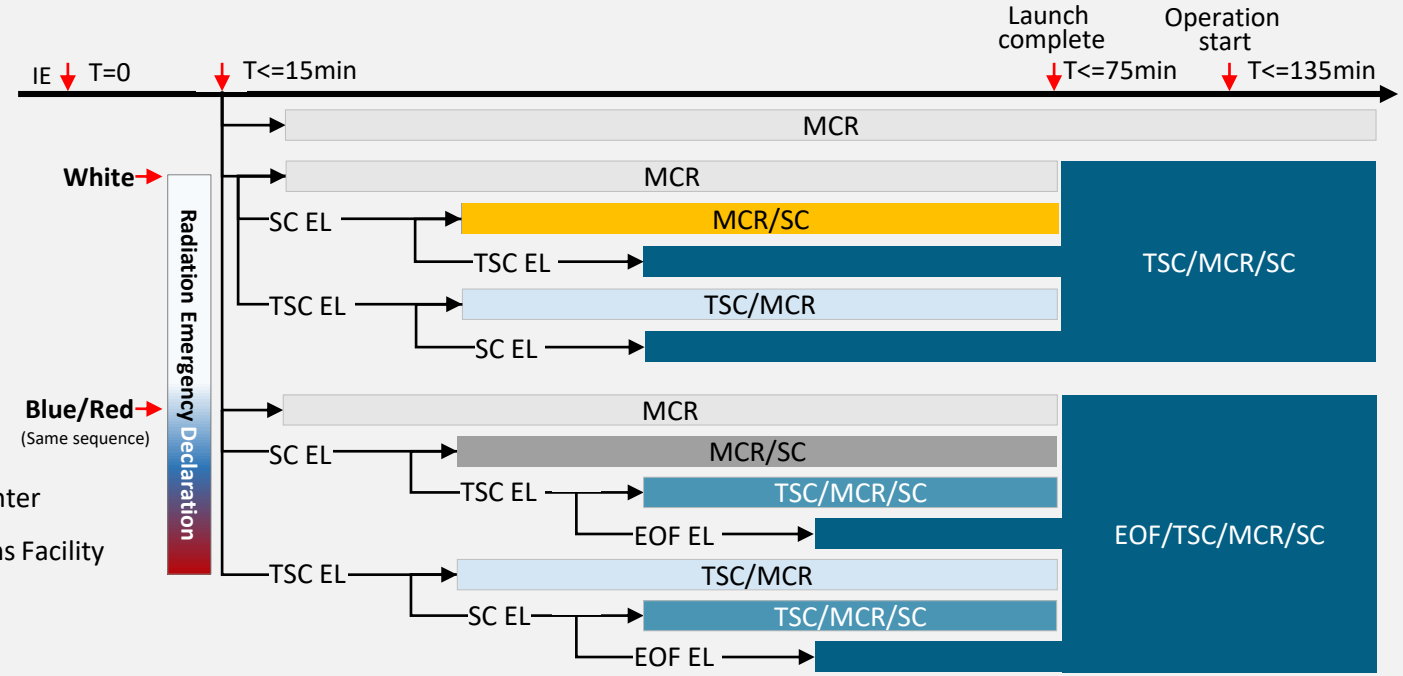
Potential tasks, $Task_i$

- **Operation of 1MWe**/3.2MWe portable generators
- Operation of Low/High pressure portable pumps
- Operation of support equipment (e.g. for transportation/installation of cables/fuel, securing transportation paths, etc.)



Configuration of responsive organizations, Org_j

$$Org_j = f(Radiation\ Emerg.Decl., Time)$$



- MCR: Main Control Room
- TSC: Technical Support Center
- EOF: Emergency Operations Facility
- SC: Safety Center
- EL: Early Launch

OSC is considered to belong to SC.

Perform STPA(1/3)

1) Define purpose of the analysis — 2) Model the control structure — 3) Identify unsafe control actions — 4) Identify loss scenario

SYSTEM BOUNDARY

Responsive organizations (system components)

Unit 1 MCR (including field operator) | SC | Other MCRs

- Unit 1 MCR requests to SC the transportation/connection of the 1MWe generator.
- The SC transports and connects the 1MWe generator.
- Unit 1 FO operates the 1MWe generator.

Environments

1MWe generator request guidance (EOP, Etc.) | personnel resources

EDG, AAC-DG | TSC | Driving path | Other inhibitory factors

LOSS

L-1: (Unit 1) Failure of power supply using the 1MWe generator

L-2: (Site) Negative impact on site resources *dependency

HAZARD

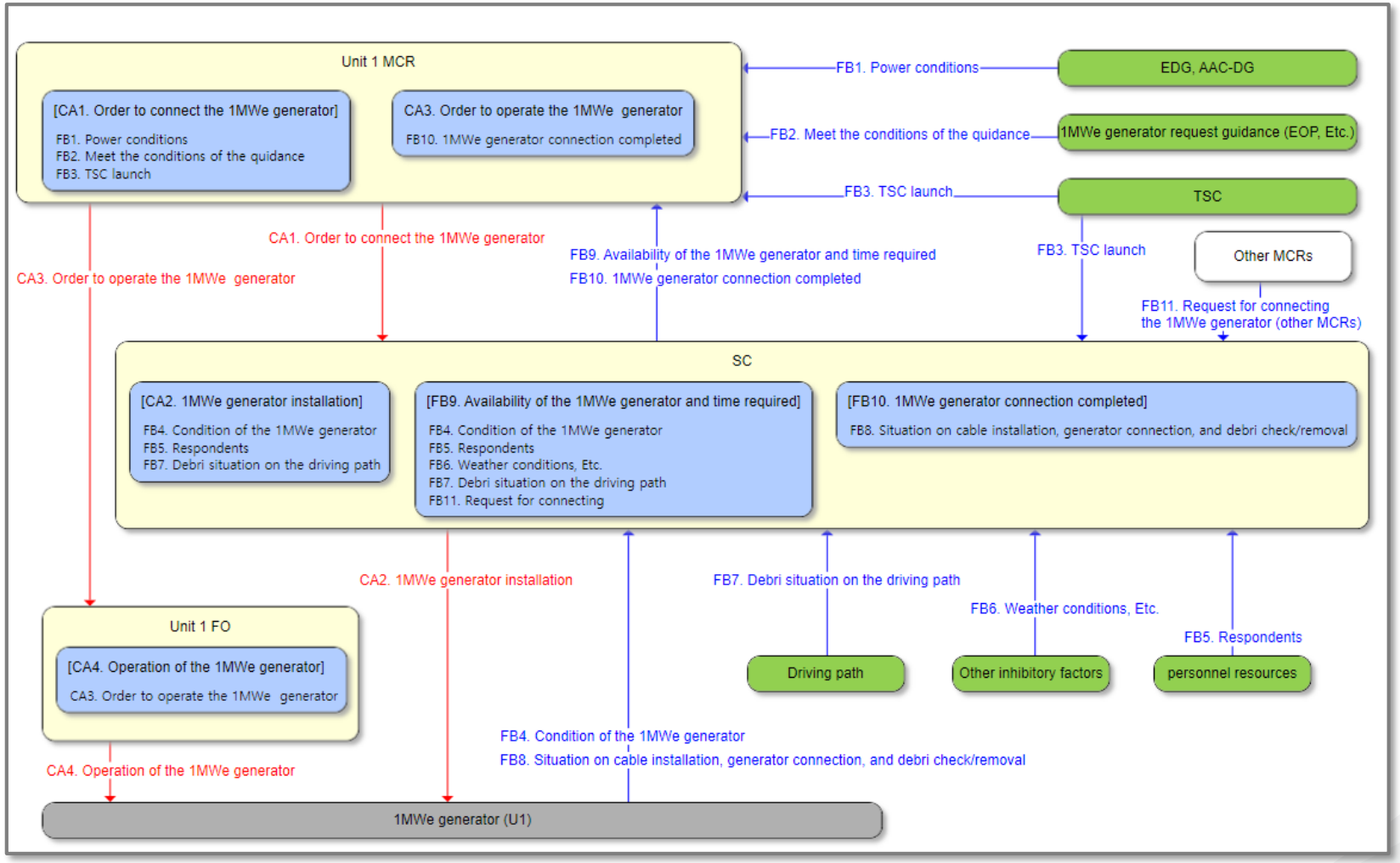
H-1: (Unit 1) Failure of connection/operation of the 1MWe generator

H-2: (Unit 1) Too late for connection/operation of the 1MWe generator

H-3: (SC) Delayed response or improper execution

Perform STPA(2/3)

1) Define purpose of the analysis — **2) Model the control structure** — 3) Identify unsafe control actions — 4) Identify loss scenario



Perform STPA(3/3)

1) Define purpose of the analysis — 2) Model the control structure — **3) Identify unsafe control actions** — 4) Identify loss scenario

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Order to install the 1MWe generator	**(UCA-1)** Unit 1 MCR does not order SC to connect the 1MWe generator when EDGs/AAC-DG failed [H-1]		**(UCA-2)** Unit 1 MCR orders SC to install the 1MWe generator too late when EDGs/AAC-DG failed [H-2]	
Mobile generator installation	**(UCA-3)** SC does not perform cable installation when Unit 1 MCR ordered to installation it [H-1] **(UCA-4)** SC does not perform 1MWe generator transportation when Unit 1 MCR ordered to installation it [H-1] **(UCA-5)** SC does not perform a fuel-hose connection when Unit 1 MCR ordered to installation it [H-1]	**(UCA-6)** SC installs the 1MWe generator when there was no order from Unit 1 MCR (misunderstanding the order from another unit) [H-3]	**(UCA-7)** SC performs cable installation too late when Unit 1 MCR ordered to installation it [H-2] **(UCA-8)** SC performs 1MWe generator transportation too late when Unit 1 MCR ordered to installation it [H-2] **(UCA-9)** SC performs a fuel-hose connection too late when Unit 1 MCR ordered to installation it [H-2]	
Order to operate the 1MWe generator	**(UCA-10)** Unit 1 MCR does not order Unit 1 FO to operate the 1MWe generator in Unit 1 when SC completed installing and reporting it [H-1]		**(UCA-11)** Unit 1 MCR orders Unit 1 FO to operate the 1MWe generator too late when SC completed installing and reporting it [H-2]	
Operation of the 1MWe generator	**(UCA-12)** Unit 1 FO does not operate the 1MWe generator when Unit 1 MCR ordered to operate it [H-1] **(UCA-13)** Unit 1 FO does not prepare pre-conditions to operate the 1MWe generator when Unit 1 MCR ordered to operate it [H-1]		**(UCA-14)** Unit 1 FO operates too late the 1MWe generator when Unit 1 MCR ordered to operate it [H-2]	

PSF[1] (Performance Shaping Factor)

- Operator experience
- Available time
- Task complexity
- Number of secondary tasks
- Workload
- Situation awareness
- And so on.

H-1: (Unit 1) Failure of connection/operation of the 1MWe generator

H-2: (Unit 1) Too late for connection/operation of the 1MWe generator

H-3: (SC) Delayed response or improper execution

1 Park, J., et., al., Inter-relationships between performance shaping factors for human reliability analysis of nuclear power plants , Volume 52, Nuclear Engineering and Technology, 2020

Insights

- It enables systematic thought experiments on countermeasures when dealing with a complex web of interests

  - The existing MACST equipment operating system is a written document. Whereas, STPA provides **a base for specifically simulating the decision-making process for MACST equipment** under multi-unit accidents.

  - The derived **UCAs** are suitable for identifying and specifying **potential sub-tasks for operation of MACST equipment.**

  - In addition, **factors** that are not task failures **but may cause disruption to site resources** (SC, TSC, EOF, etc.) **or delay response** can be specifically **identified**.

Application of the STAMP/STPA framework to the identification of a multi-unit HRA elements

Jong Woo Park[1], Sung-Min Shin[1], Yong Suk Lee[2] and Jinkyun Park[1*]

[1]Korea Atomic Energy Research Institute

[2]Future and Challenge, Co. Ltd

Abstract

The safety of nuclear power plants (NPPs) is the upmost goal to justify their sustainability. One of the traditional approaches to accomplish this goal is to identify the catalog of accident scenarios that could cause the occurrence of undesired results (e.g., core damage). Indeed, this is the virtue of the probabilistic safety assessment (PSA) or probabilistic risk assessment (PRA) technique, Fukushima Daiichi accident raised many technical issues challenging the traditional PSA mainly focusing on a single-unit. One of the technical issues is the necessity of the multi-unit PSA (MU-PSA). This implies that, in terms of the traditional human reliability analysis (HRA) supporting for the traditional PSA, various kinds of technical issues should be also resolved for supporting the multi-unit HRA (MU-HRA). One of the technical issues is the identification of HRA elements for conducting the MU-HRA. For this reason, a framework that can be used to distinguish HRA elements for supporting the MU-HRA is proposed based on the concepts of the STAMP/STPA (System Theoretic Accident Model and Processes/Systems Theoretic Process Analysis). As a result of the case study, it is expected that the proposed framework can be used as an effective tool for identifying HRA elements for supporting the MU-HRA.

Keywords: Human reliability analysis, Human reliability analysis element, System Theoretic Accident Model and Process, Systems Theoretic Process Analysis, Multi-units, Nuclear power plants

[*]Corresponding author: kshpjk@kaeri.re.kr

1/28

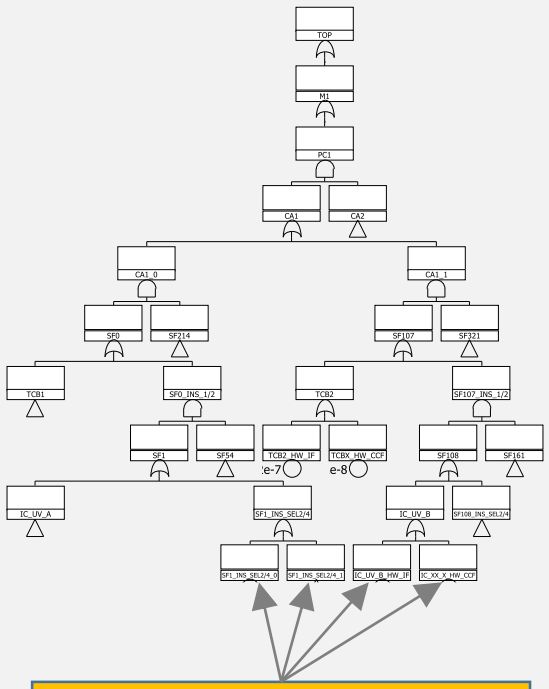
Application of the STAMP/STPA framework to the identification of a multi-unit HRA elements, Jong Woo Park, Sung-Min Shin, Yong Suk Lee and Jinkyun Park, 2023

Under review now

Part 2

A study applying the philosophy of STAMP/STPA

Research background

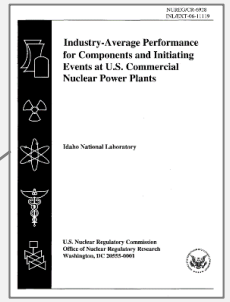


Quantitative failure information is required for PSA of DI&C system, BUT

Not enough data (Large uncertainty)

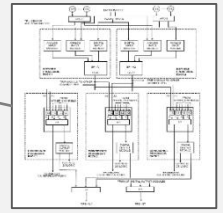
Statistical processing of failure history

No exist



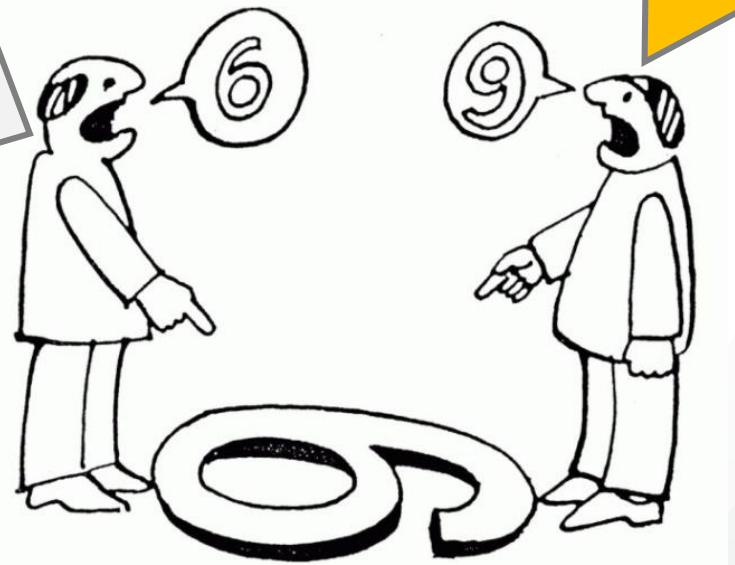
Application of industry-average

No commonly agreed methods yet

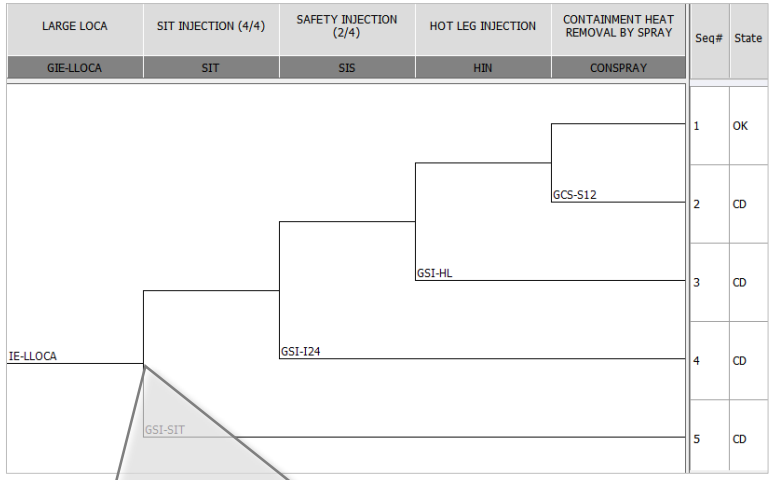


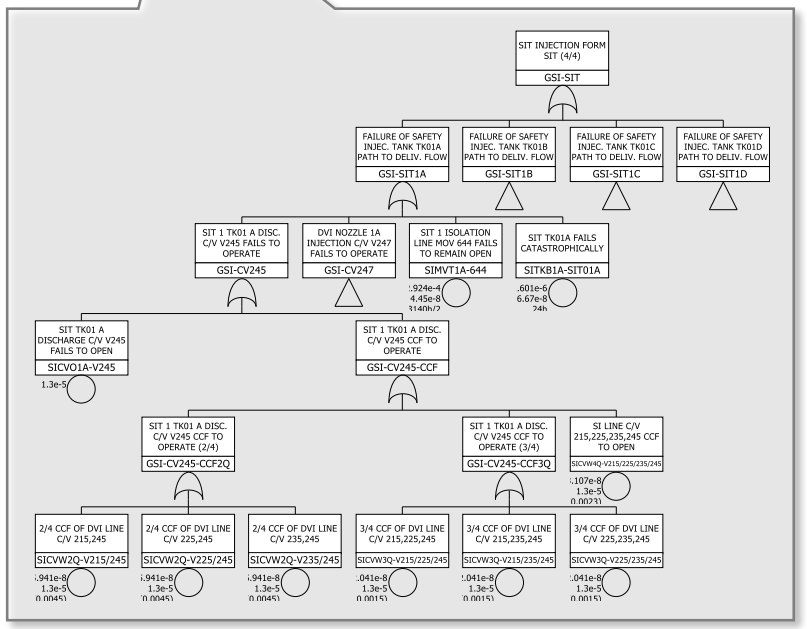
Analytical/Testing approach to system

Why don't we do a quantitative analysis without failure information?



Approaches



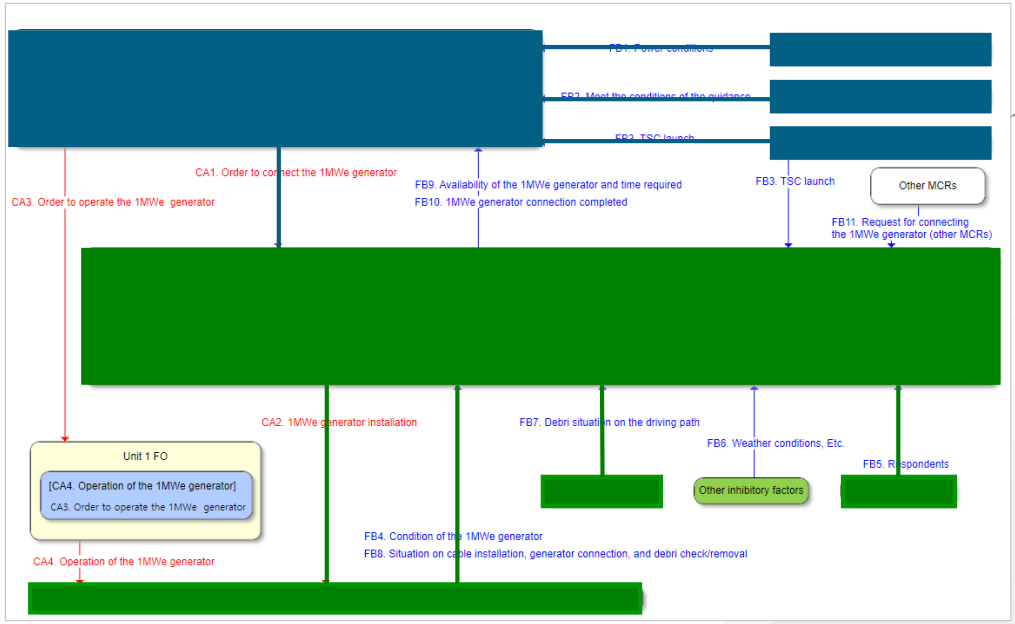


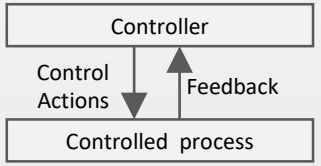
Mitigation mean 1 | Mitigation mean 2 | ... | Mitigation mean n

Control loop A has a relationship with Control loop B

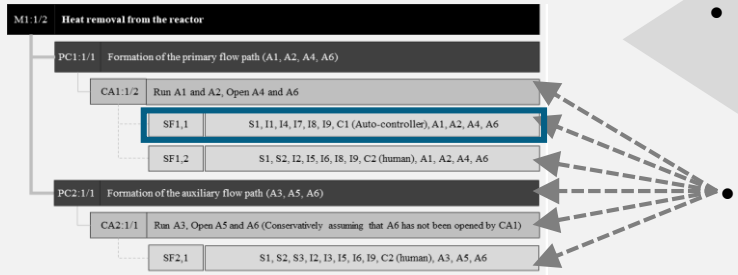
Sequential, diverse, or redundant

Assigning quantitative relative weight





Approaches

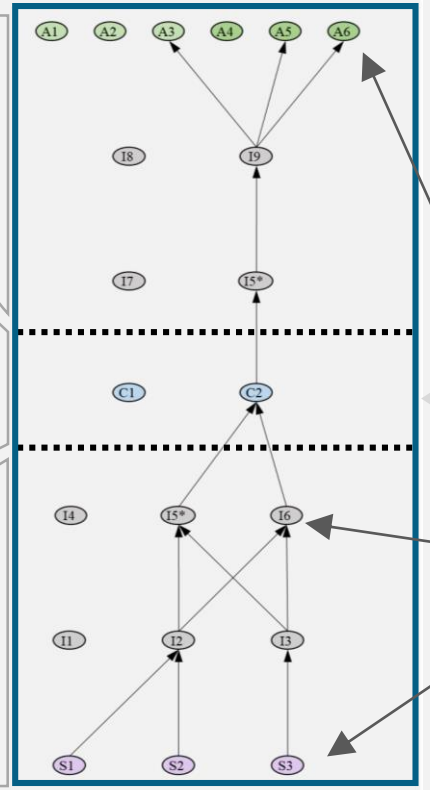


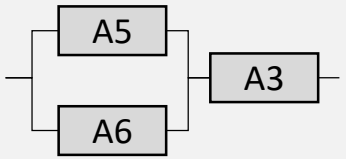
- Modeling the sequential/diverse/redundant correlation between control loops
- Assign relative weights on each control loop based on operation strategies

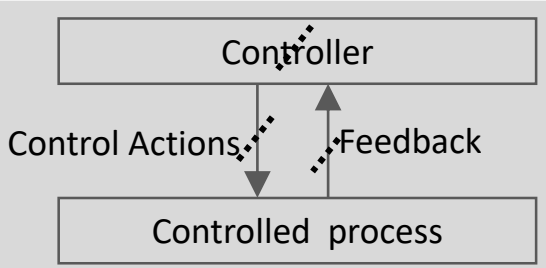
Control(CTL)
The generated CA is transmitted to the actuator(s)

Decision(DEC)
A controller determines the CA generation based on the FB(s) received

Instrumentation(INS)
FBs referred to for CA determination are generated by sensor(s) and transmitted to the controller







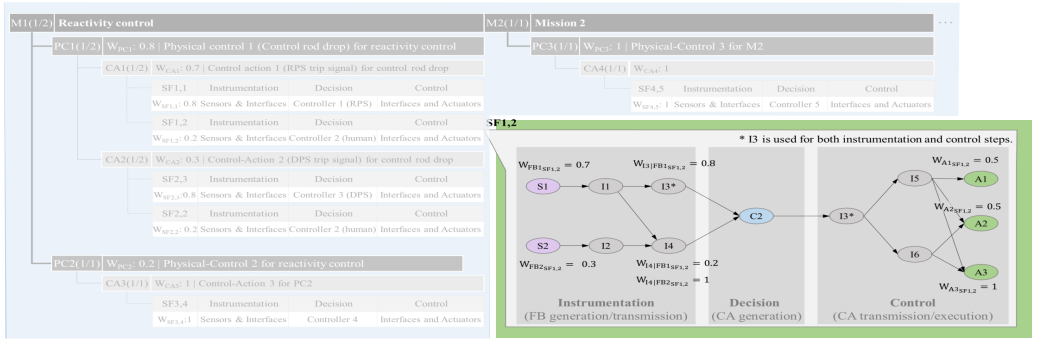
- Re-construction of each control loop in STAMP in one direction
- Assign relative weights on some components according to the impact for CA generation/decision/execution instead of failure information

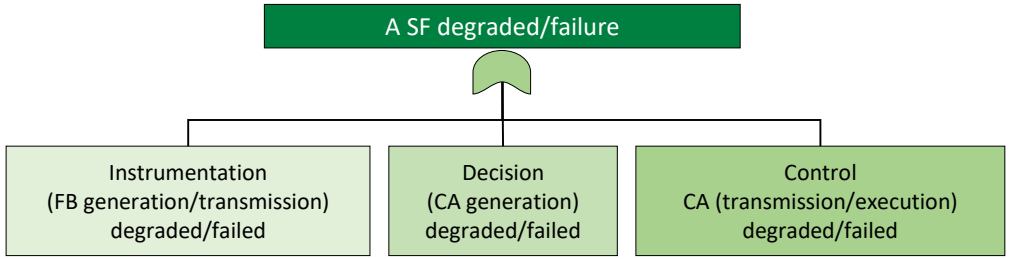
Basic principle of importance quantification

- Based on the weights assigned, the importance of each component is calculated by evaluating the extent to which a particular component impairs the soundness of each step of control loop when that component is unavailable.
- The importance calculated in one control loop is then integrated through a product with the weight assigned within that mitigation mean.

Approaches | Importance of a component in an SF

Importance of a component (IM) in an SF ∝ extent to which a particular component impairs the soundness of each step when that component is unavailable





$$\mathbf{IM}^{\mathbf{INS}}_{\mathbf{Sn|SF\ i,j}} = W_{FBk_{SF\ i,j}}\ (n = k)$$

$$\mathbf{IM}^{\mathbf{DEC}}_{\mathbf{Cn|SF\ i,j}} = 1\ (n = j)$$

$$\mathbf{IM}^{\mathbf{INS}}_{\mathbf{In|SF\ i,j}} = \sum_{k=1}^{\alpha}\left(W_{FBk_{SF\ i,j}} \frac{\sum_{g\in G_{In}|FBk_{SF\ i,j}} W_{g|FBk_{SF\ i,j}}}{\sum_{g\in G_{In}|FBk_{SF\ i,j}} W_{g|FBk_{SF\ i,j}} + \sum_{f\in F_{In}|FBk_{SF\ i,j}} W_{f|FBk_{SF\ i,j}}}\right)$$

where $G_{In}|FBk_{SF\ i,j}$: A group of front-end interfaces transmitting FB k via the interface n in SF i, j

where $F_{In}|FBk_{SF\ i,j}$: A group of front-end interfaces transmitting FB k other than the interface n in SF i, j

$$\mathbf{IM}^{\mathbf{CTL}}_{\mathbf{In|SF\ i,j}} = \max\{IM_{In|SF\ i,j}(z) : z = 1..\gamma\}$$

where γ is the number of MCS of actuators in SF i,j

$$IM_{In|SF\ i,j}(z) = \frac{\sum_{g\in G_{In}|MCSz_{SF\ i,j}} W_{g_{SF\ i,j}}}{\sum_{g\in G_{In}|MCSz_{SF\ i,j}} W_{g_{SF\ i,j}} + \sum_{f\in F_{In}|MCSz_{SF\ i,j}} W_{f_{SF\ i,j}}}$$

where $G_{In}|MCSz_{SF\ i,j}$: A group of actuators receiving CA i via the interface n in the MCSz in SF i, j

where $F_{In}|MCSz_{SF\ i,j}$: A group of actuators receiving CA i other than the interface n in the MCSz in SF i, j

$$\mathbf{IM}^{\mathbf{CTL}}_{\mathbf{An|SF\ i,j}} = W_{Ay_{SF\ i,j}}\ (n = y)$$

Approaches | Importance of a component for entire mitigation procedure

Importance of a component in a control loop being integrated with weights on the logical correlation model

$$IM_{Sn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{INS}_{Sn|SF\,i,j})\right\}$$

$$IM_{Cn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{DEC}_{Cn|SF\,i,j})\right\}$$

$$IM_{An|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{CTL}_{An|SF\,i,j})\right\}$$

$$IM_{In|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left[W_{CAi}\left\{W_{SF_{i,j}}(IM^{INS}_{In|SF\,i,j} + IM^{CTL}_{In|SF\,i,j})\right\}\right]$$

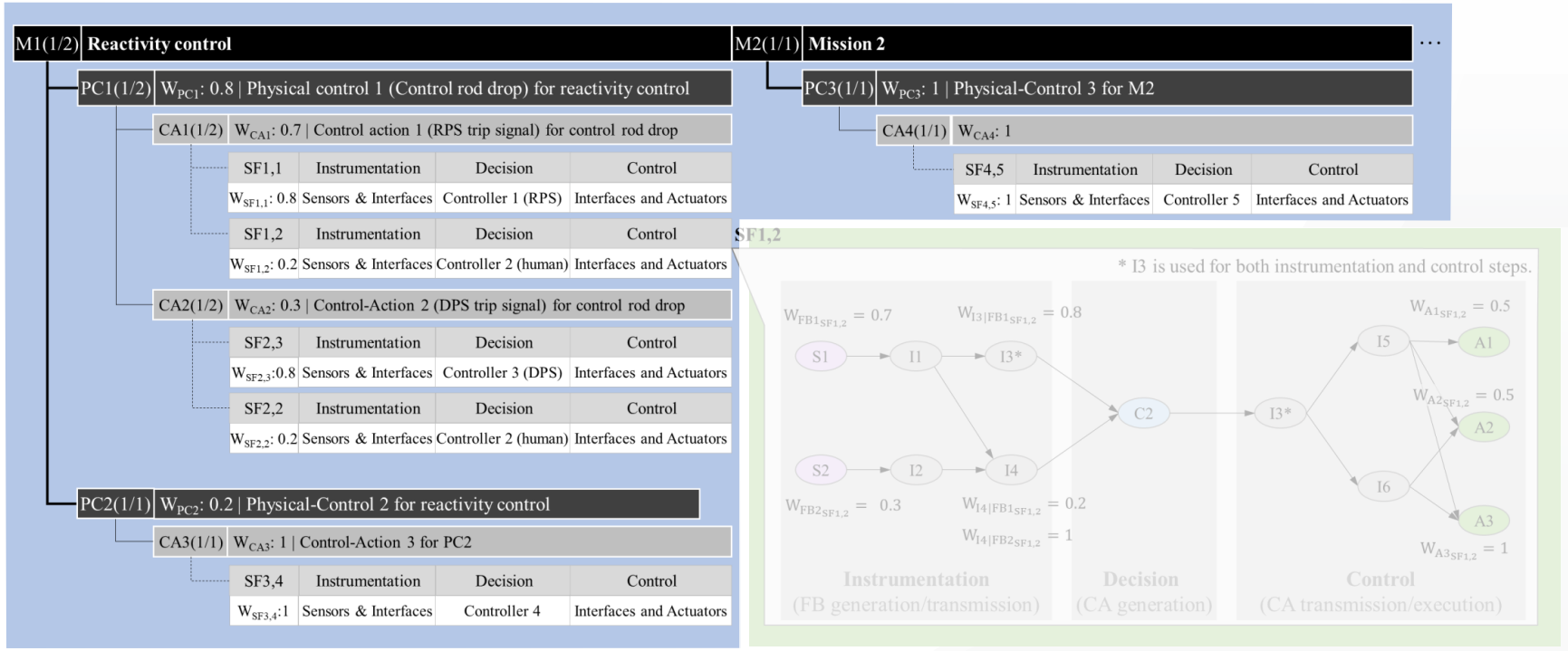
Importance of a component in a mitigation step → integrated over "all mitigation procedure"

$$IM_{Sn} = \sum_{X=1}^{T} IM_{Sn|Mx}$$

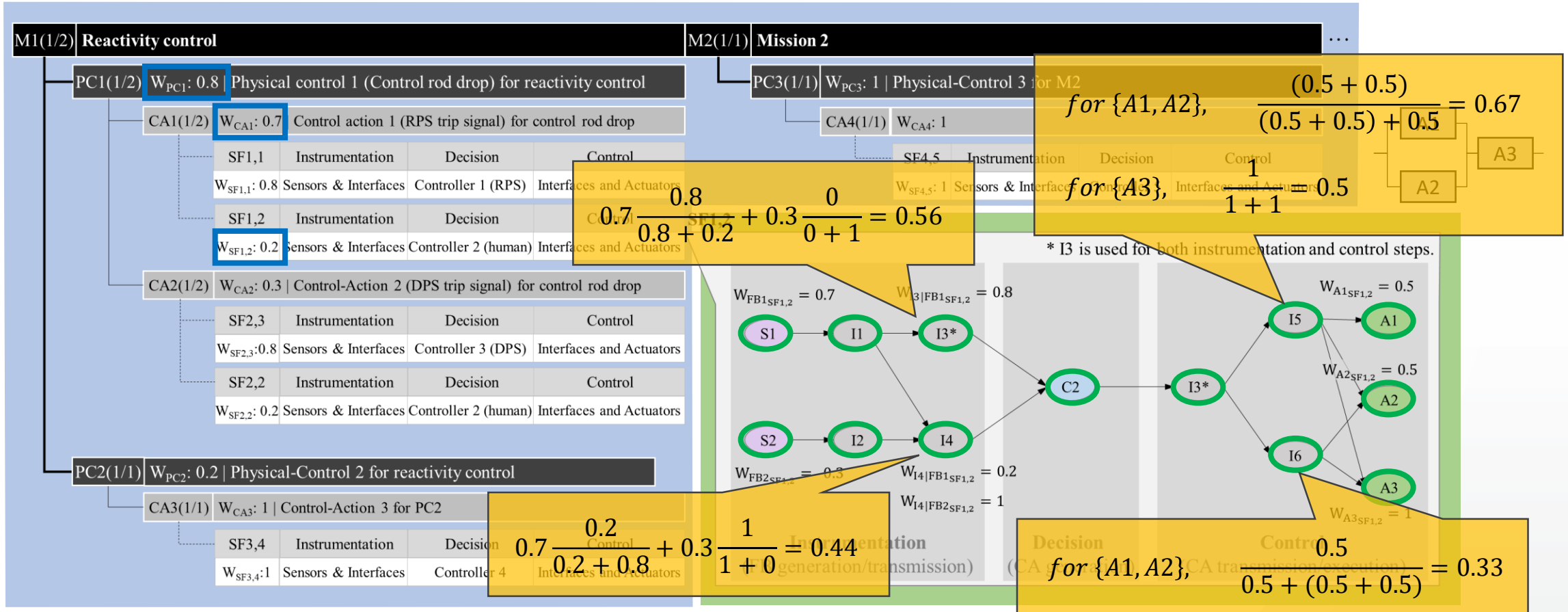
$$IM_{Cn} = \sum_{X=1}^{T} IM_{Cn|Mx}$$

$$IM_{An} = \sum_{X=1}^{T} IM_{An|Mx}$$

$$IM_{In} = \sum_{X=1}^{T} IM_{In|Mx}$$



Approaches | Exercise

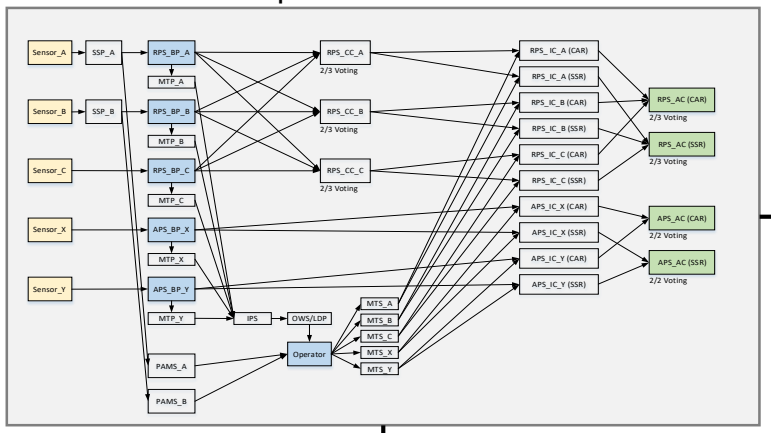


		S1	S2	I1	I2	I3	I4	I5	I6	C2	A1	A2	A3
Steps	INS	0.7	0.3	0.7	0.3	0.56	0.44						
	DEC												
	CTL					1		0.67	0.5		0.5	0.5	1
IM of each component in SF1,2		0.7	0.3	0.7	0.3	1.56	0.44	0.67	0.5	1	0.5	0.5	1

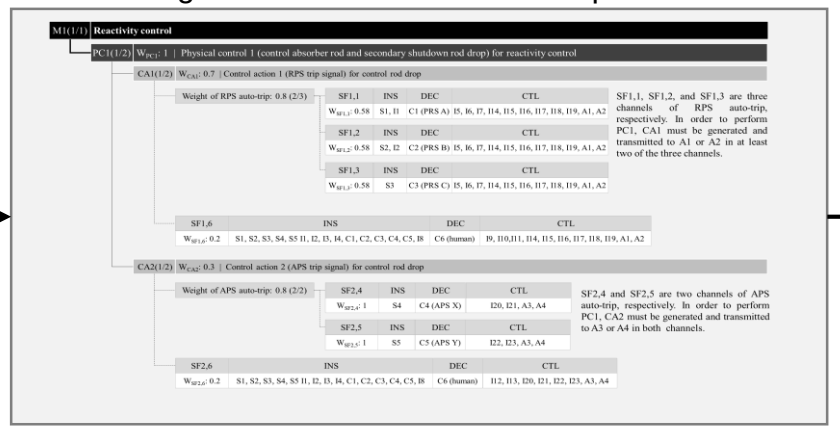
Feasibility study

The method was applied to a real-world 5 MW open-pool type research reactor, and the importance analysis was carried out for the protections systems and monitoring systems including human operators required for the reactor trip function.

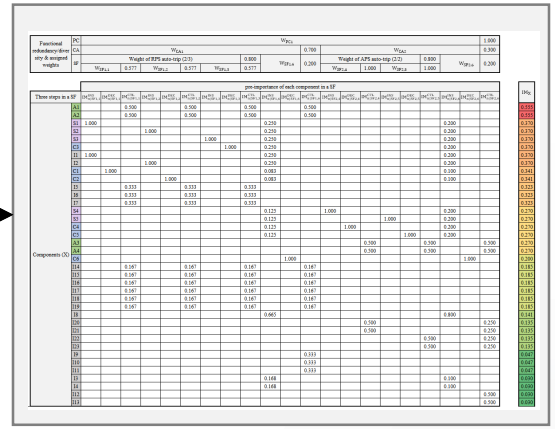
Simplified block diagram of the I&C systems for the reactor trip function in the research reactor.



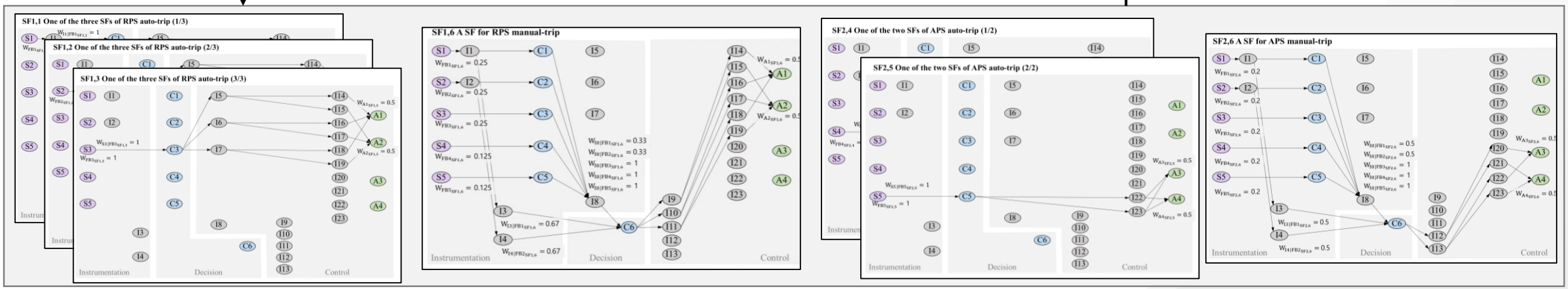
Logical correlation of control loops



Result of importance quantification

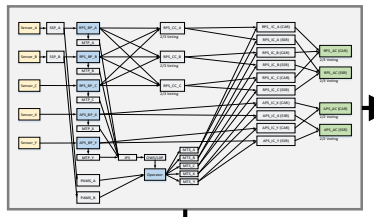


Re-construction of each control loop

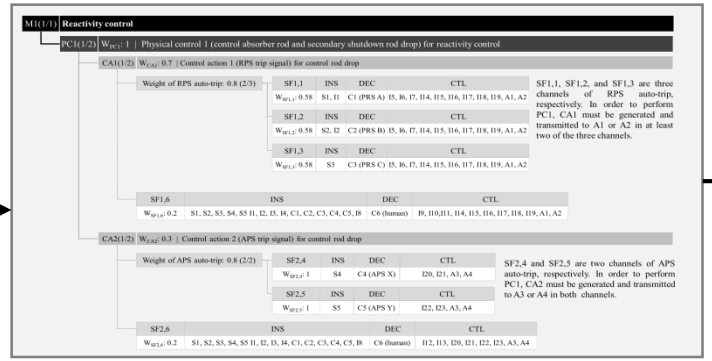


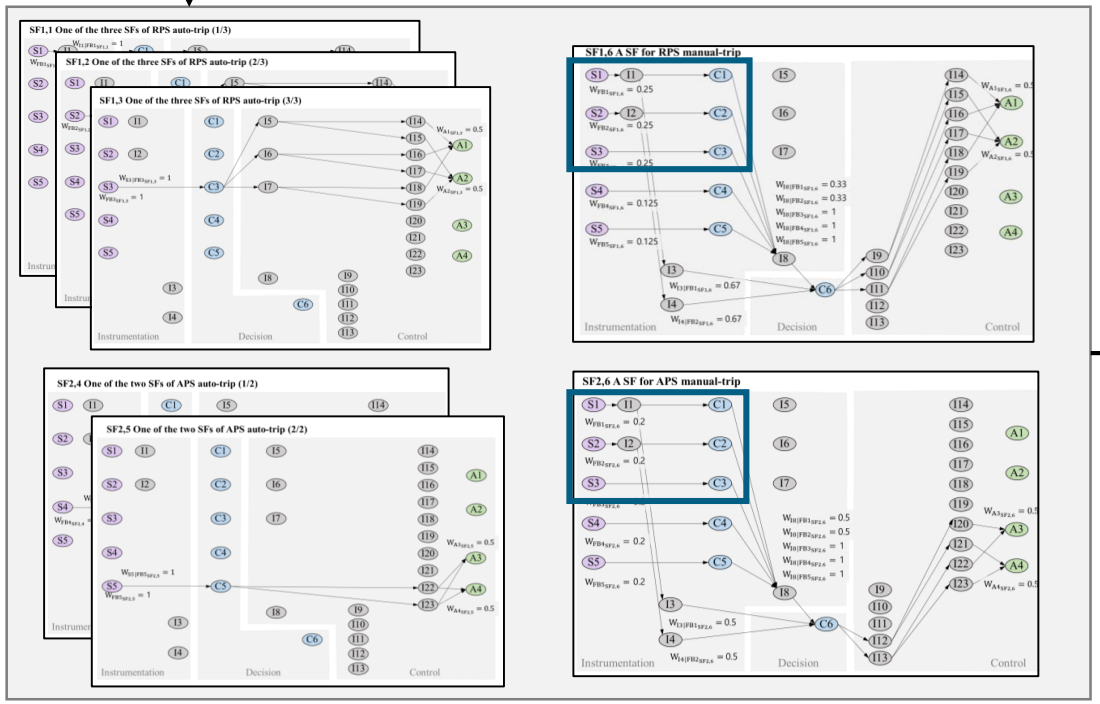
Feasibility study

Simplified block diagram of the I&C systems for the reactor trip function in the research reactor.



Logical correlation of control loops





Re-construction of each control loop

Result of importance quantification

Functional redundancy/diversity & assigned weights																								
	PC	W_{PC1}																						1.000
	CA	W_{CA1}												0.700	W_{CA2}									0.300
	SF	Weight of RPS auto-trip (2/3)								0.800	$W_{SF1,6}$		0.200	Weight of APS auto-trip (2/2)							0.800	$W_{SF2,6}$		0.200
		$W_{SF1,1}$	0.577	$W_{SF1,2}$	0.577	$W_{SF1,3}$	0.577								$W_{SF2,4}$	1.000	$W_{SF2,5}$	1.000						

Three steps in a SF		pre-importance of each component in a SF																						IM_X
		$IM^{INS}_{n\|SF1,1}$	$IM^{DEC}_{n\|SF1,1}$	$IM^{CTL}_{n\|SF1,1}$	$IM^{INS}_{n\|SF1,2}$	$IM^{DEC}_{n\|SF1,2}$	$IM^{CTL}_{n\|SF1,2}$	$IM^{INS}_{n\|SF1,3}$	$IM^{DEC}_{n\|SF1,3}$	$IM^{CTL}_{n\|SF1,3}$	$IM^{INS}_{n\|SF1,6}$	$IM^{DEC}_{n\|SF1,6}$	$IM^{CTL}_{n\|SF1,6}$	$IM^{INS}_{n\|SF2,4}$	$IM^{DEC}_{n\|SF2,4}$	$IM^{CTL}_{n\|SF2,4}$	$IM^{INS}_{n\|SF2,5}$	$IM^{DEC}_{n\|SF2,5}$	$IM^{CTL}_{n\|SF2,5}$	$IM^{INS}_{n\|SF2,6}$	$IM^{DEC}_{n\|SF2,6}$	$IM^{CTL}_{n\|SF2,6}$	
Components (X)	A1			0.500			0.500			0.500			0.500										0.555
	A2			0.500			0.500			0.500			0.500										0.555
	S1	1.000									0.250									0.200			0.370
	S2				1.000						0.250									0.200			0.370
	S3							1.000			0.250									0.200			0.370
	C3								1.000		0.250									0.200			0.370
	I1	1.000									0.250									0.200			0.370
	I2				1.000						0.250									0.200			0.370
	C1		1.000								0.083									0.100			0.341
	C2					1.000					0.083									0.100			0.341
	I5			0.333			0.333			0.333													0.323
	I6			0.333			0.333			0.333													0.323
	I7			0.333			0.333			0.333													0.323
	S4										0.125			1.000						0.200			0.270
	S5										0.125						1.000			0.200			0.270
	C4										0.125				1.000					0.200			0.270
	C5										0.125							1.000		0.200			0.270
	A3															0.500			0.500			0.500	0.270
	A4															0.500			0.500			0.500	0.270
	C6											1.000									1.000		0.200
	I14			0.167			0.167			0.167			0.167										0.185
	I15			0.167			0.167			0.167			0.167										0.185
	I16			0.167			0.167			0.167			0.167										0.185
	I17			0.167			0.167			0.167			0.167										0.185
	I18			0.167			0.167			0.167			0.167										0.185
	I19			0.167			0.167			0.167			0.167										0.185
	I8										0.665									0.800			0.141
	I20															0.500						0.250	0.135
	I21															0.500						0.250	0.135
	I22																		0.500			0.250	0.135
	I23																		0.500			0.250	0.135
	I9												0.333										0.047
	I10												0.333										0.047
	I11												0.333										0.047
	I3										0.168									0.100			0.030
	I4										0.168									0.100			0.030
	I12																					0.500	0.030
	I13																					0.500	0.030

Discussions

Meaning and utilization of analysis results

- In addition to mechanical factors, by including human factors as a controller, it is possible to present quantitative analysis results without fault information. It has the potential to be helpful in the analysis of complex and new systems.

- The derived **importance means** whether the **component is used for an important functions** and **how many times the component is used** in various mitigation process.

- The **value of importance** itself **does not mean the safety** of the system. System safety can be implemented in conjunction with the reliability of that component; Let's say there is **a component which has a very high importance** value**. If that component frequently fails, the system safety goes low.** On the other hand**, if that component rarely fails, the safety of the system goes high.**

- Therefore, **increased safety of a control** system might be achieved by modifying the system design to n**ot concentrate importance on a small number of components** or by driving the implementation of **high reliability for certain components which have high importance.**

Reliability Engineering and System Safety 228 (2022) 108765

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

A novel approach for quantitative importance analysis of safety DI&C systems in the nuclear field

Sung-Min Shin [a,*], Sang Hun Lee [b], Seung Ki Shin [a]

ARTICLE INFO

Keywords:
STAMP
Importance analysis
DI&C
PSA
Quantitative analysis
Nuclear safety

ABSTRACT

As the digitalization of the safety instrumentation and control (I&C) systems in the nuclear field causes very complex interactions between their components and difficulty in securing quantitative failure information of each component, there are considerable challenges in analyzing them via probabilistic safety assessment (PSA), the typical safety analysis framework of existing safety I&C systems. This study proposes a new approach to resolve these challenges. The suggested method develops a system model based on the systems-theoretic accident model and processes (STAMP) philosophy and assigns weights to specific components according to design information and operation strategies instead of quantitative failure information. Based on the assigned weights, the importance of each component is derived by calculating the effect of a single component failure on the overall I&C functions. The methodology is explained through simple examples and validated with an analysis of a real-world system. The proposed approach is expected to be useful in deriving insights from the design stages to the improvement stages for more diverse I&C systems by enabling quantitative importance analysis without failure information.

1. Introduction

The safety-related instrumentation and control (I&C) systems in the nuclear field are implemented with redundancy/diversity design concepts to ensure their functional availability [1–3]. This leads to complex interactions between the components in an I&C system, which may vary depending on specific accident scenarios and subsequent mitigation strategies. Moreover, many existing analog component-based I&C systems are being digitalized due to the obsolescence of the analog components, which introduces characteristics that were not previously present, such as software and networks, further increasing the complexity of the interactions between system components [4–6]. Safety analysts typically identify the complexity of such systems through system design documents. However, most of the documents written in the system design and development process focus on how the system should work, so they are not faithfully consistent with the safety analyst's view of analyzing how failures of certain system components affect the system function. For this reason, it is difficult for safety analysts to sufficiently grasp the safety characteristics of digital I&C (DI&C) systems from related documents and produce accurate analysis results. It is therefore necessary to develop a separate method to systematically analyze the complex interactions of I&C system components for the purpose of safety assessment.

One of the aforementioned redundancy/diversity design concepts is to provide an automatic or manual approach for the initiation of the safety functions. The safety of the I&C systems in the nuclear field is usually verified through probabilistic safety assessment (PSA) [7–11]. Each failure probability of an automatic or manual safety function initiation is eventually integrated into a PSA fault tree (FT), but the analysis process for each is quite different; for automatic functions, a failure logic using the module level of basic events is directly modeled into the FT, while on the other hand, for manual functions the human error probability (HEP) is derived through human reliability analysis (HRA) that considers various performance shaping factors (PSFs) such as

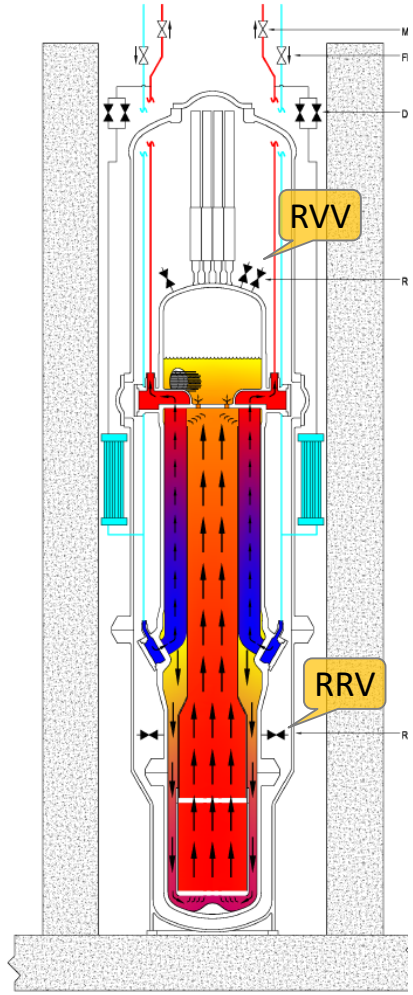
Abbreviation: APS, alternative protection system; CA, control action; CTL, control; DEC, decision; DPS, diverse protection system; DI&C, digital I&C; FB, feedback; FT, fault tree; FTA, fault tree analysis; HRA, human reliability assessment; HEP, human error probability; PSF, performance shaping factor; I&C, instrumentation and control; IM, importance; INS, instrumentation; IPS, information processing system; M, mission; MCS, minimal cut set; PSAMS, post-accident monitoring system; PC, physical control; PSA, probabilistic safety assessment; RPS, reactor protection system; SF, signal flow; STAMP, systems-theoretic accident model and processes.

* Corresponding author.
E-mail address: smshin@kaeri.re.kr (S.-M. Shin).

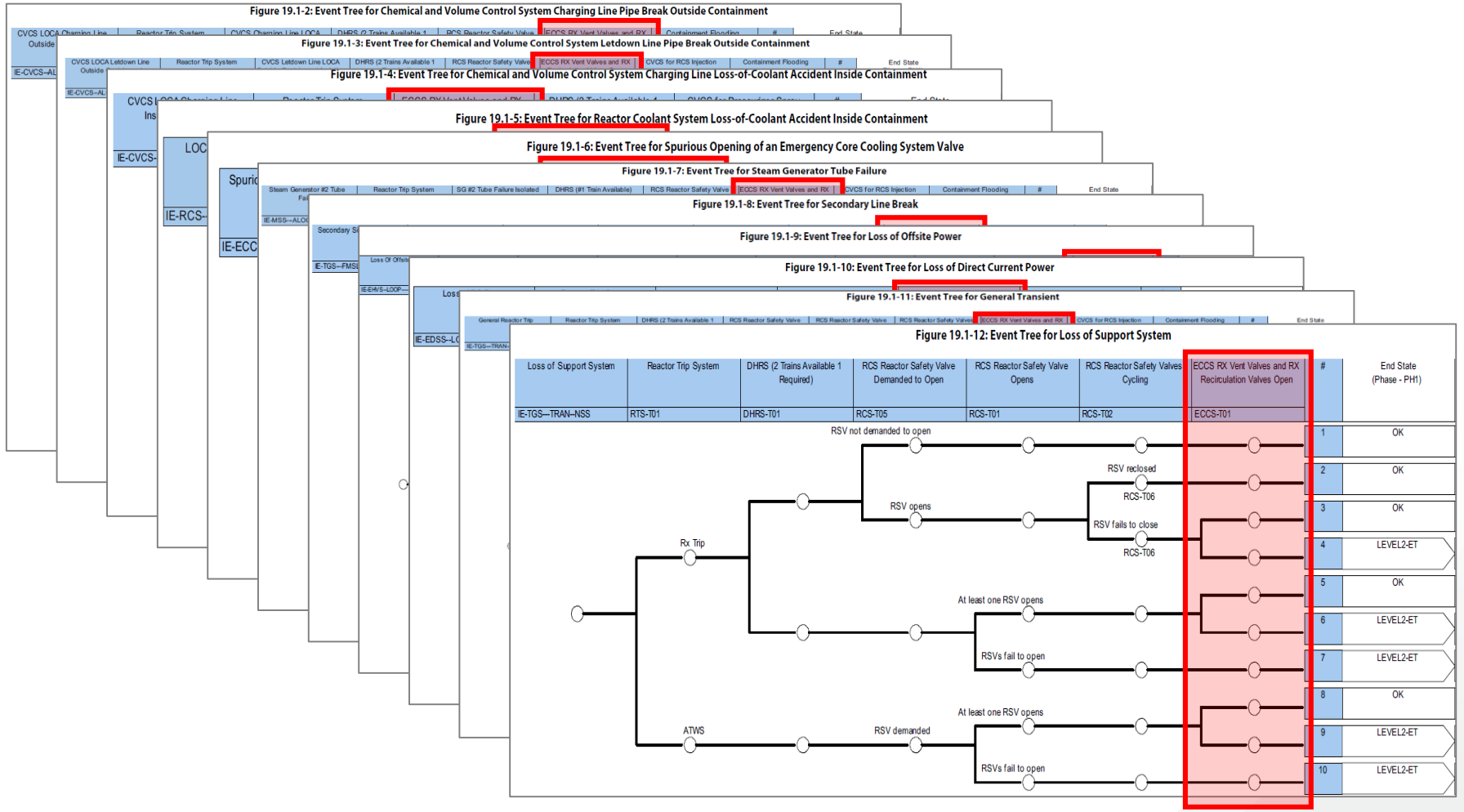
https://doi.org/10.1016/j.ress.2022.108765
Received 19 January 2022; Received in revised form 26 July 2022; Accepted 21 August 2022
Available online 29 August 2022
0951-8320/© 2022 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

A novel approach for quantitative importance analysis of safety DI&C systems in the nuclear field, SM Shin, SH Lee, SK Shin, Reliability Engineering & System Safety 228, 108765, 2022

Discussions

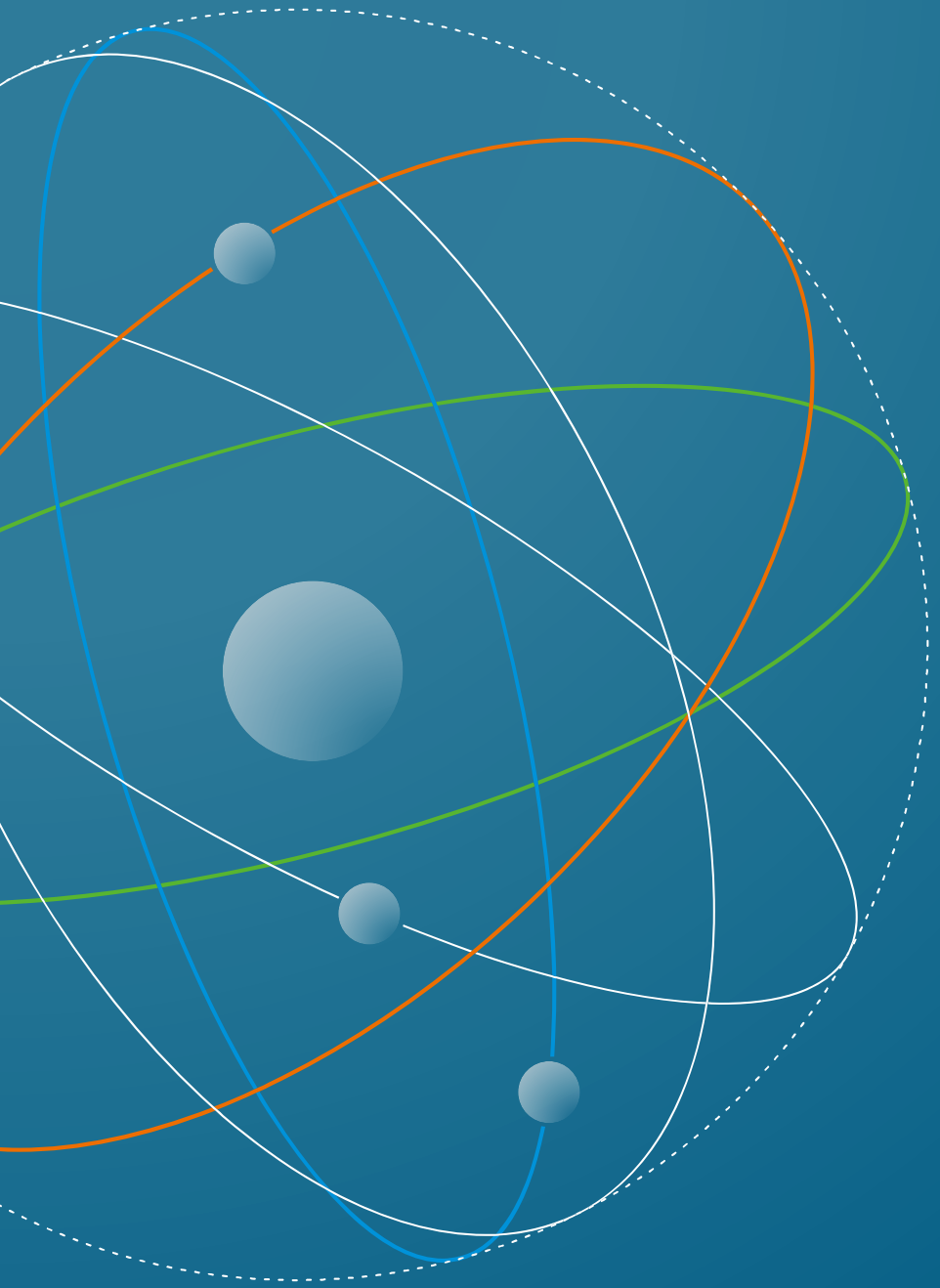


NuScale



Required probability of RVV/RRV fail to open[1]: **~1.24E-5 / ~2.25E-5**

1 NuScale FSAR



THANK YOU

smshin@kaeri.re.kr

KAERI
Korea Atomic Energy Research Institute