

# Application of STAP to ESF-CCS

**Dong-Ah Lee**

Jang-Soo Lee

Se-Woo Cheon

Junbeom Yoo

*Konkuk University*

*Korea Atomic Energy Research Institute*

# Contents

- Introduction
- Background: ESF-CCS
- Application of STPA
- Conclusion & Future Work

Application of STAP to ESF-CCS

---

# INTRODUCTION

# Introduction

- For developing the I&C system of a nuclear power plant, more than thousands reports had been produced and had to be traceable through the lifecycle from the system requirements.
- Hazard analysis of complex systems(systems of systems) with traditional methods (FTA, HAZOP) was extremely difficult to justify the safety.
- Most hazards came from the wrong interaction of the components (SW, HW, Human).
- We applied the new hazard analysis technique (STPA) based on the new accident causality model (STAMP).

Application of STAP to ESF-CCS

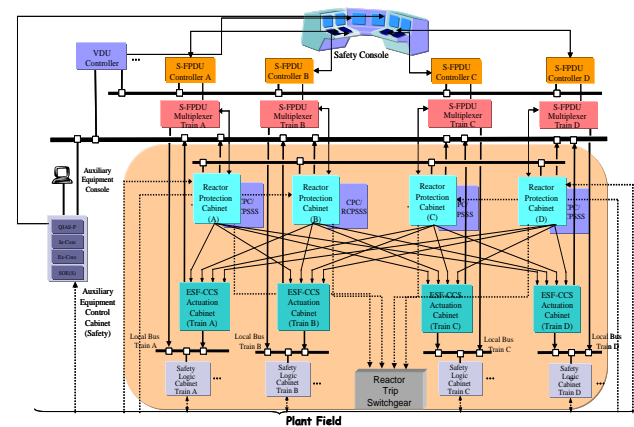
---

# BACKGROUND

# Background

## Korea Nuclear I&C System (KNICS)

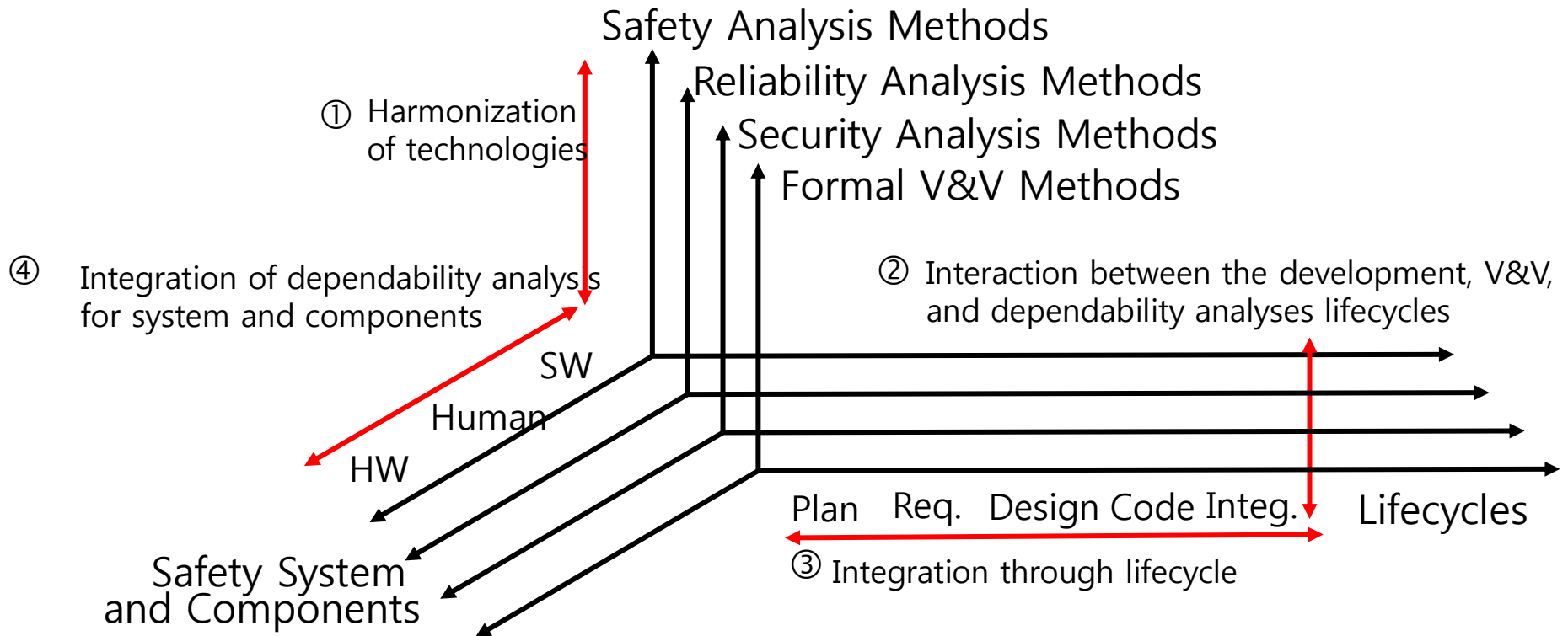
- Instrumentation and Control (I&C) systems and equipment for APR1400 Nuclear Power Plant (NPP)
- Period: July 2001 ~ April 2008 (7 years)
- Target
  - Fully digitalized I&C systems development for APR1400 (Shin-Ulchin units #1&2)
  - I&C upgrade for existing NPPs



Power Modules CPU Module Comm. Modules I/O Modules

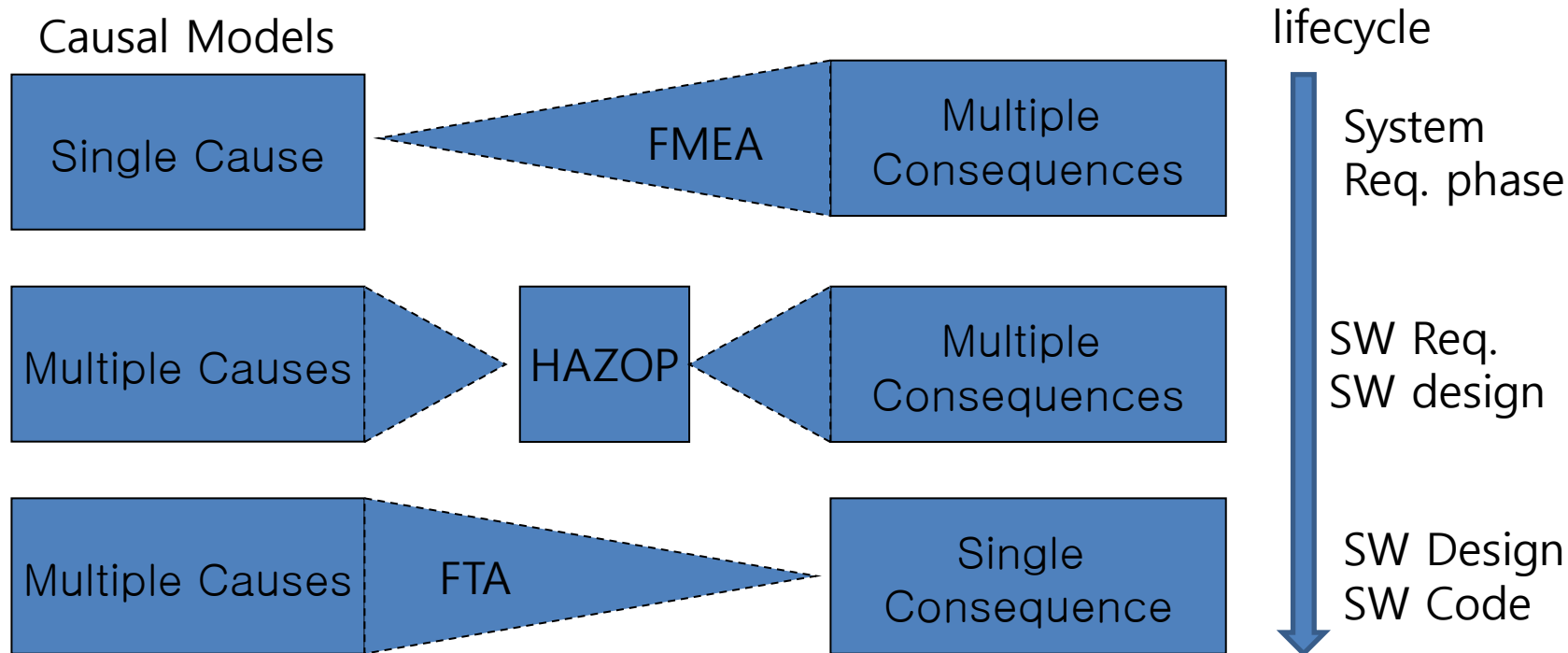
# Background

## KNICS Dependability Engineering



# Background

## Hazard Analysis of KNICS





# ESF-CCS

- Engineered Safety Features-Components Control System
- To mitigate the consequences of design-basis or loss-of-coolant accident
- 8 Operational Functions

Function	Description
<b>SIAS</b>	Safety Injection Actuation Signal
<b>CIAS</b>	Containment Isolation Actuation signal
<b>MSIS</b>	Main Stream Isolation Signal
<b>CSAS</b>	Containment Spray Actuation Signal
<b>AFAS</b>	Auxiliary Feed-water Actuation Signal
<b>CREVAS</b>	Control Room Emergency Ventilation Actuation Signal
<b>FHEVAS</b>	Fuel Handling Area Emergency Ventilation Actuation Signal
<b>CPIAS</b>	Containment Purge Isolation Actuation Signal

# ESF-CCS

## Dependability of ESF-CCS

- Failure Mode and Effects Analysis (FMEA)
  - Reg. 1.70
  - IEEE Std. 352
- SW Hazard Analysis
  - IEEE Std. 7-4.3.2
- Unavailability Analysis (FTA)
  - MIL-HDBK-217F
  - NUREG-0492

Application of STAP to ESF-CCS

---

# APPLICATION OF STAP

# Application of STPA (0)

- Target: Three functions
  - **SIAS**, CSAS, and CREVAS
- Application process
  1. Identify hazardous states of the system.
  2. Develop the control structure of the system.
  3. (STPA Step 1) Identify the potential for inadequate control of the system that could lead to a hazardous state.
  4. (STPA Step 2) Determine how each potentially hazardous control action identified in step 1 could occur.

# Application of STPA (1)

## SIAS

### Providing Emergency coolant w/ boron

- Hazard
  - Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2<sup>nd</sup>HSL, S/WP-Ex, or REA—occur.
- Safety constraint
  - The SIAS must operate when the 4 events—LOCA, 2<sup>nd</sup>HSL, S/WP-Ex, or REA—occur.

LOCA	Loss Of Coolant Accident
2 <sup>nd</sup> HSL	Second Heat Sink Loss
S/WP-Ex	Steam- and Water-pipe explosion
REA	Rod Ejection Accident

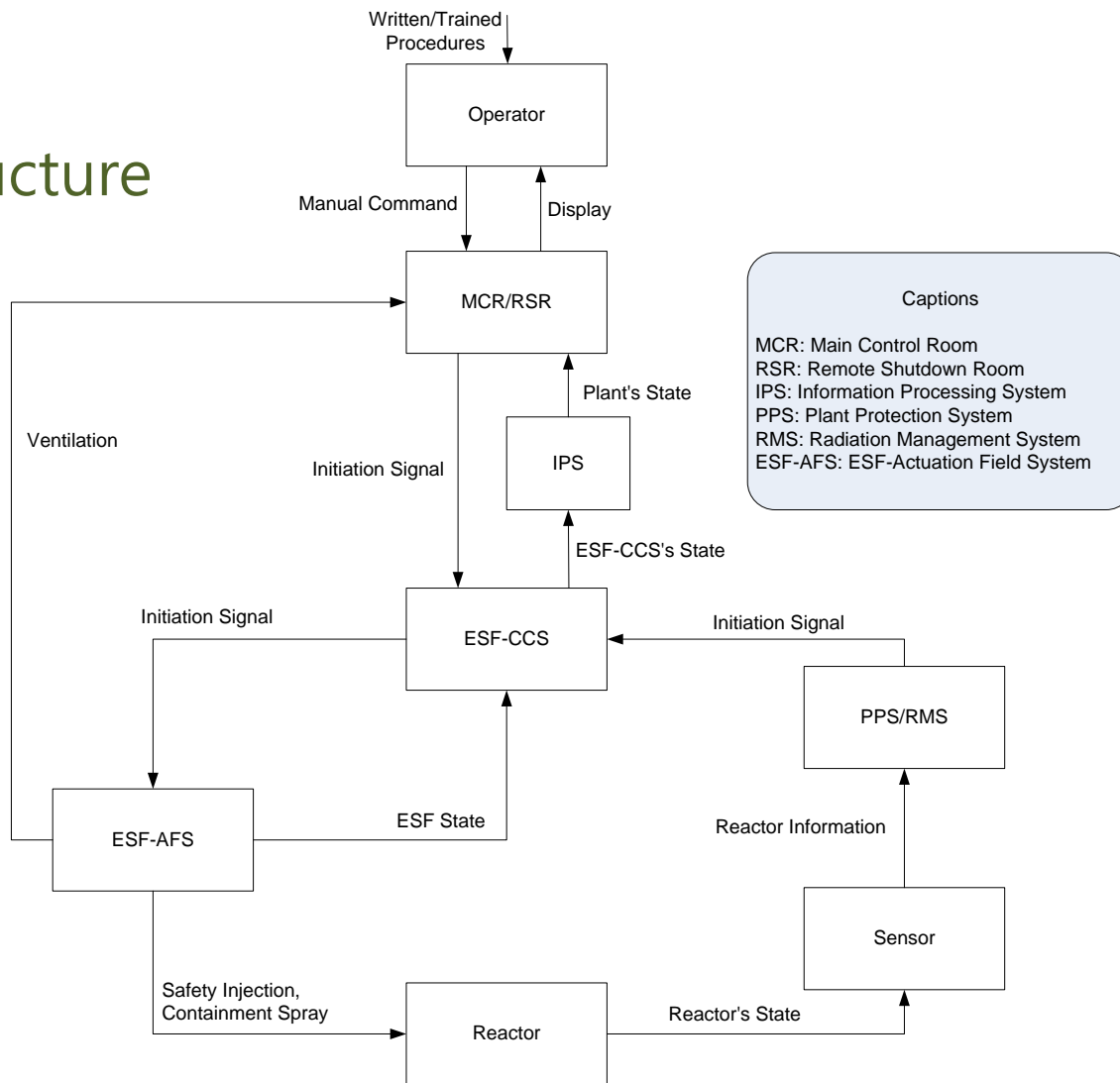
# Application of STPA (1-1)

## Hazards and Safety Constraints

Function	Hazard	Safety Constraint
<b>SIAS</b>	Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2 <sup>nd</sup> HSL, S/WP-Ex, or REA—occur.	The SIAS must operate when the 4 events—LOCA, 2 <sup>nd</sup> HSL, S/WP-Ex, or REA—occur.
<b>CSAS</b>	Heat removal and fission clean up fail when the three events—LOCA, S/WP-Ex, or the SIAS—occur.	The CSAS must operate when the three events—LOCA, S/WP-Ex, or the SIAS—occur.
<b>CREVAS</b>	Maintenance of pressure in a main control room fails when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.	The CREVAS must operate when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.

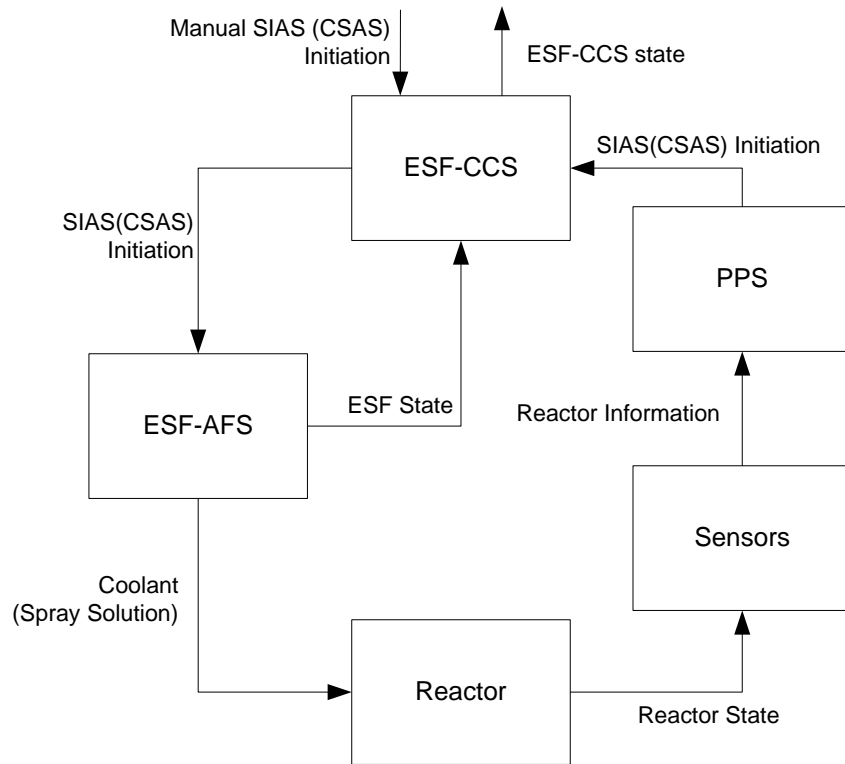
# Application of STPA (2)

## Safety control structure for the ESF-CCS

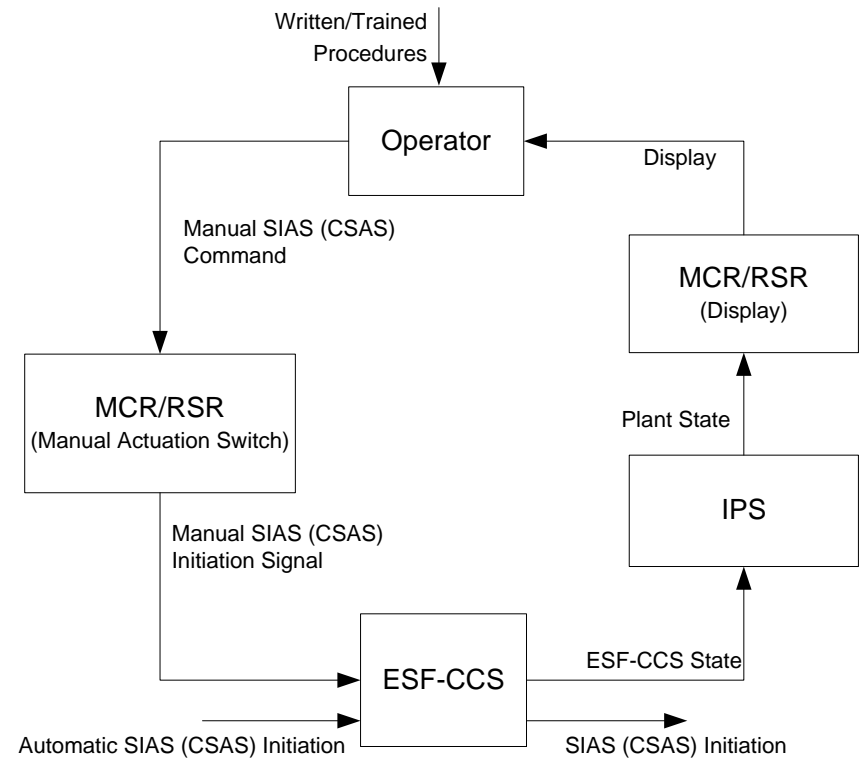


# Application of STPA (2-1)

Safety control structure for the SIAS/CSAS by the PPS



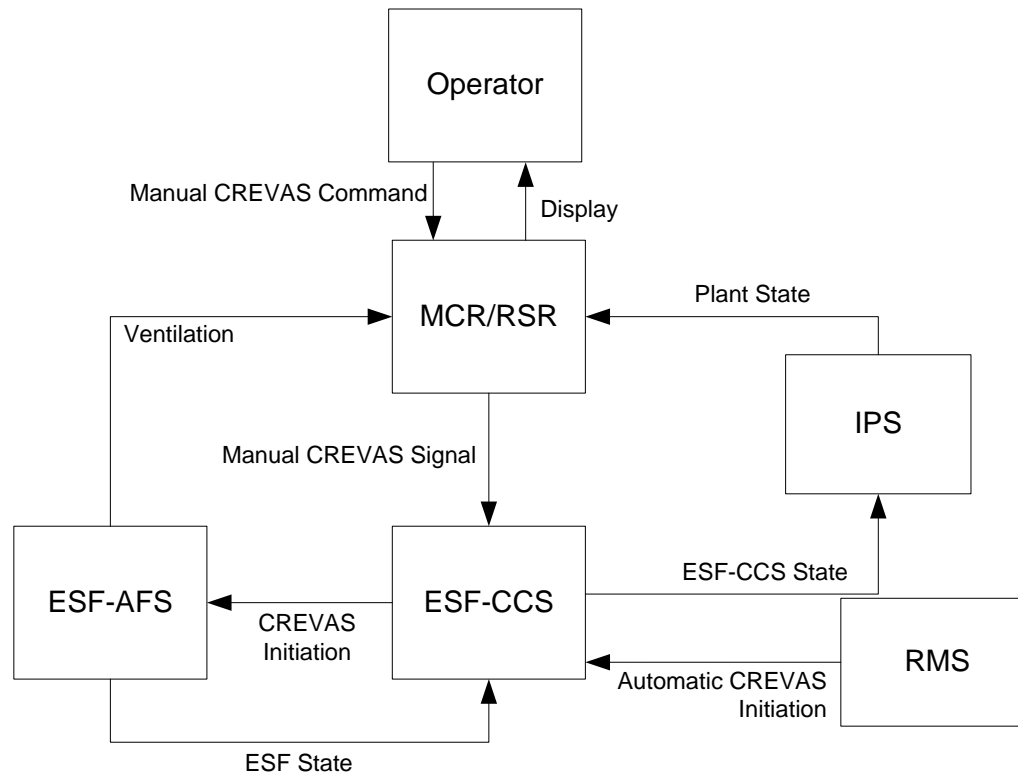
Safety control structure for the SIAS/CSAS by the Operator





# Application of STPA (2-2)

## Safety control structure for the CREVAS



# Application of STPA (3)

## Hazardous behaviors of SIAS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
<b>SIAS ON (From ESF-CCS to ESF-AFS)</b>	<p><b>Not providing SIAS ON when LOCA occurs (a1)</b>            Not providing SIAS ON when 2ndHSL occurs (a2)            Not providing SIAS ON when S/WP-Ex occurs (a3)            Not providing SIAS ON when REA occurs (a4)            Not providing SIAS ON when Manual SIAS Initiation occurs (a5)</p>	Not hazardous	<p>When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c1)            When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c2)            When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c3)            When REA occurs, ESF-CCS waits too long to turn SIAS ON (c4)            When Manual SIAS Initiation occurs, ESF-CCS waits too long to turn SIAS ON (c5)</p>	SIAS ON stops before coolant is not provided enough (d1)

# Application of STPA (3-1)

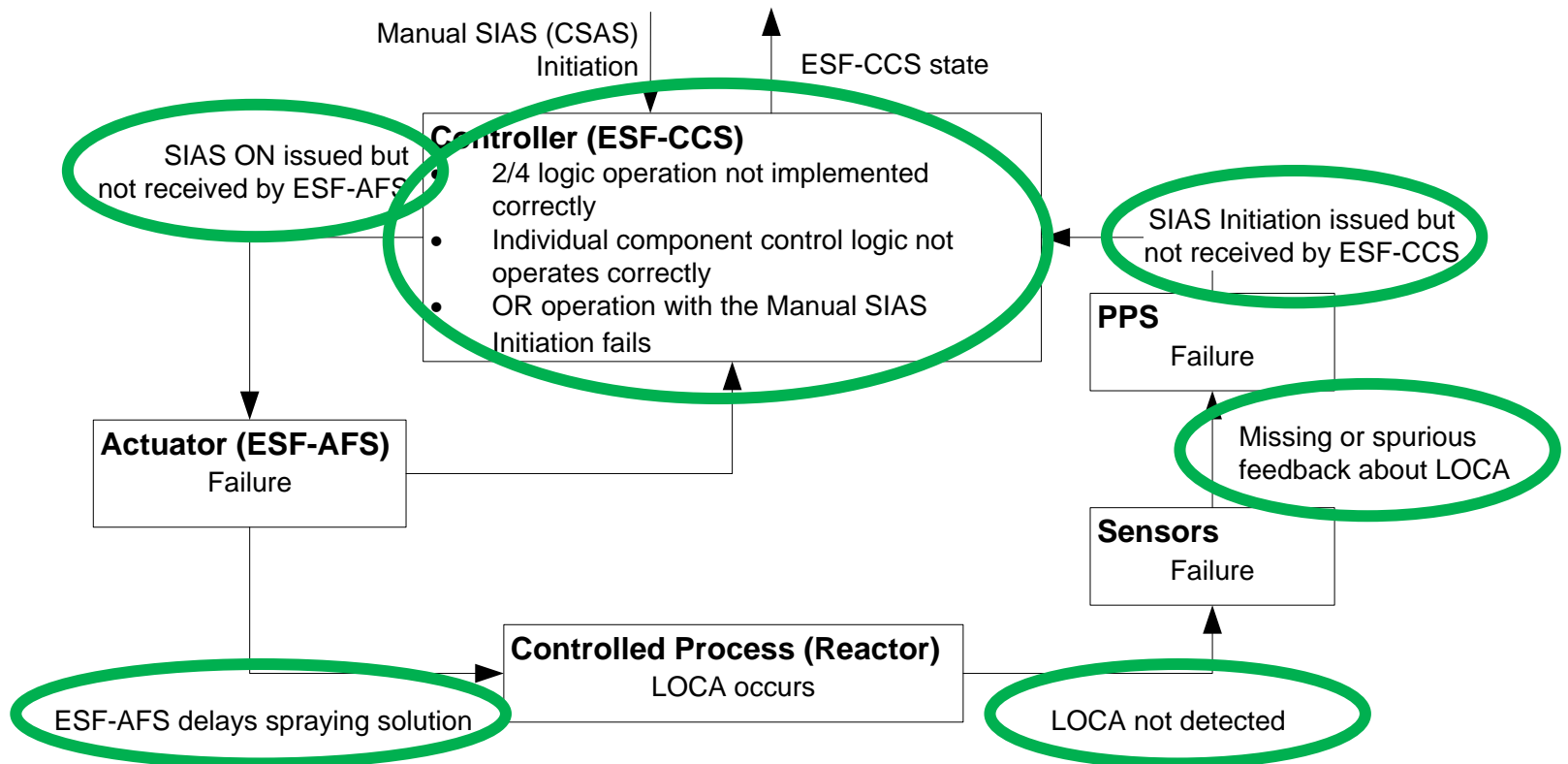
## Hazardous behavior of SIAS (Full)

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
<b>SIAS ON (From ESF-CCS to ESF-AFS)</b>	Not providing SIAS ON when LOCA occurs (a1) Not providing SIAS ON when 2ndHSL occurs (a2) Not providing SIAS ON when S/WP-Ex occurs (a3) Not providing SIAS ON when REA occurs (a4) Not providing SIAS ON when Manual SIAS Initiation occurs (a5)	Not hazardous	When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c1) When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c2) When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c3) When REA occurs, ESF-CCS waits too long to turn SIAS ON (c4) When Manual SIAS Initiation occurs, ESF-CCS waits too long to turn SIAS ON (c5)	SIAS ON stops before coolant is not provided enough (d1)
<b>SIAS OFF (From ESF-CCS to ESF-AFS)</b>	Not hazardous	Providing SIAS OFF when LOCA occurs (b1) Providing SIAS OFF when 2ndHSL occurs (b2) Providing SIAS OFF S/WP-Ex occurs (b3) Providing SIAS OFF REA occurs (b4) Providing SIAS OFF when Manual SIAS Initiation occurs (b5)	SIAS OFF is provided before the temperature decrease enough (c6)	Not hazardous
<b>Manual SIAS ON (From Operator to MCR/RSR)</b>	Not providing SIAS ON when LOCA occurs (a6) Not providing SIAS ON when 2ndHSL occurs (a7) Not providing SIAS ON when S/WP-Ex occurs (a8) Not providing SIAS ON when REA occurs (a9)	Not hazardous	When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c7) When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c8) When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c9) When REA occurs, ESF-CCS waits too long to turn SIAS ON (c10)	Not hazardous

# Application of STPA (4)

## Causal factors (a1) – Initiation

**Hazard: Not providing SIAS ON when LOCA occur (a1)**



# Application of STPA (4-1)

## Causal factors of unsafe control actions (a1-a9)

UCAs	A part of the safety control structure	Causal Factors
(a1-a4)	ESF-CCS	2/4 logic operation not implemented correctly Individual component control logic not operates correctly OR operation with the Manual SIAS Initiation fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
	Sensing (Reactor to Sensor)	The 4 events is not detected by Sensor
	Sensor	Sensor fails
	Reactor's state (Sensor to PPS)	Sensor provides spurious feedback
	PPS	PPS received the feedback correctly but does not issue SIAS Initiation
(a5)	SIAS Initiation (PPS to ESF-CCS)	SIAS Initiation issued but not received by ESF-CCS
	ESF-CCS	OR operation with the SIAS Initiation of PPS fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
(a6-a9)	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
	Operator	Judgement fails about the 4 events Misunderstanding about state of Safety Injection operation
	Manual SIAS (Operator to MCR/RSR)	SIAS Initiation issued but not received by MCR/RSR
	MCR/RSR (Manual Actuation Switch)	Manual Actuation Switch fails
	Manual SIAS Initiation Signal (MCR/RSR to ESF-CCS)	Manual SIAS Initiation Signal issued but not received by ESF-CCS
	ESF-CCS State (ESF-CCS to IPS)	ESF-CCS provides spurious information about Safety Injection Information about Safety Injection issued but not received by IPS
	MCR/RSR (Display)	MCR/RSR fails to display information
	Display (MCR/RSR to Operator)	Information of the 4 events issued but not received by Operator MCR/RSR displays spurious information about the 4 events and Safety Injection

# Conclusion & Future Work

- Analysing 3 of 8 functions and identifying hazardous behaviours and its causal factors using STPA
- An expert involved developing ESF-CCS said “STPA provides analysts with a novel view about causes of hazard”
- Future work
  - Hazard analysis with multiple controllers in progress
  - Objective hazard analysis
    - Need an automatic STPA based on a process model of system
    - STPA based on a formal (NuSCR) model

— THANK YOU —

Dong-Ah Lee  
Dependable Software Laboratory  
Konkuk University  
ldalove@konkuk.ac.kr