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
Background

KNICS Dependability Engineering

1. Harmonization of technologies
2. Interaction between the development, V&V, and dependability analyses lifecycles
3. Integration through lifecycle
4. Integration of dependability analysis for system and components

Safety System and Components

Safety Analysis Methods

Reliability Analysis Methods

Security Analysis Methods

Formal V&V Methods

Plan Req. Design Code Integ.

Lifecycles

SW

Human

HW
Background

Hazard Analysis of KNICS

Causal Models

- Single Cause
  - FMEA
    - Multiple Consequences

- Multiple Causes
  - HAZOP
    - Multiple Consequences

- Multiple Causes
  - FTA
    - Single Consequence

lifecycle

- System Req. phase
- SW Req. SW design
- SW Design SW Code
ESF-CCS

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIAS</td>
<td>Safety Injection Actuation Signal</td>
</tr>
<tr>
<td>CIAS</td>
<td>Containment Isolation Actuation signal</td>
</tr>
<tr>
<td>MSIS</td>
<td>Main Stream Isolation Signal</td>
</tr>
<tr>
<td>CSAS</td>
<td>Containment Spray Actuation Signal</td>
</tr>
<tr>
<td>AFAS</td>
<td>Auxiliary Feed-water Actuation Signal</td>
</tr>
<tr>
<td>CREVAS</td>
<td>Control Room Emergency Ventilation Actuation Signal</td>
</tr>
<tr>
<td>FHEVAS</td>
<td>Fuel Handling Area Emergency Ventilation Actuation Signal</td>
</tr>
<tr>
<td>CPIAS</td>
<td>Containment Purge Isolation Actuation Signal</td>
</tr>
</tbody>
</table>
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\textsuperscript{nd}HSL, S/WP-Ex, or REA—occur.

- **Safety constraint**
  - The SIAS must operate when the 4 events—LOCA, 2\textsuperscript{nd}HSL, S/WP-Ex, or REA—occur.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCA</td>
<td>Loss Of Coolant Accident</td>
</tr>
<tr>
<td>2\textsuperscript{nd}HSL</td>
<td>Second Heat Sink Loss</td>
</tr>
<tr>
<td>S/WP-Ex</td>
<td>Steam- and Water-pipe explosion</td>
</tr>
<tr>
<td>REA</td>
<td>Rod Ejection Accident</td>
</tr>
</tbody>
</table>
Application of STPA (1-1)

Hazards and Safety Constraints

<table>
<thead>
<tr>
<th>Function</th>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIAS</td>
<td>Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2\textsuperscript{nd}HSL, S/\textsuperscript{WP}-Ex, or REA—occur.</td>
<td>The SIAS must operate when the 4 events—LOCA, 2\textsuperscript{nd}HSL, S/\textsuperscript{WP}-Ex, or REA—occur.</td>
</tr>
<tr>
<td>CSAS</td>
<td>Heat removal and fission clean up fail when the three events—LOCA, S/\textsuperscript{WP}-Ex, or the SIAS—occur.</td>
<td>The CSAS must operate when the three events—LOCA, S/\textsuperscript{WP}-Ex, or the SIAS—occur.</td>
</tr>
<tr>
<td>CREVAS</td>
<td>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.</td>
<td>The CREVAS must operate when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.</td>
</tr>
</tbody>
</table>
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

Diagram:
- Operator
- MCR/RSR
- IPS
- ESF-AFS
- ESF-CCS
- RMS

- Manual CREVAS Command
- Display
- Ventilation
- Manual CREVAS Signal
- ESF State
- ESF-CCS State
- Automatic CREVAS Initiation
- ESF State
- ESF-CCS State
- Plant State
Application of STPA (3)

Hazardous behaviors of SIAS

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped Too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIAS ON (From ESF-CCS to ESF-AFS)</td>
<td>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)</td>
<td>Not hazardous</td>
<td>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)</td>
<td>SIAS ON stops before coolant is not provided enough (d1)</td>
</tr>
</tbody>
</table>
Application of STPA (3-1)

Hazardous behavior of SIAS (Full)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not Providing Causes Hazard</th>
<th>Providing Causes Hazard</th>
<th>Wrong Timing or Order Causes Hazard</th>
<th>Stopped Too Soon or Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIAS ON (From ESF-CCS to ESF-AFS)</td>
<td>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)</td>
<td>Not hazardous</td>
<td>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)</td>
<td>SIAS ON stops before coolant is not provided enough (d1)</td>
</tr>
<tr>
<td>SIAS OFF (From ESF-CCS to ESF-AFS)</td>
<td>Not hazardous</td>
<td>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)</td>
<td>SIAS OFF is provided before the temperature decrease enough (c6)</td>
<td>Not hazardous</td>
</tr>
<tr>
<td>Manual SIAS ON (From Operator to MCR/RSR)</td>
<td>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)</td>
<td>Not hazardous</td>
<td>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)</td>
<td>Not hazardous</td>
</tr>
</tbody>
</table>
Application of STPA (4)

Causal factors (a1) – Initiation

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

Controller (ESF-CCS)
- 2/4 logic operation not implemented correctly
- Individual component control logic not operates correctly
- OR operation with the Manual SIAS Initiation fails

Actuator (ESF-AFS)
- Failure

SIAS ON issued but not received by ESF-AFS

Manual SIAS (CSAS) Initiation

ESF-CCS state

PPS Failure
- Missing or spurious feedback about LOCA

Sensors Failure

Controlled Process (Reactor)
- LOCA occurs

ESF-AFS delays spraying solution

LOCA not detected
# Application of STPA (4-1)

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

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