SW-STPA:
A Software Hazard Analysis Technique based on STPA

Sun Hwi Lee
Dependable Software Laboratory
Konkuk University
## Contents

- Introduction

- Backgrounds
  - STAMP: Systems-Theoretic Accident Model and Process
  - STPA: System-Theoretic Process Analysis

- SW-STPA
  - New general form of Safety Control Structure

- Case Study: FBDtoC

- Conclusion & Future Work

- Q & A
INTRODUCTION
Introduction

• **Importance of software safety increases**
  – As the uses of software are various, software is germane to human’s life and property.

• **STAMP / STPA is powerful** hazard analysis technique for system
  – Many case studies showed that.

• But, it has problems to apply software
  – Subject of STPA is ‘system’ which is large and complex.

• **So, we propose SW-STPA**
  – It is expected that SW-STPA helps developer have more various sights.
BACKGROUND

STAMP
STPA
Backgrounds - STAMP

- Based on systems theory
- Treats accidents as a dynamic control problem
- Three basic concept
  - Safety constraints
  - Hierarchical safety control structure
  - Process model
- Includes
  - Entire socio-technical system
  - Component interaction accidents
  - Software and system design errors
  - Human errors
Backgrounds - STAMP

- Accidents occur when
  - Process model is inconsistent with real state of process and controller provides inadequate control actions

Control processes operate between levels of control
Backgrounds - STPA

• Goals
  – Identifying accident scenarios that encompass the entire accident process.
  – Providing guidance to users and information necessary to guide the design process and making it can be used before a design has been created.

• Uses
  – Control diagram
  – Functional requirements
  – System hazards
  – Safety constraints
  – Safety requirements for the component
Backgrounds - STPA

• Steps
  – Establish fundamentals
    • Defining accidents and unacceptable losses for system
    • System hazards
    • System safety requirements and constraints
    • Safety control structure

1. Identify the potential for inadequate control of the system that could lead to a hazardous state.

2. Determine how potentially hazardous control action identified in step 1 could occur.
Backgrounds - STPA

- General form of Safety control Structure
  - Human Controller
    • Operator of system.
  - Controller
    • Controller of system
  - Actuator
    • Actuates physical processes which are Controller ordered
  - Controlled Process
    • Physical controlled process
  - Sensor
    • Senses physical controlled process and gives feedback to Controller.
### Backgrounds - STPA

- **Four general types of inadequate control actions**
  - Used in STPA Step 1.

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Safety is not provided</th>
<th>Unsafe Action is provided</th>
<th>Wrong Timing / Order</th>
<th>Stopped too soon / too late</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Radiation Exposure</td>
<td>1. Radiates to patient regardless of exposure criteria.</td>
<td>1. Exposure criteria is saved too high</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Stop Radiation Exposure</td>
<td>-</td>
<td>-</td>
<td>1. Radiation is over the required amount.</td>
<td>1. Radiation is over the exposure limit, but radiation stopped too late</td>
</tr>
</tbody>
</table>

**Example of radiation exposure**
New general form of safety control structure
SW-STPA

- Subject of current SW-STPA
  - Not for embedded software, for stand-alone software.
  - For developed software. (Source codes are exist)
SW-STPA

• Difference of components
  – Components in STPA
    • Electromechanical, digital, human, social
  – Components in SW-STPA
    • Digital, human, social

Components and interactions in SW-STPA
New general form of safety control structure
– Differences between STPA vs. SW-STPA

**SW-STPA**

![Diagram comparing STPA and SW-STPA](image)
Safety Control Structure in SW-STPA

• **SW Controller with UI**
  – Composed of Input interface, Output interface, SW Controller
  – Interacts with Human Controller
  – Gives control actions to functional controllers

![Diagram of Safety Control Structure](image)
Safety Control Structure in SW-STPA

- **SW Controller**
  - **UI**
    - Input interface
      - Delivers Human Controller’s control actions to SW Controller
    - Output interface
      - Gives Result of control actions to Human Controller
  - **SW Controller**
    - Inputs + process model → decision
    - Gives control actions to functional controllers
    - Gives results to Output interface
Safety Control Structure in SW-STPA

• Functional Controller $n$
  – Describes each function in software
  – Ex>Digital Watch – Stop watch, Alarm, ...
  – Subject is software, not system
    • Each functional controller has to check what it did and gives feedback to SW Controller
  – Can be separated to small functional controllers.
Safety Control Structure in SW-STPA

• Information
  – STPA: Physical process vs. SW-STPA: Information
  – Subject is software, not system
    • There is no physical process in software
  – Information contains all of information which are changed, created, deleted by functional controllers
CASE STUDY: FBDTOC

Safety control structure of FBDtoC
Case Study: FBDtoC

- FBDtoC
  - Simple translator we developed

  - Functions
    - Open FBD file (in XML)
    - Translate FBD into C language
    - Save C file
Case Study: FBDtoC

- Safety Control Structure lv.1
Case Study: FBDtoC

- Safety Control Structure lv.2 (Translator)
Case Study: FBDtoC

- Safety Control Structure
CONCLUSION & FUTURE WORK
Conclusion & Future work

• Conclusion
  – STAMP/STPA is powerful hazard analysis technique for system
  – But it has problems applying STPA to software because of difference of subject
  – We propose SW-STPA and new general form of safety control structure.
  – And we described FBDtoC with SW-STPA, we developed.

• Future work
  – We will develop SW-STPA Step 2. for developed software.
    • How to describe process model for software controllers?
  – We will compare SW-STPA with other hazard analysis technique.
Thank you
Q & A

Contact: bigsaram@konkuk.ac.kr