A-STPA: An Open Tool Support for System-Theoretic Process Analysis

Asim Abdulkhaleq, Ph.D Student
Institute of Software Technology
University of Stuttgart, Germany

Joint work with:
Prof. Dr. Stefan Wagner

The 3rd STAMP Workshop, MIT, Boston, 26. March 2014
Agenda

- Motivation
- A-STPA Overview
- Challenges and Problems
- What’s Next
- A-STPA Demo
Motivation

◆ **Problem Statement:**

- STPA is a powerful hazard analysis approach which has proven to be effective on real systems.
- There is little tool support specifically for STPA.
- We usually use paper, word documents and drawing software (e.g. Visio, PowerPoint, etc.) in performing STPA which are a poor recording medium.

◆ **Research Objectives:**

- To better understand hazard analysis with STPA.
- To improve its application in practice.
- To provide tool support to automate the STPA approach as far as possible to make using STPA more efficient.
Overview: A-STPA (Automated STPA)

◆ A-STPA is:
  ➢ an open-source tool implemented in Java under Eclipse Platform.
  ➢ student project (from April 2013 to February 2014) with 9 students.

◆ The structure of A-STPA:

- STPA Components Data Model
- External Model
- Internal Model
- STPA Data Tables
- Mapping rules
- STPA Analysis Data
- Generated Data
- Control Diagrams Editor
A-STPA Main Features and Functions

◆ **Main Features:**

- Supports different operating systems:
  - Windows (32bit, 64bit): Vista, 7 or Windows 8
  - Linux and Macintosh (Mac OS X 10.6)

- Provides a semantic control structure diagram editor in which the process model can only augment the controller component.

◆ **Main Functions:**

- Edit the STPA analysis data.
- Draw the control structure diagram and process models.
- Edit tables such as the control actions table, unsafe control action table and causal factors table.
- Export control structure diagram as image and the final report of STPA analysis as PDF-file.
- Save/load the STPA hazard analysis results (as a file with extension *.haz)
Views in A-STPA

- A-STPA Explore Views
- Workbench View
- Toolbox View
Agenda

- Motivation ✓
- A-STPA Overview ✓
- Challenges and Problems 😛
- What’s Next
- A-STPA Demo
Challenges and Problems

◆ **A big Challenge is:**
  - All our students had no idea or previous experiences on the topic of safety and hazard analysis.

◆ **Issues during development:**
  - There are different control structure diagram notations.
  - Many researchers used different tables to record the causal factors analysis (step 3).

◆ **Questions arose during development:**
  - Who can connect to whom in the control loop?
  - Can the actuator connect directly to the sensor?
  - Can the actuator become a controller when it controls a component in the low level?
  - In which way shall we document the causal analysis results and scenarios?
Agenda

- Motivation ✔
- A-STPA Overview ✔
- Challenges and Problems ✔
- What’s Next 〇
- A-STPA Demo
What’s Next

◆ We plan:

➢ To distribute the download link of A-STPA to all of you and other safety experts.

➢ To conduct an online survey for evaluation of using A-STPA to help us to improve the overall quality of our tool.

➢ To use A-STPA during the tutorial sessions of 2\textsuperscript{nd} European STAMP Workshop (ESW2014), 22-23 September 2014, University of Stuttgart, Germany.

◆ Further Developments:

➢ Implement STPA Network Diagram (SND) which can help to facility the traceability between different levels of STPA analysis and view the results as tree.

➢ Export and import the STPA data table as spread sheets.

➢ Enhance the usability of the tool and add new features.

➢ Implement a simulation of causal analysis as far as possible based on process model variables.
Current Users of A-STPA in the world

Brought to you by: stupro-astpa
Home (Change File)

Date Range: 2014-03-18 to 2014-03-26

Downloads
79
In the selected date range

Top Country
Germany
60% of downloaders

Top OS
Other
48% of downloaders

OS downloads as: Percent

<table>
<thead>
<tr>
<th>Country</th>
<th>Macintosh</th>
<th>Unknown</th>
<th>Windows</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>17%</td>
<td>48%</td>
<td>35%</td>
<td>48</td>
</tr>
<tr>
<td>Portugal</td>
<td>0%</td>
<td>75%</td>
<td>25%</td>
<td>8</td>
</tr>
<tr>
<td>United States</td>
<td>0%</td>
<td>62%</td>
<td>38%</td>
<td>8</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0%</td>
<td>25%</td>
<td>75%</td>
<td>4</td>
</tr>
<tr>
<td>Israel</td>
<td>0%</td>
<td>33%</td>
<td>67%</td>
<td>3</td>
</tr>
<tr>
<td>Algeria</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>2</td>
</tr>
<tr>
<td>Singapore</td>
<td>0%</td>
<td>50%</td>
<td>50%</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
<td>1</td>
</tr>
<tr>
<td>Korea</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>1</td>
</tr>
<tr>
<td>China</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>1</td>
</tr>
</tbody>
</table>

Last Updated: < 6 hours ago. Download Stats API
To Download A-STPA

◆ A-STPA website:

http://www.iste.uni-stuttgart.de/en/se/werkzeuge/a-stpa.html

◆ To download A-STPA and get in touch with us:

  - Fill out the form on A-STPA website
  - Per Email: Asim.Abdulkhaleq@informatik.uni-stuttgart.de

◆ To provide us your feedback about using A-STPA, please fill out the online survey (It shouldn’t take 5 minutes)

The End…

Thank You for your attention. Questions?

StuPro 2013 - 2014
Adam Grahovac, Aleksander Zotov, Aliaksei Babkovich, Benedikt Markt, Fabian Toth, Jarkko Heidenwag, Jaqueline Patzek, Lukas Balzer, Patrick Wickenhäuser, Sebastian Sieber