XSTAMPP: An eXtensible STAMP Platform As Tool Support for Safety Engineering

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

Joint work with:
Prof. Dr. Stefan Wagner

The 4th STAMP Workshop  2015, MIT, Boston,
25. March 2015
Motivation: Why XSTAMP Platform?

◆ Problem Statement:

- The **A-STPA** (Automated STPA) tool was our first tool to implement STPA activities (introduced at STAMP 2014).
- A-STPA is already being used by safety analysts in different industrial domains.
- However, the current practices in using **A-STPA** face considerable obstacles:
  - **A-STPA** was developed based on the basic steps of STPA
  - The architecture of **A-STPA** is not extendable to include new requirements and further improvements.
- Consequently, these obstacles prevent **A-STPA** from supporting:
  - the application of STPA in different domains
  - The extension to support the application of CAST

◆ Research Objectives:

- To develop an extensible platform supporting the STAMP methodologies (STPA and CAST) to encourage the widespread adoption STAMP by safety analysts
- In particular, to develop a base platform for STPA that could be easily extended in the future to include CAST
Agenda

- Motivation
- A-STPA Overview
- A-STPA Shortcomings
- What is XSTAMPP?
- XSTAMPP Views
- XSTAMPP Future
- Conclusion
Overview: A-STPA (Automated STPA)

- A-STPA is open-source tool to assist safety analysts in performing STPA.
- A-STPA is already being used by safety analysts in different industrial domains in 53 countries around the world (2,832 download requests)

Source: https://sourceforge.net/projects/astpa/files/stats/map?dates=2014-03-10%20to%202015-03-16
A-STPA Main Workbench

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

Diagram showing a control system with various components and interactions, such as:
- Brake Pedal Force
- Vehicle Speed
- Brake Decelerate Request
- ACC Status
- Speed Sensor & Brake Sensor
- Engine Control System
- Acceleration Signal
- Controlled Process: Vehicle
- Radar Sensor
- Front speed Distance
- Brake Switch
A-STPA Shortcomings

● **Extensibility Issues:** *(based on the online survey with 51 safety experts)*

  - The A-STPA navigation cannot be extended to include a new user interface editor.
  - The A-STPA architecture does not support to be extended by plug-ins libraries or integrated with other existing tools.
A-STPA Shortcomings II

Describing Issues:

- The workbench of A-STPA is specified only to show one user interface view in the workbench UI.
- A-STPA does not have a project explorer to allow safety analysts to create or open more projects in the workbench.
A-STPA Shortcomings III

◆ Editing & Exporting Issues:
  - It is difficult to edit a large number of unsafe control actions (more than 100) in the unsafe control action table.
  - A-STPA does not allow the safety analysts to export the data in different formats.

◆ Functionality Issues:
  - A-STPA does not implement the context tables based on Thomas’ approach.
Agenda

- Motivation
- A-STPA Overview
- A-STPA Shortcomings
- What is XSTAMPP?
- XSTAMPP Views
- XSTAMPP Future
- Conclusion
What is XSTAMPP Platform?

- **XSTAMPP:**
  - is an open source, plug-in-based and extensible software platform
  - is based on the Eclipse Rich Client Platform (RCP) and plug-in development environment which makes our platform easier to integrate independent components.
  - is designed specially to serve the widespread adoption and use of STPA in different areas.
  - has the potential to be extended in the future to support the application of CAST for accident analysis.

We believe that XSTAMPP is a base platform to support the application of STAMP methodologies in different domains.
The XSTAMPP Architecture mainly consist of five components:

- STAMP components, STAMP UI editors, XSD specification template, plug-in development environment (PDE) and Eclipse Rich client Platform.

- Different projects
- Different STAMP components
- Independent UI editors for each STAMP component
- Independent XML Specification for each UI editor
- Extensible application framework
XSTAMPP Main Workbench

- Create different projects in the workbench
- Open different UI views in the workbench
- Draw components with different colours

Decoration button
Preferences to change the font and color
XSTAMPP vs. A-STPA

◆ XSTAMPP:
  - includes A-STPA as plug-in.
  - has the same major functions of A-STPA.
  - allows to create and open more than one project in the project explorer.
  - allows to arrange different user interface views in the workbench.
  - integrates, combines and updates easily by additional plug-in libraries.
  - allows to draw the control structure diagram components with different colours.
  - exports the whole project data as a PDF file and each individual user interface view as an Excel sheet or various image formats.

A-STPA stand alone version (current version 1.0.5)
Agenda

- Motivation
- A-STPA Overview
- A-STPA Shortcomings
- What is XSTAMPP?
- XSTAMPP Views
- XSTAMPP Future
- Conclusion
XSTAMPP supports to open different views in the main workbench.
XSTAMPP supports to export different formats Excel sheets, images and PDF.
XSTAMPP provides a help wizard to get instructions for each STPA step.
Agenda

- Motivation
- A-STPA Overview
- A-STPA Shortcomings
- What is XSTAMPP?
- XSTAMPP Views
- XSTAMPP Future
- Conclusion
XSTAMP Future?

We aim to benefit from the new architecture:

- to implement the CAST steps and provide them in the upcoming version of the platform (A-CAST plug-in)

- to integrate support for safety analyst to transform the STPA safety requirements automatically to formal specifications such as **Linear Temporal Logic** (LTL) (STPA2LTL plug-in)

- to support the safety analysts to verify design models of the system against the STPA safety requirements with model checking as well as software code. (STPA verifier)

- To support the safety analysts to generate test cases from STPA safety requirements.
Challenges and Problems

◆ A big challenge is:
  - reusing the A-STPA code and adapting all A-STPA functions which implement all necessary functions of STPA.
  - This challenge is addressed in the first version of XSTAMPP

◆ Finding bugs
  - Many bugs arose during reusing the A-STPA code which should be removed from XSTAMPP code.

◆ Testing XSTAMPP with real project in industry
  - Many safety analysts are interested in using XSTAMPP, but we do not know whether they used it in their real projects in industry and what are their problems and feedback.

Your feedback is highly appreciated and will help us to improve XSTAMPP
How to get XSTAMPP?

- **XSTAMPP website:**
  
  [http://www.iste.uni-stuttgart.de/se/werkzeuge/xstampp.html](http://www.iste.uni-stuttgart.de/se/werkzeuge/xstampp.html)

- **Download XSTAMPP and its source code:**
  

- **Online Feedback of using XSTAMPP:**
  

- **Get in Touch with us:**
  - Fill out the form on XSTAMPP website:
  - Email: [Asim.Abdulkhaleq@informatik.uni-stuttgart.de](mailto:Asim.Abdulkhaleq@informatik.uni-stuttgart.de)

- **XSTAMPP Vision:**

  XSTAMPP is free and open-source software and you are cordially invited to join us!
Thanks

◆ We would like to thank A-STPA team:
Aliaksei Babkovich, Lukas Balzer, Adam Grahovac, Jarkko Heidenwag, Benedikt Markt, Jaqueline Patzek, Sebastian Sieber, Fabian Toth and Patrick Wickenhaeuser

◆ We would like to thank Mr. Lukas Balzer who worked with us to improve and build XSTAMPP.

◆ We would like also to thank the safety experts who provided us their valuable feedback and evaluation of using A-STPA.
The End…

Thank You for your attention.

Questions?

Tool Demo will be presented during Buffet Dinner and Poster Session