www.uni-stuttgart.de

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. Viso, 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.
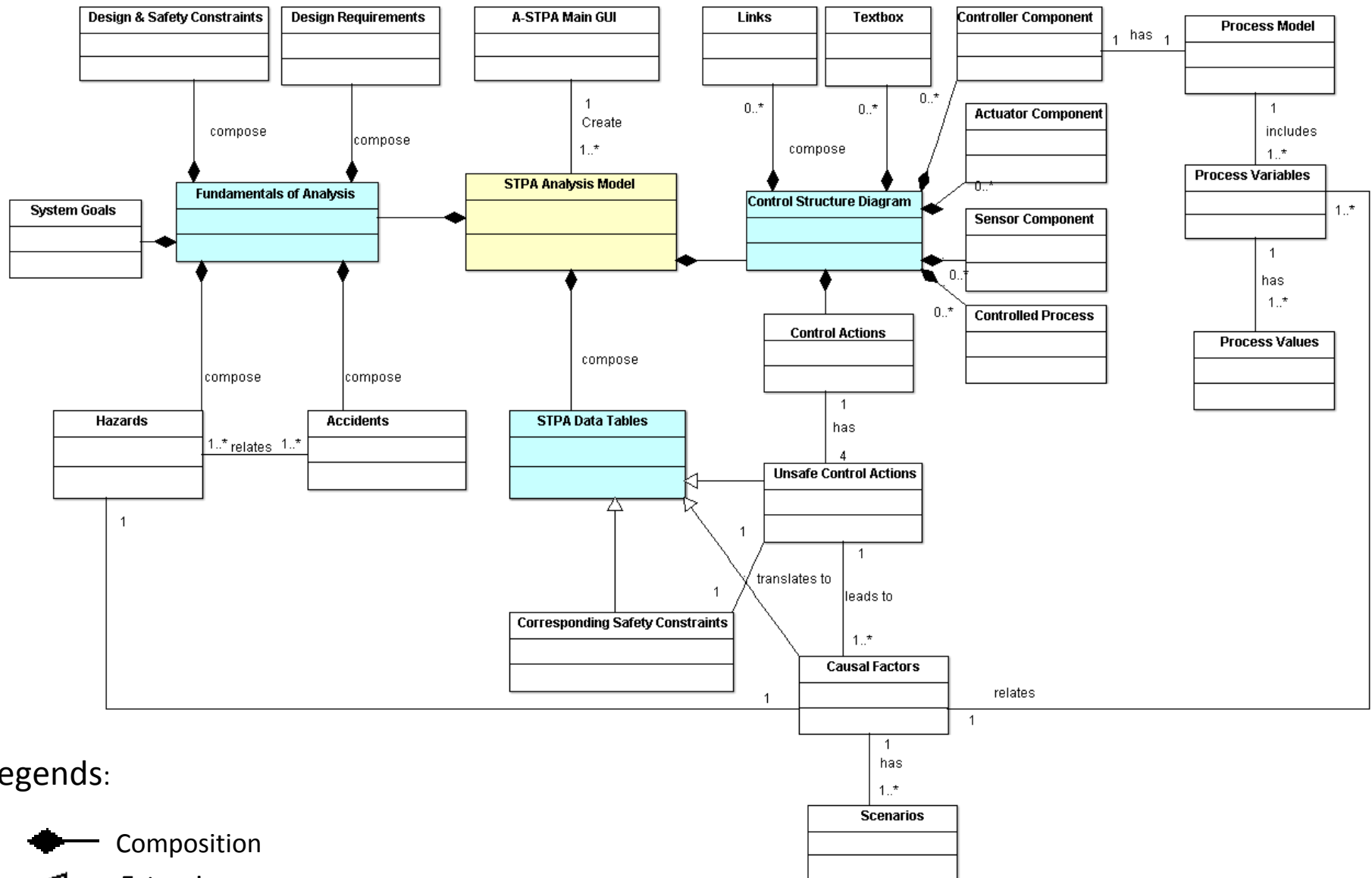
Overview: A-STPA (Automated STPA)

◆ **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 :**
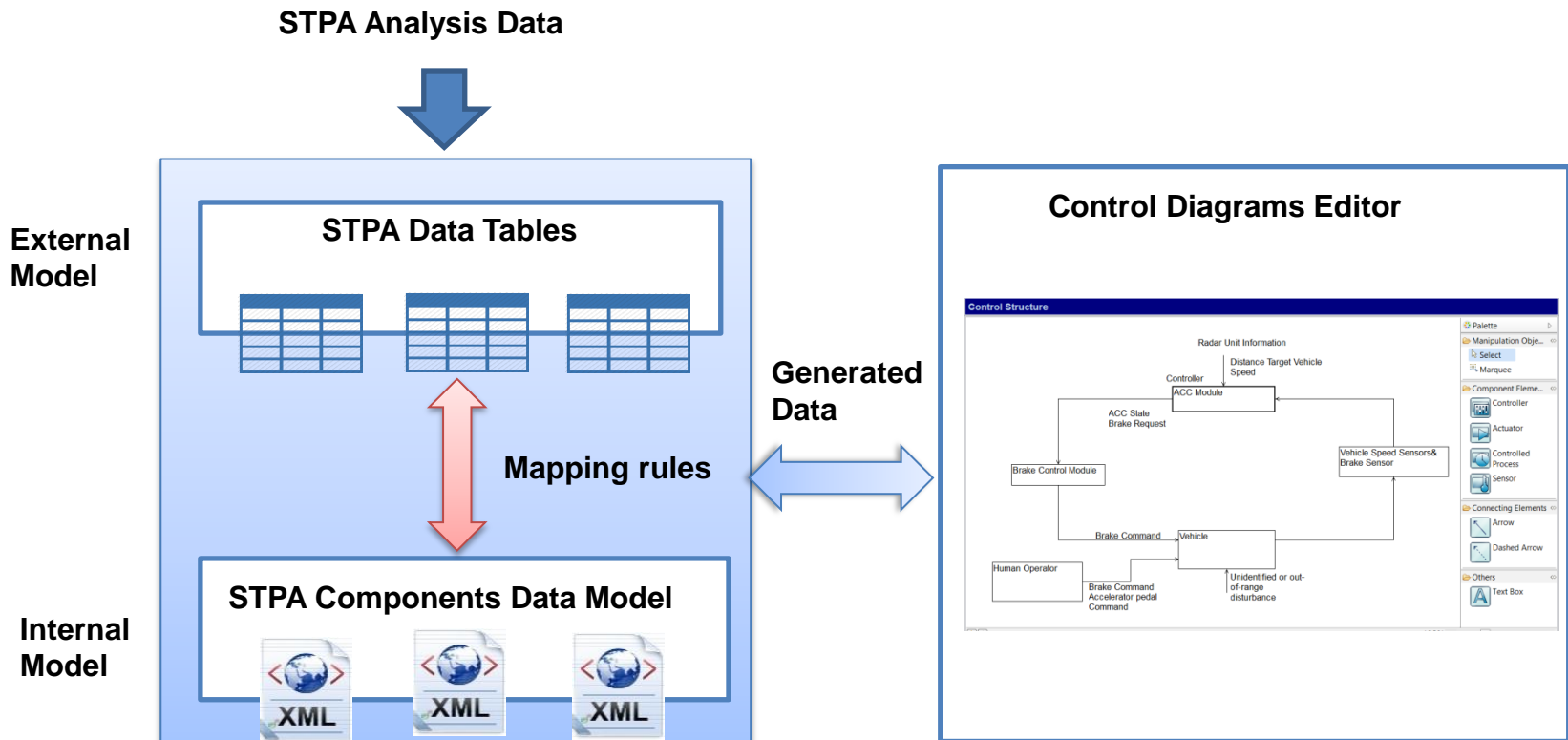
Legends:

Composition

Extension

1..*   1   Association (without aggregation)

STPA Data Modeling (Class diagram)

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.
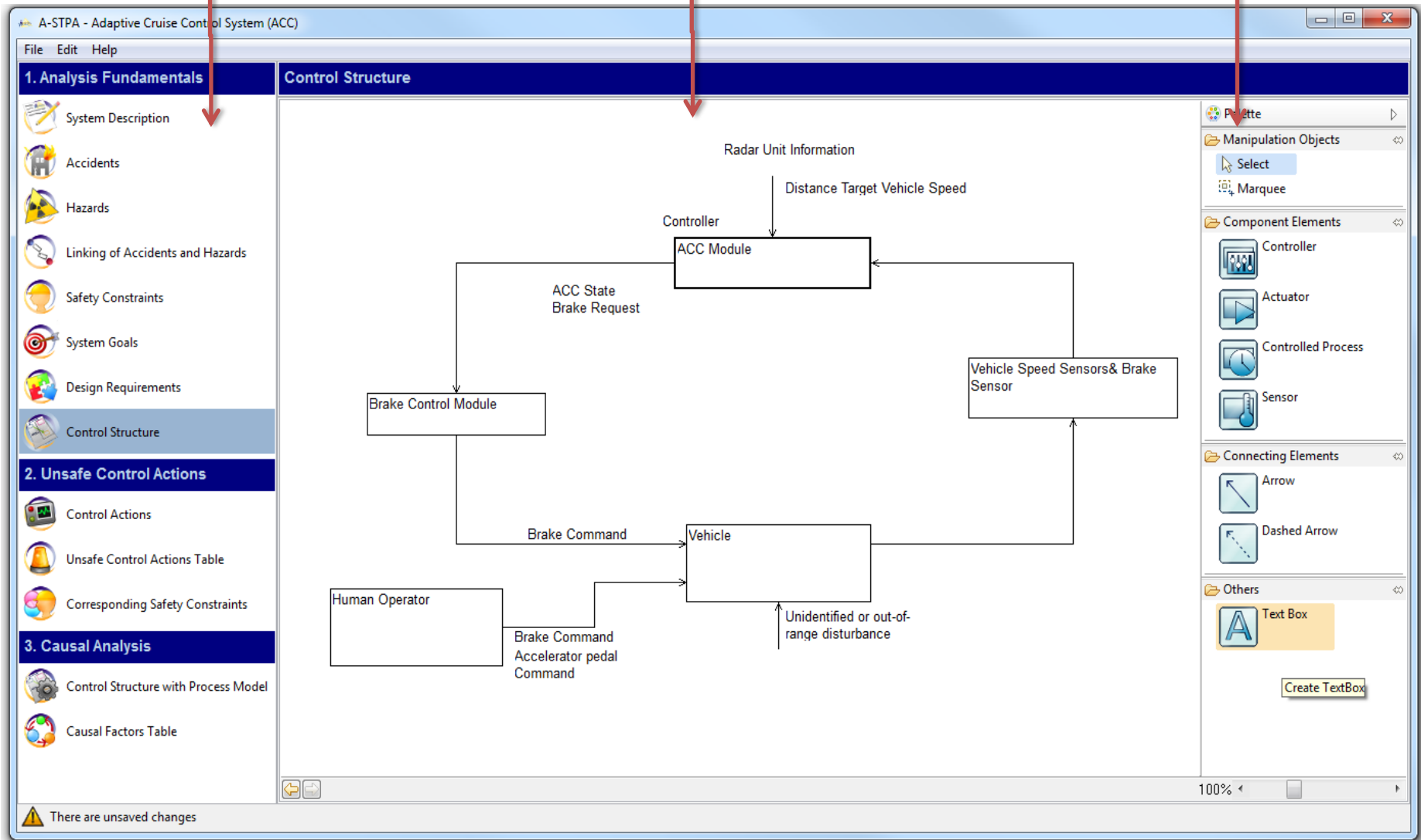
◆ **Main Functions:**

  ➢ 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

A-STPA - Adaptive Cruise Control System (ACC)

File   Edit   Help

1. Analysis Fundamentals

- System Description
- Accidents
- Hazards
- Linking of Accidents and Hazards
- Safety Constraints
- System Goals
- Design Requirements
- Control Structure

2. Unsafe Control Actions

- Control Actions
- Unsafe Control Actions Table
- Corresponding Safety Constraints

3. Causal Analysis

- Control Structure with Process Model
- Causal Factors Table

Control Structure

Radar Unit Information

Distance Target Vehicle Speed

Controller

ACC Module

ACC State
Brake Request

Vehicle Speed Sensors& Brake Sensor

Brake Control Module

Brake Command

Vehicle

Human Operator

Brake Command
Accelerator pedal
Command

Unidentified or out-of-range disturbance

Palette

Manipulation Objects
- Select
- Marquee

Component Elements
- Controller
- Actuator
- Controlled Process
- Sensor

Connecting Elements
- Arrow
- Dashed Arrow

Others
- Text Box

Create TextBox

100%

There are unsaved changes

Agenda

- ❖ Motivation ✔
- ❖ A-STPA Overview ✔
- ❖ Challenges and Problems ◎
- ❖ What's Next
- ❖ A-STPA Demo

◆ **A big Challenge is:**

  ❏ All our students had no idea or previous experiences on the topic of safety and hazard analysis
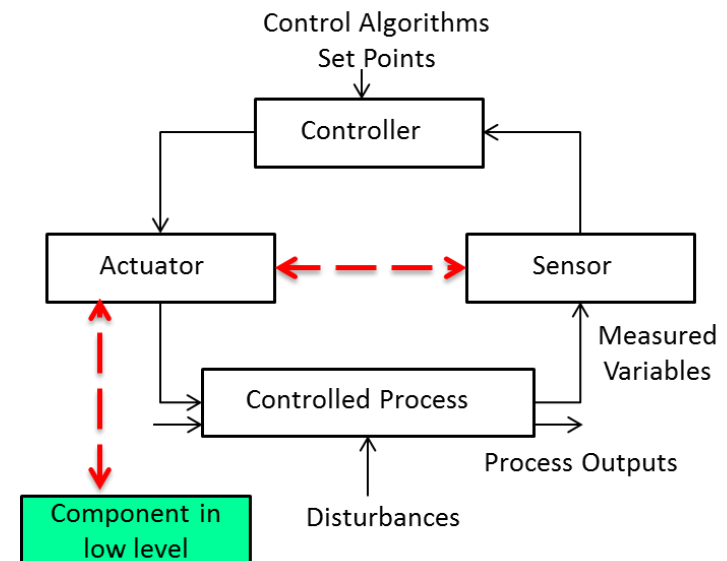
◆ **Issues during development:**

  ❏ 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 we shall document the causal analysis results and scenarios?

Seminar and tutorials on STAMP/STPA

Control Algorithms
Set Points

Controller

Actuator ◄ ▬ ▬ ► Sensor

Measured Variables

Controlled Process

Process Outputs

Component in low level

Disturbances

Agenda

- ❖ Motivation ✔

- ❖ A-STPA Overview ✔

- ❖ Challenges and Problems ✔

- ❖ What's Next ◎

- ❖ 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 2nd 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
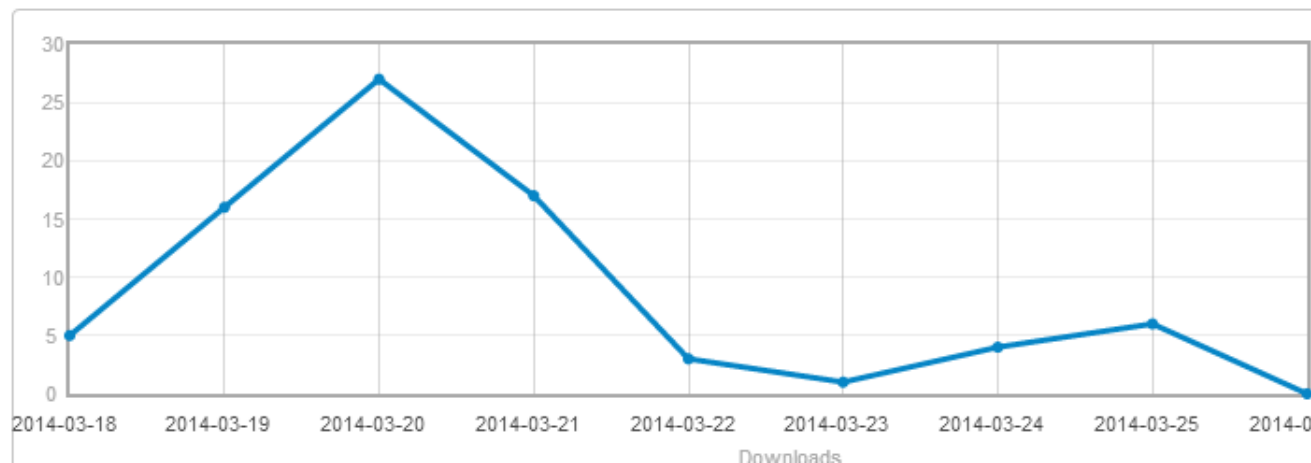
DOWNLOADS
79
In the selected date range

TOP COUNTRY
Germany
60% of downloaders

TOP OS
Other
48% of downloaders

OS downloads as: Percent ▼

	Country ⇕	Macintosh ⇕	Unknown ⇕	Windows ⇕	Total ▲
1.	Germany	17%	48%	35%	48
2.	Portugal	0%	75%	25%	8
3.	United States	0%	62%	38%	8
4.	Switzerland	0%	25%	75%	4
5.	Israel	0%	33%	67%	3
6.	Algeria	0%	0%	100%	2
7.	Singapore	0%	50%	50%	2
8.	United Kingdom	100%	0%	0%	1
9.	Korea	0%	0%	100%	1
10.	Netherlands	0%	100%	0%	1
11.	China	0%	0%	100%	1
					79

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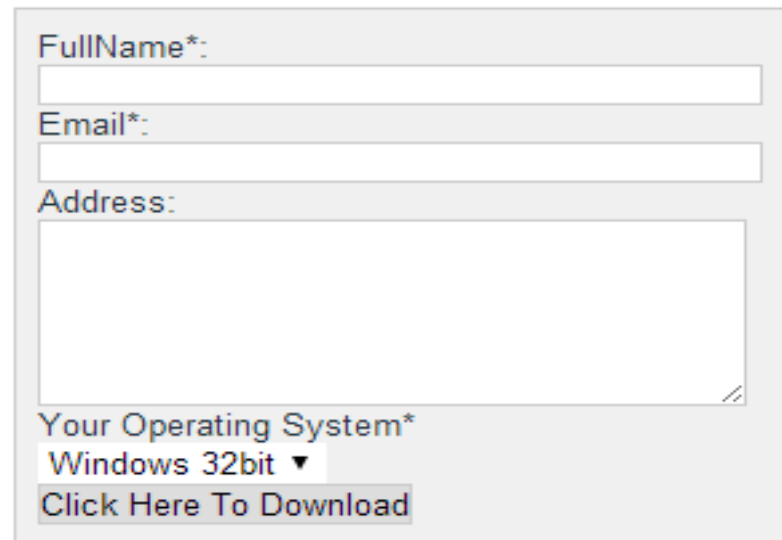
To Download A-STPA

◆ **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

   FullName*:
   [   ]
   Email*:
   [   ]
   Address:
   [   ]
   Your Operating System*
   Windows 32bit ▼
   Click Here To Download

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

   http://a-stpa.limequery.org/index.php/survey/index/sid/334679/newtest/Y/lang/en

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