

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

Asim Abdulkhaleq, Stefan Wagner Institute of Software Technology, University of Stuttgart, Germany

## A-STPA (Automated STPA)

A-STPA is an open tool to help transform STPA (Systems-Theoretic Process Analysis) to an executable STPA which automates the activities of STPA.

**Context:** A-STPA is an open-source tool based on the Eclipse platform which is developed as a student project in the software engineering programme of the University of Stuttgart. The student project started in April 2013 and will finish in February 2014. Our team consisted of 9 students and 3 teaching assistants.

## Main Functions of A-STPA

- Edit the fundamentals of the analysis
- Link the conducted information during step 1 to the other components in the next steps such as the hazards link to the accidents and safety constraints which are derived from the hazards.
- Draw the control structure diagram
- Edit tables such as the control actions table, unsafe control action table and causal factors table
- Augment the control structure diagram with a process model
- Export and import the STPA hazard analysis results

## **Research Objectives**

The overall objective of our research is to better understand hazard analysis with STPA and improve application in practice. In this paper, we its concentrate on providing tool support to make using STPA more efficient. Hence, the goal is to develop tool support to automate the STPA approach as far as possible.

. Analysis Funda

Linking of Acc., ts and Ha

Safety Constraints

Design Requirements

Unsafe Control Actions

Control Structure

Control Actions

Causal Factors Table

System Goals

Hazards

## **A-STPA User Interfaces/Views**

# File Edit Help # Welcome Always show Welcome at start up

#### Unsafe Control Actions Table Corresponding ... ty Constraints Control Struct... Process Model Offset: 0 Line: 1

• 9 • A \* E

daptive Cruise Control System (ACC) is an automotive feature that allows a vehicle's cruise control system to adapt the vehicle's speed to the traffi

stem is able to automatically adjust the driving speed as well as the distance to the vehicle ahead in accordance with the pre-settings

nvironment. ACC uses a long range radar sensor which is attached to the front of the vehicle and detects a target vehicle up to 150 meters in front. The ACC

#### **Editing Fundamentals View**

Adaptive Cruise Control System (ACC)

BIUA A A - A - Seque U







#### **Drawing Control Structure View**

| 🏎 A-STPA  |            |   |               |                   |  |
|---|------------|---|---------------|-------------------|--|
| File Edit Help  |            |   |               |                   |  |
| A-SIPA         File       Edit       Help         1. Analysis Fundamentals       Causal Factors Table         System Description       Component       Causal         Acidente       Component       Causal |            |   |               |                   |  |
| System Description  | Component  | Causal Factor   | Hazard Links  | Safety Constraint | Notes / Rationale                                      |
| Accidents   | ACC Module | control Input (from Radar<br>Sensor) wrong or missing | Not Hazardous | eo 🖬 🚥            | Radar sensor should be developed further to detect the |

#### **Welcome Screen**

| ile Edit Help  |                              |   |    |   |    |   |    |   |   |  |
|--|------------------------------|---|----|---|----|---|----|---|---|--|
| Analysis Fundamentals  | Unsafe Control Actions Table |   |    |   |    |   |    |   |   |  |
| System Description   | Control Action               | Not Given   |    | Given Incorrectly   |    | Wrong Timing  |    | Stopped Too Soon  | ļ |  |
| Accidents<br>Hazards   | Provides Brake Light Command | Vehicle does not<br>illuminate brake light to<br>warn vehicle in the behind   | ×  | Brake light commanded<br>iluminate light while ACC<br>module does not request                 | X  | Brake light command<br>illuminate late after the<br>vehicle has stopped                           | X  | Brake light iluminate<br>stopped too soon, during<br>braking situation            | 1 |  |
| Linking of Accts and Hazards   |                              | [H-2]   | 90 | Not Hazardous   | 90 | [H-2]   | 00 | Not Hazardous   | 1 |  |
| Safety Constraints   | Provides Brake Command       | Add not given UCA   | 8  | Add given incorrectly UCA   | 8  | Add wrong timing UCA  |    | Add stopped too soon UCA  |   |  |
| Design Requirements  |                              | Vehicle does not brake<br>when the vehicle has<br>detected a slowed or<br>stopped object in its path                            | ×  | Braking is commanded<br>when there is no a slowed<br>or stopped object in the<br>vehicle path | ×  | Early: Braking is<br>commanded to early when<br>the distance to the target<br>vehicle is too far  | ×  | Braking stops too soon<br>before the safety distance<br>to target vehicle reached |   |  |
| Unsafe Control Actions   |                              | [H-1] [H-3]   | 90 | [H-2] [H-3]   | 00 | [H-1]   | 00 | [H-1] [H-3]   |   |  |
| Control Actions Unsafe Control Actions Table Correspondingty Constraints |                              | Vehicle does not brake<br>when the distance<br>between an forward object<br>is less than the distance<br>that set by the driver | ×  |   |    | Late: Braking is<br>commended too late when<br>the distance to the target<br>vehicle is too close | ×  |   |   |  |
|  |                              | [H-1] [H-3]   | 90 | Add given incorrectly UCA   | ÷  | [H-1] [H-3]   | 00 | Add stopped too soon UCA  | Í |  |
| Causal Analysis<br>Control Struct Process Model                          |                              | Vehicle does not brake<br>because the driver has<br>ignored all of the warnings   | ×  |   |    |   |    |   |   |  |
| Causal Factors Table   | 1                            |   | _  | 111   | _  |   | _  |   |   |  |

**Unsafe Control Actions View** 



#### **Drawing the Process Models View**



#### **Causal Analysis View**

## **A-STPA Website**

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

## A-STPA is developed by:

Students Team: Aliaksei Babkovich, Lukas Balzer, Adam Grahovac, Jarkko Heidenwag, Benedikt Markt, Jaqueline Patzek, Sebastian Sieber, Fabian Toth and Patrick Wickenhaeuser Supervisors: Ivan Bogicevic, Daniel Kulesz and Jasmin Ramadani Customer& Contact Person: Asim Abdulkhaleq