Missing no Interaction – Using STPA for Identifying Hazardous Interactions of Automated Driving Systems

Asim Abdulkhaleq, University of Stuttgart, Germany
Markus Baumeister, Systems & Technology, Continental Chassis & Safety Division
Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work
Automated Driving
Safe and Dynamic Driving towards Vision Zero
Motivation
Automotive architecture trend

Increased chance for random & systematic failures to cause behaviour deviations of functions

Increased potential of functions to be unsafe as specified

Summary of vehicle development tendencies

Source: WRC Market Report E/E Architecture 2013
Motivation
Safety for automated driving

› Starting with AD L3: Driver may distract himself
  › No immediate human fallback!
› Thus most intelligent, independently powered safety mechanism no longer available
  › Partial fail-operational (or fail-degraded) mechanisms necessary
    › Functional Safety
› Specified behaviour must work in all situations
  › Safety in Use

Relationship between Functional Safety and Safety in Use
<table>
<thead>
<tr>
<th></th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Motivation – Safety in Automated Driving</td>
</tr>
<tr>
<td>2</td>
<td>Safety in Use vs. Functional Safety</td>
</tr>
<tr>
<td>3</td>
<td>Safety in Use Analysis</td>
</tr>
<tr>
<td>4</td>
<td>Applying STPA for Safety in Use</td>
</tr>
<tr>
<td>5</td>
<td>Results</td>
</tr>
<tr>
<td>6</td>
<td>Conclusion &amp; Future Work</td>
</tr>
</tbody>
</table>
Safety in Use vs. Functional Safety
Location in the development cycle

Collision Avoidance Example

Real World
Objects can occur in front of the car and should not be hit

Item Definition
Evasion maneuver by function, Required actuator performance, Required sensor performance

Function Spec
Spec

Architecture
Module and Interface specification Allocation of SW to Components

Implementation
Executable and Parameterization Hardware components

Execution
Behaviour in the field

Potential failures

Sensor performance insufficient for planned maneuver
Not all situation might allow evasion, breaking maneuver missing
Driver might countersteer maneuver
No interface for function to influence steering; wrong granularity of values
Function running on too slow MCU
SW steers in wrong direction
Environmental model orders objects incorrectly
OS executes SW only every 2nd cycle
SW was disabled by application driver
Sensor breaks (e.g. no video)
Bit flip in parameters disables function
Bit flip in memory causes steering in wrong direction
Safety in Use vs. Functional Safety

Different Definitions
[from Böhmert, Blüher 2016]

- **Roadworthiness (Operational Safety)**
  [property or ability of a car, bus, truck or any kind of automobile to be in a suitable operating condition or meeting acceptable standards for safe driving and transport of people, baggage or cargo in roads or streets]

- **Availability**
  [readiness for correct service]

- **Reliability**
  [continuing for correct service]

- **Safety**
  [absence of unreasonable risk]

  - **Functional safety**
    [absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems]

  - **Integrity (Functional)**
    [absence of unreasonably hazardous functionality]

  - **Safety in use**
    [absence of hazards due to human errors]

- **Maintainability**
  [ability to undergo modifications and repairs]

Source:


Safety in Use vs. Functional Safety
Safety in Use and interactions

- Specification failures often happen due to missed potential interactions

1. Driver Human-and-Driver Human Interaction (HIH)
   - misunderstanding, aggression, …
2. Driver Human-and-Driver Machine Interaction (HIM)
   - confusion, misuse, inaction, …
3. Driver Human-and-other Traffic Participants Interaction (HIP)
   - bad estimations, …
   - overload, missing participants, …
5. Automated Driving System-and-other Traffic Participants (AIP)
   - feedback loops, different behaviour,
6. Automated Driving System and other Driver Humans (AID)
Safety in Use Analysis
Approach at Continental

<table>
<thead>
<tr>
<th>Identify all (correct) functionalities of item</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each function</td>
</tr>
<tr>
<td>Identify potentially hazardous or illegal scenarios</td>
</tr>
<tr>
<td>Due to interaction</td>
</tr>
<tr>
<td>* driver with vehicle system</td>
</tr>
<tr>
<td>* vehicle system with driver in other vehicle</td>
</tr>
<tr>
<td>* vehicle system with other vehicle’s system</td>
</tr>
<tr>
<td>* vehicle system with infrastructure</td>
</tr>
<tr>
<td>Using keywords as inspiration</td>
</tr>
<tr>
<td>For each scenario</td>
</tr>
<tr>
<td>Hazard identifiable for function under consideration?</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>S and C rating obvious?</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Document rationale</td>
</tr>
<tr>
<td>Determine by analysis using simulations, driving studies, or accident databases</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>S or C = 0?</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Choose most efficient measure</td>
</tr>
</tbody>
</table>

› Situation + Behaviour = potentially hazardous scenario

› Keyword-guided brainstorming of situations
  › Dependent on experience of analyst

› Evaluation of risk
  › Similar to HARA for functional safety

Is there a method less dependent on inspiration?
Safety in Use Analysis
Excerpt of SiU Results for Lane Change

Four (out of six) SiU requirements mainly relevant for “Lane Change” functionality:

<table>
<thead>
<tr>
<th>ID</th>
<th>SiUA-Requirements</th>
<th>Cause of hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIUR-16</td>
<td>Lane changes shall only be conducted when the vehicle can determine <strong>sufficient length</strong> of the <strong>new lane</strong> for at least a brake to standstill.</td>
<td>Potential violation of known requirement in seldom situation</td>
</tr>
<tr>
<td>SIUR-33</td>
<td>There shall be no automated lane change <strong>while</strong> handing over control to the driver (<strong>Take over Request</strong>).</td>
<td>Normal behaviour causing hazard by mode interaction.</td>
</tr>
<tr>
<td>SIUR-38</td>
<td><strong>Motorcycles</strong> overtaking <strong>on the lane markings</strong> (i.e. between the lanes) shall be observed during lane changes.</td>
<td>Potential violation of known requirement in seldom situation</td>
</tr>
<tr>
<td>SIUR-45</td>
<td>The automated vehicle shall not block a formed <strong>corridor for emergency vehicles</strong> while changing lanes.</td>
<td>Normal behaviour causing hazard in special situation</td>
</tr>
</tbody>
</table>

Will STPA find these requirements or others?
Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work
Prototype Realization of Automated Driving
Layered Functional Architecture
We apply STPA to identify the hazardous situations of the lane change function and develop detailed safety requirements/controls.

Our main question: Can STPA derive the Safety in Use requirements (SiU)?
Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work
STPA Results
STPA Step 0: Establish the fundamentals of analysis

› We identify one accident which automated driving can lead to (lane change function).
› We identify 12 hazards which can lead to this accident and
› We translate these 12 hazards into system-level safety constraints.

Accident AC-1: The ego vehicle cruising chauffeur collides with a vehicle during the lane change procedure and people dies/are harmed.

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>H-1</td>
<td>The Cruising Chauffeur system did not estimate correctly the position and velocity of the other traffic participants in the lane.</td>
</tr>
<tr>
<td>H-2</td>
<td>The Cruising Chauffeur system did not recognize the lane markings.</td>
</tr>
<tr>
<td>H-3</td>
<td>The Cruising Chauffeur system did not turn on the light of the direction indicators.</td>
</tr>
<tr>
<td>H-4</td>
<td>The Cruising Chauffeur system steered the ego vehicle in the wrong direction.</td>
</tr>
</tbody>
</table>
STPA Results
STPA Step 0: Safety-Control Structure Diagram

[Diagram showing the relationship between various components such as Driver Human, HMI (Human-Machine Interface), Cruising Chauffeur System, Vehicle Dynamics Controller, etc., with arrows indicating the flow of information and control.]
# STPA Results

## STPA Step 1: Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing incorrect causes hazard</th>
<th>Wrong timing or order causes hazard</th>
<th>Stopped too soon or Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane Change</td>
<td><em>The CC system did not provide the lane change when it is involved due to an emergency situation (e.g. accident occurred before the Ego vehicle).</em></td>
<td><strong>UCA1.1</strong> The CC system provided incorrect lane change request to the motion control to change lane while there is no gap in the target lane.</td>
<td><strong>UCA1.5</strong>. Too early: The CC system started the lane change function too early while the gap has not been reached yet.</td>
<td><strong>UCA1.8</strong>. Stopped too soon: The CC system provided a lane change request too short to the motion control that was not enough to change the vehicle to the target lane.</td>
</tr>
<tr>
<td></td>
<td><em>[Not Hazardous]</em></td>
<td>[H-1][H-2][H-7][H-8][H-9][H-12]</td>
<td>[H-1] [H-2] [H-4][H-5][H-10]</td>
<td>[H-4] [H-5]</td>
</tr>
</tbody>
</table>

**Interaction:**
- AIE
- AIP
- AIE, AIP
- AIP

Each unsafe control action is translated into a corresponding safety constraint.
## STPA Results

### STPA Step 2: Causal Factor Analysis

Unsafe Control Action: UCA1.1 The CC provided incorrect lane change request to the motion control to change lane while there is no gap in the target lane.

Associated Hazards: [H-1][H-2][H-7][H-8][H-9][H-12]

<table>
<thead>
<tr>
<th>Component</th>
<th>Causal Factors</th>
<th>Safety Constraints/Controls</th>
<th>Notes / Rationale</th>
</tr>
</thead>
</table>
| **Cruising chauffeur System** | √ **Process model incorrect:** The CC estimated a wrong position of other traffic participant in the adjacent lane (target lane). The CC incorrectly believes that there is an enough gap to change lane in the target lane. The CC received a wrong ego vehicle width. The CC incorrectly estimated the traffic conditions.  
√ **Control input wrong:** The driver is request a lane change in non-highway road. | 1. Make the CC system able to be a self-adaptive system to the traffic changes during the lane change procedure.  
2. If the backend or V2x communication unit is unavailable, the CC system should be immediately warned the driver to take over control and transited automatically to inactive status. |                                                                                                                                                                       |
We identify 41 STPA safety requirements for the lane change function.

We evaluated the resulting safety requirements against the requirements created in the SiU analysis.

<table>
<thead>
<tr>
<th>ID</th>
<th>SiUA-Requirements</th>
<th>Mapping</th>
<th>Cause of hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIUR-16</td>
<td>Lane changes shall only be conducted when the vehicle can determine sufficient length of the new lane for at least a brake to standstill.</td>
<td>(SR 1.6)</td>
<td>Potential violation of known requirement in seldom situation</td>
</tr>
<tr>
<td>SIUR-33</td>
<td>There shall be no automated lane change while handing over control to the driver (ToR).</td>
<td>No mapping</td>
<td>Normal behaviour causing hazard by mode interaction.</td>
</tr>
<tr>
<td>SIUR-38</td>
<td>Motorcycles overtaking on the lane markings (i.e. between the lanes) shall be observed during lane changes.</td>
<td>No mapping</td>
<td>Potential violation of known requirement in seldom situation</td>
</tr>
<tr>
<td>SIUR-45</td>
<td>The automated vehicle shall not block a formed corridor for emergency vehicles while changing lanes.</td>
<td>(SR 1.1)</td>
<td>Normal behaviour causing hazard in special situation</td>
</tr>
</tbody>
</table>

Overall six SiU requirements were analyzed and for three of them a mapping towards STPA requirements could be found.
We evaluated the 41 STPA safety requirements against the requirements created in the SiU analysis.

<table>
<thead>
<tr>
<th>ID</th>
<th>STPA Safety Requirement</th>
<th>Type *</th>
<th>Mapping</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR 0.5</td>
<td>The traffic markings must be in a good quality and visibly.</td>
<td>?</td>
<td>Special</td>
<td>AIE</td>
</tr>
<tr>
<td>SR 0.7</td>
<td>CC must not lose the detection of other traffic participants while CC changes lanes</td>
<td>FuSa &amp; SiU</td>
<td>No mapping</td>
<td>AIP</td>
</tr>
<tr>
<td>SR 0.8</td>
<td>CC must not steer the ego vehicle in the wrong direction.</td>
<td>FuSa</td>
<td>N/A</td>
<td>AIE</td>
</tr>
<tr>
<td>SR 0.10</td>
<td>CC must estimate the lane velocity correctly.</td>
<td>FuRe &amp; FuSa</td>
<td>N/A</td>
<td>AIP</td>
</tr>
<tr>
<td>SR 1.1</td>
<td>The CC must not send a lane change request to the motion control while it is not allowed due to the traffic road conditions.</td>
<td>SiU</td>
<td>(SIUR-45)</td>
<td>AIE/AIP</td>
</tr>
<tr>
<td>SR 1.6</td>
<td>CC must abort a lane change due to unexpected changes in the prerequisites of the lane change function.</td>
<td>SiU</td>
<td>(SIUR-16)</td>
<td>AIE</td>
</tr>
</tbody>
</table>

*Legends: FuSa (Functional Safety), SiU (Safety in Use), FuRe (Functional Requirements), ? Difficult to classify

Overall 41 STPA requirements were found on different analysis levels. Many of these are related to the basic driving task as SR0.8 und SR 0.10.
Discussion

› **Quantity**: STPA created safety requirements also outside the domain of SiU in the form of functional safety requirements, and “normal” functional requirements.

› **Abstractness**: Many STPA safety requirements describing SiU issues are relatively abstract with respect to the involved hazard.

› **Level of analysis**: On detailed analysis level (i.e. causal factor analysis), the discovered STPA safety requirements are in a great majority not SiU-related due to analyzing the malfunction of some system component.

› **Scenarios**: Whereas STPA analyzed only the two traffic situations, the SiU analysis typically has analyzed a different scenario for each resulting requirement.
The Safety-in-Use Approach based on STPA

› We proposed an extension to STPA for safety in use analysis by including the traffic situation analysis as a part of the STPA Step 0 to help the safety in use analysis engineers to focus the time and efforts only on safety in use aspect.

› We include also a step for identifying design requirements at the end of each STPA steps to help the safety in use engineers to identify/refine their design based on the STPA results.

Diagram: 
- Identify the traffic situations in which the accident scenarios could occur
- Identify accident Scenarios
- Identify the hazards that could lead to accident scenarios
- Translate the system-hazard into system-level safety constraints
- Identify the design requirements
- Draw the safety control structure diagram
- Identify the potential interactions of interest in the safety control structure diagram
- Evaluate each unsafe interaction and translate it into a corresponding safety constraint
- Identify /update the design requirements
- Identify the causal scenarios, including safety in Use scenarios
- Develop the safety requirements/ controls
- Identify/update the design requirements
- Design Changes (Safety by Design)
Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work
STPA for Safety in Use Analysis
Conclusion and Future Work

› We investigated the application of the STPA approach in identifying the safety in use requirements.

› We applied STPA to the Cruising Chauffeur© at Continental.

› We found that the STPA approach can address different kinds of the interaction between the automated driving system and others.

› We found also STPA is a useful approach for identifying more types of the detailed requirements, including safety in use.

› One challenge is that the STPA approach is not specific for any safety aspects (functional safety or system-level safety). Therefore, output of STPA includes different types of safety requirements.

› As a future work, we plan to improve our first proposed extension to STPA for safety in use to help the safety in use experts in addressing only the safety in use requirements.
Thank you for your attention!

With contribution from
Hagen Boehmert (Continental, Frankfurt)
Prof. Dr. Stefan Wagner (University of Stuttgart)
Safe and Dynamic Driving towards Vision Zero
Introduction to STAMP/STPA

Safety Analysis Approach

Systems Theoretic Process Analysis (STPA)

› Sees hazards as a control problem (based on STAMP = Systems-Theoretic Accident Model and Processes)

› Models process control cycles within the system

› Searches for inadequate control actions
  
  › Identifies causal factors and flaws leading to them

› Results in safety constraints for the system

STPA Process

Input

STPA Step 1: Identify unsafe control actions

STPA Step 2: Identify how each unsafe control action could occur

Define Analysis Scope

Develop Control Structure Diagram

Results

System-Leve Accidents, related hazards, design and safety constraints

Fundamentals

STPA Safety Analysis Report

(Causal Factors)

New/Refined Safety Constraints

Unsafe Control Actions

Corresponding Safety Constraints

Hierarchical Control Structure Diagram

[Abdulkaleq 2017]