International Journal of Safety Science
Vol. 02, No. 01, (2018), pp. 115 - 124
DOI: 10.24900/ijss/0201115124.2018.0301

Special Issue Article: The 5th European STAMP Workshop (ESW) 2017, Chief Editor: Svana Helen Bj örnsdottir, Reykjavik University

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

Asim Abdulkhaleq[1], Markus Baumeister[2], Hagen B öhmert[2], Stefan Wagner[1]
[1] *Institute of Software Technology, University of Stuttgart, Germany*
[2] *Continental, Frankfurt am Main, Germany*

Abstract

The next challenge of the automotive industry is marked by automated or even self-driving vehicles and shall enhance the safety, efficiency, and comfort of mobility. But to overcome this challenge, the systems within the vehicle need to take over tasks that were formerly under the responsibility of the driver. This leads to an increase of complexity of the automated driving systems. Especially, the interactions of an automated driving system with humans, other automated systems or other participants in the traffic. These interactions need to be well investigated. Under certain circumstances, interactions may lead to unforeseen situations in which the specified behavior of the function causes a hazard. Thus, the functional specification of the automated driving systems must avoid missing or incorrect interactions due to oversight. Analyzing the system specification for such overlooked interactions is still mostly a "creative" task using e.g. brainstorming. Hence, new analysing approaches may be required to identify safe system engineering solutions. One of the possible analysis approaches is STPA (System-Theoretic Process Analysis). In this paper, we investigated the application of STPA for the concept of safety-in-use, which aims to identify the hazardous interactions in the absence of system malfunctions. As a result, by using STPA we could address all kinds of interactions and generate different types of requirements, including the safety-in-use requirements. We conclude that STPA is a holistic approach which can be used for addressing different kinds of interactions and generating different types of safety requirements for automated driving systems.

Keywords: *STPA, Safety in Use, ISO 26262, Automated Driving, functional safety*

1. Introduction

Safety is a system problem that emerges from interactions among many components within the system and its environment [7,10]. Traditionally, safety was considered as a component failure problem. However, many accidents have occurred because of inadequate interactions among components without any individual component failures [1]. Different analysis approaches have been developed for analyzing the individual component failures. Fault Tree Analysis (FTA) [8] and Failure Modes, Effects and Criticality Analysis (FMECA) [9] have been used in the automotive industry for a long time in reliability engineering to identify component faults and failures to prevent accidents of systems. However, they are not well equipped to consider accident causes by different factors such as humans or the unsafe and unintended interactions among the system components [1, 10]. A few analysis approaches exist, which consider the system as a whole entity and take into account the complex relationships and interactions among its different components (e.g. human, hardware and software). One of these approaches is STPA (System-Theoretic Process Analysis) which was developed based on system and control theory rather than reliability theory. STPA treats safety as a control problem by analyzing the safety of a system with many components interacting together [1].

In the automotive domain, there are different factors which play an important role in the safety of road vehicles such as the driver's experience and skills, vehicle capabilities (active and passive safety systems), road environment and infrastructure (weather, road conditions, traffic density) and the behavior of the other participants in the resulting traffic situations. The negative influences of these factors and their interactions should be considered during the development of automated driving systems of new vehicles to ensure the safe operation of the vehicle on the road. However, the complexity of the automated driving systems makes the risk assessment process of these factors with traditional approaches more difficult. Traditionally, automotive systems are evaluated using a Hazard Analysis and Risk Assessment Process (HARA) [2] to check whether a driving function is causing risks in case it malfunctions. Nevertheless, this is still not sufficient to ensure the safety of the automated driving systems. Therefore, a holistic consideration is needed to evaluate all safety factors during the development process of the automated driving systems in the automotive domain to ensure operational safety [3]. An additional concept called "safety-in-use" is a key factor in the safety of automated vehicles, which has recently become an interesting topic in the automotive domain. This standard focuses on building the functional safety concept for individual E/E (Electrical/Electronic) components by covering hardware errors and errors during design, including software.

Problem Statement ISO 26262, the safety standard in the automotive domain, is intended for hazards which occur due to malfunctions of components but not for hazards occurring in the absence of malfunctions. These hazards are instead caused by insufficiently or incorrectly specified behavior in situations where interactions with the environment or other entities becomes relevant. Moreover, traditional hazard analysis approaches such Hazard and Risk Analysis (HARA) or Event Tree Analysis (ETA) are not adequate to address safety-in-use risks of the automated driving systems [6] because none of these approaches aims at systematically finding scenarios in which the specified function can have shortcomings. E.g. ETA analyses the probability that certain situations can lead to hazards but is not useful for a systematic exploration of all such situations.

Research Objectives The main research objective aims at evaluating the application of the STPA approach for safety-in-use to identify hazardous interactions of automated driving systems in the absence of malfunctions of the systems.

Contributions This paper explores the application of STPA for safety-in-use in a similar way as a HARA is used for risk identification and evaluation according to ISO 26262. It applies STPA to the existing architecture design of the automated driving system at Continental called Cruising Chauffeur® to identify the hazardous interactions between the automated driving and other participants in the road traffic. We also compared the obtained results by STPA with the results obtained by a safety expert who used the brainstorming method.

Context This work is conducted in the form of a cooperation of Continental, Frankfurt am Main, with the University of Stuttgart during the development process of the automated driving system called Cruising Chauffeur®.

Terminology

Functional safety is defined in ISO 26262 as ″absence of unreasonable risk due to hazards related to system malfunctions" [2].

Safety-in-use [4,5] is defined complementary to functional safety as absence of unreasonable risk due to hazards not caused by malfunctioning.

1. Background

1.1. STPA Hazard Analysis Approach

STPA (Systems-Theoretic Processes Analysis) [2] is a top-down hazard analysis approach built based on STAMP (Systems-Theoretic Accident Model and Processes) accident model, developed by Leveson in 2004. The main goal of developing STPA is identifying system hazards and safety-related constraints necessary to ensure a low level of the risk. The idea behind STPA is to develop a new analysis method that overcomes the limitations of the traditional hazard analysis techniques in terms of identifying design errors, flawed requirements, human factors implications, software failures and unsafe and unintended component interactions failures. STPA uses a feedback loop safety control structure diagram to identify the unsafe scenarios and develop the detailed safety constraints. STPA can be performed within three main steps: *1) Step 0: Fundamentals analysis; 2) identify the unsafe control actions, and 3) identify the causal factors and scenarios.*

1.2. Cruising Chauffeur®: Automated Driving System

Cruising Chauffeur® is an automated driving system (SAE level 4) which is expected to handle relevant traffic situations on its own with the driver returning to control only after a potentially long time. This project is currently under development at Continental, Frankfurt am Main for driving in the highway and freeway environment including the handling of the traffic jams and stop-and-go traffic. It aims at making the mobility and driving more comfortable and relaxing. Cruising Chauffeur® is able to take over from the driver and automatically drive the vehicle along the highway, adjusting its speed to traffic conditions and regulations. Figure 1 shows the functional architecture of the Cruising Chauffeur® which composes from three parts:

1) Sense which contains several sensors to sense the vehicle, other objects and the environment. It provides information data to the Plan component;
2) Plan evaluates the information which is received from the sense part and makes a decision; and
3) Act is responsible to execute the commands and actions of the Plan component.

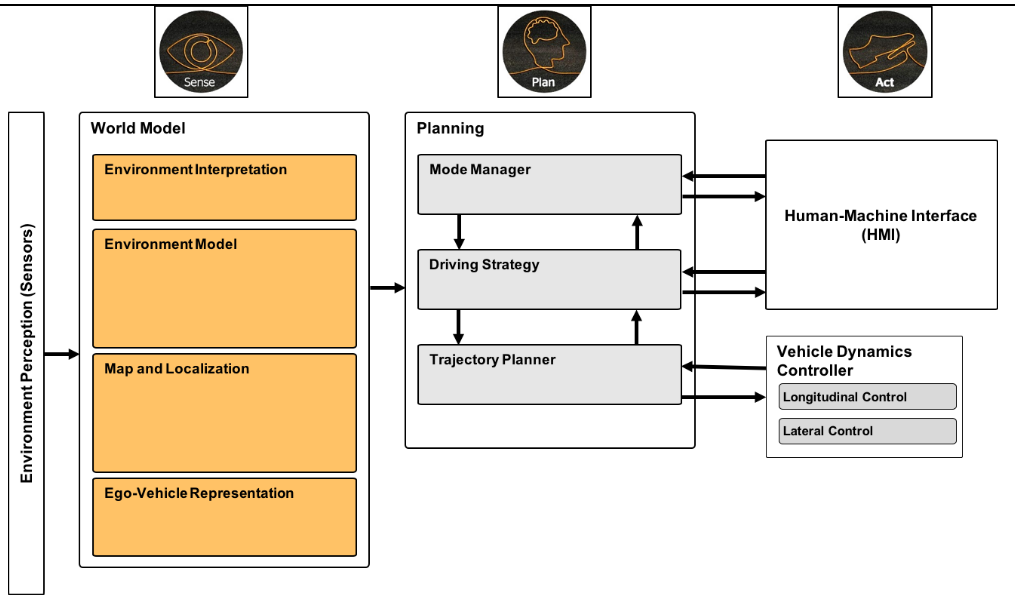


Figure 1. Layered Functional Architecture of Automated Driving Systems

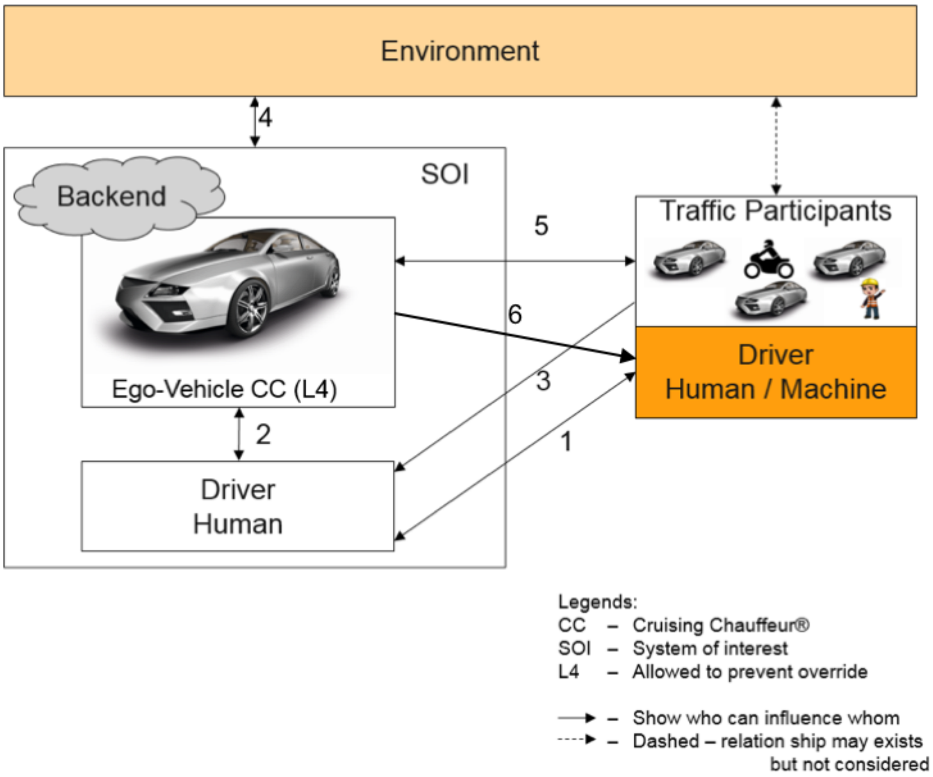


Figure 2. Types of Interactions Between the Cruising Chauffeur Automated Driving System and Others (Driver, Environment, Traffic Participants).

1.2.1. Types of Interactions in the Cruising Chauffeur®

Figure 2 shows different types of interactions between human and other traffic participants in the automated driving system. We classify the interactions between the different objects into the following possible types: 1) Driver Human-and-Driver Human Interaction (**HIH**), e.g. mutual waving signals at a deadlocked priority-to-the-right crossing; 2) Driver Human-and-Driver Machine Interaction (**HIM**), e.g. activation of automated driving mode by the driver; 3) Driver Human-and-other Traffic Participants Interaction (**HIP**), e.g. observation of unsteady bicyclist; 4) Automated Driving System-and-its Environment Interaction (**AIE**), e.g. usage of road-side communication infrastructure; 5) Automated Driving System-and-other Traffic Participants (**AIP**), e.g. mutual prediction of trajectories; and 6) the Automated Driving-and other Driver Humans (**AID**), e.g. using the indicator to signal upcoming lane changes.

As shown in Figure 2, we have three main players (driver human, traffic participants, and automated driving system). These players might interact together in the automated driving system. An inadequate interaction between one or more of these players during the operation time of the Cruising Chauffeur system might lead to an accident, which can result in injures, loss of human life or damaged property. For example, the automated driving system might be controlling the vehicle during a lane change but does not use its indicator before changing. This lack of interaction with the driver of a vehicle coming on from behind leads to a hazard. Thus, erroneous interaction with other traffic participants can lead to an accident. Therefore, the interactions between these main players should be assessed during the development process of the automated driving system to identify the potential unsafe interaction scenarios and develop the safety requirements. Please note that the interaction types 1 and 3 of figure 2 are out the scope of this paper.

1.3. Safety in Use (SiU)

Nowadays, different aspects of road safety in the automotive industry have been introduced. ISO 26262 functional safety is the most common safety aspect in the automotive domain, which focuses on addressing the E/E systems' failures and developing the appropriate safety concepts. However, the functional safety does not handle other factors which might lead or contribute to an accident such as human errors or unsafe and inadequate interactions between the participants shown in Figure 2. To overcome this shortcoming, a new safety aspect for the automotive systems called "*safety in use*" was introduced in the literature and other discussions [4-6]. "Safety in use" aims at addressing the hazards occurring in the absence of malfunctioning behaviors of a system. For example, *partially* automated systems still require driver oversight. However insufficient occupation of the driver and supervision of her or his awareness can lead to driver overconfidence or drowsiness. The resulting misuse of the system with insufficient oversight can then lead to potentially deadly accidents. Therefore, a holistic consideration of all safety factors is required in the risk assessment of the automotive systems to evaluate not only risky situations caused by technical error of the system, but also risky situations caused by other safety factors (e.g. unsafe interactions with other traffic participants, driver human machine interactions, etc.).

2. Related Work

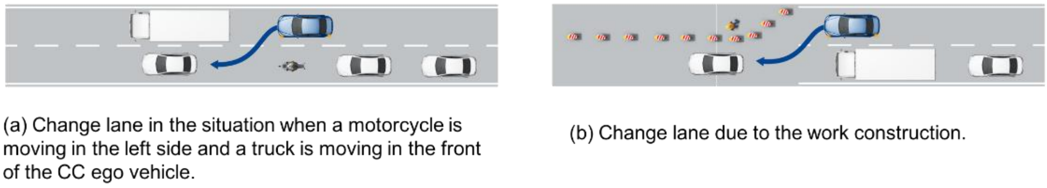
France (2017) [11] proposed a new extension to STPA for examining the role of humans in complex automated systems using STPA. The method called STPA-Engineering for Humans and provides guidance for eliciting causal scenarios related to interactions between humans and machines. The proposed method focuses only on identifying the unsafe interactions in the automotive between human and system (e.g. human interaction machine). The proposed method is evaluated within a cause study of an automated driving system called Automated Parking Assist (APA).

Husemann et al. (2017) [12] presented a holistic assessment of possible risks for analysis of safety in use. Their proposed method is based on using the event tree as a systematic analysis for the safety in use in which the traffic situations and its event chain are explored as an event tree rather than fault tree. However, the event tree analysis has a shortcoming to explore all hazardous situations of safety in use. The event tree analyses the probability that certain situations can lead to hazards but is not useful for safety in use.

Abdulkhaleq et al. (2017) [3] classified the safety of automated driving systems into three categories: Functional safety (FS), safety of intended functionality (SOIF) and the safety in use (SIU). In this preliminary work, we proposed a systematic method based on STPA for considering the operational safety of the automated driving. We defined the operational safety as a set of the dependability properties that are necessary to be addressed at early stage of development process of the fully automated driving systems with their required artefacts of safety, security, availability and reliability as well as maintainability. In this paper, we extended our work for analysis of safety in use.

3. Application of STPA for Safety in Use

The aim of this research is to explore the application of STPA for safety in use analysis for the automotive systems. Our work here is conducted within two main steps: 1) Apply STPA to the Cruising Chauffeur® system; and 2) evaluate the STPA safety requirements against the safety in use requirements obtained by a brainstorming approach. To limit the required effort of the STPA analysis, we only focused on applying STPA to the "Lane Change" functionality of Cruising Chauffeur®. "Lane Change" is a capability of the crusing chauffer system to move the ego-vehicle from one a lane to another on a highway with respect to the road and environmental conditions. Figure 3 shows examples of the "Lane Change" traffic situation.


(a) Change lane in the situation when a motorcycle is moving in the left side and a truck is moving in the front of the CC ego vehicle.

(b) Change lane due to the work construction.

Figure 3. Examples of Lane Change Traffic Situations of Cruising Chauffeur®

3.1. STPA Safety Analysis Results

First, we establish the fundamentals of the STPA safety analysis by identifying the system-level accidents, system-level hazards, and safety constraints. For example, the system-level accident AC1 is: *The ego vehicle cruising chauffeur collides with a vehicle during the lane change procedure and people dies/are harmed*. We also identified 12 system-level hazards. For example, the system-level hazard H-1 is: *The Cruising Chauffeur® system (CC) did not detect other traffic participants, which might be interfered by his lane change.* Next, we translated 12 system-level hazards into 12 the safety constraints. For example, *The CC must detect other traffic participants in the lane.* Then, we drew the safety-control structure diagram of the Cruising Chauffeur® system regarding to the "Lane Change" function as shown in Figure 4.

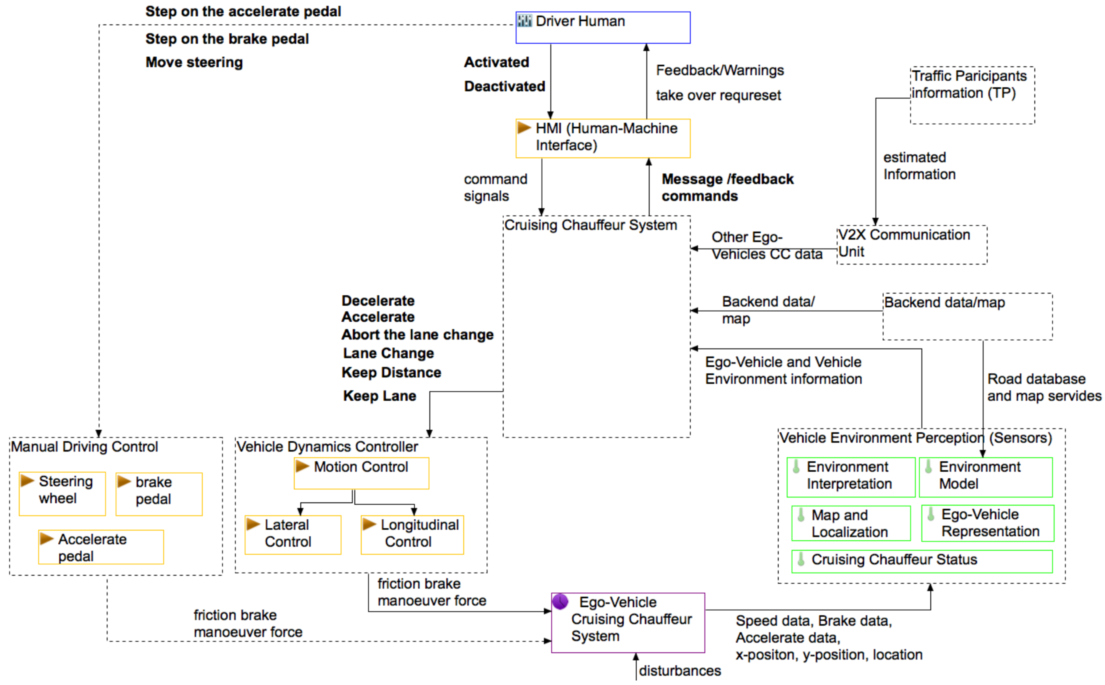

Step on the accelerate pedal
Step on the brake pedal
Move steering
Driver Human
Activated
Deactivated
Feedback/Warnings
take over requreset
Traffic Participants information (TP)
HMI (Human-Machine Interface)
estimated Information
command signals
Message /feedback commands
Cruising Chauffeur System
Other Ego-Vehicles CC data
V2X Communication Unit
Decelerate
Accelerate
Abort the lane change
Lane Change
Keep Distance
Keep Lane
Backend data/ map
Backend data/map
Ego-Vehicle and Vehicle Environment information
Road database and map servides
Manual Driving Control
Steering wheel
brake pedal
Accelerate pedal
Vehicle Dynamics Controller
Motion Control
Lateral Control
Longitudinal Control
Vehicle Environment Perception (Sensors)
Environment Interpretation
Environment Model
Map and Localization
Ego-Vehicle Representation
Cruising Chauffeur Status
friction brake manoeuver force
friction brake manoeuver force
Ego-Vehicle Cruising Chauffeur System
Speed data, Brake data, Accelerate data, x-positon, y-position, location
disturbances

Figure 4. The Safety Control Structure Diagram of the Cruising Chauffeur System ("Lane Change")

We identified 14 unsafe control actions for the lane change function. For example, the UCA1.1: *The CC system provided incorrect lane change request to the motion control to change lane while there is no gap in the target lane (related Hazards are [H-1, -2] [H-7,-8-9] [H-12], the type of interaction is AIP).* We translated each unsafe control action into a corresponding safety constraint. For each unsafe control action, we identified the causal factors. For example, a causal factor CF1.1.1 for the unsafe control actions UCA1.1 is **Process model incorrect-** *The CC incorrectly believes that there is enough gap to change lane in the target lane.*

3.2. Mapping STPA Requirements to Safety in Use Requirements

After performing the STPA safety analysis, we evaluated the resulting safety constraints against the requirements created in the SiU analysis of Cruising Chauffeur® to discover whether all requirements found by one analysis could be mapped to those found by the other. We also tried to determine a reason for any deviations we found.

Table 1. Excerpt of Requirements Found by SiUA and Respective Mappings

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

Overall six SiU requirements were analyzed[1] and for three of them a mapping towards STPA requirements could be found. Four of these SiU requirements are shown in Table 1, together with an attempted classification of the cause of the hazard they avoid.

Table 2. Excerpt of Requirements Found by STPA and Respective Mappings

ID	STPA Safety Requirement	Type	Mapping	Interaction
SR 0.5	The traffic markings must be in a good quality and visibly.	?	Special	AIE
SR 0.7	CC must not lose the detection of other traffic participants while CC changes lanes	FuSa & SiU	No mapping	AIP
SR 0.8	CC must not steer the ego vehicle in the wrong direction.	FuSa	N/A	AIE
SR 0.10	CC must estimate the lane velocity correctly.	FuRe & FuSa	N/A	AIP
SR 1.1	The CC must not send a lane change request to the motion control while it is not allowed due to the traffic road conditions.	SiU	(SIUR-45)	AIE/AIP
SR 1.6	CC must abort a lane change due to unexpected changes in the prerequisites of the lane change function.	SiU	(SIUR-16)	AIE
SR 2.2	If backend or V2X are unavailable, CC shall warn the driver and hand over control to him.	FuSa	N/A	HIM
SR 2.6	CC must not allow its activation by the driver when the ego vehicle is approaching non-highway roads.	SiU	Exists but outside Lane Change topic	HIM

Overall 41 STPA safety requirements were found on different analysis levels. Many of these are related to the basic driving task such as SR0.8 and SR0.10 in Table 2 above and/or belong into the domain of functional safety or can even be mapped to existing requirements in the functional requirements specification (and are thus excluded as SiU requirements).

Some entries in Table 2 need further explanation. SR0.5 is difficult to classify as it is a requirement towards the environment. Nevertheless, it leads to the discovery of a new SiU requirement during its discussion: "*The vehicle shall not conduct a lane change if the crossed lane marking is (temporarily) not detected. This shall avoid crossing a solid line.".* Also, SR0.7 can be seen as SIU requirement of the "Violation of known requirement by seldom situation" type if sensors involved in object detection can be disturbed by lateral or yaw movements occurring during lane changes.

3.3. Discussion

As can be seen in the above tables each approach detected SiU requirements the other did not. There seems to be no clear relationship between the requirements found by an approach and the interactions or hazard causes involved in them. Nevertheless, we see the following differences:

- **Quantity**: STPA created requirements also outside the domain of SiU in the form of functional safety requirements and "normal" functional requirements. This is a mixed blessing: On the one hand, it increases the effort of requirement creation over an approach focusing on SiU, on the other hand it increases the value of STPA as exploratory tool at the beginning of development.

[1] The SiU analysis generated further requirements but those do not belong primarily to the „Lane Change" feature used to limit the size of the study.

- **Abstractness**: Many STPA requirements describing SiU issues are relatively abstract with respect to the involved hazard. Compare for example SR1.1 & SR1.6 vs. SIUR-45 & SIUR-16 from Table 2 and Table 1 respectively. This abstractness runs the risk that function developers do not see the hazardous situation and implement a solution which will not work in the respective special case.

- **Level of analysis**: On detailed analysis level (i.e. causal factor analysis), the discovered STPA 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 shown in Figure 3, the SiUA typically has analyzed a different scenario for each resulting requirement. The situations analyzed for the requirements of Table 1 are shown below in Figure 5 from a) to d). Due to this, "completeness" of the SiUA depends to a large extend on the completeness of the situation brain-storming. It thus appears that also STPA could profit from identifying and analyzing more traffic situations if the traffic situations analysis takes part at the beginning of the STPA process (as shown in Figure 6) or in the course of the causal factors analysis (STPA Step 2).

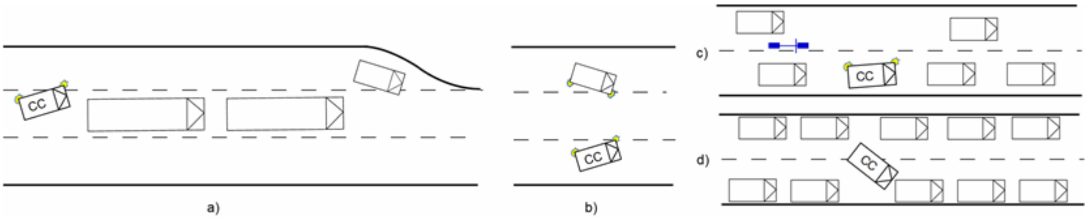


Figure 5: Traffic Situations belonging to SIUR-16, -33, -38, -45

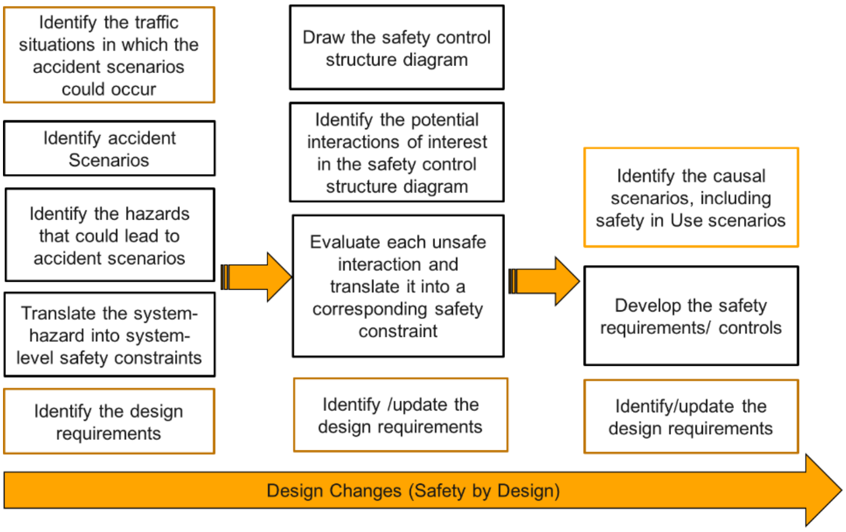

Identify the traffic situations in which the accident scenarios could occur
Identify accident Scenarios
Identify the hazards that could lead to accident scenarios
Translate the system-hazard into system-level safety constraints
Identify the design requirements
Draw the safety control structure diagram
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)

Figure 6. The Safety-in Use Approach based on STPA

4. Conclusion and Future Work

In this paper, we investigated the application of the STPA approach in identifying safety in use requirements. We applied the STPA approach to the Cruising Chauffeur® automated driving system at Continental. Our work showed that STPA can address all kinds of the interactions between the automated driving system and others (e.g. traffic participants, environments, human driver). We also found that STPA is a useful approach for identifying more types of detailed requirements in addition to the safety in use requirements. One challenge is that the STPA approach is not specific for any safety aspect (functional safety or system-level safety); therefore, the output of STPA includes different types of requirements which requires user expertise, effort and time to determine their relationship to safety-in-use. As future work, we plan to develop a specific approach for the safety in use analysis based on STPA to help the safety-in-use analysis experts in addressing only the safety-in-use requirements when they apply STPA to their systems.

References

[1] N. G. Leveson, "Engineering a Safer World", MIT Press, **(2011)**.

[2] ISO, "ISO 26262 International Standard, Road Vehicles- Functional Safety", Part 1- **(2011).**

[3] A. Abdulkhaleq, D. Lammering, S. Wagner, J, Röder, N. Balbierer, L. Ramsauer, T. Raste, H. Böhmert, "A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles", Procedia Engineering., vol. 179, (**2017)**, pp. 41-51.

[4] T. Weigl, Development Process for Autonomous Vehicles, Master thesis, TUM, **(2014).**

[5] K. Richard, "Gebrauchssicherheit vs. Funktionale Sicherheit bei BMW", Hanser, **(2012).**

[6] H. Ross, "Functional Safety for Road Vehicles: New Challenges and Solutions for E-mobility and Automated Driving", Springer, (2017).

[7] N. G. Leveson, "SafeWare: System Safety and Computers". Addison-Wesely.xvii, 680p (1995).

[8] W. Vesely, F.F. Goldberg, N.H. Roberts, D.F. Haasl, Fault Tree Handbook NUREG-0492, U.S. Nuclear Regulatory Agency, Washington, 1981.

[9] Society for Automotive Engineers, Design Analysis Procedure for Failure Modes, Effects and Criticality Analysis (FMECA), ARP926, Warrendale, USA, 1967

[10] R. Martínez, "System Theoretic Process Analysis of Electric Power Steering for Automotive Applications", Master thesis, MIT **(2015).**

[11] M. E. France, "Engineering for Humans: A new Extension to STPA", Master Thesis, MIT, (**2017**)

[12] A. Huesmann, M. Farid, E. Muhrer: From Controllability to Safety in Use: Safety Assessment of Driver Assistance Systems, Automated Driving pp. 495-518, Springer International Publishing, (2017)

Dr. Asim Abdulkhaleq is a postdoctoral research assistant at the software engineering group in the Software Technology institute at University of Stuttgart. Mr. Abdulkhaleq received his Ph.D. in the field of System-Theoretic Safety Engineering for Software-Intensive Systems in 2017. His interest includes safety engineering, system-Theoretic Dependability Engineering for Autonomous Vehicles, and Safety-based Testing. He collaborated with different automotive companies in the field of the safety engineering of the automotive systems.

Dr. Markus Baumeister is an employee of Continental Teves AG & Co. oHG, Frankfurt. He received his Ph.D. in the field of Database Models for Chemical Process System Engineering from the RWTH Aachen in 2000. He is working in the area of Functional Safety for automotive microcontrollers as well as driver assistance systems since 2007 and extended this to the area of Safety in Use in 2015.

Hagen Böhmert is an employee of Continental Teves AG & Co. oHG, Frankfurt. He received his diploma in Electrical Engineering and Information Technology from the University of Applied Sciences and Arts in Hanover in 2007 before working within the automotive industry (focus on verification and validation) in Michigan, USA. After his return in 2010 he was employed as safety engineer for series development of chassis components before switching to Continental in 2013 as functional safety manager for automated driving.

Prof. Dr. Stefan Wagner is a full professor of software engineering at the Institute of Software Engineering of the University of Stuttgart, Germany. He studied computer science in Augsburg and Edinburgh, and he received a PhD in computer science from the Technical University Munich. His research interests include requirements engineering, software quality, safety & security, agile software development and empirical and behavioural software engineering. He is a member of ACM, IEEE Computer Society and the German GI.