Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-11 (2016) 576–581

On Functional Safety of Vehicle Actuation Systems in the Context of Automated Driving

Torben Stolte * **René S. Hosse** ** **Uwe Becker** ** **Markus Maurer** *

* *Technische Universität Braunschweig, Institute of Control Engineering, Braunschweig, Germany (e-mail: [stolte,maurer]@ifr.ing.tu-bs.de).*
** *Technische Universität Braunschweig, Institute for Traffic Safety and Automation Engineering, Braunschweig, Germany (e-mail: [r.hosse,u.becker]@tu-braunschweig.de)*

Abstract: One of the most important trends in the automotive domain is the increasing automation of driving functionalities. Demonstrated functionality of all contributors in this field is steadily increasing. The development moves towards systems where the driver's tasks are executed more and more by electronic systems. With increasing automation, the driver vanishes as central safety element. Thus, the driver's contribution to overall vehicle safety must be implemented in electronic systems. In this contribution, the impact of vehicle actuation systems on functional safety of automated vehicles is examined. By understanding automated driving as a control problem, a systems theory based analysis systematically reveals generic malfunctional behavior related to steering, brakes, and drives. Furthermore, different aspects which must be considered for designing functionally safe actuation systems are presented.

Keywords: Functional Safety, Automated Driving, Vehicle Actuation, Systems Engineering, Systems-Theoretic Accident Model and Processes, STAMP

1. INTRODUCTION

Recently, a major trend in the automotive industry is the increasing automation of the vehicle guidance. In the long term, industry aims at full automation of vehicle guidance in the sense of the SAE definition (SAE, 2014). Driverless operation of vehicles imposes high demands on functional safety throughout the vehicles' product life cycle. Conventionally, the driver serves as fallback strategy in a safety concept. He or she has to compensate for, or at least to mitigate, malfunctional behavior of vehicles operated up to SAE level 2 utilizing the mechanical or hydraulic link between driver inputs and wheels. This fallback layer vanishes for vehicles operating at SAE levels 4 and 5. The same applies to SAE level 3, with the constraint that the driver has to take over control after a defined period of time (Reschka and Maurer, 2015). Consequently, these systems induce new hazards and must implement countermeasures to compensate for absence of the driver.

Hazards and malfunctional behavior are understood according to the definition of the ISO 26262 standard [1]. Malfunctional behavior comprises failures as well as unintended behavior of systems. Hazards are the outcome of a system's malfunctional behavior and potentially lead to harm of traffic participants. For causing harm, a hazard must be considered in a specific operational situation, together yielding a hazardous event.

[1] See definitions of *hazard*, *harm*, *malfunctional behavior*, and related terms in the ISO 26262 standard (ISO, 2011, Part 1).

Concentrating on vehicle actuation systems deployed in automated vehicles operated at SAE levels 3-5, the aim of this contribution is to generically identify malfunctional behavior associated with these systems. This is required as very early input for top-down design approaches as for instance proposed in the ISO 26262 standard. The focus of this contribution is on malfunctional behavior only. Operational situations are not considered as these strongly depend on the actual automated driving functionality. By identifying malfunctional behavior systematically, aspects to be taken into account when designing functionally safe actuation systems shall be derived as well.

2. ANALYZING VEHICLE ACTUATION SYSTEMS

In order to identify malfunctional behavior related to the actuation system a systems theory based approach is selected as reasoned in section 2.1. Then, the actual analysis consisting of two steps is presented. In section 2.2, the first step, a functional control structure of an exemplary actuation system is developed. In section 2.3, the second step, this control structure is utilized for a detailed investigation of malfunctional behavior of vehicle actuation systems.

2.1 Systems Theory based Hazard Analysis

For designing functionally safe systems in the automotive domain, the international ISO 26262 standard is the most

10.1016/j.ifacol.2016.08.084

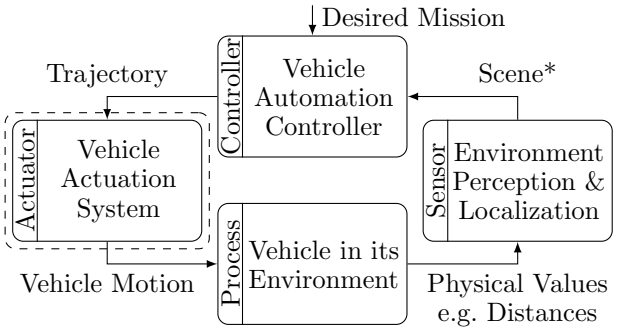

Fig. 1. Automated Driving as Control Problem (Dashed: Focus of this contribution); *According to the Definition of Ulbrich et al. (2015)

recent standard available. It generically describes a holistic safety life cycle of electronic vehicle systems (ISO, 2011). Thereby, it focuses on the system development which starts with the concept phase. During the concept phase, the standard requires a hazard analysis and risk assessment, yielding a classification of the system's criticality. This classification strongly influences efforts which need to be conducted during the subsequent phases system development, production, service, and decommissioning. For hazard analyses, the ISO 26262 standard requires that "hazards shall be determined systematically by using adequate techniques" (ISO, 2011, Part 3, 7.4.2.2.1). This challenges the automotive safety community. It is not yet clear what hazard analysis method does fit best to identify hazards adequately, especially in the case of automated driving. One challenge during hazard analysis is to determine a sufficient list of potential malfunctional behavior as root of system hazards. For this, different techniques can be used. The ISO 26262 standard itself suggests some techniques such as brainstorming or failure modes and effects analysis (FMEA) (ISO, 2011, Part 3, 7.4.2.2.1).

The limitation of traditional methods – like FMEA – is seen in the chain-of-events causality that links single events to accidents (Leveson, 2011). It assumes that systems can be safely operated when preventing the chain-of-events that leads to an accident. However, this perspective requires a method which is capable of capturing every possible event that leads to an accident. Leveson (2011) shows that traditional methods cannot meet this requirement. Concerning automotive applications, this is supported by the work of Van Eikema Hommes (2012). According to her review of the ISO 26262 standard, especially interactions between system components and system failures (there: a system causes an accident although safety-related requirements are met) can hardly be identified. Furthermore, methods like FMEA or HAZOP (hazard and operability study) are highly dependent on expert's experience with the method itself. Less experienced analysts will create varying findings. This stems from the fact that these methods use brainstorming procedures and provide little understanding of how a system should be analyzed in a structured manner.

A promising approach to overcome these issues is systems theory where safety is seen as a control problem. One methodology in this field is the *System-Theoretic Accident Model and Processes* (STAMP) developed by Leveson (2011). By modeling and analyzing a system's control structure, the objective of STAMP is to identify adequate safety constraints and to formulate safety requirements (Leveson, 2011). In contrast to traditional methods, the safety control structure utilized by STAMP creates a structured top-down procedure of how safety-relevant functions of a system should be analyzed. A recent review of safety analysis methods for software intensive systems as encountered in the context of automated driving found that STAMP – in contrast to FMEA, FTA, and HAZOP – was the only method which was capable of identifying real world accidents out of the system design (Teikari, 2014).

STAMP provides specified methods for selected safety engineering problems. In this contribution, the System-Theoretic Process Analysis (STPA) is applied which was recently used in the context of automated driving (Raste, 2015). Raste sees its application at early design stages including the hazard analysis, summed up as concept phase in terms of the ISO 26262 standard. For that, STPA requires a qualitative model which represents the control structure of a system of interest. Within these control structures, controllers, control actions, processes, as well as feedbacks are represented in a hierarchical manner.

2.2 Control Structures of Vehicle Actuation Systems

Fig. 1 illustrates the functionality of automated vehicles as control problem (Zapp, 1988). All parts of the control loop are required to enable the functionality of automated vehicle guidance. Likewise, all parts contribute to the challenge of ensuring functional safety of automated vehicles. Vehicle actuation systems are subordinate control systems of the control system depicted in.

Defining the control input of vehicle actuation systems is subject of recent research at the Institute of Control Engineering at Technische Universität Braunschweig. So far, common understanding is that a trajectory – describing the desired longitudinal and lateral vehicle motion – is a suitable interface. Hence, the overall functionality of vehicle actuation systems is understood as trajectory follow control. For realizing this control task, control algorithms access all available actuators, namely steering, brakes and drives. Negating the overall functionality yields the hazard evoked by vehicle actuation systems: The vehicle is not able to follow its intended trajectory. This hazard is potentially caused by various malfunctional behavior to be identified in the following. Simultaneously, impacts of malfunctional behavior on vehicle dynamics differ as well.

Control structures of vehicle actuation systems strongly depend on actuator topologies and technical implementations as each actuator requires its own controller. Recent research projects in the context of automated driving such as the Stadtpilot project of Technische Universität Braunschweig (Wille et al., 2010) or the Bertha Drive of Karlsruhe Institute of Technology and Daimler AG (Ziegler et al., 2014) are based on series production vehicles featuring front axle steering, one driven axle (front or rear) and four wheel brake. Yet, future vehicles might feature a more modular actuator topology as for instance demonstrated by Audi's e-tron quattro concept (Audi AG, 2015), which is equipped with three electric drives aiming for extended capabilities regarding longitudinal as well as lateral