Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 179 (2017) 61 – 71

Procedia Engineering

www.elsevier.com/locate/procedia

4th European STAMP Workshop 2016

Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle

Gerrit Bagschik[a*], Torben Stolte[a], Markus Maurer[a]

[a]*Technische Universität Braunschweig, Institute of Control Engineering, Braunschweig, 38106, Germany*

Abstract

The project "Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works" (aFAS) aims at developing an unmanned protective vehicle to reduce the risk of injuries due to crashes for road workers on German highways. The application of the unmanned protective vehicle has a limited or reduced number of operational situations compared to other use cases and shall show the development and validation of a highly automated vehicle system. To ensure functional safety during operation in public traffic, the system is developed following the ISO 26262 standard. After defining the functional range in the item definition, a hazard analysis and risk assessment has to be conducted. The ISO 26262 standard gives hints on how to process this step and demands a systematic way to identify system hazards. Best practice standards provide systematic ways for hazard analysis, but lack applicability for automated vehicles due to high variety and number of different driving situations, which have to be controlled by the automation system, even with a reduced functional range as met in the project aFAS. Human machine-interaction is changing towards less interaction but more important influence, as the driver must select the right operating mode and depending on the level of automation act as a fallback layer. This contribution applies a new method based on systems theory, System-Theoretic Process Analysis (STPA), to the unmanned protective vehicle concept. A crucial topic of this process is to generate a proper control structure for the system and investigate it regarding all (representative) operational situations. We will show our experiences with STPA for the unmanned protective vehicle and summarize questions to the application on automated vehicles.

Peer-review under responsibility of the scientific committee of the 4th European STAMP Workshop 2016

Keywords: Automated driving; hazard analysis and risk assessment; ISO 26262; scenario generation; STPA;

* Corresponding author. Tel.: +49 531 391-3828.
E-mail address: bagschik@ifr.ing.tu-bs.de

Peer-review under responsibility of the scientific committee of the 4th European STAMP Workshop 2016
doi:10.1016/j.proeng.2017.03.096

1. Introduction

The project Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works (aFAS - German abbreviation for Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Autobahnen) aims at developing an unmanned protective vehicle (AFA - German abbreviation for Automatisch fahrerlos fahrendes Absicherungsfahrzeug) to reduce the risk of injuries by crashes for road workers. The unmanned protective vehicle follows a leading vehicle in a defined distance on the hard shoulder of a highway without a safety driver. On- and off-ramps are passed virtually coupled in very close distance to the leading vehicle. In these reduced operating scenarios, compared to other highly automated systems, the AFA shall operate without external supervision by a human. A detailed outline of the project aFAS and the main objectives are described in [1].

Despite the operation on a hard shoulder of a highway, this project aims at showing the first operation of an unmanned vehicle in public traffic on German roads. This safety related system shall be developed applying the ISO 26262 standard [2] for ensuring functional safety. During the concept phase the standard requires to process three steps. After defining the systems functional range and operating scenarios including system boundaries in the item definition, a hazard analysis and risk assessment has to be conducted. The ISO 26262 standard requires that all hazards shall be determined “systematically by using adequate techniques” [2, Pt. 2] and assessed afterwards.

The resulting safety concept, based on the analysis with a certain accident model, will mitigate or avoid hazards by suppressing or eliminating identified causes. Thus, the effectiveness of a safety concept is influenced by the chosen accident model. Transferred to automated and/or unmanned vehicles, we want to identify all possible hazardous states of the system, which includes functional failures but also intended behavior of the vehicle. A system can have unsafe definitions in its description, which has to be revised in a safety analysis besides functional failures. In the ISO 26262 standard, the intended behavior and the operational environment have to be defined in the item definition.

When analyzing possible accidents and causing hazards, the results may vary with the underlying accident model approaches. According to Qureshi, accident models based on event chains or epidemical models (e.g. Hazard and Operability Analysis (HAZOP), Failure Mode and Effects Analysis (FMEA) or Event Tree Analysis (ETA)) are not sufficient to identify risks resulting from complex socio-technical systems [3]. Lundberg et al. discuss the effectiveness of different accident analysis models in relation to the principles investigated by the processes [4]. An important aspect is that accident models follow a certain *What-You-Look-For-Is-What-You-Find* principle. That means, they provide interests on selected mechanisms and for these mechanisms find different causalities.

Systems theoretic approaches extend the component based view to model interactions among systems and provide methods to understand relationships between functional system parts. A main difference in these approaches is, that accidents are not only understood as caused by single or multiple failures of components, but also as inappropriate system performance including technical parts, human interactions, requirements and management processes.

Rasmussen describes a hierarchical model of socio-technical systems with different system-levels as interacting control loops [5]. Starting from government on the top level over regulators, companies, management to staff and the operative work on lowest level, this model emphasizes the necessary interactions between different disciplines of research. In 2004, Leveson introduced an accident model called Systems-Theoretic Accident Model and Processes (STAMP) [6]. The STAMP model describes accidents not only by individual component failures but includes design and nominal performance flaws. Modeled systems are described as control systems and thus safety can be expressed and managed by control structures in socio-technical systems. In this case socio-technical systems include hard- and software, human and organizational factors. Leveson proposed the Systems-Theoretic Process Analysis (STPA) as a method to analyze systems based on the STAMP accident model [7].

This contribution aims at applying STPA for vehicle guidance systems and at evaluating whether the process is applicable in the development of an unmanned protective vehicle. Therefore, STPA should contribute to the hazard analysis and risk assessment and parts of the development of a functional safety concept of the ISO 26262 process. Section II describes STAMP- and STPA-related work, followed by challenging topics regarding application of STPA in the field of automated vehicles. Section III shows selected parts of our analysis and section IV concludes our experiences.