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.

2. Related Work

STPA has been applied to various systems for example trains, space stations, shuttles and (nuclear) power plants. As this contribution focuses on vehicle automation and operation of unmanned vehicles, the related work is limited to this field of research.

To the knowledge of the authors, van Eikema Hommes is the first publishing researcher, who applied STPA to an automotive adaptive cruise control (ACC) [8]. System descriptions including functional and safety requirements for ACC systems are available in the international standards ISO 22179 and SAE J 2399. *Injury to vehicle occupants while the ACC is engaged* was defined as the system loss (accident). The identified or chosen hazards were a) not to maintain a safe distance and b) to decelerate the vehicle too abruptly, which would not be controllable by the following traffic. It is not clearly stated, how the accidents and hazards were determined. The paper shows examples for STPA process steps based on the control loop between the main-component and the brake control component. Resulting design requirements cover cross system aspects as well as requirements for interaction with the operator in the vehicle (mainly the driver). In comparison to ISO 22179 and SAE J 2399, the resulting number of requirements is increased and the requirements could be translated into design measures. Yet, van Eikema Hommes points out, that a comparison against standards based on pure numbers is not valid because standards represent only a least set of requirements for specific systems. Yet, the generated requirements cover all requirements demanded by the standards. STPA identified further demands regarding driver control authority versus computer authority, advanced topics in sensors, actuators, communication buses and maintenance requirements. Again it has to be stated that standards contain only a minimum consent of multiple car manufacturers for a specific system and further requirements are implemented in series products but not explicitly published.

Abdulkhaleq et al. also apply the STPA process to an ACC system and shows selected steps in greater detail including examples for process models in certain controllers of the system [9]. As an advantage of STPA over aforementioned traditional analysis methods, the results show potential improvements like a greater scanning angle of the radar sensor and a backward sensor to verify braking maneuvers. As ACC is, according to SAE levels of driving automation [10], a level 1 system (driver assistance), the driver has to monitor the driving environment and is a permanent supervisor for the automation task.

The process model of the driver could be extended by an environment model and kind of a supervision task in terms of assisted driving. Abdulkhaleq et al. also identify difficulties in determining control structures and unsafe control actions, as STPA does not provide systematical guidelines on this crucial topic. Another less covered aspect of STPA is, that multiple controllers can provide contradictory command values, which can lead to hazardous states of the system. It seems to be unclear how the proposed analysis methods can analyze or resolve such issues.

In further investigations, Abdulkhaleq et al. [11] use an extended STPA process introduced by Thomas [12] and proposes a comprehensive safety engineering approach for software intense systems. In this process, a functional model of the system and identified safety constraints are transformed to linear temporal logic and/or computation tree logic, which both can be verified using model checkers. These model checkers can generate counter examples for formulated safety statements and thus show, if unsafe system states exist, at least in software and simulated scenarios.

Sulaman et al. apply the STPA process to an automotive forward collision avoidance system, which slightly differs from the original proposal of the process [13]. The forward collision system senses the space in front of the vehicle and warns the driver in case of a possible collision with obstacles. If the driver does not react to the warning the system applies an automated brake maneuver to mitigate the effects of a resulting collision. Sulaman et al. start the analysis with identifying unsafe control actions in a control structure. After this they derive related hazards if an unsafe control action occurs. This process differs from the STPA process described in [14] according to the order of analysis steps, where the accidents and hazards are identified before the control structure. The hazards were then rated from negligible to catastrophic severity levels. Determining a wrong brake pressure or reaction time due to unsafe vehicle status signals and object status signals was shown as an example for catastrophic hazards. Leveson defines a hazard as “a system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).” [7, Ch. 7.2]. Sulaman et al. do not distinguish different operational scenarios for resulting hazards.

For example, determining an unnecessary brake pressure at low speeds in an environment without other traffic participants should not be rated as catastrophic.

So far, STPA has been applied to ACC and forward collision avoidance systems. The results show some improvements regarding socio-technical interaction in automotive systems. However, these systems are categorized as driver assistance (level 1) according to SAE levels of driving automation for on-road vehicles [10]. Level-1-systems must be permanently observed and supervised by a human operator (driver). System with higher degree of automation like the AFA (level 4, high automation [1]) are not supervised during the designed task and thus have less safety-critical human interaction during automated operation. The human machine interaction still is a very important topic to investigate, as the AFA does not cover all scenarios on the hard shoulder automatically and thus has to be transited to the appropriate operating mode. A detailed hazard analysis on a functional view (without a system realization) in several environment conditions and more complex automation levels has not been investigated so far.

Another important topic for the development of automated vehicles is compliance of the STPA process to the concept phase of the ISO 26262 standard. When STPA is used to develop a safety concept, the requirements of the work products from the ISO 26262 standard must be fulfilled.

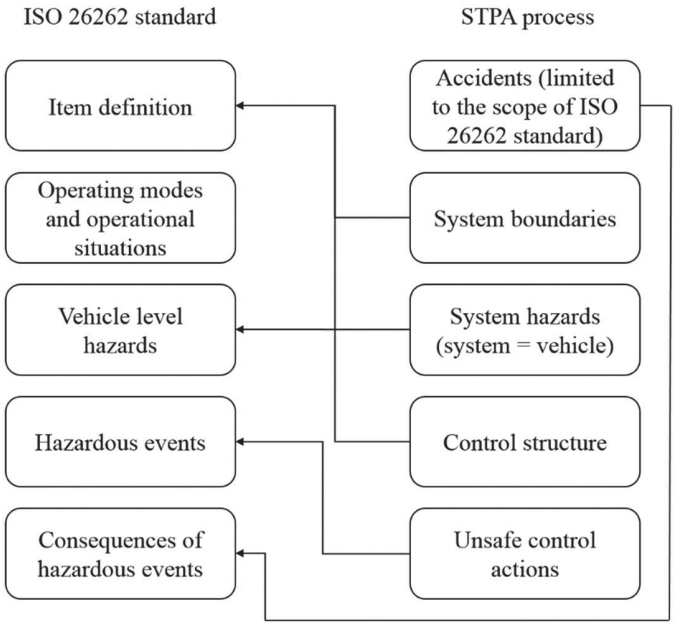

Figure 1: Mapping of STPA process and concept phase of ISO 26262 standard adopted from [15]

Mallya [15] shows the usage of STPA in an ISO 26262 standard compliant process. Fig. 1 shows an adapted mapping of both processes before the ASIL determination is conducted (which is out of scope in this contribution). An important aspect is that Mallya suggests to extend the STPA process with a generation of hazardous events by combining hazards and operational scenarios which consist of unsafe control actions, causal factors explicit worst environmental conditions under which hazards lead to an accident. This extension results from ISO 26262 concept phase, where the first part of the hazard analysis and risk assessment is divided into *situation analysis* and *hazard identification.*

Thomas extends the STPA process, by including a self-defined system state into the process and proposes a systematical way to identify unsafe control actions [12]. The following description shows an example provided by Thomas of contextual information for a control action of an automatic train-door system:

“Operator provides open train door command when train is moving.”

The *operator* is the source of the control action, *provides* describes the type, *open train door command* is a control action and *when train is moving* is the context in which the control action shall be investigated. In the proposed extension, every process variable of the system is combined with all other variables and their states.

Tab. 1 is an exemplary table with process variables *object in front* and *driving state* and the control action *stop vehicle*. The control action, which stops the vehicle, is only unsafe when it is not provided, if an object is in front of the car. The context involves further information about other controllers and their process variables for more complex systems.

Table 1: Extension of STPA process with system context

Control action	Object in front	Driving state	Not providing causes hazard
Stop vehicle	Yes	Driving	Yes
Stop vehicle	No	Driving	No
Stop vehicle	Yes	Stopped	No
Stop vehicle	No	Stopped	No

Thomas further defines a two-step analysis for the systematically generated contexts. At first, all contexts and control actions are analyzed by following categories:

- Providing control action at any time in contexts causes hazard
- Providing control action too early in contexts causes hazard
- Providing control action too late in contexts causes hazard

In the second step the control action is assessed towards, whether not providing a control action is hazardous in the context.

For automated vehicles, a description of the system context is very challenging due to the high number of context variables (e.g. domain, road network, signals and signs, traffic participants and weather) and the even larger amount of entities of these variables and the possible combinations. To overcome this topic in a hazard analysis processes, we proposed a systematic way, to generate potential hazardous events (which were afterwards filtered to only hazardous events) for the unnamed protective vehicle [16]. These events contain a high level abstracted description of the environment, the current operating mode and a functional error of the system. We will further investigate, how these events can be integrated in the STPA process.

To extend the application of STPA towards automated vehicles, we want to contribute our experiences with STPA applied to the unmanned protective vehicle. The application will show the STPA process in the context of level 4 automation.

3. Application of STPA

This section describes the application of STPA in the ISO 26262 standard concept phase. A description of the individual steps can be taken from the STPA Primer [7]. The STPA Primer [14] provides a more detailed description and examples for the application.

3.1 Establishing fundamentals

By applying the ISO 26262 standard in the project aFAS, a functional system description is available in terms of the item definition [2, Part 3]. The item definition in the project contains functional behavior, an adapted preliminary functional system architecture based on Matthaei and Maurer [17], a description of operational environments and

functional system boundaries, beyond which the unmanned protective vehicle is not purposed to operate (safely). Accidents caused by the AFA were identified as following:

- A-1 AFA collides with moving traffic during unmanned operation.
- A-2 AFA collides with leading vehicle.
- A-3 AFA collides with solid obstacle on hard shoulder.
- A-4 AFA collides with vulnerable obstacle on hard shoulder.
- A-5 AFA collides with embankment.
- A-6 AFA collides with moving traffic during manual operation.

A more general formulation like *AFA collides with an obstacle* was not chosen, because the hazardous events and accidents will be assessed using the automotive safety integrity level (ASIL) afterwards [2, Pt. 2]. This metric includes severity of a potential accident, exposure to the driving scenario and controllability of the scenario by affected persons as parameters. To be able to determine these values later in the process, we divided the accidents in the categories above.

Related hazards were divided into two categories as demanded by the ISO 26262 standard: hazards caused by normal operation and hazards caused by operation outside of functional system boundaries. The operation beyond functional system boundaries addresses system states caused by confusion in control authority between computer and operator or the AFA "is incorrectly used in a foreseeable way", as demanded to be analyzed by the ISO 26262 standard [2, Pt. 3]. Identification of these failures regarding control authority between humans and technical systems is stated as an advantage of the STPA method [8]. This aspect is important for this analysis, because the AFA cannot detect all its system boundaries itself and relies on the operator to change the operating mode according to the current scenario.

For the formulation of hazards Leveson states that hazards shall not contain *failure* or *error*, as those statements only provide little information about the hazardous system state [14]. We identified the following hazards which can lead to the aforementioned accidents:

- H-1 AFA leaves hard shoulder to the left / right.
- H-2 AFA drives to close to leading vehicle.
- H-3 AFA does not react to a path-blocking object.
- H-4 AFA performs unintended braking / steering / acceleration.
- H-5 AFA performs safe halt on on- / off-ramp.
- H-6 AFA operates in follow mode on on- / off-ramps.
- H-7 AFA operates unmanned at forbidden weather conditions.
- H-8 AFA operates unmanned on too narrow hard shoulder.

Unintended acceleration, braking or steering was only assessed during manual operation, where the AFA is driven by a roadworker. In automated states, unintended actuator functions are causes for several hazards and thus shall be identified by further steps in STPA. It is important to distinguish between hazards including human-machine-interaction and pure system operation. System boundary related hazards are covered by H-6, H-7 and H-8. The system boundaries are taken from the item definition.

Tab. 2 shows linking of accidents and hazards from the eXtensible STAMP platform (XSTAMPP), which was used as tool support [18].

Accident	Hazards
Collision with traffic (A-1)	H-1, H-5, H-6, H-7, H-8
Collision with leading vehicle (A-2)	H-2, H-3, H-6, H-7
Collision with (vulnerable) obstacle (A-3, A-4)	H-3, H-6, H-7

Collision with embankment (A-5)	H-1, H-5, H-6, H-7, H-8
Collision during manual operation (A-6)	H-4

Table 2: Linking of accidents and hazards

The next step in the STPA process is to identify top-level safety constraints for the system. These constraints are interchangeable with safety goals from the ISO 26262 standard. Safety goals are defined as "top-level safety requirements as a result of the hazard analysis and risk assessment (1.58)" [2, Pt. 1]. With this definition top-level safety constraints can be seen as implementation-independent safe system behavior. A remark regarding the safety requirements is to generate positive forward requirements [14, Ch. 2]. Negative requirements like *the AFA must never leave the hard shoulder* cannot be verified with testing as testing does not show the absence of failures in the system. A forward requirement would be, *the AFA always must maintain a defined distance to the hard shoulder boundary*. This requirement does not contain a negation of a hazard but the word *always*.

The AFA is designed to operate in a very limited operational scenario and operational environment, but it is still hard to test every (as demanded by *always*) possible scenario which can occur. However, safety constraints where formulated in a forward manner for this project.

The following and last step in preparation of the STPA process is to define the systems control structure. The main components of the system shall be identified followed by a determination which components control each other.

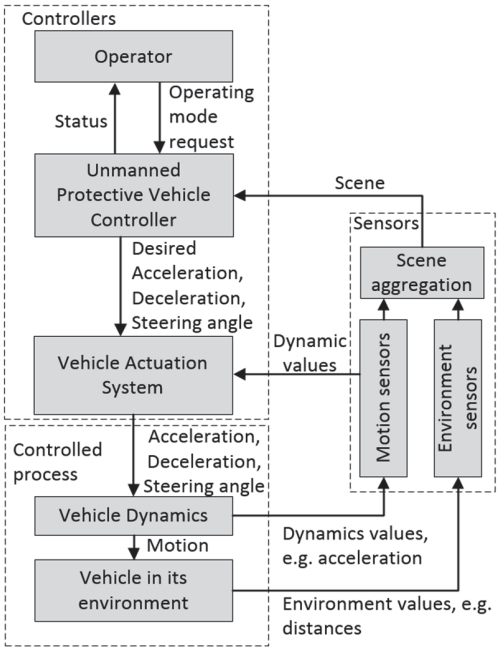

Figure 2: Top-level control structure

Fig. 2 shows the identified top-level control structure of the AFA system. We divided the controlled process in two sub-processes:

- vehicle dynamics, influenced by the actuators (drive, steering and brakes),
- vehicle in relation to its environment, influenced by vehicle dynamics over time.

These parts of the controlled process can be measured by different sensor setups consisting of motion sensors, environment sensors and chassis sensors. The sensor readings can be aggregated to a scene describing the vehicles status, dynamics and the relation to other objects around the vehicle. Ulbrich et al. [19] define, after a review of several definitions, that

> "a scene describes a snapshot of the environment including the scenery and dynamic elements, as well as all actors and observers' self-representations, and the relationships among those entities. Only a scene representation in a simulated world can be all-encompassing (objective scene, ground truth). In the real world, it is incomplete, incorrect, uncertain, and from one or several observers' points of view (subjective scene)."

The scene aggregation is a complex system for itself with multiple tasks like model based filtering, object tracking, motion estimation and generation of contextual information. After defining the process and the sensors, we identified two main controllers for the driving task. The vehicle actuation system is an abstraction for complex control structures of different vehicle actuation topologies as Stolte et al. describe [20]. This control loop controls the vehicle dynamics with a sampling time at the order of 10 ms. The superimposed control loop (at about 100 ms) generates the input for the vehicle actuation system and gets inputs from the sensors in form of an aggregated scene and from the operator. As the unmanned protective vehicle is a SAE level 4 automation system [10], the operator only controls operating modes. At this level of abstraction, the control structure could be used for several kinds of automated vehicle systems.

3.2 Identification of Unsafe Control Actions

After the STAMP fundamentals were identified, the first analysis step is to identify unsafe control actions for the modeled system/control structure. Control actions are given by controllers to change a state of a controlled process. For this purpose, every controller contains a process model, which is the base for deciding how control actions are executed. In this first step, the identified control actions from our model shall be investigated, if they can be unsafe in any manner. Leveson proposes four categories to investigate control actions [7]:

- not providing a control action causes hazard,
- providing a control action causes hazard,
- providing control action in wrong timing/order causes hazard,
- control action stopped to soon or is applied too long causes hazard.

In our understanding, sensors are giving feedback from the controlled process to several controllers. This differs from other authors models where e.g. a radar, which is not providing an objects state, was classified as an unsafe control action. Feedback information will be handled in the following step of the STPA process, which identifies causes of unsafe control actions. Leveson mentions a fifth category of unsafe control actions, where a control action which is required to enforce a safety constraint is provided but not followed. This can cover failures e.g. in actuators where a control action is given, but the actuator does not react.

Starting with the control action *desired steering angle* from Fig. 2, we are facing a challenge regarding the high number of possible operational scenarios. The desired steering has to be provided all the time, even if the unmanned protective vehicle shall drive a straight line. When analyzing the second category (providing a control action causes hazard), we have to brainstorm possible scenarios where the control action can be hazardous. As mentioned in Section II, a hazard is defined by a system state and a set of environment conditions, which together lead to an accident or a loss. To identify whether a control action is unsafe or not, a (environment) system context is needed.

Thus, we used the extension of STPA proposed by Thomas [12] to analyze the unmanned protective vehicle. We started with the operating mode as first the context separation. The system has four operating modes: manual mode, safe halt, follow mode and coupled mode. In the manual mode, the system is used as a normal vehicle without intended automated actuation. Safe halt decelerates the vehicle to a full stop and holds it in standstill. This operating mode does not take any information about the environment into account. Follow mode is used to operate the vehicle as protective vehicle where the system follows the hard shoulder and keeps a defined distance to the leading vehicle. In case of any objects on the hard shoulder, the AFA immediately transits the operating mode to safe halt by itself. The coupled

mode is used to pass on- and off-ramps with a very small distance to the leading vehicle by following the driven trajectory. The environment perception and the dynamic state of the leading vehicle, which is send via a radio interface, are used to enable the coupled mode.

To analyze the AFA at the top level, we choose the following context variables and entities:

- Operating mode
  - Manual mode, follow mode, coupled mode, safe halt
- Vehicle dynamic state
  - stopped, driving (10 km/h), driving (60 km/h)
- Environment
  - Highway/rural, hard-shoulder, on/off-ramp
- Obstacle present
  - yes (solid), yes (vulnerable), no

Following the thoughts of Thomas in the STPA-Primer [14, Ch. 3], the entities were chosen by abstraction of variables (environment classes and obstacles) and discretization of continuous process variables (dynamic states). With all possible combinations of the process variables we obtain 108 identified contexts. To further reduce the number of contexts, we took a closer look on combinations of operating modes and environments. During unmanned operation (safe halt, follow and coupled mode) the protective vehicle is prohibited to access streets besides a hard shoulder on a highway and on- and off-ramps. In manual mode the AFA is operated on highways or rural roads, thus we removed combinations including other environments. Other irrelevant combinations were unmanned operation at 60 km/h (this is only allowed up to 10 km/h) and manual operation at 10 km/h (because 60 km/h include 10 km/h). This reduction of relevant combinations is based on the assumption that the road workers will not operate the AFA outside of these functional system boundaries. With these reductions, we obtained 36 contexts in total. We used the control structure from Fig. 2 with all 36 contexts to start the analysis. By applying the different categories of unsafe control actions on our top-level control actions, we identified some unclear information in the process:

- Unclear or inappropriate categorization:

We extended the categories by the information, if a control action was needed or not needed in the certain context. For example, braking and accelerating can only be hazardous when it is required but not provided and vice versa.

- Missing context information:

The case *braking torque not provided when required* in safe halt on hard shoulder when the AFA is stopped is hazardous, if the vehicle is standing on slope. In this case the vehicle can roll towards the moving traffic and thus causes an accident.

- Control action is chosen too abstract:

Operating mode request is a control action which has influence on the system depending on which operating mode is requested. We decided, to verify all possible change requests in every context, which results in 72 additional contexts for this control actions.

- Vehicle movement consists of continuous control actions:

Continuous control actions are not greatly covered by the categories for unsafe control actions of the STPA-process. Stolte et al. [20] show that the continuous control actions can be transformed to discrete ones for the analysis in the STPA process.

Despite the difficulties in the modelling process and the application we found that STPA extends the traditional hazard analysis methods to the socio-technical aspect of the system. The road workers have to select the appropriate operating mode for several scenarios during the work process. For example, driving in follow mode on the hard shoulder followed by switching to safe halt for a change to coupled mode to pass an on- or off-ramp. The operating modes don't have to monitor all functional system boundaries of the whole driving task. If the wrong operating mode is active in an environment, which the mode is not designed for, the operation is hazardous. We identified multiple hazardous events were inappropriate actions of road workers (mainly operating mode requests) or erroneous HMI-signalization

can be root cause for crashes of the AFA with moving traffic on the neighboring lanes. These are information regarding the mental model of the road workers and the interaction of them with the AFA system which are not covered by hazard analysis techniques mentioned in the ISO 26262 standard.

4. Conclusion

In this contribution, we investigated the application of a System-Theoretic Process Analysis (STPA) to an unmanned protective vehicle. In the first step, we found a likely generic control structure for automated vehicles with human interaction. To investigate different operational scenarios, we used an extension of the process by Thomas [12]. The extension includes guidelines for generating context variables and entities. After all we found that a more detailed modeling of environment system context is needed, to get more information about the systems (unsafe) behavior. For the application of STPA to the area of automated driving some identified challenges have to be investigated in the future. These challenges are partly specific to modelling of automotive systems in (discrete) control structures for STPA and partly a more general problem of automated driving to deal with high numbers of possible events and combinations in hazard analysis and testing.

Automated driving has some crucial parts in human-machine-interaction like selecting an appropriate operating mode or in some automation levels provide a fallback layer for the automation system. STPA connects the “classic” technical part with aspects of the socio-technical challenges, which are not covered by hazard analysis techniques mentioned in the ISO 2626 standard.

Based on the experiences with STPA so far, we will investigate the process steps and will try adopt this method for the application of automotive systems in complex environments.

Acknowledgements

We would like to thank our partners from the project consortium namely MAN Truck - Bus AG (consortium leader), TRW Automotive GmbH (ZF TRW), WABCO Development GmbH, Robert Bosch Automotive Steering GmbH, Hochschule Karlsruhe, Hessen Mobil - Road and Traffic Management, and BASt - Federal Highway Research Institute for their support. The project is partially funded by the German Federal Ministry for Economic Affairs and Energy.

References

[1] T. Stolte, A. Reschka, G. Bagschik, and M. Maurer, “Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works,” in 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), Las Palmas, 2015, pp. 672–677.
[2] ISO, 26262 Road vehicles – Functional safety. ISO, Geneva, Switzerland, 2011.
[3] Z. H. Qureshi, “A review of accident modelling approaches for complex socio-technical systems,” in Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems - Volume 86, Darlinghurst, 2007, pp. 47–59.
[4] J. Lundberg, C. Rollenhagen, and E. Hollnagel, “What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals,” Safety Science, vol. 47, no. 10, pp. 1297–1311, Dec. 2009.
[5] J. Rasmussen, “Risk management in a dynamic society: a modelling problem,” Safety Science, vol. 27, no. 2–3, pp. 183–213, Nov. 1997.
[6] N. Leveson, “A new accident model for engineering safer systems,” Safety Science, vol. 42, no. 4, pp. 237–270, 2004.
[7] N. Leveson, Ed., Engineering a safer world: systems thinking applied to safety. Cambridge, Massachusetts: MIT Press, 2011.
[8] Q. Van Eikema Hommes, “Applying System Theoretical Hazard Analysis Method to Complex Automotive Cyber Physical Systems,” in ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Chicago, 2012, pp. 705–717.
[9] A. Abdulkhaleq and S. Wagner, “Experiences with applying stpa to software-intensive systems in the automotive domain,” in Second STAMP Workshop, Cambridge, Massachusetts, 2013.
[10] SAE, “J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems - SAE International.”
[11] A. Abdulkhaleq, S. Wagner, and N. Leveson, “A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA,” Procedia Eng., vol. 128, pp. 2–11, 2015.
[12] J. P. Thomas, “Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis,” Massachusetts Institute of Technology, 2013.
[13] S. M. Sulaman, T. Abbas, K. Wnuk, and M. Höst, “Hazard Analysis of Collision Avoidance System using STPA,” in Proceedings of the

11th International Conference on Information Systems for Crisis Response and Management, Pennsylvania, 2014, pp. 424–428.
[14] MIT Partnership for a Systems Approach to Safety (PSAS), “STPA Primer.” [Online]. Available: sunnyday.mit.edu/STPA-Primerv0. pdf.
[15] A. Mallya, “Using STPA in an ISO 26262 compliant process,” 2015.
[16] G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, “Identification of Potential Hazardous Events for an Unmanned Protective Vehicle,” in 2016 IEEE Intelligent Vehicles Symposium Proceedings, Gothenburg, 2016.
[17] R. Matthaei and M. Maurer, “Autonomous Driving - A Top-Down Approach,” - Autom., vol. 63, no. 4, pp. 1014–1136, 2015.
[18] A. Abdulkhaleq and S. Wagner, “XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering,” in Fourth STAMP Workshop, Boston, 2015.
[19] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, “Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving,” in 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), Las Palmas, 2015, pp. 982–988.
[20] T. Stolte, R. S. Hosse, U. Becker, and M. Maurer, “On Functional Safety of Vehicle Actuation Systems in the Context of Automated Driving,” in Advances in Automotive Control 2016, Norrköping, 2016.