Analysing Driver Assistant Systems with a Socio-Technical Hazard Analysing Methodology

R S Hosse*, D Beisel* and E Schnieder*

*Institute for Traffic Safety and Automation Engineering, Technische Universität Braunschweig, Langer Kamp 8, 38106 Braunschweig, Germany

Abstract - Nowadays human-created systems are increasing in complexity due to the interaction of humans and technology. Especially road traffic systems are composed of multitudinous resources (e.g. personnel, vehicles, organizations, etc.), which make it even harder to anticipate the positive and negative effects on safety. One key in achieving a significant reduction of fatalities is seen in driver assistant systems counterbalancing the lack of drivers' capabilities. But the actual outcome of implementing these sophisticated technologies especially on influencing driver's capabilities are yet unknown. Latest research exemplifies an increase of reaction times of drivers in case of dysfunctional driver assistant systems. This research paper applies STAMP/STPA (STAMP = systems-theoretic accident model and processes; STPA = systems-theoretic process analysis) to the German automobile traffic system focusing on the effects of driver assistant systems on drivers. By doing so, the potential hazards caused by technology can be identified.

NOTATIONS

A	standstill state
B	safe-movement state
C	unsafe-movement state
D	accident state
p	velocity profile
s	range
t	transition
v	speed
γ	individual driver capabilities
τ	situational driving tasks

INTRODUCTION

Increasing Complexity in Road Traffic Systems

Purely mechanic systems of the past, without electronic- or software-based components, are simple to analyse: all interactions are anticipatable by the analyser. Today systems include a high degree of interactions between human and automated system's resources (like personnel, organization, technology), which abet the systems' complexity and strengthen the need for renewed analysing methodologies in order to increase safety. [1] There is a need for treating modern systems as complex socio-technical systems, including the social as well as the technological system into the safety analysis. The notion of the so-called socio-technical systems can be described profoundly by the DOCAS model (dynamic open complex adaptive systems), which was introduced by [2]. These types of complex systems are seen as highly dynamic networks of subsystems, acting together for a consistent purpose. In the case of this research road traffic systems can be consequently defined as complex socio-technical systems, due to its human-based, technology-based and software-based resources. The behaviour of DOCAS tends to be apparently chaotic, but shows intermittently structured self-organizing behaviour. [2] Also there exist some developments in technology, which are continuously increasing complexity of socio-technical systems; ergo the analysers' capability to conceive entirely the system's behaviour and ascendancies on safety is inhibited.

Relevant trends affecting system's safety are, for instance

- fast pace of technological change,
- new kinds of accidents,
- decreasing acceptance for simplified causal accidents, and
- changing public views on safety [1]

The fast pace of technological change, especially in vehicles, can be seen in the increased number of features provided by automated controllers, but the number of control components is decreasing at the same time [3]. Also the period of vehicles' life cycle is decreasing continuously [4]. The use of software in socio-technical systems generates new kinds of accidents, which do not stem from solely mechanical dysfunctions and/or human error. Another aspect not to dismiss, is the fact that applying computers in systems means that the system's designers are implementing formerly non-purpose systems (the computer itself) to a socio-technical system. Then software gives the actual purpose to the computer. If the system components are not designed in the right way the interactions between hard-, software and humans may cause hazardous system's states. "The operation of some systems is so complex that it defies the under-standing of all but a few experts, and sometimes even they have incomplete information about its potential behaviour." [1] Ergo, a significant amount of knowledge and information is required to control a social-technical system.

The less is known about the causality of an accident, the more often is personnel accused. [1] Thence, human behaviour is reported to higher levels of an organization's hierarchy, if it generates an undesired outcome. But oftentimes humans need to intervene in a system's operative process if an accident is already inevitable [5]. It has to be put up the question if human interventions in a dysfunctional system can be charged as the cause of an accident. Hence the tolerance of simplified accidents depletes and the examination of accidents must be based on the analysis of lacks within system's design [6]. The system design itself is causing/allowing hazardous states, which can only be prevented by changing the system's design adequately by implementing principles of systems theory.

Empiricism and Safety Potentials of Active and Passive Safety

One way of increasing safety within road traffic systems are driver assistant systems. The safety potential of driver assistant systems can be measured by its capability to decrease fatalities and severe accidents [7]. Generally driver assistant systems can be divided into active and passive safety systems. Firstly are accident-impeding provisions, like emergency brake assistant systems. These technological approaches try to prevent an accident (ex ante). Secondly are crashworthiness-impeding provisions, like safety belts. These kinds of safety provisions try to reduce injuries caused by accidents (post ante). Reviewing the development of casualties within Germany, a significant reduction can be seen since the compulsory implementation of safety belts in the 1950s. But comparing the safety potentials, of active safety to passive safety, it can be shown that the passive safety potential is almost outbid [8] (fig.1).

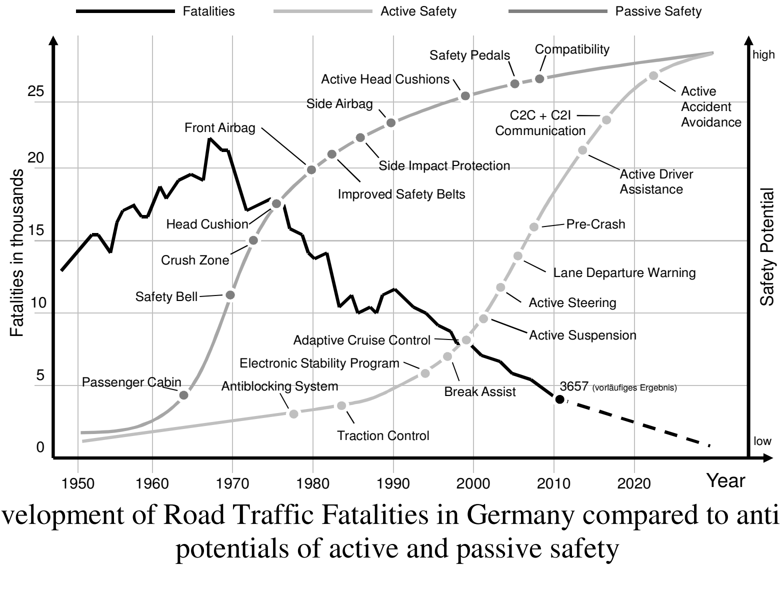

Figure 1. Development of Road Traffic Fatalities in Germany compared to anticipated safety potentials of active and passive safety

The applications of technological sophisticated provisions seem to be the obvious strategy in order to achieve a significant reduction of fatalities and severe accidents. The main question here is, whether the active safety has got the safety potential to decrease the number of fatalities, or if its impact on safety is already utilized and the lasting growth of congestion results again in a rise of fatalities, this is what the latest statistics is showing[9] [10]. It raises the question if the overall road traffic system is faulty in itself and the provisions undertaken will not be capable of decreasing the number of fatalities and severe accidents. They do fight the symptoms slightly, but do not cure the systemic causes within the road traffic system.

SYSTEMS THEORY MODELS APPLIED ON ROAD TRAFFIC SAFETY

Defining Traffic Safety by Composing Engineering and Psychology

"Effectively preventing accidents in complex systems requires using accident models that include that social system as well as the technology." [11] Therefore analysing safety requires an approach, which is capable of identifying effects between social and technical controllers of a socio-technical system [12]. In other words: the disciplines of society, politics, economics, engineering and psychology need to find a coherent definition of safety in order to increase it, but foremost understand it capacious. In the following will be introduced an approach, which harmonizes the interdisciplinary requirements to a coherent definition of safety within road traffic systems:

Systems theory defines safety basically as a system's state without undesired events [13]. Furthermore safety is seen as a property of the system itself, which is achieved and sustained by interactions of varying systems' resources – it is an emergent property and control problem [14]. Especially safety within road traffic systems can solely be measured by its complements (undesired accidents). Near losses (hazardous states without losses) are not identifiable compared to train or flight traffic systems [15]. In order to create a coherent definition for safety in road traffic systems a composition between different models of various disciplines will be needed. The hybrid state model by [16] and the task-capability-interface model by [17] can fulfil this purpose.

Engineering discipline has developed the hybrid state model approach. Within this model the overall system's processes can be allocated to single global system states. The model is based on Petri net logics and Markov chains, identifying states and transitions leading to accidents, in this case of driving manoeuvres. The hybrid state model distinguishes between four global states:

- standstill state, (A)
- safe movement state, (B)
- hazardous movement state, and (C)
- accident state. (D)

The state-transitions enable the system to alter between four global states depending on the behaviour of the ego-driver and other vehicles engaged in the driving manoeuvres. Overall the standstill state (A) and safe movement state (B) can be categorized as safe; accidents (D) cannot be reached directly from (A) and (B) (see figure 2).

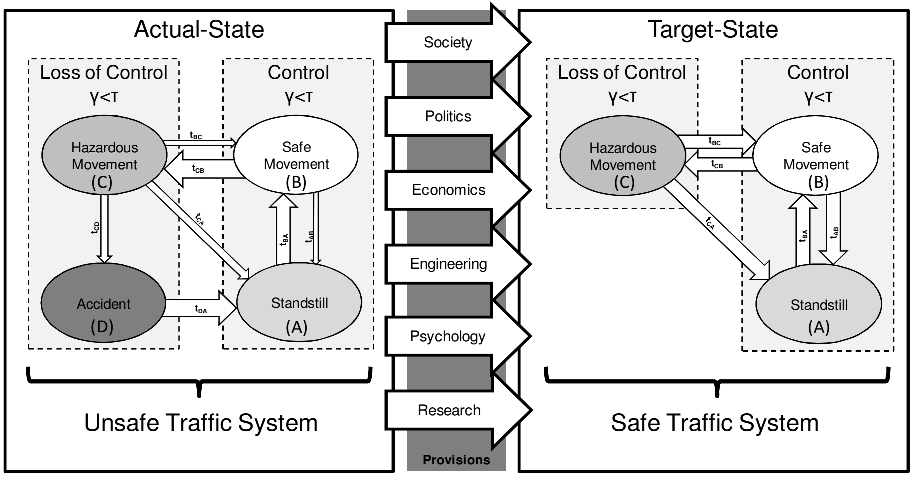

Figure 2. Hybrid State Model including Adequate Adaptations

In (A) and (B) the driver has continuously the ability to handle safely the vehicle. For instance, a car keeping the prescribed speed limit is to be located in (B). The state of unsafe movement (C) is the only state transitioning directly to the accident state (D). The hybrid state-model implies that safety is, although being an emergent property of road traffic systems, basically the individual car's liability. The driver of a car can decide which state to take according to her/his driving behaviour, but it is not always cognoscible if the driving manoeuvre is in (B) or (C).

Seeing the driver as a controller in the system helps to understand what provisions must be taken in order to increase safety. Therefore the objective of safety increasing provisions should support drivers in carrying out driving tasks and keep constantly driving manoeuvres in (B) (it is intentionally not mentioned (A) because the system is not available due to standstill). [16] Noticing that the individual driver is in the centre for sustaining safety in road traffic systems, one must focus on societal and psychological effects influencing drivers' behaviour.

The task-capability-interface model by [17] defines safety in road traffic systems as a difference between the situational tasks of driving manoeuvres τ and the individual driver capabilities γ. On the one hand τ is the sum of influencing factors, which is defined by

$$\tau \in (\textit{constitutional criterion, education, training, experience, competence, human factors}) \tag{1}$$

On the other hand γ is defined as:

$$\gamma \in (\textit{speed, vehicle type, other road users, environment}) \tag{2}$$

The task-capability model puts equally the individual driver into the focus of traffic safety by detecting the level of controllability of driving manoeuvres just like the hybrid state model [17] [16]. As long as γ is inferior to τ driving manoeuvres are in (A) or (B), which means that the driving behaviour is safe. Aggregating both models into graph theory, the following equations of controllability for drivers of driving manoeuvres can be defined:

Driving manoeuvres are controllable while it is in (A) or (B), and

$$(\gamma,\tau) :\Leftrightarrow \forall \gamma \cup \tau : \gamma \geq \tau \tag{3}$$

Driving manoeuvres are uncontrollable while it is in (C) or (D), and

$$(\gamma,\tau) :\Leftrightarrow \forall \gamma \cup \tau : \gamma < \tau \tag{4}$$

The equations (3) and (4) define safety in road traffic systems by concluding the kind of movement of a single vehicle in contrast to the degree of situational tasks and the individual capabilities of drivers.

It can be shown that using interdisciplinary research approaches can create a coherent definition of traffic safety. Of course driver assistant systems aim at supporting drivers in the natural lack of capabilities, but those technologies must be designed in the right way.

Using Cybernetics for Hazard Analysis

After showing how systems theory can be used to find an interdisciplinary definition of safety within road traffic systems, one must now focus on methodologies helping to analyse the overall socio-technical systems to identify hazards and design adequate safety-increasing provisions. This can be done by the application of STAMP/STPA (Systems-theoretic accident model and processes / Systems-theoretic process analysis).

The STAMP-Model of Accidents

A hazard analysis methodology for socio-technical systems based on cybernetics theory is provided by STAMP. "[STAMP] is a new approach to hazard analysis that enables model-based simulation and analysis of risk throughout the system life cycle, including complex human decision-making, software errors, system accidents (versus component failure accidents), and organizational risk factors." [1] The objective of STAMP is to identify adequate safety constraints in a systems' structure, which are capable of sustaining safety by constraining human and automated controllers to safe behaviour. Instead of traditionally seeing accidents as the result of event-chains (like failure mode and effect analysis / FMEA), STAMP defines an accident as an inadequate implementation of safety constraints in a system's structure. Or in other words: An accident is a dysfunctional interaction of various system resources and thus a control problem. The root cause of accidents, even though STAMP implies that there exist no root cause but systemic causes, lie in different mental models of human and automated controllers (equally to system's resources) about the system's structure and its potential behaviour. The mental model of human operators can vary significantly to the models implemented in the automated controllers, especially concerning non-linear system's behaviour. This can result in inadequate and conflicting control actions by human and automated controllers, which create a hazardous behaviour of the system a lead to accidents. [18] The primary objectives of STAMP are

- determining control limits for safe behaviour,
- generating awareness of permissible behaviour towards human and automated controllers,
- developing of strategies for coping with hazardous states,
- supporting of optimization and adaptation processes on contextual influences,
- admitting fault tolerances,
- ensuring visibility and reversibility of errors, and
- liberating decision makers and system's operators of performance pressures. [1]

STAMP can be seen as the basic model, which defines safety differently than traditional models. STPA is a hazard analysing methodology, which applies the principles by STAMP to a real system. This methodology can be applied during a system development. Generally it can be shown that STPA identifies almost twice the number of hazards in a system than a FMEA or FTA. Another methodology provided by STAMP, but not applied in this paper, is CAST (causal analysis based on STAMP), which is an accident analysis. It creates a deeper understanding of accidents, especially when it comes to organizational faults (see fig. 3).

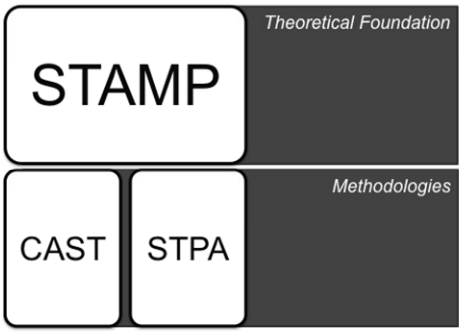

Figure 3. Theory and methodologies by STAMP

Systems-Theoretic Process Analysis

STAMP/STPA uses the so-called safety control structures of a system to analyse control loops affecting the safety-critical operative processes of a system and thus identify lacks in control. It needs to be emphasized that STPA is a top-down analysis. The analyser can focus on the overall system, including very high-level control components, or focus on the technology-based controllers, software and algorithms in the control devices. STPA follows a defined procedure, which is described in very detail in [1].

Generally in the first step STPA method models a safety control structure of the system to be analyzed. A quantitative system dynamics model can create a deeper understanding afterwards in unintended system behaviour. But it is criticized that this means of description lacks in validation and verification. Interactions of control components in socio-technical systems are represented in safety control structures as cascaded control loops. The safety control structure models the in- and outputs of each control component and generates virtual containers, which can be quantified by differential equations. Generally control components can be divided into two categories:

- system-designing control components, and
- system-operating control components.

The first category subsumes all control components, which inhere in the ability to define the system's design itself, e.g. legislative authority or management. This category of control components can undertake provisions to increase safety by changing the structure of the system. The second category of control components is directly involved in the operative process of the system. But system-operating control components do explicitly not have the ability to change the system's structure. These control components are directly involved in the safety-relevant processes and the implemented safety constraints must act on these control components. [1] The basic assumption by safety control structures is sourced by the socio-technical framework of Rasmussen.

System Dynamics Model of Accident Occurrence

Generally the system dynamics modelling conducted by STAMP is primarily helping to understand the effects, which occur in the system affecting the operative processes and showing the dysfunctional control actions. After developing the control structure of the safety-critical system, the analyser defines for each control component one or more system dynamics variables, which will then be linked together in the final model. The following findings are based on a qualitative analysis assisted by various experts' interviews:
The basic dynamic hypothesis of the system dynamics model about the occurrence of accidents assumes that the *accident rate*[1] is foremost depending on the *level of control* by the driver, which is defined as a function of the *situational tasks* and the *individual capabilities* (figure 4).

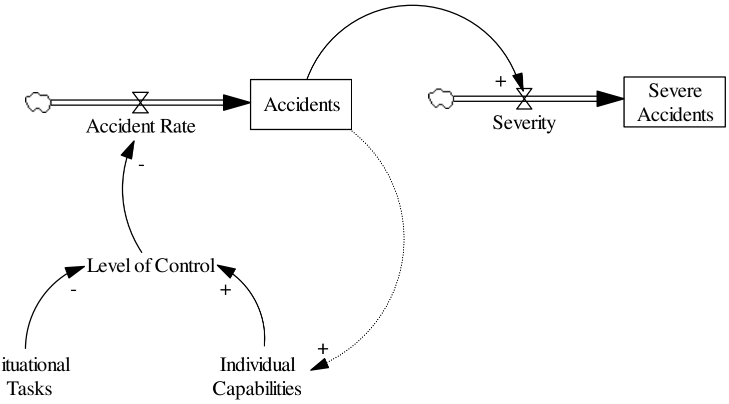

Figure 4. Hypothetic system dynamics model about the occurrence of accidents and severe accidents [19]

Thus the higher the grade of *individual capabilities* the higher is the *level of control*, and vice versa. Contrary to the *individual capabilities* are the *situational tasks*. The higher the *situational tasks* the lower is the *level of control* by the driver about the driving situation (e.g. fog, high speed, etc.). Depending on the *accident rate* the number of *accidents* is increased or decreased. Also this model assumes that an accident needs to occur, which then, depending on speed, clearance and other factors, generates severe accidents including fatalities. [19] There are numerous other feedbacks, which are not shown within this paper due to their relevance.

[1] italic words mark the system dynamics model's variables

FINDINGS AND RESULTS

Effects in the Hybrid State Model of Driver Assistant Systems

The focus of STAMP lies in identifying lacks in the safety control structure, which generates hazardous behaviour of the socio-technical system. Therefore it is crucial to analyse which impact safety-increasing provisions do have within the safety control structure, exemplified on the German road traffic system.

Translating the hybrid state model into a speed-velocity diagram one can ascertain the states (A) to (D) according to the speed-profile selected by the individual driver (see figure 5).

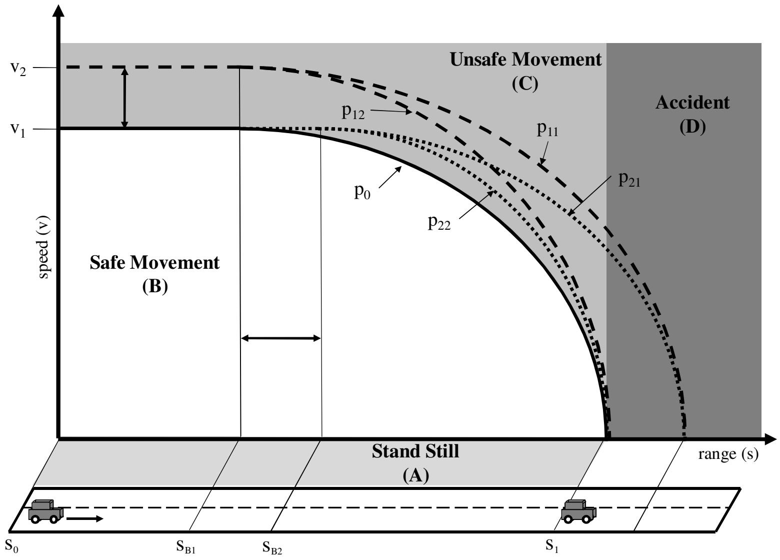

Figure 5. VS-Diagram of Hybrid State Model

Following the consequences of a specific driving manoeuvres of increasing speed and breaking later will be illuminated. p_0 shows the optimal speed profile if the driver reacts in compliance to rules and breaks safely before (D) can be reached:

- p_{11}: this speed profile differs to p_0, because the initial speed has been increased by the driver from v_0 to v_1, which means:

  $$v_0 < v_1 \tag{5}$$

  Regarding the four states, the ego-vehicle moves constantly in the hazardous state (C). Thus the system's state can switch into (A), (B) and (D) by transitions t_{CA}, t_{CB} and t_{CD}. Actually transition t_{CD} is the only one unwanted because it leads directly into the accident state. the speed profile is equal to p_0, which only hampers the accident due to the adapted speed reduction. Consequently p_{11} will not be able to hamper the accident. But in order to keep the system out of the accident state (D) the transitions t_{CB} or t_{CA} must switch.
- p_{12}: Speed profile p_{12} shows an increased speed reduction rate in contrast to p_{11}, which enables the ego-vehicle to stop before crashing into the other vehicle. The initial speed v_1 is equal to the former speed profile case. But adapting driving behaviour to speed profile p_{12} the transition t_{CD} will not be able to switch; the system returns to a safe state (A) in case of a braking manoeuvres.
- p_{21}: In contrast to speed profile p_{11} and p_{12} the speed v is constant, but the local starting point of breaking is closer to the other vehicle than before, which means:

  $$s_0 < s_1 \tag{6}$$

In the case of not adapting the speed reduction rate, like it is done in speed profile p_{21}, again the ego-vehicle brings the system into an hazardous state (C), which (if not adapted) will lead to the accident state (D) by transition t_{CD}. The necessary adaption in order to not bringing the system into a hazardous state is represented by speed profile p_{22}.

- p_{22}: This speed profile has also a constant starting speed v_0, but has also a later breaking point, which is shown in s_1. In contrast to the previous speed profile, this one has a higher speed reduction rate. This driving behaviour, adapted to the driving situation, shows the adequate breaking manoeuvres in order to hinder the overall system to transition into the accident state (D). Even though in this case the transition t_{CA} is acting.

The question is, which effects safety-increasing technological provisions undertaken by the automobile industry actually do generate within the road traffic system? The latest research processed by the ADAC exemplifies that especially breaking assistant systems do bring certain driving situations into hazardous states (C) when decelerating. Thus a proposed safety-increasing driver assistant systems is actually not hampering the transition t_{BA} to switch, furthermore if the driver is not acting on the hazardous manoeuvres, the breaking assistant system does decelerate speed, but does not stop transition t_{CD} to bring the system into the accident state (D).
Another safety-decreasing aspect generated by driver assistant systems is seen within the allowed spacing of adaptive cruise control systems (ACC). One aspect of the features of ACC is that they actually allow (equally to breaking assistant systems) too low spacing between approaching vehicles. Consequently the road traffic system is brought into hazardous states (C) again [7]. Other research strengthens also that the hazards caused by inadequate designed technological approaches within road traffic systems can lead to an increase of severe accidents, especially fatalities. For instance failure functioning of driver assistant systems, on which the driver is used to and trusts, leads to an incremental increase of reaction times [20].

Exemplified Safety Control Structure of Emergency Braking Assistant System

The STPA analysis has been performed on the example of a braking assistant system. This system is intended to break automatically in case of a hazardous movement and thus improve the natural lack of drivers' capabilities. The identified safety control structure, shown in fig.6, shows all relevant technological and social control components involved in the operative safety-critical control process. This includes the ego-vehicle as well as the lead vehicle, which gives information to the radar and LIDAR.

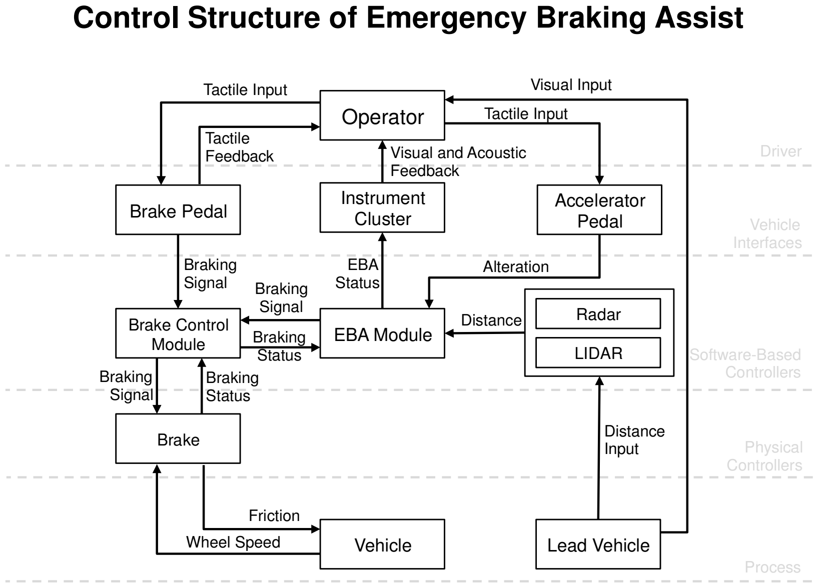
Control Structure of Emergency Braking Assist

Figure 6. Control structure of emergency braking assist

This information is provided to the EBA (emergency brake assistant system) module, which then gives control actions to the brake control module. Its physical controller, the brake, decelerates the ego vehicles speed. Further components included in the safety control structure are the instrument cluster as well as the brake pedal and the accelerator pedal. These interfaces are provided to the driver and the operative control process can thus be manipulated. This control structure shows the emergency brake assist at a very top-level of the analysis. The control structure can be developed to show precise components and software interactions.

After the safety control structure of the system has been developed, the next step includes an detailed analysis of general flaws in the control loops. The general control flaws are shown in the generic control loop in fig.7. The basic idea is to adapt control theory to safety design analysis. A controller is involved by its actuators and sensors into the controlled process, which itself can be a controller. The controller itself can be influenced by other controllers; this means the integration of cascaded control loops in the safety control structure. Otherwise another controller may have influence on the controlled processes and is in parallel loop. The generic flaws, like missing or wrong communication between the controllers, can influence the overall behaviour of the control loop.

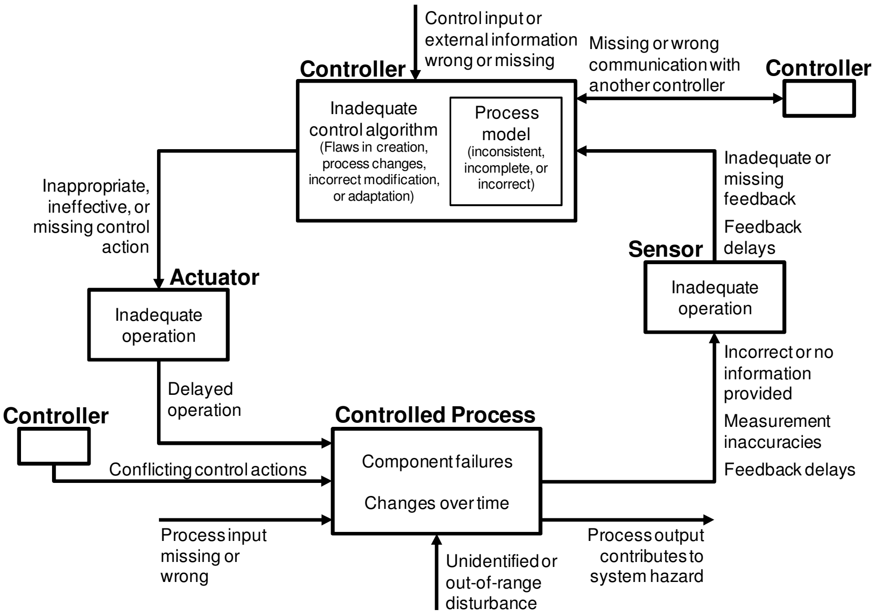
Control input or external information wrong or missing
Missing or wrong communication with another controller
Controller
Controller
Inadequate control algorithm
(Flaws in creation, process changes, incorrect modification, or adaptation)
Process model
(inconsistent, incomplete, or incorrect)
Inappropriate, ineffective, or missing control action
Inadequate or missing feedback
Feedback delays
Sensor
Actuator
Inadequate operation
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 7. Generic Control Flaws

When the control structure has been completed, each control loop needs to be analyzed. [1] identifies four generic unsafe control actions which may occur in a control loop:

1. Action required but not provided:
   In the example of emergency braking assistant system means this flaw that the driver does not brake, if braking is required. A control action by a controller is required, but the controller does not have an adequate model of the process, or information about the process, and thus does not provide the required control action.
2. Unsafe action provided:
   In this generic control flaw a controller provides the wrong control action. For instance if a boiler heats up water, but receives the wrong information about the water temperature (e.g. the information provided is lower than in real), the boiler's controllers increases continuously heat, which may create a hazard temperature.
3. Incorrect timing / order:
   This means, that the right control action is provided by the controller, but it is in the wrong timing or order. In the example of the braking manoeuvres is this happening if the driver brakes too late or if the EBA brakes after the driver already started breaking.
4. Stopped too soon:

This generic flaw in a safety-critical process occurs, if the right control action is provided, but it stops too soon. For instance, if the EBA brake decelerates the car, but stops too soon. Thus the car may crash into the lead vehicle.

The examples listed above are exemplified in Tab1. These kinds of tables identify all relevant control actions throughout the whole safety control structure. In the end this delivers a hazard log, which shows, what kind of safety constraints still needs to be implemented in the safety control structure.

Table 1. Indentifying unsafe control actions (Example)

Control action	Action required but not provided	Unsafe action provided	Incorrect timing / order	Stopped too soon
Execute braking manoeuvre	*Driver does not execute braking manoeuvre* *Vehicle remains at same speed*	*Driver reduces speed too slow*	*Driver brakes too late*	*Driver does not complete entire braking manoeuvre, e.g. vehicle does not brake before lead vehicle*

After the identification of unsafe control actions within the safety control structure, the next step is to create safety constraints based on these unsafe control actions and thus design the hazards out of the system. Tab.2 exemplifies two missing safety constraints in the control structure. It needs to be created a safety constraint, which enables the driver to brake at the right timing. The EBA provides this function partly, but even though different systems are designed not to prevent an accident, but still crash into the lead vehicle. Otherwise an information system for the driver about its actual driving behaviour and the degree a hazards may feedback an adequate information for the driver to brake at the right timing. Another unsafe control action provided by the driver may be that the driver brakes too slow and the rate of deceleration is inadequate. This safety constraint can also be coped with providing adequate feedback to the driver about his/her adequacy of driving behaviour to safety.

Table 2. Defining Safety Constraints (Example)

Unsafe Control Action	Safety Constraint
Driver brakes too late	*Driver must reduce speed adequately to lead vehicle*
Driver reduces speed too slow	*Driver must reduce speed-decrease-rate adequately to lead vehicle*

This is only exemplified on the brake assistant system, but the complete STAMP/STPA analysis on the German road traffic system, show some other significant missing safety constraints, which will be exemplified within the next part.

Required Structural Adaptation of Road Traffic Systems

Systems theory can be used to design the structure of socio-technical systems to ensure a safe behaviour over the whole life cycle [1] The coherent and generic definition of traffic safety developed in this paper enables the system's analyser to define an adequate target state of road traffic systems in order to achieve a significant decrease of fatalities and thus develop adequate provisions.

The actual design of road traffic systems enables a state-transition from (C) to (D), which is enabling accidental states. In order to ensure traffic safety (D) must be excluded, which can be achieved by eliminating t_{CD} transitioning from (C) to (D) (figure 2) [16]. The exclusion of transition t_{CD} and consequently t_{DA} requires structural adaptations of road traffic systems to constrain system's behaviour. At this point is to be accentuated that hazardous movement states (C), which is defined by equation (4), is necessary to maintain in traffic systems due to behavioural aspects of humans. For human controllers it is important to take intentionally hazardous states for getting to know limitations of safe behaviour. Otherwise it is not possible to experience limits of safe system's behaviour. [1]

In order to shape human behaviour intentionally it requires reliable and short-term feedbacks. Especially socio-technical systems tend to drift into a hazardous state due to positive consequences on negative behaviour by human controllers [18]. Another aspect concerning the task-capability model by Fuller, the driver does not consciously receive a feedback about her/his adequacy of driving behaviour to safety compliance. In other words: the controllability of driving manoeuvres is invisible to drivers. In order to ensure a safe behaviour and an adequate mental model of driving manoeuvres one must implement a provision, which is aiming at balancing the driver's lacks.

Like mentioned before, the disciplines of society, politics, economics, engineering, psychology and research need to develop provisions in order to translate the actual state of road traffic systems to the prescribed target-state of road traffic systems without accidental states (D) (figure 2). This approach is equal to the principles of STAMP.

Perceptions of STAMP-analysis for Road Traffic Systems on the example of Germany

The most important perception by performing the STAMP-analysis on the German road traffic system is that the driver is actually at no point of time of driving able to get an adequate feedback about the driving behaviour in contrast to safety compliance. According to the coherent and generic definition of traffic safety within road traffic systems, the lack of feedback on the level of control, created by the difference of individual capabilities and situational tasks of a single driving manoeuvre, is the primary missing constraint, which must be implemented within the system. One-way of doing so is represented by the VIDE display concept, which feeds back the actual hazard potential of the driving manoeuvres. Another aspect concerning the feedback received by the driver is that generally drivers are punished for rule contradicting driving behaviour, but never receive benefits directly. Thus the latency between behaviour and reaction is too long, as it could have a direct impact on the general driving behaviour. One approach, which is trying to overcome this problem, is represented by so called PAYD-insurance (pay-as-you-drive) concepts. Driver can use a box, which is measuring the driving behaviour. This information is available to the insurances companies. Those can now, with the knowledge of the adequacy of behaviour, calculate a proper insurance fee. This creates an almost direct link between the individual driving behaviour and a positive (or negative) consequence (in this case money). Ergo drivers can benefit of safety-compliant driving behaviour. [19]

CONCLUSIONS

This research showed how a new hazard analysing methodology STAMP/STPA could be adopted to analysing driver assistant systems, by taking into account the overall socio-technical system. We are facing increasing complexity within human created socio-technical systems, especially traffic systems. The causal factors of accidents are not identifiable completely anymore; consequently new accident-analysing and hazard-analyzing approaches are required, which cope with the high degree of complexity and uncertainty. Modern provisions like driver assistant systems may not achieve their expected safety potential of decreasing the number of fatalities. Due to the generic and coherent definition of traffic safety in road traffic systems developed within this paper, the driver as well as the driver assistant system is capable of transitioning the traffic system between the safe states standstill and safe movement, and the hazardous states hazardous movement and accident. Depending on the individual driving behaviour and diver's capabilities the system tends to certain global states.

The introduced cybernetic-based hazard analysing methodology STAMP defines safety consequently as an exclusion of the accident state of the traffic system. Therefore one must develop systems' structural safety constrains, which are capable of limiting humans' and automated controllers to safe behaviour. By analysing the German traffic system, the primary lack within the system's structure is seen in the missing feedback of the adequacy of driving-behaviour to the actual tasks of the driving manoeuvres. It can be shown that drivers are simply punished for unsafe behaviour, but the latency of positive reactions of safe behaviour is too long as the drivers could connect the positive outcome to certain behaviour**.**

REFERENCES

[1] Leveson NG. Engineering a safer world: Systems thinking applied to safety. Massachusetts: MIT Press; 2011.

[2] Holbrook M. Adventures in Complexity: An essay in dynamics open complex adaptive systems, butterfly effects, self-organizing order, coevolution, the ecological perspective, fitness landscape, market spaces, emergent beauty at the edge of chaos, and all that jazz. Academy of Marketing Science Review 2003;Volume 2003(No.6):1–181.

[3] Schũffele J. Automotive Software Engineering: Grundlagen, Prozesse, Methoden und Werkzeuge effizient einsetzen. 4th ed. Wiesbaden: Vieweg + Teubner; 2010.

[4] Kuder M. Kundengruppen und Produktlebenszyklus: Dynamische Zielgruppenbildung am Beispiel der Automobilindustrie. Univ., Diss.--Chemnitz, 2004. 1st ed. Wiesbaden: Dt. Univ.-Verl; 2005.

[5] Repenning NP, Sterman JD. Nobody ever gets credit for fixing problems that never happened: Creating and sustaining process improvement. California Management Review 2001;Volume 43(No.4):64–88.

[6] Leveson NG. A New Accident Model for Engineering Safer Systems. Massachusetts; 2004.

[7] Hummel T, Kühn M, Bende J, Lang A. Fahrerassistenzsysteme: Ermittlung des Sicherheitspotentials auf Basis des Schadensgeschehens der Deutschen Versicherer. Unfallforschung der Versicherer. Berlin: Gesamtverband der Deutschen Versicherungswirtschaft e.V; 2011.

[8] Brühning E, Seeck A. Bewertungen: Der Sicherheitsgewinn bisher entwickelter Fahrerassistenzsysteme und ein Blick in die Zukunft. In: Fahrerassistenzsysteme: Im Dienste der Sicherheit. Bonn; 2006, p. 18–22.

[9] Färber B. (Un)sichtbare Beifahrer: Was Autofahrer von Fahrerassistenzsystemen erwarten (könne). In: Fahrerassistenzsysteme: Im Dienste der Sicherheit. Bonn; 2006, p. 6–13.

[10] MacDonald R, Carpenter K. Reducing Traffic Safety Deaths: A System Dynamics Perspective. 19th International Conference of System Dynamics Society; 1998.

[11] Lim K. Enhancing Vehicle Safety Management in Training Deployments: An application of system dynamics. Dissertation. Massachusetts; 2008.

[12] Vieweg K. Thesen Zum Problemfeld Technische Sicherheit aus Juristischer Sicht. In: Winzer P, Schnieder E, Bach F, editors. Sicherheitsforschung-Chancen und Perspektiven: Springer Berlin Heidelberg; 2010, p. 117–29.

[13] Winzer P, Schnieder E, Bach F (eds.). Sicherheitsforschung-Chancen und Perspektiven: Springer Berlin Heidelberg; 2010.

[14] Drewes J. Verkehrssicherheit im systemischen Kontext. Dissertation. Braunschweig; 2009.

[15] Schnieder E, Schnieder L. Verkehrssicherheit: Maße, Modelle und Methoden. 1st ed. Berlin: Springer; 2013.

[16] Schnieder E. Methoden der Automatisierung: Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme ; mit 56 Tabellen. Braunschweig: Vieweg; 1999.

[17] Fuller R, Santos JA. Human factors for highway engineers. 1st ed. Amsterdam: Pergamon; 2002.

[18] Dulac N. A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems. Dissertation. Massachusetts; 2007.

[19] Hosse RS. Modellierung von Regelkreisen der Verkehrssicherheit mit einem systemtheoretischen Ansatz. Diplomarbeit. Braunschweig; 2011.

[20] Niederée U, Vollrath M. Evaluation der Mensch-Maschine-Schnittstelle eines Längsführungsassistenten. In: ITS Niedersachsen e.V., editor. AAET 2012: Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel. Braunschweig: DLR; 2012.