Thesis for the Degree of Doctor of Philosophy

Safe Transitions to Manual Driving From Faulty Automated Driving System

Josef Nilsson

Department of Signals and Systems
Chalmers University of Technology
Gothenburg, Sweden 2014

Safe Transitions to Manual Driving From Faulty Automated Driving System
JOSEF NILSSON
ISBN 978-91-7597-035-6

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 3716
ISSN 0346-718X

Department of Signals and Systems
Mechatronics
CHALMERS UNIVERSITY OF TECHNOLOGY
SE–412 96 Gothenburg
Sweden

Telephone: +46 (0)31 – 772 10 00

Email: josef.nilsson@sp.se

Typeset by the author using LaTeX.

Chalmers Reproservice
Gothenburg, Sweden 2014

to Karin and Thea

Abstract

This thesis presents a method to assess the safety of transitions from automated to manual driving when vehicle automation fails. The method is based on contributions to the understanding of human driving behavior, also presented in this thesis. Interviews with drivers and driving simulator studies of driving with automation, and particularly analyzes of situations where automation failed provided the base for the proposed method. Among the results of the studies, it was found that drivers were more likely to control an automation failure if automation was only replacing the driver in longitudinal control of the vehicle, i.e., steering still managed by the driver. Moreover, the studies found that drivers responded to the failures with varying success. For the most critical failures, almost half of the drivers collided, while for a less critical failure, about two thirds of the drivers managed to control the situation and avoid a collision.

Individual differences between drivers were considered to have contributed to the varying success to control automation failures. The proposed method for assessing the safety of transitions therefore adapts online to the individual driver. While the vehicle is driven manually, the driver's capability to control the vehicle is estimated and described as a subset of the vehicle's state-space. In the event of an automation failure, the proposed method assesses whether vehicle states are within this subset or not. If vehicle states are within the subset, the driver is deemed capable of taking over, and the transition to manual control is classified as safe.

The method has been evaluated on data from real vehicles, with human drivers, to demonstrate its performance. Results indicate that the proposed method correctly classifies transitions as safe or unsafe.

Keywords: Driver takeover, safety, functional safety, automated driving, vehicle automation, controllability, brake failure, driver capability, driving simulator.

List of publications

This thesis is based on the following publications:

Paper 1

Niklas Strand, Josef Nilsson, I. C. MariAnne Karlsson, and Lena Nilsson, “Exploring end-user experiences: self-perceived notions on use of adaptive cruise control systems”, *IET Intell. Transp. Syst.*, vol. 5, no. 2, 2011.

Paper 2

Josef Nilsson, Niklas Strand, Paolo Falcone, and Jonny Vinter, “Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance”, in *Proc. 2013 43rd Annu. IEEE/IFIP Conf. Dependable Syst. Networks Work.*, Budapest, 2013, pp. 1–10.

Paper 3

Niklas Strand, Josef Nilsson, I. C. MariAnne Karlsson, and Lena Nilsson, “Semi-automated versus highly automated driving in critical situations caused by automation failures”, *Transp. Res. Part F Traffic Psychol. Behav.*, in press.

Paper 4

Josef Nilsson, Paolo Falcone, and Jonny Vinter, “Safe Transitions From Automated to Manual Driving Using Driver Controllability Estimation”, submitted for publication.

Other publications

In addition to the publications above, the following publications by the thesis author are related to the topic, but not included in the thesis:

Stuart Chalmers, Josef Nilsson, Håkan Edler, and Graham Kemp, “An Ontology-Based Approach to Car Simulation and Design”, in *Proc. Third Asian Semant. Web Conf. Work.*, Bangkok, 2008.

Josef Nilsson, Paolo Falcone, Jonny Vinter, Jonas Sjöberg, Lena Nilsson, and Jan Jacobson, “A brief paper on improving active safety systems via HMI and dependability analysis”, in *Proc. 3rd IET Int. Conf. Syst. Saf.*, Birmingham, 2008.

Niklas Strand, Josef Nilsson, I. C. MariAnne Karlsson, and Lena Nilsson, “Exploring end-user experiences: Self-perceived notions on use of adaptive cruise control systems”, in *Proc. Eur. Conf. Hum. Centered Des. Intell. Transp. Syst.*, Berlin, 2010.

Niklas Strand, Josef Nilsson, I. C. MariAnne Karlsson, and Lena Nilsson, “Interaction with and use of driver assistance systems: A study of end-user experiences”, in *Proc. 18th World Congr. Intell. Transp. Syst.*, Orlando, FL, 2011.

Roozbeh Kianfar, Bruno Augusto, Alireza Ebadighajari, Usman Hakeem, Josef Nilsson, Ali Raza, Reza S. Tabar, Naga VishnuKanth Irukulapati, Cristofer Englund, Paolo Falcone, Stylianos Papanastasiou, Lennart Svensson, and Henk Wymeersch, “Design and Experimental Validation of a Cooperative Driving System in the Grand Cooperative Driving Challenge”, *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 994–1007, 2012.

Josef Nilsson, Carl Bergenhem, Jan Jacobson, Rolf Johansson, and Jonny Vinter, “Functional Safety for Cooperative Systems”, in *Proc. SAE 2013 World Congr. Exhib.*, Detroit, MI: SAE International, 2013.

Cristofer Englund, Kristoffer Lidström, and Josef Nilsson, “On the need for standardized representations of cooperative vehicle behavior”, in *Proc. Second Int. Symp. Futur. Act. Saf. Technol. Towar. zero-traffic-accident*, Nagoya, 2013, pp. 1–6.

Josef Nilsson, Lars Strandén, and Cristofer Englund, "Fault Model for Cooperative Semi-Automated Vehicles", in *Proc. 20th World Congr. Intell. Transp. Syst.*, Tokyo, 2013, pp. 1–10.

Niklas Strand, Josef Nilsson, I. C. MariAnne Karlsson, and Lena Nilsson, "Driving with failing automation in longitudinal control – a driving simulator study", submitted for publication.

Contents

I Introductory chapters

II Included papers

Acknowledgments

First, I want to acknowledge my supervisors Dr. Paolo Falcone at Chalmers and Dr. Jonny Vinter at SP for their dedication to my work. Together with my co-supervisor Prof. Jonas Sjöberg you have all provided much appreciated knowledge and guidance.

The collaboration and co-authoring of papers together with Niklas Strand is also recognized as both fun and a source of important insights. I look forward to future cooperation and to continue our discussions. Perhaps we can write new publications together with Prof. MariAnne Karlsson and Dr. Lena Nilsson. Their knowledge, especially in the field of human factors has been indispensable and has helped me develop my competence in the field.

Most of the work of this thesis has been conducted in the SHADES and SHADES II projects. The support from the advisory board of these projects is gratefully acknowledged.

The people I have met and worked with at SAFER, VTI, and at the department of Signals and Systems at Chalmers should also feel acknowledged. I especially want to thank Bruno and Roozbeh for the countless hours we have spent preparing for experiments and collecting data.

I also want to express my appreciation to my colleagues at SP who have always been supportive and open for discussions. A special thanks to Henrik for proofreading this thesis.

Finally, I want to thank my friends and family for their support. Last but certainly not least I want to thank Thea for inspiring me to finish this thesis. Now I am all yours - at least until next year.

This work has been carried out in association with SAFER - Vehicle and Traffic Safety Centre at Chalmers, Sweden.

Josef Nilsson
Gothenburg, May 2014

Part I

Introductory chapters

Chapter 1

Introduction

The task of driving a vehicle is changing for the driver. Instead of relying only on his or her own skills to safely control the vehicle, the driver is now assisted by computer-based systems in several driving-related tasks. For instance, a driver assistance system that has been on the market for more than ten years is the adaptive cruise control (ACC). This system assists the driver with the task of controlling vehicle speed and respecting a minimum distance to traffic ahead [1]. More recently, manufacturers have introduced lane keep assist (LKA) systems in their vehicles to prevent unintentional lane changes, for example by applying a corrective torque to the steering wheel [2]. With the LKA the task of keeping the vehicle in the lane is shared between the driver and the system. Development of driver assistance does not stop at that. A next step taken in the automobile industry is to combine automated speed control with steering to assist the driver in traffic jams [3], sometimes referred to as the traffic jam assist (TJA) system. While the driver is still required to keep the hands on the steering wheel, direct control of throttle, braking, and steering are automated. Future systems are expected to increase the level of automation further. An example is the platooning system that allows several vehicles to form road trains [4]. As the vehicle joins the platoon the driver hands over control of both speed and steering to the platooning system.

An increased level of automation in aviation has been shown to improve safety, reliability, fuel economy, and comfort [5]. These benefits are now expected in the automotive domain, partly because human driving capabilities are considered to be limited [6]. As an example, the short inter-vehicle distance required to take advantage of reduced aerodynamic drag in platooning is not considered controllable by a human driver [7]. Another expected benefit is that problems with driver distraction will be reduced when the human operator is removed [8].

Besides improving safety and traffic efficiency, automation is also targeting improved comfort. Since the driver is relieved of routine tasks, he or she can engage in other, non-driving related activities, or simply relax as the vehicle cruises to its destination [1]. The results of Paper 1 suggest that improved comfort is achieved with the ACC, even if this automation system still requires the driver to maintain full attention on driving. Here, drivers reported that they felt more rested when arriving at their destination after driving with ACC compared to driving manually.

However, the introduction of automation also brings potential hazards. A potential cause of hazards originating from technical systems, that must be accounted for to ensure safety, is technical failures [9, 10]. With increasing technical complexity, growing size of software content, and additional electro-mechanical interfaces, the potential for failures increases [11, 12]. This thesis is focused on the effects that technical failures in vehicle automation have on safety. Specifically, the interaction between automation and the driver in situations of automation failure is investigated.

1.1 Problem description

Vehicle automation that has the authority to directly control throttle, brakes, or steering can potentially cause severe accidents. Failure of automation may therefore have serious safety implications. However, as long as automation has not completely replaced the human driver, vehicle control can be taken over by the driver when automation fails. If this transition to manual driving is successful, the failure is prevented from causing an accident and safety maintained.

The performance of the driver is essential for the success of a transition. The driver has to realize that it is time to take over and come to a correct conclusion about the state of the system. The decision on an appropriate response as well as the execution of that response before the failure has caused an accident are also required [13]. Unfortunately, previous research suggests that automation degrades drivers' awareness and indicates that monitoring for failures of automation is a task ill-suited to humans [14, 15].

The thesis is dedicated to the study of transitions from automated to manual driving when automation fails. Specifically, the following questions are addressed:

- How do drivers respond to failures of vehicle automation?
- What are the consequences for safety when the driver is required to take over in situations where automation fails?
- How can safety of transitions to manual driving be improved?

1.2 Thesis outline

The remainder of Part I is structured as follows:

Chapter 2 Presents how automation has been implemented in road vehicles and gives a classification of levels of automation. The chapter also presents a logical architecture of vehicle automation highlighting its typical components.

Chapter 3 Provides definitions of automation failure and related concepts, including sections on how to assess the risk associated with failures and how to attain an acceptable level of safety.

Chapter 4 Introduces theory on driving behavior related to safety of driver takeover, and presents a review of previous research on driver takeovers when vehicle automation fails. The chapter ends with a section on how to improve safety of takeovers.

Chapter 5 Summary of the papers included in Part II of the thesis.

Chapter 6 Concludes the thesis with a presentation of contributions and suggestions on future work.

Chapter 2

Vehicle automation

The primary control functions of a vehicle include steering, throttle, and brakes. Human drivers have traditionally been the operators of these control functions. Potentially, automation can replace the driver completely and take over all control of the vehicle. While research has shown that it is technically possible, there are yet no commercially available vehicles for public roads that do not have a human driver. The current approach to automation, implemented with the ACC and LKA, is instead to automate the control functions for a limited set of driving tasks under a limited set of operational conditions.

This chapter explains how the control functions of the vehicle can be decomposed. An architecture and a classification of vehicle automation into levels are also presented.

2.1 Longitudinal and lateral vehicle control

Vehicle control is commonly separated along the longitudinal and lateral directions [16, 17]. This is illustrated in Figure 2.1.

For automation as for the driver, the primary functions for longitudinal control are throttle and brakes. Steering is the primary function for lateral control. There are however important exceptions, like some stability control

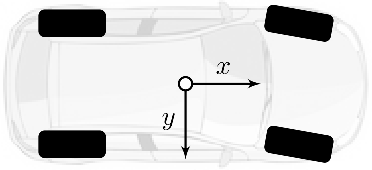

Figure 2.1: Vehicle model where the longitudinal direction is denoted by x and the lateral direction denoted by y.

systems which use differential braking (braking on right or left side) or active torque distribution (independent control of drive torque to each wheel) for lateral control [17].

For automation of longitudinal control, the objective may be to maintain a desired speed, keep a desired distance to other vehicles, or to avoid collisions. Here, automated braking for avoidance or mitigation of rear-end collisions [18] and ACC for speed and distance keeping, are examples of systems currently available in cars [1]. The control objective of currently available lateral automation systems is typically to keep the vehicle within the lane [2, 17], e.g., LKA. Future systems are however envisioned to provide both collision avoidance and lane changing through automated lateral control [1].

2.2 Continuous and event-based automation

The time duration that automation takes control the vehicle varies greatly between automation systems. Stability control systems are active as they intervene to avoid skidding or spinning out of control. LKA systems that apply a corrective torque when the driver fails to keep within the lane but otherwise leaves lateral control to the driver, is another type of system that is only active for short periods of time. Also collision avoidance systems are examples of what is here referred to as *event-based automation*, i.e., automation that takes control of the vehicle during a short period of time (not more than a couple of seconds), in response to an event. For collision avoidance, the event is an impending collision where the response may be an application of the brakes [18].

Automation that is not targeting a specific event but instead controls the vehicle continuously is here referred to as *continuous automation*. The ACC is an example of a continuous automation system. When the driver activates the ACC, control of vehicle speed and distance to other vehicles are automated. While the ACC provides continuous longitudinal automation, lateral automation may also be continuous. Vehicle platooning is one example [4]. Here, both longitudinal and lateral control of the vehicle are automated. From the time the vehicle joins the platoon until it leaves it, automation is continuously active.

When the driver is replaced as the operator of the vehicle, there is a risk for loss of situational awareness, i.e., the driver losing awareness of the states and processes of the system [14]. This may have serious safety implications for driver takeovers. With reduced situational awareness, the driver may not notice or take an inappropriate action in the takeover situation [14, 19]. Also drivers' trust in automation may have implications for safety. Too much

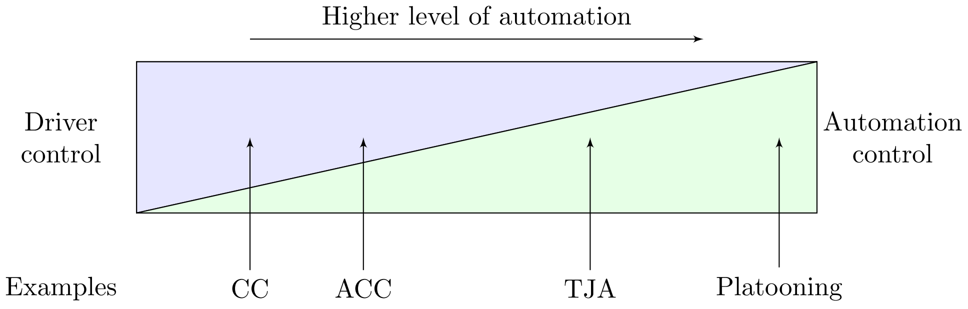

Figure 2.2: Spectrum of automation degree between driver control and automation control. Examples show how four systems can be mapped to the spectrum of automation degree. The four systems are: cruise control (CC), adaptive cruise control (ACC), traffic jam assist (TJA), and platooning.

trust in automation can lead to overreliance where the driver fails to notice when he or she is required to take over. Research indicates that these issues are more likely to appear for continuous automation than for event-based automation [20]. A study by Breyer *et al.* [21] did not observe overreliance to event-based automation provided by a lane-keeping assistance system. The system used in their study provided a corrective steering torque when the driver got too close to the lane markings, i.e., the system provided event-based automation. On the other hand, for continuous automation, as we show in Paper 3, driver performance degrades as an effect of automation that we attribute to loss of situational awareness. Several other studies have also shown that continuous automation degrades driver performance (see for example [22–25]). The topic of driver-automation interaction will be covered further in Chapter 4.

2.3 Levels of automation

Automation is not a matter of all or nothing. Flemisch *et al.* [26] argue for a continuous spectrum of automation degree, between completely manual (100 % driver control) and fully automated (100 % automation control), see Figure 2.2. This spectrum may be divided into discrete intermediate *levels of automation*. A general approach to define levels of automation is taken by Parasuraman, Sheridan, and Wickens [13], addressing automation of any type of control process. Recently, government institutions and a standardization organization have published definitions of levels of automation specific for road vehicles, see reports from the German Federal Highway Institute [27], the National Highway Traffic Safety Administration in the U.S. [28], and the SAE International [29].

The general approach, proposed in [13], describes a model for types and levels of human interaction with automation. According to that model, automation may be characterized by the type of automated functions. The authors list the following four types of functions: information acquisition, information analysis, decisions and action selection, and action implementation. For each of these types of functions, automation can range from fully manual to fully automated. A specific automation system can provide automation to any degree in the four functions, e.g., a high degree of automation in one of the functions and low in the rest. While this approach to characterization of automation is independent of the process (e.g., an airplane, a chemical process, or an assembly line), it is not trivial how to apply it to road vehicles.

The more recently published report from the German Federal Highway Institute [27], specifies five levels of automation specifically for road vehicles. The first of the five levels, "Driver Only", represents completely manual vehicle control. The remaining four levels are: "Assisted", "Partial automation", "High automation", and "Full automation". Their definition of "Assisted" includes systems which deliver either lateral or longitudinal automation where the driver must monitor the system and be ready to take over at any point. "Partial automation" is defined as a combination of both longitudinal and lateral automation. The driver is still required to monitor the system and be ready to take over at any point. For "High automation" the responsibility on the driver changes, longitudinal and lateral control are automated and the driver is not required to permanently monitor the situation. Driver takeovers are still required at this level of automation, but here the driver is given a sufficient lead time to respond to a takeover request. "Full automation" is defined as longitudinal and lateral automation without relying on the driver. Also here, driver takeovers may be possible. However, in case the driver fails to respond to a takeover request, the system is capable of safely bringing the vehicle to a safe state, e.g., brake the vehicle to a standstill.

The National Highway Traffic Safety Administration in the U.S. proposes a similar classification of levels of automation [28], but reserves the highest level for automation that provides longitudinal and lateral automation for an entire trip without driver involvement.

The report from SAE International (SAE J3016) [29] proposes a classification with an additional sixth level. Compared to [27] and [28], this approach makes a distinction between automation that completely replaces the driver for parts of journey and for a complete journey. Following SAE J3016, the first four levels ("Driver Only", "Assisted", "Partial Automation", and "Conditional Automation") correspond to the first four level of

[27] and [28]. The fifth level, called "High Automation" refers to automation that, for parts of a journey, replace the driver completely in longitudinal and lateral control. Here, the driver is not required to be ready to take over. The sixth and final level, called "Full Automation", is reserved for automation that completely automates lateral and longitudinal control throughout a journey.

Another term that is used to describe a level of automation is *semi-automated*. In [26] it is suggested that semi-automated is used when either longitudinal or lateral control is automated. Semi here implies that control of the vehicle is shared between the driver and automation. A similar definition is used in Paper 3, where semi-automated driving refers to driving a vehicle that has only longitudinal automation and the driver has to be prepared to take over at any time.

2.4 System architecture

This section presents a logical architecture of vehicle automation systems. The intention is not to give an exhaustive description of a complete architecture and all its constituent components, nor is the architecture intended to capture complex interaction between automation and the human driver (driver-automation interaction will be treated in Chapter 4). Instead, the architecture is provided as an example to highlight some aspects relevant for the topic of this thesis. One of these aspects is the type of hardware and software components (e.g., sensors, actuators, and control units) that automation can be expected to include. These examples of components serve as input to the identification of potential causes of failures of vehicle automation, see Section 3.1.

The architecture also indicates possible component redundancy, e.g., complementing sensors that provide independently acquired information about the same entity. This type of redundancy can be used for handling failures in automation systems (see for example [30–32]).

An illustration of the logical architecture is shown in Figure 2.3. It was compiled from recent publications on vehicle automation systems [17, 33–35]. The sensors and actuators included in the architecture are examples of what an automation system may use. A system implementing a low level of automation may use only a few of these sensors and actuators while a high level of automation may use them all and additional ones.

The architecture is divided into three main parts: *perception*, *decision and control*, and *actuation*.

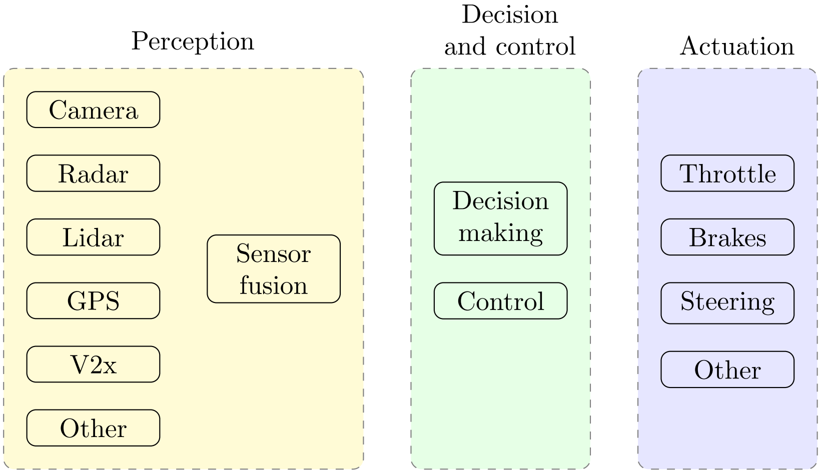

Figure 2.3: A logical architecture of vehicle automation with examples of components that may be included in the three parts: *perception*, *decision and control*, and *actuation*.

Perception Automated vehicles are equipped with a range of sensors for perception of their environment. *Camera*, *radar*, and *lidar* are common sensors for identifying and classifying objects around the vehicle. Measures provided by these sensors include relative distance, speed, and acceleration with respect to surrounding objects. The *GPS* gives the position of the vehicle relative the Earth.

Through *sensor fusion*, information from these and other sources can form a common picture of the vehicle's own state and its environment. Because some sensors complement each other, the fused information can be more accurate and reliable than information from a single sensor. An example is the identification of objects in the range of both the camera and the radar. If both sensors report the presence of an object at the same position, it is more likely that the object really is where the sensors report it is. On the other hand, if one sensor indicates an object and the other sensor does not, sensor fusion can provide an indication of the object along with a measure of uncertainty due to the conflicting information from the two sources.

Beside sensors there is ongoing work to provide vehicles with *V2x* (e.g., Vehicle-to-vehicle, Vehicle-to-infrastructure, and Vehicle-to-pedestrian) technology, i.e., radio communication for exchanging information with other road users and infrastructure. Advantages are that information can be distributed between vehicles with short delays, and the physical range of sensors can be overcome since radio signals can travel longer distances than sensors are able to measure. Communication also enables negotiation and other types of cooperation between road users. It is expected that automation will use V2x to benefit from these advantages [28].

Decision and control With information from sensors and other sources, *decision making* algorithms decide on the appropriate actions to take. This can be a threat assessment algorithm that decides whether to initiate a collision avoidance maneuver [36] or a lane keep assist system that decides whether to apply steering [17]. If the algorithm decides to act, this is also the part of automation that generates *control* commands to the actuators. In the case of longitudinal automation, this command can be a desired acceleration sent to either the power train or brake system [34].

A decision may also be to deactivate continuous automation. Here, an example is the ACC system which deactivates in case the driver shows that he or she wants to take over control, e.g., by depressing the brake pedal. Another reason for automation to deactivate is the detection of a failure to generate the correct control commands [37]. If an automation failure is caused by a failure to generate a correct command to the actuators, the driver may still be able to command the actuators. In such a case a driver takeover may be appropriate. However, successful driver takeovers also depend on the situation, i.e., the driver may not capable of controlling the vehicle in the current situation. The topic of automation deactivation and associated driver takeover is addressed in Paper 4 and will be further covered in Chapter 4.

Actuation The primary control functions are the same for automation as for the driver, i.e., *throttle*, *brakes*, and *steering*. Throttle and brakes are typically used for longitudinal control and steering is mainly for lateral control. There is however inherent redundancy in these control functions. Differential braking and driving-torque distribution can be used to generate lateral motion if the steering actuator fails [32].

This type of redundancy is outside the control of the driver, i.e., the driver cannot distribute braking or driving-torque between wheels. Therefore, if a driver takeover is to be a successful strategy for handling a failure of automation, the actuators which the driver uses must still be functional. Most essential is that braking and steering are available to the driver. If these control functions are unavailable to the driver, there is no advantage in given him or her control of the vehicle when automation fails. On the other hand, if the actuators are fully functional and the cause of the failure is due to a fault in the sensors or the decision and control parts, then a driver takeover may be appropriate.

Chapter 3

Automation failures

This chapter presents definitions of concepts related to automation failures. There is a section on potential causes of failures as well as a section on means to attain dependable automation. The chapter also presents how to assess the risk of potential failures and how this relates to the driver's capability to take over in order to control automation failures.

First, the concept of automation failures is defined. An *automation failure* occurs when automation no longer delivers correct service (following the definition of a failure in [38]). Correct service is delivered when automation provides its intended functionality, which is usually defined in the functional specification. However, it should be remembered that an incorrect specification can itself be the source of failure [9].

3.1 Causes of automation failure

Vehicle automation is made of a complex combination of hardware and software. The complexity allows for advanced functionality, but also implies numerous sources of failure.

Vehicle automation systems typically consist of a perception part, a decision and control part, and an actuation part (see Section 2.4). When allocated to the electronic architecture of the vehicle, these parts are generally implemented on computer nodes that are inter-connected via a communication bus network [9, 39–42], see schematic illustration in Figure 3.1. The components of a specific node depend on its functionality, e.g., a node that has an interface to the video camera may have some circuits dedicated to video processing. There are also generic hardware components present in most nodes. Examples of these generic components are shown for the *Control unit* in Figure 3.1.

All components of the automation system are potential sources of fail-

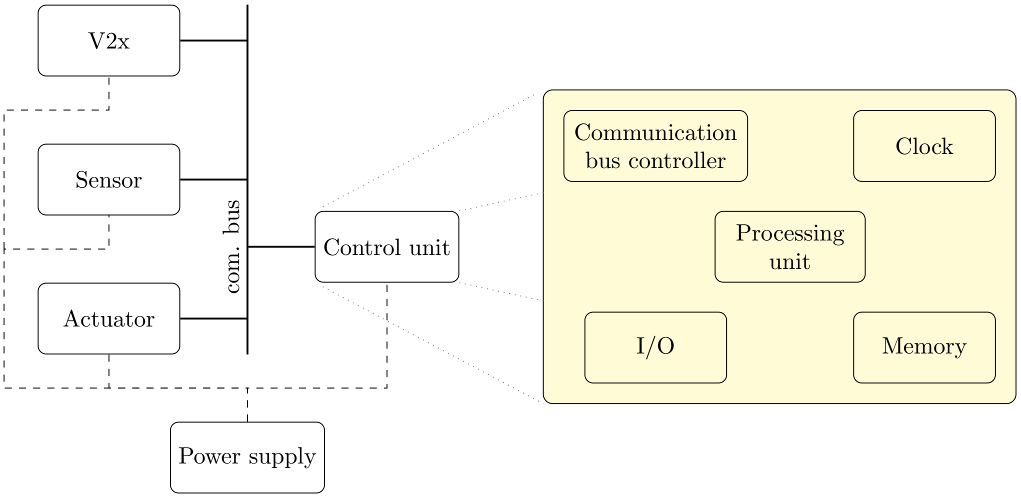

Figure 3.1: Generic components of automotive electronic systems including nodes, communication bus, and power supply. The expanded view of the control unit node shows some of the constituent hardware parts of this node. Also the sensor, actuator, and V2x nodes generally share this set of hardware parts.

ure. When a component or a complete system fails, its delivered service deviates from the correct (intended) in some way. The way in which a component or system fails is called a *failure mode*. Examples of failure modes of automotive systems are given in Table 3.1.

Table 3.1: Examples of failure modes for components of automation

Component	Failure mode examples [6, 9, 43]
Sensor	Out of range, Stuck in range, Offset, No output
Actuator	No response, Response stuck, Offset
Communication	Loss, Delay, Corruption
Power supply	Under and over voltage, Voltage drift, Power spikes
Processing unit	Stuck, No software code execution, Execution too slow
Memory	Stuck high or low, Bit flips
I/O	Stuck high or low, Drift
Clock	Stuck, Incorrect frequency, Period jitter

An indication of what can fail in a highly automated vehicle was presented by Lygeros, Godbole, and Broucke [30]. Their analysis of faults in an automated highway system (AHS) focused on the system capabilities that may be affected by faults. This included sensor capabilities such as measuring of velocity and relative distance to other vehicles, actuator capabilities including braking, throttle, and steering, and finally communication capabilities which for the AHS was infrared and radio.

3.2 Attaining dependable automation

Means to attain dependability may be described as fault prevention, fault tolerance, fault removal, or fault forecasting [38]. Fault removal and fault forecasting serve as means to justify the dependability of the system, i.e., provide confidence that the functional and dependability requirements are adequate and met. The two concepts for providing dependability are fault prevention and fault tolerance. Fault prevention is applied to prevent the occurrence or introduction of faults by means of a rigorous development process or by appropriate design principles. The purpose of fault tolerance on the other hand, is to avoid failures when faults are present. The use of redundancy is one approach to achieve fault tolerance. For vehicle automation this may include redundancy of sensors and actuators but also other components such as power supplies, communication buses, and control units, see Section 2.4.

Fault tolerance and fault prevention measures applied to vehicle automation often aim at ensuring safety. However, availability (readiness for correct service) and reliability (continuity of correct service) are two related attributes of dependability that are also commonly considered. Improving one of these attributes does not necessarily have to improve the other and the result may be a tradeoff [38]. It can for example be safer to disable (at the expense of availability) automation under some conditions, rather than to allow it to operate with poor reliability. Disabling automation may be a viable approach when the driver can safely take over control of the vehicle (see Section 2.4). For high levels of automation where the driver cannot be expected to take over, availability and reliability are both crucial to safety. As a result, the requirements on dependability are stricter for higher levels of automation. Here, the necessary level of fault tolerance may be achieved by including an alternative control system that maintains safety in case the nominal automation system fails [44]. This alternative control system could for example bring the vehicle to a safe stop by the side of the road.

3.3 Functional safety

Functional safety is the part of a system's dependability that is concerned with safety of the service that the system delivers [11]. If a system fails to deliver its intended service this can cause a *hazard*, here defined as a potential source of harm. An example of a hazard relevant for functional safety is loss of braking capability due to a failure of the brake system. Hazards related to electric shock, toxicity, fire, and heat are not part of functional safety unless directly caused by a service failure.

One of the measures that the automotive industry has implemented to achieve an acceptable level of functional safety is the use of a rigorous development process, defined by commonly accepted guidelines and standards [9, 45]. These guidelines and standards typically define a safety process that complements the overall development process. Identification and classification of hazards caused by failures is a fundamental part of this safety process. The process identifies what hazards need to be considered and also determines the amount of effort that needs to be dedicated to avoiding the occurrence of these hazards. The amount of effort is given by a risk assessment of the hazards. In conclusion, this means that each individual hazard identifies an issue that must be considered, whereas the hazard with the highest risk sets the required amount of effort for avoiding the hazards.

3.3.1 Risk function

The concept of risk is defined as a combination of the probability of harm to persons and the potential severity of that harm [9, 45]. In order to perform risk assessment, this can be formulated as a function (F) of the three parameters, frequency of occurrence (f), ability of the persons involved to control the situation and avoid harm (C), and severity of the potential harm (S):

$$R = F(f, C, S)$$

The frequency parameter (f) can be further subdivided into the failure rate (λ) of the system causing the hazard and the probability of being exposed (E) to a situation where the hazard can cause harm. The resulting function is the following:

$$R = F(\lambda, E, C, S)$$

This representation of risk and its factors are illustrated in Figure 3.2. A *hazardous event* is in this case a state where people are exposed to a hazard. Unless the driver or other involved persons are able to control the situation, an *accident* will occur, where severity represents the amount of harm.

When risk is to be assessed, the individual factors of the risk function are estimated. Exposure is determined by analyzing the operational situations of the vehicle, to find out how often the situation is such that the hazard

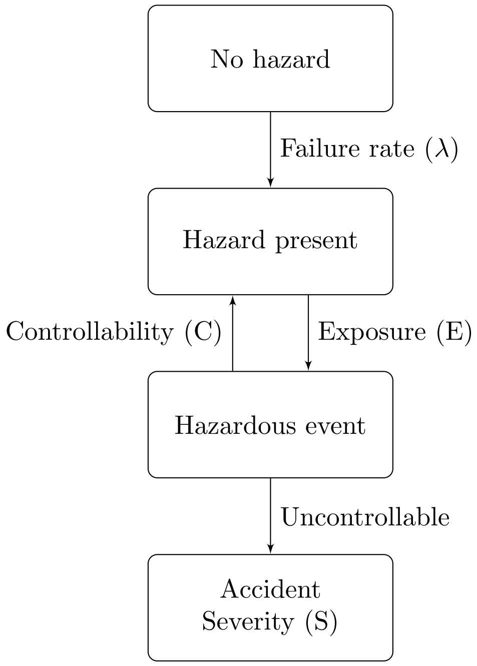

Figure 3.2: Model of risk function for vehicle hazards. Adapted from [9, 45].

may cause harm. Severity is assessed by considering the potential amount of harm on a scale from no injuries to life threatening. Controllability is determined by assessing the percentage of drivers or other persons that would control the hazardous event.

Papers 1, 2, and 3 give some guidance on how to assess controllability in automated driving. The results of Paper 1 indicate that drivers may fail to respond in a hazardous event because they are not aware of the full functionality of automation. Paper 2 found that when longitudinal automation partially failed to decelerate, fewer drivers managed to control the situation than when automation completely failed to decelerate. A conclusion of Paper 3 is that an increased level of automation leads to decreased controllability.

Chapter 4

Safety of transitions to manual driving

It is easy to illustrate why transitions from automated to manual driving can be hazardous. Imagine being the driver of a highly automated car when suddenly, in the middle of a busy intersection, automation disengages without notice, requiring you to take over control. This situation is an extreme example given to show the potential safety implications of inappropriate transitions to manual control. Nonetheless, it is important that drivers are aware and capable of taking over when automation disengages. A vehicle that is not operated by either an automation system or a human driver may quickly enter into a hazardous event.

This thesis focuses on driver takeovers specifically in situations when automation fails. However, there are other, more frequently occurring situations that also involve driver takeover. Situations where automation reaches its functional limitations are typical examples. Specifically for the ACC, its ability to adjust to stationary objects is limited and therefore requires the driver to take over when approaching stationary vehicles, e.g., a queue of vehicles. It is expected that also higher levels of automation will have functional limitations [27–29]. A difference compared to ACC may be that systems providing a higher level of automation have the ability to detect when the vehicle approaches its functional limitations. This ability would allow the system to alert the driver in due time before exceeding the limitations. Still, it is essential that the driver and the automation system have a common view about who has control of the vehicle.

The following sections of this chapter present theory on driving behavior relevant in the context of driver takeovers. This is followed by results from studies of driver takeovers before the chapter ends with a section on how to improve safety of takeovers.

4.1 Related theory on driving behavior

When automation is introduced to assist or replace the human operator it often affects human behavior [15, 46]. This is true also for vehicle automation where the role of the driver changes as the task of driving is different in manual compared to automated modes (see for example [23, 47]). Instead of only involving direct control of the vehicle, the driving task also involves interaction with automation. This has implications for driving behavior that may affect safety.

An effect of automation related to driving behavior that is argued by Parasuraman and Manzey [48] is *complacency*. Typically operationalized as poorer detection of malfunctions under automation than under manual control, complacency has been used to explain the lack of driver response to vehicle automation failures [19]. The presence of complacency has primarily been observed in a multitask environment (i.e., the driver is responsible for both automated and manual tasks) with high workload, where drivers actively reallocate their attention away from the automated and towards the manual tasks [48].

Degraded driving performance as a result of the implementation of automation has also been explained by the *out-of-the-loop performance problem*. Linked by Endsley and Kiris [14] to "loss of manual skills and loss of awareness of the state and processes of the system", this potential problem with automation was identified as a contributing factor to the results in Paper 3. It was shown in Paper 3 that a higher level of automation negatively affected driving performance in situations with automation failure.

In addition to complacency and situational awareness, driving behavior may be explained by the driver's *mental model* of automation. The mental model is used to predict system behavior, guide drivers' actions [49], and is important for drivers' ability to detect automation failures. A driver that detects a difference between predicted and actual behavior may question the accuracy of the mental model but with confidence in the model, he or she may question whether the actual behavior of automation is correct, i.e., question if automation is failing. The results of Paper 1 suggest that some drivers with an ACC system in their vehicle have a somewhat rudimentary mental model of the system and could therefore overlook signs of failure.

Developing an accurate mental model of automation is achieved through both theoretical information (e.g., from a user manual) and experience of use [50, 51]. In order for experience of use to improve the model, the driver needs feedback from automation. As the driver interacts with automation and receives feedback about how the vehicle behaves in automated mode, the driver learns how automation responds to various traffic situations. Additionally, there is research suggesting that providing feedback about vehicle and automation states on in-vehicle displays have a positive effect of drivers' ability to control failures and to deal with functional limitations of automation [52, 53]. This will be further examined in Section 4.3.

4.2 Studies of transitions to manual driving

For a transition to manual driving to be safe, the driver has to recognize the need for a takeover as well as apply the correct actions. The time available to the driver to take over control before an accident occurs is essential to the success of the takeover [54]. The ability of the driver to predict the takeover and the driver's previous experience of taking over are also important. In manual driving, it has been shown that drivers are faster at applying braking when the event they are responding to is expected, i.e., the driver can predict its occurrence [55]. The same effect is observed in automated driving where drivers have been observed to respond faster to expected take over requests than to takeovers which appear as a surprise to the driver [56]. As argued in Paper 2, automation failures occur unexpectedly and the driver has no experience of taking over control when it happens. Hence, takeovers initiated by automation failures are believed to be associated with longer response times than takeovers initiated by expected events.

Takeovers initiated by functional limitations are to some extent expected takeovers as they are part of the intended functionality of automation. Drivers may have previous experience of such takeovers and can potentially predict their occurrence. Results from studies of takeovers initiated by functional limitations are therefore not necessarily representative for unexpected takeovers initiated by automation failures. Nevertheless, for a takeover initiated by a functional limitation to be expected by the driver, he or she needs to know what the limits are. As observed in Paper 1, drivers may not have this knowledge as mental models of automation may be somewhat rudimentary.

Studies of driver takeovers that focus on unexpected takeovers, initiated by automation failures, suggest that drivers do not always take over when the situation demands. It has been found that 50% of the participants of a driving simulator study did not take over when the automated vehicle (both longitudinal and lateral automation), failed to brake in order to maintain a safe distance to the vehicle ahead [19]. Another study, conducted on a test track, concluded that drivers were late in taking over control from an ACC system when the system failed and accelerated towards the vehicle ahead [23].

Inappropriate or complete lack of driver response was also observed by Stanton, Young, and McCaulder [57] in a driving simulator study of ACC failure. Their study was designed such that the drivers had to take over or otherwise collide with the vehicle ahead when the ACC incorrectly accelerated. It was found that 4 out of 12 drivers collided with the vehicle ahead. Papers 2 and 3 further analyzed driver takeovers when automation fails by studying differences between complete and partial failures, as well as differences between different levels of automation. Among the results, the two papers confirm the conclusion of previous studies that drivers cannot be assumed to constantly monitor the situation and always be ready to take over control when automation fails.

4.3 Improving safety of transitions to manual driving

Instead of relying on the driver in a takeover situation, automation can maintain some functionality to achieve safety, e.g., bring the vehicle to safe stop if the driver fails to take over [27, 29, 58]. This approach addresses safety of takeovers and will be necessary for high levels of automation, where the human driver is relieved of safety responsibilities. However, implementing such functionality will be technically challenging due to the wide range of possible traffic situations and limited capabilities of sensor systems.

An alternative approach to achieve safety of driver takeovers is to provide the driver with information. Studies of the effects of providing information to the driver have shown promising results. Seppelt and Lee [52] showed that by continuously providing feedback about the states of automation, driver performance was improved when situations where functional limitations of the ACC required driver takeover. Also, providing drivers with information about uncertainty has been demonstrated to improve safety of driver takeovers [53]. Here, participants using an ACC in a driving simulator were presented with uncertainty information about the reliability of the sensor readings. Results of the study showed that safety of takeovers was improved when drivers were provided with the uncertainty information.

Safety of driver takeovers can also be improved by alerting the driver when a takeover is necessary. An ACC developed according to ISO 15622 [37] shall for example notify the driver if it deactivates automatically or becomes unavailable due to a failure. However, for automation to be able to notify the driver, it requires that automation knows when a takeover is necessary. ACC systems that ignore stationary objects require the driver to take over when approaching stationary vehicles [23]. Because the system ignores stationary objects it is also unable to determine when the takeover is required and therefore cannot notify the driver. Such behavior will not be acceptable for higher levels of automation, where the driver is no longer required to constantly monitor automation and be prepared to resume control. Instead, automation will have to recognize its functional limitations and issue a takeover request to the driver with sufficient advance notice [27–29].

Paper 4 proposes a method to improve safety of transitions to manual driving that builds on the approaches mentioned in this section. First, it assumes the existence of functionality to maintain safety (keep the vehicle in a safe state) even if the driver fails to take over. Second, the method requires a human-machine-interface for notifying the driver of requests to take over. The contribution of Paper 4 is that it adds a method to assess whether the individual driver is capable of taking over control in a given situation. If the driver is not expected to be capable of taking over, safety is maintained by keeping the vehicle in an automated mode of operation. The method proposed in Paper 4 requires automation to have such a mode of operation, where safety is maintained despite the lack of driver takeover. Thus, the method is primarily intended for high levels of automation, where such a mode is available [27, 29].

4.3.1 Driver capability

The framework for safer transitions to manual driving, presented in Paper 4, uses an estimate of driver capability to determine whether a driver takeover can be performed safely or not. Here, driver capability refers to the capability of the driver to safely control the vehicle in a given traffic situation. The capability is expressed mathematically, as a subset of the vehicle's state-space, denoted Driver-Controllability-Set (DCS). If the vehicle states belong to the DCS the driver is expected to be capable of controlling the situation. If vehicle states are outside the DCS, it is uncertain whether the driver is capable of safely controlling the vehicle in the situation. A schematic illustration of the sets is provided in Figure 4.1, where $\mathcal{V}$ and $\mathcal{D}$ denote the vehicle's state space and the DCS, respectively. The figure also shows two trajectories (T1 and T2), where T1 represents a situation where the vehicle states start and remain within $\mathcal{D}$, whereas T2 represents a situation where the vehicle states exit $\mathcal{D}$. Driver takeovers are only assessed as safe for T1. Here the driver is given time to take over control of the vehicle since the vehicle states remain within $\mathcal{D}$. For T2 it is uncertain whether the driver will be capable of taking over since vehicle states leave the set that is considered controllable by the driver.

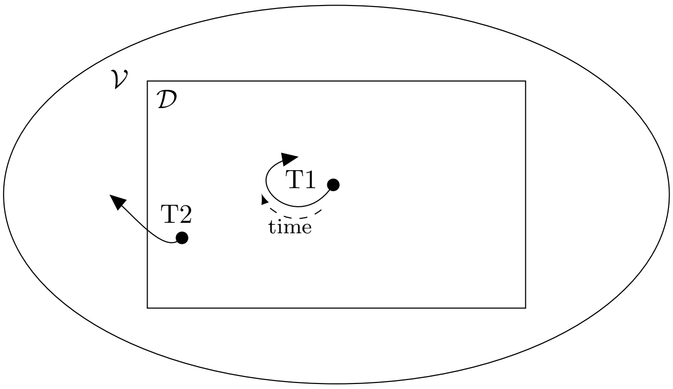

Figure 4.1: Schematic illustration of vehicle state-space and driver-controllability-set.

Chapter 5

Summary of included papers

This chapter provides brief summaries of the appended papers. Full versions of the papers are included in Part II.

Paper 1 Exploring end-user experiences: self-perceived notions on use of adaptive cruise control systems

Summary

This paper explores drivers' experiences of using vehicle automation systems. It was expected that drivers' use of automation would change with time-of-use. The study therefore engaged drivers with experience of commercially available ACC systems. A total of 17 drivers took part in the study which was conducted as three focus group interview sessions.

The study focused on four topics: usage of the system, trust in the system, implications of the ACC's functional limitations, and changes in behavior after use.

Concerning usage of the system, most participants reported using the ACC primarily on rural roads when traffic density was not high. However, others gave accounts of using it in roundabouts and in high-density traffic.

Related to trust, some drivers stated that they believed the system could not fail in an unsafe manner, whereas others indicated lower levels of trust. Trust was also found to be linked to functional limitations, as drivers felt they could put more trust in the system when they learned about limitations in its functionality. Even if these limitations are clearly stated in the manual, users learned about them after using the system in situations it was not designed for. The study also indicated that some drivers had somewhat rudimentary mental models of the system. As a consequence, these drivers would likely not be able to detect automation failures since they were not fully of aware of the correct functionality of the ACC.

Author's contribution

The study was carried out by the thesis author in collaboration with N. Strand. This included all stages of the study, from designing and planning it, to analysis of the collected data. The paper was mainly written by N. Strand with input from the thesis author.

Paper 2 Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance

Summary

Previous research has found that drivers may have problems taking over control of the vehicle when automation fails, see Chapter 4. The results of Paper 1 also indicate that some drivers are ill-prepared to respond to automation failures.

Paper 2 describes a driving simulator study investigating ACC-related failures. While the previous studies have focused on one type of failure each (i.e., Stanton, Young, and McCaulder [57] and Rudin-Brown and Parker [23] looked at an acceleration failure and Waard *et al.* [19] looked at a deceleration failure), this paper compared the outcome of unintended acceleration, complete deceleration failure, partial deceleration failure, and speeding failure.

The purpose of the study was to analyze the effect of the failures and identify differences between the four types of failures. The analysis was focused on the strategy applied by the drivers, i.e., what response they chose to apply to control the hazardous events caused by the failures.

Results showed that the participating drivers primarily used steering to avoid collisions when the ACC failed to decelerate, and when the ACC incorrectly started to accelerate towards a preceding vehicle. It was also found that the subjects were more successful in controlling a complete deceleration failure compared to a partial deceleration failure. This suggests that safety can be improved by forcing partial deceleration failure into complete deceleration failure. However, the subjects colliding after a partial deceleration failure had a much reduced impact speed compared to those exposed to a complete deceleration failure. This, on the other hand, suggests that partial deceleration failures may be less critical.

Author's contribution

The study was carried out by the thesis author in collaboration with N. Strand. This included all stages of the study, from designing and planning it, to analysis of the collected data. The paper was written by the thesis author.

Paper 3 Semi-automated versus highly automated driving in critical situations caused by automation failures

Summary

The results of Paper 2 indicated that a partial deceleration failure was more difficult for drivers to control than a complete deceleration failure. A follow-up study was conducted to further investigate this difference between deceleration failures and to also look at the effect of level of automation on driver takeovers. An experimental design with two levels of automation and three degrees of deceleration failure was set up. An ACC system and a TJA (Traffic Jam Assist) system were used as a lower and higher level of automation, respectively. For the failures, a moderate, a severe, and a complete failure to decelerate were used in the experiments.

Results of this study did not observe a significant difference between the deceleration failures, i.e., a partial failure were not found to be less controllable than a complete deceleration failure. No single reason explained the inconsistency between the studies; instead it was argued that differences in driving simulators, differences in scenarios, and differences between implementations of automation may have contributed.

The effect of level of automation was found to be significant, with more safety critical and fewer successful takeovers with higher level of automation. The out-of-the-loop performance problem caused by loss of situational awareness, described in Section 4.1, was believed to have contributed to this effect.

A conclusion from this result was that lateral automation affects driver takeovers of longitudinal control. The automation failures only affected longitudinal automation. Still the group that drove with both longitudinal and lateral automation (TJA) performed worse than the group that drove with only longitudinal automation (ACC).

Author's contribution

The study was carried out by the thesis author in collaboration with N. Strand. This included all stages of the study, from designing and planning it, to analysis of the collected data. The paper was jointly written by the thesis author and N. Strand.

Paper 4 Safe Transitions from Automated to Manual Driving using Driver Controllability Estimation

Summary

Papers 1, 2, and 3 all indicate that driver takeovers, when vehicle automation fails, may be hazardous. At the same time, a successful takeover can ensure that the failing automation system is contained and prevented from causing a hazard. Another benefit of driver takeover is that the vehicle is kept operational. After a successful takeover, the driver can continue to drive the vehicle manually.

Considering these benefits while respecting the potential problems with driver takeovers, it is desirable to be able to assess when a takeover is safe. Paper 4 proposes a method to perform such an assessment using an estimate of the driver's capability to control the vehicle. It is recognized that capabilities vary between individuals and an estimation is therefore online adapted. While the vehicle is operated in manual mode (i.e., the driver is in control), data on safety-related vehicle states are collected. The distribution of the collected data reveals what vehicle states the driver has experience of and typically operates under. The driver's capability is expressed as the subset of the vehicle's state space that is typically used by the individual driver, defined as the Driver-Controllability-Set (DCS), see Section 4.3.1.

The assessment of whether the driver can safely take over is performed by checking if the states of the vehicle are within DCS. This involves the prediction of future vehicle states over the time horizon that the takeover is assumed to require to complete. Finally, it is checked whether the current and predicted vehicle states are within DCS. If they are, the driver is deemed capable of taking over control of the vehicle.

The method for estimating DCS was evaluated on data from four drivers, showing that the method successfully finds each drivers typical region of operation. One of the four drivers was also used to evaluate the assessment of whether a takeover is safe. Given the limited scale of evaluation, further validation is necessary. Nevertheless, results indicate that the method is able to assess when takeovers can be performed safely.

Author’s contribution

The work behind the paper, including development of ideas, planning of experiments, and collection and analysis of data, was performed by the thesis author. Most of the paper was written by the thesis author.

Chapter 6

Concluding remarks

This chapter concludes the thesis by presenting its contribution and suggesting directions for future research.

6.1 Contribution

The goal of this thesis is to improved safety of transitions to manual driving when vehicle automation fails. This is achieved by first contributing to the understanding of driving behavior in takeover situations. Second, based on the improved understanding, present a method for assessing the safety of given control to the driver when automation fails. The method can be used to avoid unsafe transitions from automated to manual driving when the driver is incapable of taking over.

On the topic of understanding driving behavior, the first contributions of this thesis concern some of the underlying processes behind drivers' responses to failing automation:

- Through interviews with users of vehicle automation it was found that drivers have been involved in critical situations because they, as a result of using automation, did not pay enough attention to the road ahead. The results of Paper 1 confirm that this effect, which is a well know side effect of automation and which has been observed in other domains (e.g., aviation), is present also in road vehicles with the type of automation provided by ACC.

- Drivers' mental model of vehicle automation may be lacking important aspects even after several months of usage. The testimonials from users of ACC systems reported in Paper 1 indicate that drivers' mental model, including their understanding of system capabilities and functional limitations may be incomplete or inaccurate. This has implications for drivers' ability to detect and diagnose failures of automation. Without a complete and accurate mental model, the driver lacks the necessary knowledge to distinguish faulty from correct system behavior.

While these contributions give an indication of how drivers may control automation failures, the following contributions specifically show the effects of failures.

- Steering may be a commonly applied strategy by drivers when they are faced with a hazardous event in which longitudinal automation fails. This conclusion was drawn in Paper 2 after studying driving behavior in a driving simulator equipped with an ACC for longitudinal automation. In situations where automation failed to decelerate for a braking preceding vehicle and the adjacent lane was free from traffic, steering was the most commonly applied strategy by the drivers. A safety implication of applying steering, as opposed to braking, is that the hazardous event may reappear the next time automation is required to decelerate. If the driver instead applies braking, this is typically interpreted as a signal to disengage longitudinal automation and give control to the driver.

- The probability that drivers control a hazardous event caused by a failure of automation to decelerate, may depend on the extent of the failure, i.e., how much the level of deceleration deviates from the correct. Paper 2 compared a partial deceleration failure with a complete deceleration failure and observed more collisions after a partial deceleration failure than after a complete deceleration failure. However, the subsequent study, reported in Paper 3, compared three levels of deceleration failures and did not observe an increased number of collisions for partial compared to complete deceleration failures.

- An increased level of automation has a negative effect on controllability in hazardous events caused by deceleration failures. The study outlined in Paper 3 showed that fewer drivers controlled hazardous events caused by deceleration failures when the level of automation was increased. The two levels of automation compared in the study were longitudinal automation and a combination of longitudinal and lateral automation. The conclusion was that lateral automation has a negative effect on driver controllability for hazardous events cased by longitudinal automation failures.

This far the contributions have focused on the effects of failing automation and associated driver responses. A relationship has been identified between the outcome of a hazardous event caused by failing automation, the type of automation provided in the vehicle, the type of failure occurring, and the response applied by the driver. With these findings taken into account, the following contributions are made on the topic of improving safety of transitions to manual driving:

- A framework for deciding, in a given driving situation, if it is safe to transfer control from the automation system to the driver. The framework is presented in Paper 4 and proposes a decision logic that is based on an estimate of the individual driver's capability to control the vehicle.

- A method to estimate drivers' takeover capability that adapts to the individual driver, see Paper 4. While the driver operates the vehicle in manual mode, the capability of the driver is estimated as the subset of the vehicle's state space where the driver typically operates. Takeovers conducted within this subset are considered safe from a driver capability perspective since the driver normally operates the vehicle manually in this region of the state space.

6.2 Future work

The aim of Papers 1, 2, and 3 was to build knowledge on vehicle automation in general. For practical reasons, the studies investigated the two systems ACC and TJA. Future work should also look at other systems and especially higher levels of automation, where the driver is not required to constantly supervise automation. An important issue here is how much time the driver requires to safely take over control. This time probably depends on several factors including the situation, the state of the driver, and the capabilities of the driver.

While the method proposed in Paper 4 considers the capabilities of the driver in takeover situations, it does not take into account the current state of the driver. Driver state (i.e., drowsiness/fatigue and distraction) is recognized as an important factor to the success of a driver takeover [59] and should be considered for future work.

The approach to driver capability estimation proposed in Paper 4 should also be the subject of future research. Studies should be conducted using driving simulators as well as with real vehicles to validate the approach on a larger number of drivers and under varying driving conditions.

Another interesting direction for future work is to extend the framework presented in Paper 4 with a method to steer the states of the vehicle into the set that is controllable by the driver. Currently the framework only includes a method to give a yes or no answer to whether the driver is capable of taking over. If it is found that the driver is not capable of taking over, it may still be possible to move the vehicle into a state that is controllable by the driver and delay the takeover until this state is reached. A trivial example can be to brake the vehicle in order to increase the distance to a preceding vehicle. More involved maneuvers may use both longitudinal and lateral control to reach a state where the driver can take over control of the vehicle.

References

[1] A. Vahidi and A. Eskandarian, “Research advances in intelligent collision avoidance and adaptive cruise control”, *IEEE Trans. Intell. Transp. Syst.*, vol. 4, no. 3, pp. 143–153, 2003.

[2] Toyota Motor Corporation, *Lane Keeping Assist*, 2013. [Online]. Available: `http://www.toyota-global.com/innovation/safety_technology/safety_technology/technology_file/active/lka.html` (visited on 02/05/2014).

[3] J. Markoff, “At High Speed, on the Road to a Driverless Future”, *New York Times*, 2013.

[4] E. Coelingh and S. Solyom, “All aboard the robotic road train”, *IEEE Spectr.*, vol. 49, no. 11, pp. 34–39, 2012.

[5] C. A. Miller and R. Parasuraman, “Designing for flexible interaction between humans and automation: delegation interfaces for supervisory control.”, *Hum. Factors*, vol. 49, no. 1, pp. 57–75, 2007.

[6] S. Shladover, “Automated vehicles for highway operations (automated highway systems)”, *Proc. Inst. Mech. Eng. Part I J. Syst. Control Eng.*, vol. 219, pp. 53–75, 2005.

[7] R. Horowitz and P. Varaiya, “Control design of an automated highway system”, *Proc. IEEE*, vol. 88, no. 7, pp. 913–925, 2000.

[8] P. Varaiya, “Smart cars on smart roads: problems of control”, *IEEE Trans. Automat. Contr.*, vol. 38, no. 2, pp. 195–207, 1993.

[9] ISO, *ISO 26262: Road vehicles - Functional safety*, 2011.

[10] W. Spiessl and H. Hussmann, “Assessing error recognition in automated driving”, *IET Intell. Transp. Syst.*, vol. 5, no. 2, p. 103, 2011.

[11] N. Storey, *Safety Critical Computer Systems*. Boston, MA: Addison-Wesley Longman Publishing Co., Inc., 1996, p. 453.

[12] K. Heckemann, M. Gesell, T. Pfister, K. Berns, K. Schneider, and M. Trapp, “Safe Automotive Software”, in *Knowledge-Based Intell. Inf. Eng. Syst.* Ser. Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2011, pp. 167–176.

[13] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, “A model for types and levels of human interaction with automation”, *IEEE Trans.*

Syst. Man, Cybern. - Part A Syst. Humans, vol. 30, no. 3, pp. 286–297, 2000.

[14] M. R. Endsley and E. O. Kiris, “The Out-of-the-Loop Performance Problem and Level of Control in Automation”, *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 2, pp. 381–394, 1995.

[15] R. Parasuraman and V. Riley, “Humans and Automation: Use, Misuse, Disuse, Abuse”, *Hum. Factors*, vol. 39, no. 2, pp. 230–253, 1997.

[16] H. B. Pacejka, *Tyre and Vehicle Dynamics.* 2005, p. 672.

[17] R. Rajamani, *Vehicle Dynamics and Control*, F. F. Ling, Ed., ser. Mechanical Engineering Series. New York: Springer-Verlag, 2006, p. 471.

[18] E. Coelingh, A. Eidehall, and M. Bengtsson, “Collision Warning with Full Auto Brake and Pedestrian Detection - a practical example of Automatic Emergency Braking”, in *Proc. 13th Int. IEEE Conf. Intell. Transp. Syst.*, Ieee, 2010, pp. 155–160.

[19] D. de Waard, M. van der Hulst, M. Hoedemaeker, and K. A. Brookhuis, “Driver Behavior in an Emergency Situation in the Automated Highway System”, *Transp. Hum. Factors*, vol. 1, no. 1, pp. 67–82, 1999.

[20] O. Carsten, F. C. H. Lai, Y. Barnard, a. H. Jamson, and N. Merat, “Control Task Substitution in Semiautomated Driving: Does It Matter What Aspects Are Automated?”, *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 54, no. 5, pp. 747–761, 2012.

[21] F. Breyer, C. Blaschke, B. Farber, J. Freyer, and R. Limbacher, “Negative Behavioral Adaptation to Lane-Keeping Assistance Systems”, *IEEE Intell. Transp. Syst. Mag.*, vol. 2, no. 2, pp. 21–32, 2010.

[22] G. Francesco, A. Simões, C. Manuel, and M. Leitão, “Assessing driver’s mental representation of Adaptive Cruise Control (ACC) and its possible effects on behavioural adaptations”, *Work A J. Prev. Assess. Rehabil.*, vol. 41, pp. 4396–4401, 2012.

[23] C. M. Rudin-Brown and H. A. Parker, “Behavioural adaptation to adaptive cruise control (ACC): implications for preventive strategies”, *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 7, no. 2, pp. 59–76, 2004.

[24] M. Hoedemaeker and K. A. Brookhuis, “Behavioural adaptation to driving with an adaptive cruise control (ACC)”, *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 1, no. 2, pp. 95–106, 1998.

[25] N. Dragutinovic, K. A. Brookhuis, and M. P. Hagenzieker, “Behavioural effects of Advanced Cruise Control Use - A meta-analytic approach”, *Eur. J. Transp. Infrastruct. Res.*, vol. 5, pp. 267–280, 2005.

[26] F. Flemisch, J. Kelsch, C. Löper, A. Schieben, and J. Schindler, “Automation spectrum , inner / outer compatibility and other potentially useful human factors concepts for assistance and automation”, in *Hum.*

Factors Assist. Autom. D. de Waard, F. Flemisch, B. Lorenz, H. Oberheid, and K. Brookhuis, Eds., Maastricht, the Netherlands: Shaker Publishing, 2008, pp. 1–16.

[27] T. M. Gasser, C. Arzt, M. Ayoubi, A. Bartels, L. Bürkle, J. Eier, F. Flemisch, D. Häcker, T. Hesse, W. Huber, C. Lotz, M. Maurer, S. Ruth-Schumacher, J. Schwarz, and W. Vogt, "Legal consequences of an increase in vehicle automation (English translation)", Tech. Rep., 2013.

[28] National Highway Traffic Safety Administration, *Preliminary Statement of Policy Concerning Automated Vehicles*, 2013.

[29] SAE International, *SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, 2014.

[30] J. Lygeros, D. Godbole, and M. Broucke, "A Fault Tolerant Control Architecture for Automated Highway Systems", *IEEE Trans. Control Syst. Technol.*, vol. 8, no. 2, pp. 205–219, 2000.

[31] B. Song, J. K. Hedrick, and A. Howell, "Fault Tolerant Control and Classification for Longitudinal Vehicle Control", *J. Dyn. Syst. Meas. Control*, vol. 125, pp. 320–329, 2003.

[32] R. Hayama, M. Higashi, S. Kawahara, S. Nakano, and H. Kumamoto, "Fault-tolerant automobile steering based on diversity of steer-by-wire, braking and acceleration", *Reliab. Eng. Syst. Saf.*, vol. 95, no. 1, pp. 10–17, 2010.

[33] T. Nothdurft, P. Hecker, S. Ohl, F. Saust, M. Maurer, A. Reschka, and J. R. Böhmer, "Stadtpilot: First fully autonomous test drives in urban traffic", in *Proc. 2011 14th Int. IEEE Conf. Intell. Transp. Syst.*, Washington, D.C.: IEEE, 2011, pp. 919–924.

[34] R. Kianfar, B. Augusto, A. Ebadighajari, U. Hakeem, J. Nilsson, A. Raza, R. S. Tabar, N. V. Irukulapati, C. Englund, P. Falcone, S. Papanastasiou, L. Svensson, and H. Wymeersch, "Design and Experimental Validation of a Cooperative Driving System in the Grand Cooperative Driving Challenge", *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 994–1007, 2012.

[35] U. Franke, D. Pfeiffer, C. Rabe, C. Knoeppel, M. Enzweiler, F. Stein, and R. G. Herrtwich, "Making Bertha See", in *Proc. IEEE ICCV Work. Comput. Vis. Autounomous Veh.*, Sydney, Australia, 2013, pp. 1–10.

[36] M. Brännström, E. Coelingh, and J. Sjöberg, "Model-Based Threat Assessment for Avoiding Arbitrary Vehicle Collisions", *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 3, pp. 658–669, 2010.

[37] ISO, *ISO 15622: Transport information and control systems - Adaptive Cruise Control systems - Performance requirements and test procedures*, 2002.

[38] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing”, *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 1, pp. 11–33, 2004.

[39] T. L. Fruehling, “Delphi Secured Microcontroller Architecture”, in *SAE Tech. Pap. 2000-01-1052*, Detroit, MI, 2000.

[40] R. Isermann, R. Schwarz, and S. Stolzl, “Fault-tolerant drive-by-wire systems”, *IEEE Control Syst. Mag.*, vol. 22, no. 5, pp. 64–81, 2002.

[41] T. Yoshida, H. Kuroda, and T. Nishigaito, “Adaptive Driver-assistance Systems”, *Hitachi Rev.*, vol. 53, no. 4, pp. 212–216, 2004.

[42] E. G. Leaphart, B. J. Czerny, J. G. D’Ambrosio, C. L. Denlinger, and D. Littlejohn, “Survey of Software Failsafe Techniques for Safety-Critical Automotive Applications”, in *SAE Tech. Pap. 2005-01-0779*, SAE 2005 World Congress, 2005.

[43] S. E. Shladover, “Cooperative (rather than autonomous) vehicle-highway automation systems”, *IEEE Intell. Transp. Syst. Mag.*, vol. 1, no. 1, pp. 10–19, 2009.

[44] L. Sha, “Using simplicity to control complexity”, *IEEE Softw.*, vol. 18, no. 4, pp. 20–28, 2001.

[45] MISRA, *Guidelines for safety analysis of vehicle based programmable systems*. Warwickshire, UK: MIRA Limited, 2007.

[46] L. Bainbridge, “Ironies of automation”, *Automatica*, vol. 19, no. 6, pp. 775–779, 1983.

[47] M. Vollrath, S. Schleicher, and C. Gelau, “The influence of cruise control and adaptive cruise control on driving behaviour - A driving simulator study”, *Accid. Anal. Prev.*, vol. 43, no. 3, pp. 1134–9, 2011.

[48] R. Parasuraman and D. H. Manzey, “Complacency and Bias in Human Use of Automation: An Attentional Integration”, *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 52, no. 3, pp. 381–410, 2010.

[49] D. A. Norman, “Design rules based on analyses of human error”, *Commun. ACM*, vol. 26, no. 4, pp. 254–258, 1983.

[50] D. A. Norman, “The ’Problem’ with Automation: Inappropriate Feedback and Interaction, not ’Over-Automation’”, *Philos. Trans. R. Soc. B Biol. Sci.*, vol. 327, no. 1241, pp. 585–593, 1990.

[51] B. Rajaonah, F. Anceaux, and F. Vienne, “Trust and the use of adaptive cruise control: a study of a cut-in situation”, *Cogn. Technol. Work*, vol. 8, no. 2, pp. 146–155, 2006.

[52] B. D. Seppelt and J. D. Lee, “Making adaptive cruise control (ACC) limits visible”, *Int. J. Hum. Comput. Stud.*, vol. 65, no. 3, pp. 192–205, 2007.

[53] J. Beller, M. Heesen, and M. Vollrath, “Improving the Driver-Automation Interaction: An Approach Using Automation Uncertainty”, *Hum. Factors J. Hum. Factors Ergon. Soc.*, 2013.

[54] C. Gold, D. Dambock, L. Lorenz, and K. Bengler, “"Take over!" How long does it take to get the driver back into the loop?”, *Proc. Hum. Factors Ergon. Soc. Annu. Meet.*, vol. 57, no. 1, pp. 1938–1942, 2013.

[55] M. Green, “"How Long Does It Take to Stop?" Methodological Analysis of Driver Perception-Brake Times”, *Transp. Hum. Factors*, vol. 2, no. 3, pp. 195–216, 2000.

[56] F. Flemisch, S. Griesche, M. Heesen, A. Kaussner, J. Niemann, I. Petermann, A. Schieben, and N. Schoemig, “HAVEit Deliverable D33.3 Validation of preliminary design by simulation”, European Commission, Tech. Rep., 2009, p. 115.

[57] N. A. Stanton, M. Young, and B. McCaulder, “Drive-by-wire: The case of driver workload and reclaiming control with adaptive cruise control”, *Saf. Sci.*, vol. 27, no. 2-3, pp. 149–159, 1997.

[58] F. Flemisch, M. Heesen, T. Hesse, J. Kelsch, A. Schieben, and J. Beller, “Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative control situations”, *Cogn. Technol. Work*, vol. 14, no. 1, pp. 3–18, 2011.

[59] N. Rauch, A. Kaussner, S. Boverie, and F. Flemisch, “The importance of driver state assessment within highly automated vehicles”, in *Proc. 16th World Congr. ITS*, Stockholm, 2009, pp. 1–8.

Part II

Included papers