EVS26
Los Angeles, California, May 6 - 9, 2012

Survey on fault-tolerant vehicle design

Daniel Wanner[1], Annika Stensson Trigell[1], Lars Drugge[1], Jenny Jerrelind[1]
[1]*KTH Royal Institute of Technology, School of Engineering Science, Department of Aeronautical and Vehicle Engineering, SE–100 44 Stockholm, Sweden, dwanner@kth.se*

Abstract

Fault-tolerant vehicle design is an emerging inter-disciplinary research domain, which is of increased importance due to the electrification of automotive systems. The goal of fault-tolerant systems is to handle occuring faults under operational condition and enable the driver to get to a safe stop. This paper presents results from an extended survey on fault-tolerant vehicle design. It aims to provide a holistic view on the fault-tolerant aspects of a vehicular system. An overview of fault-tolerant systems in general and their design premises is given as well as the specific aspects related to automotive applications. The paper highlights recent and prospective development of vehicle motion control with integrated chassis control and passive and active fault-tolerant control. Also, fault detection and diagnosis methods are briefly described. The shift on control level of vehicles will be accompanied by basic structural changes within the network architecture. Control architecture as well as communication protocols and topologies are adapted to comply with the electrified automotive systems. Finally, the role of regulations and international standardization to enable fault-tolerant vehicle design is taken into consideration.

Keywords: reliability, safety, wheel hub motor, diagnosis, control system

1 Introduction

In the last two decades, the electrification of automotive chassis systems enable extended functionalities and active safety systems. Recent studies have shown a reduction of single vehicle accidents of about 50% for vehicles equipped with electronic stability control systems (ESC) [1, 2], and thereby highlighting the potential of these systems. Incentives by governments, research foci of vehicle manufacturers and the shortage of natural resources support the prediction from several studies to a widespread adoption of hybrid electric and electric vehicles (HEV) as well as by-wire applications in the coming decades [3–5]. Both aspects, electrification of chassis and drive train systems, lead to higher degree of over-actuation, and thus to an increased flexibility of the vehicle behaviour.

Vehicular systems have certain requirements that shall be fulfilled during the design of a new system. The most important ones are active and passive safety, dynamic driving performance, driving dynamics and handling as well as driving comfort [6]. High system dependability is needed to fulfil these requirements. However more electric and electronic (E/E) components increase the complexity and can possibly fail. Thus the probability of a faulty vehicle is higher with the future vehicle generation. Faults of E/E components appear in general more randomly than mechanical faults. Software faults are however more systematic, as errors produced in the development phase are not uncommon. These faults can appear in different forms, both locally and globally.

The breakdown statistics of the German Automobile Club for passenger cars in 2010 show that two thirds of all breakdowns are based on E/E faults. The electrical components with battery, generator and starter motor have the highest percentage (42%) [7]. Over 20% are based on controller faults. Mechanical failures excluding punctures are rather seldom. However studying electrical machines in more detail it can be found that over 50% of all failures are mechanical due to bearings, stator windings and external equipment [8]. The power electronic con-

verter has most failures on the semiconductor level, which can also be explained by mechanical failures due to overload, temperature or moisture [9]. Thus quality of mechanical components in electrical machines and electric components for power converters is crucial for dependability of the whole system. However, it also shows the need for solutions that can handle these faults. Therefore truly inter-disciplinary research is needed to connect the application areas (such as control theory, mechatronics, vehicle dynamics) with each other [10, 11].
Fault-tolerant vehicle systems can be achieved by the combination of several measures. A holistic view shall be applied to avoid bottlenecks in the system design. Fault detection and diagnosis (FDD) defines the type of fault that can occur and its characteristics like location, time and appearance. The actual goal of the early detection and diagnosis is to have enough time to take counteractions such as reconfiguration, maintenance, repair or other operations [12]. The control system of over-actuated vehicles plays a crucial role as it has to handle the fault. The malfunctioning components and subsystems have to be considered within the control system, when controlling the vehicle. If this is not guaranteed, the vehicle might lose function even though the controller is working and the fault is diagnosed. Cooperation of all subsystems is the key for fault-tolerant vehicle design.
This paper describes premises to achieve fault-tolerance in Section 2. Different vehicle motion and fault-tolerant control approaches are presented in Section 3 as well as a brief overview of fault detection and diagnosis methods. Network architectures on controller and physical level are discussed in Section 4. Current and prospective legislation and international standards regarding the fault-tolerant discussion are depicted in Section 5, followed by conclusions.

2 Fault-tolerant design premises

High dependability of a system can be increased by fault-tolerance. A fault-tolerant system remains operational even if one or several faults occur [11]. Thus, a fault shall not lead to a system failure, instead compensation shall be achieved to continue normal or degraded operation. Fault-tolerance leads to more reliable systems and attempts to provide uninterrupted system operation [13]. The reliability of a system can be improved by a perfect, non-failing system design or by one that is tolerant towards faults. In practice the latter is preferred as a perfect modeling of complex engineering systems is not possible [10]. Redundancy and a quality oriented holistic design process are two key features to reach fault-tolerant system design.

2.1 Degradation of faults

Redundant systems are grouped into different degradation levels of fault-tolerance. Some components in a system need a higher level of fault-tolerance (e.g. brake system) than others (e.g. sunroof motor). Depending on how strict the requirements on fault-tolerance are, the following degradation levels can be distinguished:

- Fail-operational (FO) - The component stays operational after one failure, thus one failure is tolerated.
- Fail-safe (FS) - The component is brought actively or passively to a safe state, if one or more failures occur.
- Fail-silent (FSIL) - The component is switched off (externally quiet) and does not send wrong signals to the rest of the system, if one or more failures occur.

FO is necessary if no safe state can be reached directly after the component fails. For adjusting to the fault severity, FO can be split into the classes long and short time [14]. One other option is the graceful degradation [15], where the less critical functions are shut down to allocate the resources to the more critical function and maintain availability. A safe state can be reached faster and easier in the automotive domain compared to other domains, e.g. aerospace [15]. Therefore the fault-tolerance level in road vehicles is usually limited to one or two failures due to cost, weight and package reasons. However with emerging x-by-wire systems, other electronic systems can bring the system to a safe state, i.e. through a still operational unit or an active FS unit, as mechanical backup is omitted. This brings the fault-tolerance in the automotive domain to a new stage, where it has to attain more attention in the development process [16]. The FSIL principle has the advantage to appear only as one fault towards the external world, namely the shutdown of the component itself. This fault is visible for the whole system and can be intercepted by active replication of the component, i.e. redundancy. Thus a fault is localized, encapsulated and explicitly dealt with at its source. A spread of faults within the system is then not possible. This method simplifies the fault handling strategies drastically [17].

2.2 Redundancy

The goal of a fault-tolerant system is to have enough time for counteractions in the event of a serious failure, i.e. provide a ”self-repairing” capability to enable the driver to stop the vehicle safely [10]. Redundancy keeps the system operational and is reached by adding backup hardware, software, information processes and subsystems with the same function to the system as the original unit. Sensors, actuators, microcontrollers and the communication network are typical electrical and mechanical components that have a redundant design scheme [14].
The two basic types of electronic hardware redundancies are the static and the dynamic redundancy. The static redundancy has three or more parallel units with the same input, e.g. hydraulic airplane actuators. All units are active and connected to a voter, which compares the

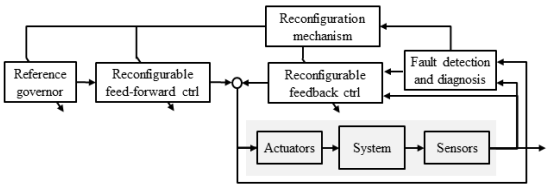

Figure 1: Fault-tolerant control scheme [18].

signals to each other. The correct signal is chosen by a majority decision. Having one-out-of-three faulty units, the voters will output the two healthy units. No sophisticated fault detection is needed in this case. Due to higher costs and weight the dynamic redundancy is often used instead [11]. Dynamic redundancy as alternative option desires less units, but more information processing within the system. If a fault is detected, the system is switched to the redundant standby unit. Two different standby systems can be distinguished. Hot standby units are continuously operating and fast switching times can be accomplished. However these units age faster, hence they are only used in safety-critical systems like aviation. The cold standby is only activated when needed, e.g. backup power generator. Therefore the start-up time is longer and two additional switches are needed, but the unit has less wear. An additional standby unit, typically added in parallel, allows the system to tolerate also an additional fault. For vehicular x-by-wire systems, the fault-tolerance with dynamics redundancy with cold standby is attractive.
Different redundancy structures can be used to increase availability. If one fault shall be tolerated, thus to fail-operational and thereafter switch to a fail-safe state, either a triplex, quadruplex or duo-duplex structure each with static redundancy or a duplex structure with dynamic redundancy can be used. However the easiest to realize is the duo-duplex (two static redundancies in parallel) structure, as no fault detection is needed and the modularity makes is simpler.
Actuators are designed as fault-tolerant if the above described redundancies are applied. Furthermore, smart sensors, that have self-diagnostic capability, are used in vehicles more often nowadays [14].

2.3 Design process

The ability to design a technical system in a fault-tolerant manner is described by the term system dependability. This includes all aspects of reliability, availability, maintainability, and safety (RAMS) for safety-critical and fault-tolerant systems. System dependability shall be given at all times [10, 16]. In order to achieve a dependable system, information about what actually can happen to the system and what that means for the behavior of the system is necessary, i.e. RAMS is crucial for the design phase of a fault-tolerant system. Several methods to analyse a system regarding RAMS, such as reliability analysis [19], hazard analysis [20], event and fault tree analysis [21] or failure mode and effect analysis [21–23], are gathered under the domain fault avoidance and removal. Usually several of these methods are combined in the development process of a new system to achieve a more detailed analysis [14, 21]. This leads to increased quality throughout the whole design process.

3 Fault-tolerant control concepts

Control systems with a feed-forward structure are generally reacting onto any kind of fault in the system with a different output signal. Feedback control on the other hand has due to the higher complexity a certain robustness, which also covers small or multiplicative faults in the actuator or the process. Sensor faults however lead directly to deviations.
An active fault-tolerant control system is required, if the fault is too large to be covered through the robustness of the controller, otherwise the dynamic behaviour becomes sluggish or less damped and might get unstable. In Figure 1 this system is illustrated. Additionally to the actuators, process, sensors and feedback controller, the active fault-tolerant control system consists of FDD methods and fault management containing decision methods and reconfiguration to keep the system operational in an acceptable way.
This section provides an overview on methodologies of vehicle motion and fault-tolerant control as well as fault detection and diagnosis.

3.1 Vehicle motion control

Vehicle motion control is originally based on functional control. Today, the integration of different functional subsystems, such as ESC or super imposed steering system [24, 25], into an enclosed and functioning automotive system gets more important with the amount of subsystems. This since functions overlap and might interfere with each other [26, 27]. The anti-lock braking system for instance is today an integral part of the ESC. Studies comparing the effects of single functional subsystems, acting mainly onto the lateral dynamics, have shown different vehicle dynamical potentials. A co-existent application of these subsystems can even lead to negative vehicle behavior; while their rule-based integration exploits the benefits to a better extent [28, 29]. The integrated chassis control approach merges single control tasks into a functional or directional control and distributes the signals according to the driving situation, the input of the driver and the dynamic limitations of every actuator. This enables safety and performance improvements simultaneously [30–34].
Bottom-up approaches are the common pragmatic approaches in the industry. The integration of existing chassis control systems with heuristic control laws is simple and enables to use existing control laws [35]. Integrated chassis control can be seen as an intermediate step striving towards a generic control [30, 36]. Integrated chassis control is developed by the industry, such as Bosch

[37], BMW [38] or Opel [39]. A main problem remains even with company specific controller design. Depending on the actuators built into the vehicle, the vehicle motion is affected and limited to different extends, which results in a huge amount of combination possibilities [40].

The more theoretical top-down approach calculates control actions by solving a model of the vehicle dynamics, which is a generic control approach. Direct access to the actuator from a centralized controller exploits the full potential efficiently. This reduces complexity and thus efforts for achieving RAMS [35, 41]. An overview of control systems in the field of aeronautics and robotics is given by [36]. One approach is the global force allocation, which is common in other over- and under-actuated vehicles, such as aircrafts [42, 43] and vessels [44]. This approach distributes global forces and moments that describe the vehicle motion, to each wheel under certain constraints and limitations. As the problem is underdetermined, optimization methods are needed to find solutions. An early application with pure torque distribution is seen in [45]. A complex optimisation algorithm for vehicles with individual torque, single wheel steering and active suspension is analysed by [46]. Constraints are given by the minimization of the adhesion potential utilization of all tyres. A slim and transparent top down control approach for integrated chassis control with an inversion based feedforward control was proposed by [40, 41, 47], and further developed in [48]. The results show considerable improvements and lead to the conclusion that more over-actuation in a vehicle configuration increases the handling performance of the vehicle in the tested manoeuver. As the optimization has no unique solution, typical constraints like minimizing the utilization of the tyre grip [40] or maximize energy-efficiency in HEV [49] has to be used for achieving reasonable results. The force allocation method was further developed for real-time application with different simplifications of the optimisation [50–54]. Other applicable control laws for the force allocation are e.g. nonlinear adaptive H∞ control theory [55], model predictive control [56, 57] and sliding mode control [58]. Recently, verification of the force allocation with scaled vehicles [50, 59] and prototypes [60] was conducted.

First combined force allocation with fault-tolerance for vehicles are considered in [40, 47]. Thereby a comparison of all useful configurations of actively and passively controlled influencing variables of vehicle dynamics can be done. The impact of actuator failures on vehicle dynamics for safety and redundancy investigations is handled by automatic on-board reconfiguration. Furthermore, the effect of actuator failures such as hydraulic or mechatronic systems acting on the vehicle dynamics can be analysed for safety and redundancy investigations.

Another goal of current research is to develop flexible control structures that can be applied to several levels of over-actuation, thus different vehicle configurations [40, 61].

3.2 Fault-tolerant control

Fault-tolerant control (FTC) strategies aim to prevent a fault from becoming a system failure. An operational system shall be guaranteed despite if one or several faults occur, thus FTC accommodates component failures automatically. They are capable of maintaining overall system stability and acceptable performance in the event of such a failure [18]. A FTC system is a holistic approach that includes control, FDD and reconfiguration of the system. FTC is divided into two different types - passive and active FTC.

3.2.1 Passive FTC

Passive FTC strategies react on a set of presumed failure modes. Their design is fixed and robustness is only given for this presumed set of failure modes. The recent developments in vehicle motion control are designed with respect to robustness and adaptability and thus can be seen as passive FTC. The control algorithm is hereby adjusted to handle certain disturbances and a class of presumed faults without fault isolation. FDD or reconfiguration is not needed for this approach; however this limits the fault-tolerant capabilities [18, 62]. Certain adaptive passive FTC systems, where an active FDD is included, are displayed here. An adaptive passive FTC including an active FDD for an electric vehicle with four individually controlled in-wheel motors is analysed in [63]. Simulation shows the reaction of the system when a fault in one in-wheel motor occurs. The FTC estimates the control gain for driving the vehicle with only small error. Thus the forces are redistributed in a manner that the faulty in-wheel motor is used as little as possible in the tested manoeuvres and the forces between tyre and road are better exploited for the other three motors. However faults appearing in HEVs, like the failure of an electric synchronous machine with permanent magnets used for propulsion, can possibly be more severe. This is why a fault-tolerant control with active reconfiguration is recommended for new electrified vehicle types in order to preserve dependability.

3.2.2 Active FTC

Active FTC strategies respond actively in real-time to the occurrence of a fault, assuming the latter is diagnosed before [62]. This type of strategy compensates faults either by selecting a pre-computed control law or by synthesizing a new one online. Transient and steady-state performance for the controlled process in normal operation and under fault condition are the desired overall goals of active FTC, often also called reconfiguration. These two modes differ significantly. The quality of the system behaviour shall be stressed under normal operation, while during fault condition the system shall survive with an acceptable (degraded) performance [64]. The first keeps the operating behaviour on an acceptable level of the vehicle performance, while the latter guarantees safety, which affects the vehicle

performance noticeably [14, 16]. Thus an acceptable solution will be provided even if the solution is not optimal [64]. Which mode and degradation level is chosen depends mainly on the overactuation level of the vehicle and the severity of one or several faults. The most serious measure will bring the failing vehicle to an immediate and safe stop, due to a severe system failure, without harming the passengers or interfering with other traffic participants [10, 14]. This enables an optimal performance of the controlled system [65]. A typical active FTC structure (Figure 1) includes:

- easy reconfigurable controller,
- a highly sensitive, but robust fault detection and diagnosis scheme,
- reconfiguration mechanism that ultimately achieves the pre-fault performance,
- a reference governor.

One critical issue is the limited amount of time for FDD and control system reconfiguration. From that, the two main design objectives can be derived. First of all, a precise FDD scheme shall be provided, which delivers information about a fault (time, type and magnitude) and the post-fault model. Secondly, the compensation of the fault-induced changes within new reconfigured control scheme shall be designed, so that the stability and acceptable closed-loop system performance can be maintained. Therefore the parameters of the controllers and, what is even more important, the structure of the new controllers (in terms of order, numbers and types) might have changed. A good summary about methods and applicable algorithms for reconfigurable control and active fault-tolerant control is provided by [18], where it is shown that a combination of different reconfigurable control algorithms for active FTC achieves the best results.
In the automotive domain, early adoption of FTC strategies is found in powertrain management [66]. Other than that, the FTC strategies are often derived from other domains. Recently more attention is brought to it through by-wire vehicles. A hybrid active FTC approach is presented by [65]. Dynamical systems often consist of a continuous and a discrete time process, where these two are connected with logical or decision-making processes, are called hybrid systems. Different hybrid systems are presented and analysed in simulation and tested in a prototype vehicle. A combination of the linear quadratic control method and the control Lyapunov function technique are applied. Four different failure modes are analysed; complete break-down of a wheel torque controller, deterioration of wheel torque controller gain, complete break-down of a steering controller and deterioration of steering controller gain. The case study shows reasonable results for these severe faults and indicates the potential of this type of control system. A model-based bond graph approach for vehicular reconfiguration is found in [67]. Residuals are generated for FDD and have to be recalculated every time a fault occurs, so that the equipment availability database is updated as well. The control system is a lateral force control, which considers slip condition of the wheels [68]. It selects the best option to reconfigure the system such that the given control objectives are achieved. An active FTC method for lateral dynamics of a nonlinear vehicle, based on a bank of two observers, is also presented by [69]. After applying the uncertain Takagi-Sugeno (T-S) fuzzy model, a robust output feedback controller is designed using linear matrix inequalities. Besides the fault detection, this control algorithm adapts the control law online and thus compensates for the fault effects. A separate controller mode is activated that guarantees stability and an acceptable level of performance. Combining passive and active FTC technique for longitudinal control is analysed in [70]. As passive FTC, a convex optimization is applied for a known class of faults. Fault classification decides if the passive FTC is capable of compensating for a non-specified fault or reconfiguration has to be activated.

3.3 Fault detection and diagnosis

A fault-tolerant control structure incorporates a fault detection and diagnosis system. The fault detection shall make a decision whether a fault has occurred or not. This objective is achieved by different types of methods that can be classified into analytical and heuristic symptom generation. The first is based on quantifiable information like measured process parameters (e.g. limit value checking and signal analysis of direct, measureable signals as well as process analysis by using mathematical process models), while the latter are based on qualitative information such as statistical data gained from experience (former faults, repairs, wear, load measures, etc.). Fault diagnosis consists of the fault isolation and fault identification and determines the type, size and location of a fault, as well as its time of detection [11, 71]. In order to process the detected fault two kinds of fault diagnosis and evaluation methods can be used. The heuristic classification methods include statistical and geometrical methods, neural networks or fuzzy logic. The second type is inference methods based on explicit conditions and conclusions, e.g. fault-tree analysis [10, 14, 16]. Selected methods are classified in Table 1. Details on the methods can be found in the corresponding technical report [72].

4 Automotive network systems

The shift towards integrated control leads to new requirements for the control architecture in order to cope with the changed complexity. Besides smart actuators, smart sensors and fault-tolerant control, the communication architecture has also to be dependable to achieve a fault-tolerant overall system.

4.1 Control architecture

The fault cycle and vehicle control are embedded in the vehicle control architecture. The structure

Table 1: Classification of FDD methods [18].

	Quantitative	Qualitative
Model-based	State estimation *-Kalman filter (normal, extended, unscented, 2-stage)* *-other observers* Parity equations Parameter estimat. *-Recurs. least square* *-Regression analysis*	Causal models *-Structural graphs* *-Fault trees* *-Qualitative physics* Abstract. hierarchy *-Structural* *-Functional*
Data-based	Statistical *-Partial least square* *-Statistical classifiers (e.g. spectrum or correlation analysis)* Neural networks	Expert Systems Fuzzy logic Pattern Recognition Time-frequency analysis Qual. trend analysis

of this architecture has evolved from a decentralized coexistent control, where each function is controlled independently from each other, to a centralized supervisory control, where all function are managed from one master controller and assigned to the appropriate subsystem. A multilayer architecture to handle the growing complexity in E/E systems is suggested by various authors [73, 74]. Such network architecture enables fault-tolerance and thus integration of the control systems described in Section 3.

4.2 Communication architecture

On the physical and data link layer dependable communication systems have to be provided in real-time. Their dependability includes deterministic and time-triggered behaviour, support for distributed control, fault-tolerant services and fast data transfer [75]. The event-triggered CAN protocol does not fulfil these requirements. Protocols with time-triggered behaviour and a global synchronized time are implemented instead. Messages describing the current state (e.g. ”brake pressure 50%”) instead of an event (e.g. ”deceleration started”) and the time slot allocation, which results in less time delays at fluctuating load conditions, enables an exact prediction of the time delay of each state message [75–77]. Communication protocols for fault-tolerant systems are designed according to the fault hypothesis, which have certain requirements describing number, type and arrival rate of tolerated faults [78]. A methodology for the development and analysis of time-triggered systems is established for existing software development process of the automotive industry [79].

4.2.1 TTCAN

The Time-Triggered CAN protocol is essentially built upon the event-triggered CAN structure with the difference that all data is sent within a time-triggered system matrix. A redundant time master ensures the deterministic behavior [80, 81]. The system matrix consists of several basic cycles that can have different amounts of deterministic and non-deterministic windows. TTCAN supports no dependability services, but implementation as middleware is possible [81]. Different TTCAN buses can be synchronized to achieve fault-tolerant TTCAN networks [82]. Transfer rates are limited to the typical CAN bandwidth of 1 Mbit/s.

4.2.2 TTP/C

The Time Triggered Protocol (TTP/C) is a pure time-triggered protocol. Safety is its main objective, thus strict deterministic sequential order leads to a low flexibility. Redundancy on two channels is given. Dependability services (Section 4.2.4) such as bus guardian, the group membership algorithm, clique avoidance algorithm and the support for mode changes are available directly in the protocol without the need of middleware [75, 80, 83]. The fault hypothesis for TTP/C is well defined and restrictive as faults have to arrive at least two rounds apart. Outside the fault hypothesis the recovery strategy is well defined with a ”never gives up” strategy as well [78, 80]. A degraded mode is then activated for keeping the system operational. Transfer rates up to 1 Gbit/s are analysed [78].

4.2.3 FlexRay

FlexRay is a robust, scalable and fault-tolerant bus system specifically designed for automotive x-by-wire applications. Like TTCAN, FlexRay implements the event-triggered function as a lower layer of the time-triggered structure. Hence, flexibility is ranked higher as the mere safety of the protocol [75, 81]. Fault-tolerance is covered by a two channel redundancy and certain integrated dependability services, i.e. bus guardian and clock synchronization. Middleware is needed for other fault-tolerant features. FlexRay can be combined with TTCAN to achieve bit rates of up to 20 Mbit/s, or work redundantly, thereby implementing fault-tolerance to the system [75].

4.2.4 Dependability services

Fault prevention is achieved by declining the members of the communication system to block it by transmitting continuously (’babbling idiot’ problem). A bus guardian mediates message transmission by an interface [76, 80, 84]. In distributed systems it is important that all nodes agree on the operational state and work together towards a common goal. Replicating certain nodes is one method [80]. Another option is to develop different algorithms that support the fault-tolerance of the protocols. Group membership provides to all non-faulty processors a consistent view of which nodes are operational and

which are not [84]. Cliques are partitioned clusters, which are not able to communicate with each other. The clique avoidance algorithm always selects one clique to win and causes all nodes of other partitions to shut down, so that a deterministic behavior is always available [85].

4.2.5 Middleware

Dependability services for x-by-wire applications are achieved by middleware, a software layer located above the platform. The automotive industry has developed a modularized architecture called AUTOSAR (AUTomotive Open System Architecture) [86]. This standardized and open software architecture enables an easy integration and update of new software and hardware modules into an existing structure. Hence prospective safety requirements for vehicles can be met, so that a high E/E system reliability is given. Due to standardized interfaces and modularity the flexibility is increased while the costs are reduced at the same time [87]. The EAST-EEA [88] and the OSEK -VDX consortium [89] are two earlier corporations between automotive partners to achieve open and standardized architectures for distributed control in vehicles. The small operating system for time-triggered applications OSEKTime and the Fault-Tolerant Communication layer (FTCom), which manages redundancy of data in the software layer, are two results of interest for dependable systems [80].

4.2.6 Network topologies

Networks have different types of topologies, with star, bus and ring as the basic topologies. The basic network topologies can be combined in different ways to exploit the advantages and minimize the drawbacks at once. These hybrid topologies have a higher fault-tolerance and specifically suited for vehicular by-wire applications [90].

5 Standards and legislation

Standards and the legislative framework are constraining the design of vehicular systems, and have to be considered. A description of upcoming and recently released regulations and the new developed standard for functional safety (ISO 26262 [91]) is presented. Without achieving perfection, complex systems always contain some sort of errors, due to lack of time and reduction of costs [11]. Thus, standards and regulations for safety-critical systems are necessary to ensure their dependability and standardize functional safety. Regulations are laws that have to be followed or considered during a lifecycle of a product, especially during the development process. The main goal of a regulation is the welfare of the society, which is in the case of road vehicles the health of humans and the environment. While regulations are mandatory, standards are recommendations. It is not only important for industry to follow regulations, but also standards are highly significant. The latter are treated as published state by lawyers, hence liability issues are reduced by following them. Standards shall simplify the development of new products and introduce a common vocabulary, which makes the intra- and inter-company communication easier.

5.1 ISO 26262

Providing safety-compliant systems in the automotive industry takes more effort with the increase of complexity. Validation and testing of critical E/E systems such as by-wire systems, active systems or ESC are challenging and shall therefore be standardized. The ISO 26262 was developed to cope with these matters. It guides the design process of a safety-critical system in order to avoid risk by systematic identification of design faults and random hardware faults. ISO 26262 addresses the needs for an automotive specific, unified, international standard that focuses on safety-critical components. Therefore the unifying standard ISO 26262 was adapted from the previous, more generic safety standard IEC 61508 to fit the specific needs of the automotive industry [92, 93]. Car manufacturers and suppliers mostly comply with ISO 26262 to reduce liability issues, thus the standard is establishing. Two of the features of the ISO 26262 are the safety lifecycle and the risk-based approach for determining risk classes [92]. The automotive safety lifecycle includes a holistic view on the safety-critical component from the management, via development, production, operation and service to decommission. Testing of the component is conducted throughout the entire process. This reduces development costs, time and mistakes and increases efficiency. The automotive safety integrity level (ASIL) is an automotive specific approach for assigning risk levels and key component of the ISO 26262. The intended functions of the system are analysed with respect to possible hazards. ASIL asks about what will happen to the driver and associated road users, if a failure arises. It is independent from the technology used and based on probability of exposure, the possible controllability by a driver, and the possible severity if a critical event occurs. The levels are defined from A to D, where D is the most critical level with the strictest testing regulations [94]. Automated ASIL allocation for multiple functions, failures and complex, hierarchical networked architectures to encourage the usage of ISO 26262 is presented in [95]. In an ISO 26262 certified development process, hardware and software components have to be qualified for the use in the overall system by testing procedures including fault injection. The so called ”proven in use” argument allows application of existing components that did not change with the ISO 26262 adoption. First results for applying ISO 26262 were summarized by [96]. As main result the centric working style with isolated tools for single analysis tasks was recomended to shift to a model centric workflow with full fine-grained traceability and supporting automatic generation of role-based reports. This includes the development of integral han-

dling tools with high flexibility and adoptability to support the integration process in all stages. An application example for a reliability analysis of a by-wire braking system according to ISO 26262 was conducted by [19].

5.2 Legislation

The last two decades legislations are pushing especially for lower emissions and safety of vehicles. The result is the electrification of the drivetrain and the increase of complexity in controlling a vehicle with more electric actuators. X-by-wire is a generic term referring to the replacement of mechanical or hydraulic systems, such as braking or steering, by electronic ones [80]. The ECE-Homologations are international agreed, unified technical regulations for vehicles and their components. Three safety-critical systems for vehicle stability control systems, steering systems and braking systems are presented here. The potential of ESC is highlighted in [1, 2]. The World Forum for Harmonization of Vehicle Regulations (WP29) of the United Nations Economic Commission for Europe (UN-ECE) is responsible for a technical regulation for future legislative efforts on ESC. The regulation draft GTR-ESC-2008-06 has been approved in 2008 [97]. Since November 2011 ESC is mandatory for all new registered passenger cars and commercial vehicles in the European Union. The US National Highway Traffic Safety Administration (NHTSA) and Canadian Transport Canada decided already earlier on the same regulation to be required for all vehicles with a weight of up to 4.5 tons that are manufactured from September 2011. Other markets will follow this trend, such as Australian introducing the regulation up to 3.5 ton vehicles in November 2013 [98]. New regulations for by-wire systems are adjusted from the existing regulations, which usually stress a mechanical connection between the driver and the road contact. A conventional steering system consists of the steering wheel, the steering actuator and their mechanical link, as well as a power source. The new steer-by-wire systems have no mechanical linkage, but an electronic connection instead. This brings a lot of safety and comfort benefits for passengers as well as cost, design and environmental benefits. Due to this discrepancy between legal and technical status for a safety-critical E/E systems, a new legislative regulation had to be developed, making the mechanical linkage dispensable. After the application of steer-by-wire systems without mechanical backup in off-highway production machines, the UNECE approved the regulation ECE R79 for road vehicles as well [99]. Other regulations like the self-centering of the steering system are still mandatory for the design [100]. Brake systems have the crucial safety function of decelerating a vehicle safely and effectively regardless its speed, load and road gradient. For new electric regenerative brakes in a HEV, electric and magnetic fields shall not affect the braking system. Furthermore a static total braking force when ignition and start switch switched off has to be generated [100, 101]. Commonly used systems rely on hydraulic and pneumatic actuation. Electronic brake actuation or by-wire braking systems have no such physical connection, but an electronic connection instead. The ECE R13 is the regulation for brake systems, for passenger cars as well as for commercial vehicles. The EU project highly automated vehicles for intelligent transport (HAVEit) showed good results in adapting the regulation to by-wire braking systems for a commercial vehicle. All technical requirements of ECE R13 could not be met though, due to the nature of the electro-mechanical braking system. HAVEit made proposals for updating ECE-R13 to meet the lack of requirements [102].

6 Conclusion

Electrification of automotive drive train and chassis systems enables higher levels of overactuation, which leads to improved controllability and higher flexibility. This also implies an increased number of fault possibilities. Hence, safe and reliable vehicles can be developed by adding more focus on fault-tolerant aspects. A holistic view has to be considered to avoid bottlenecks within a subsystem, i.e. get a harmonised level of fault-tolerance.
New legislations and standards have been developed in the field to enable by-wire systems with special focus on guaranteeing functional safety. Their adaption demands new control strategies to control a vehicle in a safe way. Passive and active fault-tolerant control are new approaches to the automotive field indicating high potential. Quick and precise fault detection and diagnosis methods have been established and flexible generic control is implemented in various ways, enabling an optimisation of the overall system. Reconfiguration strategies to handle faults in vehicles show promising results and encurage for future research in the area including vehicle validation.

Acknowledgemment

The financial support from Swedish Hybrid vehicle Center and the Swedish Energy Agency is gratefully acknowledged.

References

[1] A. Erke. Effects of electronic stability control on accidents: A review of empirical evidence. *Accident Analysis & Prevention*, 40(1):167–173, 2008.

[2] S.A. Ferguson. The effectiveness of electronic stability control in reducing real-world crashes: a literature review. *Traffic Injury Prevention*, 8(4):329–338, 2007.

[3] H. Riener, T. Mrazek, and A. Roth. Virtual simulation of x-by-wire control systems for commercial vehicle with steer-

by-wire applications. In *5. Internationales CTI-Forum Nutzfahrzeuge*, 2005.

[4] Roland Berger. Powertrain 2020 - the future drives electric. Case study available on www.rolandberger.com, 2009.

[5] International Energy Agency. Technology roadmap - electric and plug-in hybrid electric vehicles. Study available on www.iea.org, 2009.

[6] B. Heissing and M. Ersoy. *Chassis Handbook*. Vieweg and Teubner, 2010.

[7] ADAC e.V. ADAC Pannenstatistik 2010. Accessed at 2011-11-17.

[8] O.V. Thorsen and M. Dalva. A survey of faults on induction motors in offshore oil industry, petrochemical industry, gas terminals, and oil refineries. *IEEE Industry Applications*, 31(5):1186–1196, 1995.

[9] S. Yang, A. Bryant, P. Mawby, D. Xiang, L. Ran, and P. Tavner. An industry-based survey of reliability in power electronic converters. In *IEEE Energy Conversion Congress and Exposition*, 2009.

[10] R.J. Patton. Fault-tolerant control systems: The 1997 situation. In *IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes*, 1997.

[11] R. Isermann. *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer, 2006.

[12] K. Patan. *Artificial neural networks for the modelling and fault diagnosis of technical processes*. Springer, 2008.

[13] S. Tosunoglu. Fault-tolerant control of mechanical systems. In *21st International Conference on Industrial Electronics, Control, and Instrumentation*, 1995.

[14] R. Isermann, R. Schwarz, and S. Stolzl. Fault-tolerant drive-by-wire systems. *IEEE Control Systems Magazine*, 22(5):64–81, 2002.

[15] O. González, H. Shrikumar, J.A. Stankovic, and K. Ramamritham. Adaptive fault tolerance and graceful degradation under dynamic hard real-time scheduling. In *18th IEEE Real-Time Systems Symposium*, 1997.

[16] R. Isermann. Fehlertolerante mechatronische Systeme I. *at-Automatisierungstechnik*, 55(4):170–179, 2007.

[17] E. Dilger, T. Führer, B. Müller, S. Poledna, and T. Thurner. X-by-wire: Design of distributed fault tolerant and safety critical applications in modern vehicles. *VDI-Berichte*, 1374:427–443, 1997.

[18] Y. Zhang and J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, 32(2):229–252, 2008.

[19] P. Sinha. Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives. *Reliability Engineering & System Safety*, 96:13491359, 2011.

[20] S. Amberkar, B.J. Czerny, J.G. D'Ambrosio, J.D. Demerly, and B.T. Murray. A comprehensive hazard analysis technique for safety-critical automotive systems. In *SAE Transactions*, 2001.

[21] Y. Papadopoulos and C. Grante. Evolving car designs using model-based automated safety analysis and optimisation techniques. *Systems and Software*, 76(1):77–89, 2005.

[22] Dyadem Engineering Co. *Guidelines for failure mode and effects analysis for medical devices*. CRC Press, 2003.

[23] M. Walker, Y. Papadopoulos, D. Parker, H. Lönn, M. Törngren, D. Chen, R. Johansson, and A. Sandberg. Semi-automatic fmea supporting complex systems with combinations and sequences of failures. *Passenger Cars - Mechanical System*, 2(1):791–802, 2009.

[24] K.P. Jaschke. *Lenkregler fr Fahrzeuge mit hoher Schwerpunktlage*. Doctoral thesis, Braunschweig University of Technology, Braunschweig, Germany, 2002.

[25] T. Bünte. *Beitrge zur robusten Lenkregelung von Personenkraftwagen*. Doctoral thesis, RWTH Aachen University, Aachen, Germany, 1998.

[26] G. Roppenecker and H. Wallentowitz. Integration of chassis and traction control systems what is possible–what makes sense–what is under development. *Vehicle System Dynamics*, 22(5):283–298, 1993.

[27] N.A. Schilke, R.D. Fruechte, N.M. Boustany, A.M. Karmel, B.S. Repa, and J.H. Rillings. Integrated vehicle control. In *International Congress on Transportation Electronics*, 1988.

[28] S. Beiker and M. Mitschke. Verbesserungsmglichkeiten des Fahrverhaltens von Pkw durch zusammenwirkende Regelsysteme. *Automobiltechnische Zeitschrift*, 1:38–43, 2001.

[29] H. Smakman. Functional integration of active suspension with slip control for improved lateral vehicle dynamics. In *5th International Symposium on Advanced Vehicle Control*, 2000.

[30] R. Schwarz and P. Rieth. Global Chassis Control - Systemvernetzung im Fahrwerk. *at-Automatisierungstechnik*, 51(7):300–312, 2003.

[31] A. Zin, O. Sename, P. Gaspar, L. Dugard, and J. Bokor. Robust LPV∞ control for active suspensions with performance adaptation in view of global chassis control. *Vehicle System Dynamics*, 46(10):889–912, 2008.

[32] C. March and T. Shim. Integrated control of suspension and front steering to enhance vehicle handling. *Automobile Engineering*, 221(4):377, 2007.

[33] M. Valasek, O. Vaculin, and J. Kejval. Global chassis control: integration synergy of brake and suspension control for active safety. In *7th International Symposium on Advanced Vehicle Control*, volume 1, 2004.

[34] P. Gaspar, Z. Szabo, J. Bokor, C. Poussot-Vassal, O. Sename, and L. Dugard. Towards global chassis control by integrating the brake and suspension systems. In *Advances in Automotive Control*, 2007.

[35] W.J. Manning, M. Selby, D.A. Crolla, and M.D. Brown. IVMC: Intelligent Vehicle Motion Control. In *SAE Transactions*, 2002.

[36] J. Andreasson, C. Knobel, and T. Bünte. On road vehicle motion control-striving towards synergy. In *8th International Symposium on Advanced Vehicle Control*, 2006.

[37] A. Trächtler. Integrated vehicle dynamics control using active brake, steering and suspension systems. *Vehicle Design*, 36(1):1–12, 2004.

[38] H. Leffler and W Foag. Prospects and aspects of an integrated chassis management ICM. In *SAE Transactions*, 2000.

[39] R. Hiemenz and A. Klein. Interaktion von fahrwerkregelsystemen im integrated chassis control(icc). In *7th Tag des Fahrwerks, RWTH Aachen*, 2003.

[40] J. Andreasson and T. Bünte. Global chassis control based on inverse vehicle dynamics models. *Vehicle System Dynamics*, 44:321–328, 2006.

[41] T. Bünte and J. Andreasson. Integrierte fahrwerkregelung mit minimierter kraftschlussausnutzung auf der basis dynamischer inversion. In *Autoreg*, 2006.

[42] W.C. Durham. Constrained control allocation. *Guidance, Control, and Dynamics*, 16(4):717–725, 1993.

[43] G.J. Balas. Flight control law design: An industry perspective. *European J. of Control*, 9(2-3):207–226, 2003.

[44] N.P.I. Aneke. *Control of underactuated mechanical systems*. Doctoral thesis, Technische Universiteit Eindhoven, Eindhoven, Netherlands, 2003.

[45] Y. Hattori, K. Koibuchi, and T. Yokoyama. Force and moment control with nonlinear optimum distribution for vehicle dynamics. In *6th International Symposium on Advanced Vehicle Control*, 2002.

[46] R. Orend. Steuerung der ebenen Fahrzeugbewegung mit optimaler Nutzung der Kraftschlusspotentiale aller vier Reifen. *at-Automatisierungstechnik*, 53(1):20–27, 2005.

[47] C. Knobel, A. Pruckner, and T. Bünte. Optimized force allocation - a general approach to control and to investigate the motion of over-actuated vehicles. In *4th IFAC-Symposium on Mechatronic Systems*, 2006.

[48] M. Jonasson and J. Andreasson. Exploiting autonomous corner modules to resolve force contraints in the tyre contact patch. *Vehicle System Dynamics*, 46(7):553–573, 2008.

[49] Y. Chen and J. Wang. Energy-efficient control allocation with applications on planar motion control of electric ground vehicles. In *American Control Conference*, 2011.

[50] J. Edrén, J. Jerrelind, A. Stensson Trigell, and L. Drugge. Implementation and evaluation of force allocation control of a down scaled prototype vehicle with wheel corner modules. *Submitted for publication*, 2011.

[51] M. Jonasson and O. Wallmark. Stability of an electric vehicle with permanent-magnet in-wheel motors during electrical faults. *World Electric Vehicle Journal*, 1:100–107, 2007.

[52] M. Jonasson and O. Wallmark. Control of electric vehicles with autonomous corner modules: implementation aspects and fault handling. *Vehicle Systems Modeling and Testing*, 3(3):213–228, 2008.

[53] J. Wang and R.G. Longoria. Coordinated and reconfigurable vehicle dynamics control. *IEEE Control Systems Technology*, 17(3):723–732, 2009.

[54] M. Bodson. Evaluation of optimization methods for control allocation. *Guidance, Control, and Dynamics*, 25(4):703–711, 2002.

[55] Z. He and X. Ji. Nonlinear robust control of integrated vehicle dynamics. *Vehicle System Dynamics*, 50(2):247–280, 2011.

[56] L. del Re, P. Ortner, and D. Alberer. Chances and challenges in automotive predictive control. *Automotive Model Predictive Control*, 402:1–22, 2010.

[57] G. Palmieri, O. Barbarisi, S. Scala, and L. Glielmo. A preliminary study to integrate ltv-mpc lateral vehicle dynamics control with a slip control. In *48th IEEE Conference on Decision and Control*, 2009.

[58] W. Cho, J. Yoon, J. Kim, J. Hur, and K. Yi. An investigation into unified chassis control scheme for optimised vehicle stability and manoeuvrability. *Vehicle System Dynamics*, 46(S1):87–105, 2008.

[59] J. Edrén. *Exploring force allocation control of over actuated vehicles*. Licentiate thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2011.

[60] N. Mutoh, Y. Takahashi, and Y. Tomita. Failsafe drive performance of FRID electric vehicles with the structure driven by the front and rear wheels independently. *IEEE Industrial Electronics*, 55(6):2306–2315, 2008.

[61] J. Andreasson, L. Laine, and J. Fredriksson. Evaluation of a generic vehicle motion control architecture. In *FISITA Transactions*, 2004.

[62] T. Steffen. *Control reconfiguration of dynamical systems: linear approaches and structural tests*. Springer, 2005.

[63] R. Wang and J. Wang. Fault-tolerant control with active fault diagnosis for four-wheel independently-driven electric ground vehicles. In *IEEE American Control Conference*, 2011.

[64] Y. Zhang and J. Jiang. Issues on integration of fault diagnosis and reconfigurable control in active fault-tolerant control. In *Fault Detection, Supervision and Safety of Technical Processes*, 2006.

[65] H. Yang, B. Jiang, and V. Cocquempot. *Fault tolerant control design for hybrid systems*, volume 397. Springer, 2010.

[66] Y.W. Kim, G. Rizzoni, and V.I. Utkin. Developing a fault tolerant power-train control system by integrating design of control and diagnostics. *Robust and Nonlinear Control*, 11(11):1095–1114, 2001.

[67] P.M. Pathak, R. Merzouki, A.K. Samantaray, and B. Ould-Bouamama. Reconfiguration of directional handling of an autonomous vehicle. In *3rd IEEE Conference on Industrial and Information Systems*, 2008.

[68] S. Jung and T.C. Hsia. Explicit lateral force control of an autonomous mobile robot with slip. In *IEEE Conference on Intelligent Robots and Systems*, 2005.

[69] M. Oudghiri, M. Chadli, and A. El Hajjaji. Robust observer-based fault-tolerant control for vehicle lateral dynamics. *Vehicle Design*, 48(3):173–189, 2008.

[70] B. Song and J.K. Hedrick. Fault tolerant nonlinear control with applications to an automated transit bus. *Vehicle System Dynamics*, 43(5):331–350, 2005.

[71] F. Gustafsson. *Adaptive filtering and change detection*, volume 5. Wiley, 2000.

[72] D. Wanner. Aspects on fault-tolerant vehicle design. Technical report, KTH Royal Institute of Technology, 2012.

[73] L. Laine. *Reconfigurable motion control systems for over-actuated road vehicles*. Doctoral thesis, Chalmers University of Technology, Gothenborg, Sweden, 2007.

[74] T. Gordon, M. Howell, and F. Brandao. Integrated control methodologies for road vehicles. *Vehicle System Dynamics*, 40(1):157–190, 2003.

[75] H. Kopetz. A comparison of ttp/c and flexray. *Research Report*, 10:2001, 2001.

[76] R. Belschner, J. Berwanger, C. Bracklo, C. Ebner, B. Hedenetz, W. Kuffner, P. Lohrmann, J. Minuth, M. Peller, A. Schedl, et al. Requirements towards an advanced communication system for fault-tolerant automotive applications. *VDI-Berichte*, 1547:23–42, 2000.

[77] E. Dilger, T. Führer, and B. Müller. Distributed fault tolerant and safety critical applications in vehicles-a time-triggered approach. *Computer Safety, Reliability and Security*, 1516:267–283, 1998.

[78] J. Rushby. Bus architectures for safety-critical embedded systems. In *Embedded Software*, 2001.

[79] T.K. Ringler. *Entwicklung und Analyse zeitgesteuerter Systeme*. Doctoral thesis, University of Stuttgart, Stuttgart, Germany, 2002.

[80] C. Wilwert, N. Navet, Y.Q. Song, F. Simonot-Lion, et al. Design of automotive x-by-wire systems. *Industrial Communication Technology Handbook*, 1:1–34, 2004.

[81] M. Fernström and D. Ungerdahl. TTCAN Reference Application - An investigation of time-triggered network performance. Master thesis, Chalmers University of Technology, 2006.

[82] B. Müller, T. Führer, F. Hartwich, R. Hugel, H. Weiler, et al. Fault tolerant ttcan networks. *CAN Newsletter, CiA*, 1:18, 2002.

[83] S. Poledna, W. Ettlmayr, and M. Novak. Communication bus for automotive applications. In *27th IEEE Solid-State Circuits Conference*, 2001.

[84] H. Pfeifer. Formal verification of the ttp group membership algorithm. In *FORTE XIII / PSTV XX*, 2000.

[85] G. Bauer and M. Paulitsch. An investigation of membership and clique avoidance in ttp/c. In *19th IEEE Symposium on Reliable Distributed Systems*, 2000.

[86] H. Heinecke, J. Bielefeld, K.P. Schnelle, N. Maldener, H. Fennel, O. Weis, T. Weber, J. Ruh, L. Lundh, and T. Sandén. Autosar–current results and preparations for exploitation. In *7th EUROFORUM conference - software in the vehicle*, 2006.

[87] T. Scharnhorst, H. Heinecke, K.-P. Schnelle, H. Fennel, J. Bortolazzi, L. Lundh, P. Heitkmper, J. Leflour, J.-L. Mat, and K. Nishikawa. AUTOSAR–Challenges and Achievements. *VDI-Berichte*, 1907:395–408, 2005.

[88] V. Debruyne, F. Simonot-Lion, and Y. Trinquet. East-adlan architecture description language. *Architecture Description Languages*, 176:181–195, 2005.

[89] OSEK Consortium. Osek-vdx time-triggered operating system - v1.0, 2011.

[90] FlexRay Communication System - Protocol Specification - Version 3.0.1.

[91] International Standard ISO/DIS 26262 - Road vehicles–Functional safety.

[92] National-Instruments. What is the ISO 26262 Functional Safety Standard?, 2011. Accessed at 2011-12-17.

[93] Parasoft. ISO 26262 Software Compliance with Parasoft C++ test, 2010. Accessed at 2011-12-17.

[94] L. Coyle, M. Hinchey, B. Nuseibeh, and J.L. Fiadeiro. Guest editors' introduction: Evolving critical systems. *Computer*, 43(5):28–33, 2010.

[95] Y. Papadopoulos, M. Walker, M.O. Reiser, M. Weber, D. Chen, and M. Törngren. Automatic allocation of safety integrity levels. In *1st Workshop on Critical Automotive applications*, 2010.

[96] M. Born, J. Favaro, and O. Kath. Application of ISO DIS 26262 in practice. In *1st Workshop on Critical Automotive Applications: Robustness & Safety*, 2010.

[97] UNECE. DRAFT ESC GTR Version 5, Feb. 2008.

[98] Esc legislation worldwide. Accessed at 2011-12-14.

[99] UNECE. Regulation No. 79 - Amend. 78 - Rev. 2, Jan. 2006.

[100] D. Frede, M. Khodabakhshian, D. Malmquist, and J. Wikander. A survey on safety-critical vehicular mechatronics. In *IEEE Conference on Mechatronics*, 2011.

[101] UNECE. Regulation No. 13 - Amend. H - Rev. 2, Oct. 2011.

[102] J. Svendenius, A. Nilsson, and F. Segl. Deliverable D42.2 - Brake-by-Wire Truck Prehomologation. Technical report, Highly automated vehicles for intelligent transport, 2011.

Authors

Daniel Wanner is a Ph.D. student at Vehicle Dynamics at the Royal Institute of Technology (KTH) in Stockholm, Sweden. He graduated at RWTH Aachen University as Diplom-Wirtschaftsingenieur in 2010. His research covers fault-tolerant control of over-actuated hybrid electric vehicles.

Annika Stensson Trigell is Professor in Vehicle Dynamics at KTH. She graduated with a Ph.D. from Luleå University of Technology (LTU) in 1994. Her research interests are modelling, simulation, analysis and experimental evaluation of vehicle behaviour, and its dynamic interaction with driver and environment.

Lars Drugge is an Associate Professor in Vehicle Dynamics at KTH. He received his Ph.D. from LTU in 2000. His research interests are modelling, simulation and experimental evaluation of the dynamic behaviour of on- and off-road vehicles and overhead power systems.

Jenny Jerrelind is an Assistant Professor in Vehicle Dynamics at KTH. In 2004, she received her Ph.D. in Vehicle Engineering at KTH. Her research interest is on vehicle dynamics with special focus on suspension design and non-linear characteristics.