2

Redesigning Vehicle Electronics: A Systems Engineering Approach

> "The world we have made as a result of the level of thinking we have done thus far creates problems we cannot solve at the same level of thinking at which we created them."
>
> *Albert Einstein*

Automotive systems engineering

This thesis follows an Automotive Systems Engineering approach as introduced by Maurer [2013] to address existing and arising problems with individual components in the vehicle by taking into account vehicle-wide cross dependencies and interactions. This way, new solutions to existing problems can be found by a targeted analysis and reorganization of existing systems, and opportunities to realize novel functions become obvious. The thesis especially focuses on novel approaches for Drive-by-Wire systems. To further clarify the goals and contributions of this thesis, a short assessment of typical development processes in the automotive field (Sec. 2.1) is given. Complementary, important standards and legislative demands relevant to this work are referenced, required terminology is defined, and the contribution of this work is put into relation to existing approaches. An overview of the structure of this document (Sec. 2.2) and a short introduction of the project background (Sec. 2.3) conclude the thematic identification.

2.1. Current Practices: Process Models and Methods

Process models

Processes relied on in industry play a vital role in mastering the complexity of the development of modern vehicles [Bender, 2005, p. 1]. The product development process is defined as a "system of defined steps and tasks such as strategy, organization, concept generation, marketing plan creation, evaluation, and commercialization of a new product. It is a cycle by which an innovative firm routinely con-

© Springer International Publishing Switzerland 2015

P.J. Bergmiller, *Towards Functional Safety in Drive-by-Wire Vehicles*,
DOI 10.1007/978-3-319-17485-3_2

verts ideas into commercially viable goods or services" [BusinessDictionary, 2012][1]. Appropriate structuring and control of these processes significantly impacts the economic success of a company [Mehrle et al., 2012; Ward and Sobek, 2014]. For that reason, a multitude of process and phase models[2] have been developed and applied [Benington, 1983; Hammerschall, 2008]. These models support planning, control, monitoring, and execution of product development by introducing reference procedures. Nowadays, multiple proprietary[3] and standardized process models are applied, such as the Unified Process [Jacobson et al., 1999], the OPEN Process [Graham et al., 1999], or the V-Model in its different derivatives (V-Model 92/97/XT) [Kuhrmann et al., 2011]. Further models and detailed comparisons can be found in Hammerschall [2008]. Due to its widespread usage in the automotive domain, the research in the MOBILE project refers to the V-Model as a basis for the thematic identification.

The V-Model

The V-Model XT 1.4 (XT standing for Extreme Tailoring) structures product development both for the orderer and the contractor [V-Modell, 2012]. Therefore, it includes various steps from project approval and system development to the project end. For smaller projects, the V-model XT can be adapted to reduce project overhead. Prominent institutions and international standards refer to the V-model and thus further push its development. For example, the Federal Republic of Germany relies on the V-model for IT projects [BMI, 2010][4], and the important automotive standard ISO 26262 "Road Vehicles – Functional Safety" relies on the V-model to structure the development process.

The V

In this thesis, only the part of the V-model dealing with technical product development is referenced. This "core" of the V-model, first developed by Rook [1986], was successively supplemented in follow-up versions to create the current V-Model XT and is structured as given in Fig. 2.1. Based on the description of the requirements, the overall system is specified and the (functional) architecture of the system is derived. Then, the system is detailed in sub-systems and modules, which are specified and finally implemented (coding). Afterwards, the hierarchical path is followed back up to the final acceptance test of the system. At each hierarchical layer, the implemented systems are tested for compliance with the previously defined requirements.

V-model for mechatronic systems

All process models referenced before, including the V-model, originate from the field of software engineering and therefore are targeted primarily at software development. When mechatronic systems for vehicles are developed, new challenges arise

[1] A similar definition can be derived, if the perception of a process as "a series of things that are done in order to achieve a particular result" by [Wehmeyer, 2005, p. 1202] is combined with the definition of "new product development" by [Collins, 2013] as "the process of developing new products for the market". For this work, the formulation by [BusinessDictionary, 2012] is found more appealing and therefore referenced.

[2] Phase models describe only the top-level development flow, e.g., analysis, design, implementation, whereas process models include additional information, e.g., which results are expected in detail and who is responsible for a task [Hammerschall, 2008, p. 31].

[3] specialized for a specific organization; not further considered here

[4] Federal Ministry of the Interior of Germany

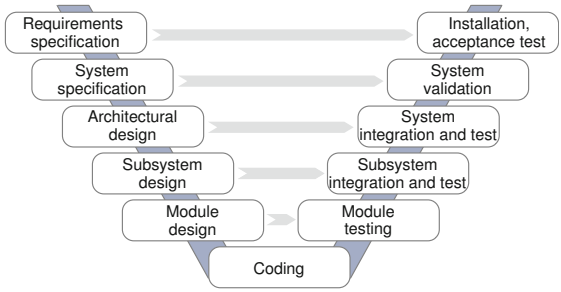


Figure 2.1.: V-model based development; figure according to Redmill [1997]

due to the close coupling of newly designed mechanics, EE components, and software. These aspects are not considered sufficiently in the V-model as introduced. Within the EQUAL research project, an accordingly adapted "3-Ebenen-Modell" (3-Layer-Model) was developed [Bender, 2005, p. 45]. Figure 2.2[5] outlines the resulting V-shaped process with the three disciplines (mechanics, EE, and software) executed in parallel. Each discipline performs a V-shaped development process, but the 3-Layer-Model synchronizes and merges tasks at relevant steps during product development. This indicates the increase in complexity and interdependencies between the different fields during product development. Especially during the testing phases at system and subsystem level, products from multiple disciplines must be available to allow component and integration tests. One missing part is enough to delay the overall process. For the same reason, testing at system or vehicle level under realistic conditions during the early phases of product development is barely possible. Still, such early iterations are necessary [Hermes and Schultze, 2009; Maurer, 2012] especially in pre-development and research and to support the Automotive Systems Engineering approach. Accordingly, methods[6] and tools to evaluate changes applied at the system level during early development phases have to be provided. The V-Model itself does not specify any methods for the individual development steps [Wieczorrek and Mertens, 2011]. On the one side, this contributes to the success of the V-Model in different domains. On the other side, methods suitable to support certain process steps have to be found independently. As this work introduces and applies amongst others such a method, a brief assessment of typical elements of a method and the relation to processes, principles, and heuristics is given. The differentiation is performed following Hammerschall [2008].

Methods

The core of a method is a process, which is defined as a "series of things that are done in order to achieve a particular result" [Wehmeyer, 2005, p. 1202]. Thus, a detailed process provides a suitable guideline for what has to be done to achieve a

[5] The numbers and highlighting in the figure are for later reference.

[6] A method is defined as "a way of proceeding or doing something, esp. a systematic or regular one" [Collins, 2013]. During a development process, (multiple) methods can be applied to achieve necessary results [Hammerschall, 2008]. Further details are given in the next paragraph.

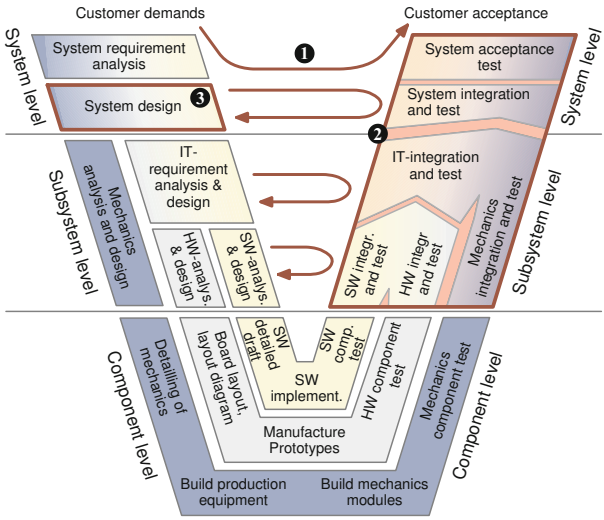


Figure 2.2.: "3-Ebenen-Modell" (3-Layer-Model) [Bender, 2005, p. 45][8]

certain result. But, to maximize the number of possible fields of application for a method, the process specified by a method can deliberately be incomplete. Missing parts allow adaptation of the method to multiple fields of application. In order to ensure that these adaptations focus on the purpose of a method, methods can additionally specify principles[7]. The principles describe general conditions for the process. Well known examples that are also applied in this work are the "top-down" or the "bottom-up" principle [Hammerschall, 2008, p. 61]. Additionally, supportive heuristics can be included in a method. Heuristics can assist in "solving problems by finding practical ways of dealing with them learning from past experience" [Wehmeyer, 2005, p. 730]. Figure 2.3 summarizes the relations between method, principle, and process in a modified UML structure diagram according to Gnatz [2005]. The additional arrows and text markings indicate the meaning of the links and the reading direction.

Standards, legislation

As complex mechatronic systems that have been developed according to the outlined automotive development processes and using suitable methods are increasingly taking over safety critical tasks (compare Cha. 1), they are attracting increased public interest and also, therefore, normative and legislative regulations. These additional requirements complement the challenges for system level development outlined so far and will be referenced in the appropriate sections. Sec. A.1

[7] A principle is defined as "an underlying or guiding theory or belief" [Collins, 2013].

[8] The permission to print Fig. 2.2 in the proposed English translation from the German original version was received from Klaus Bender at January 31st 2013.

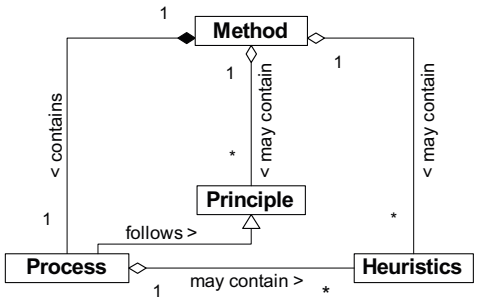


Figure 2.3.: Relations between method, process, principle, and heuristics

provides a summary of important standards and regulations that were taken into account and briefly introduces the relevant standardization institutions.

2.2. Structure and Contribution of This Thesis

The given glance at current development processes in the automotive industry clarified the challenges that exist during the development of mechatronic systems. Drive-by-Wire systems are especially effected due to the high safety criticality of the vehicle control task. Accordingly, this thesis proposes methods and designs that assist with achieving functional safety in Drive-by-Wire vehicles by exploiting the vehicle level context. Challenges that are hard to address efficiently at component level are handled at vehicle level. Still, the review of the V-model development process revealed that especially iterative work on higher hierarchical layers, such as vehicle/system layer, is barely supported by methods and tools nowadays, which necessitates to consider these aspects in this thesis. As will be outlined, the resulting contributions are mostly not restricted to Drive-by-Wire systems but can be transferred to other fields of application of vehicle electronics.

Tools and solutions

Specifically, this work introduces (a) a toolchain for development and evaluation of interconnected vehicle electronics at system level, and (b) an architecture for a highly flexible Drive-by-Wire vehicle. The architecture explicitly targets system wide interaction of components to meet safety goals. It is flanked by an appropriate safety concept relying on novel monitoring and intervention mechanisms and an appropriate method to assess functional safety at vehicle level. The development of the toolchain and the architecture are closely linked: on the one side, the architecture is implemented on a real experimental vehicle using the toolchain. On the other side, the experimental vehicle, which features the flexibility enabled by the novel architecture, becomes a core part of the toolchain, as it provides the platform for test runs in a real vehicle. In summary, this work will paint a “big picture” of a novel approach based on the proposed architecture and the developed vehicles,

but will also enrich this picture with some details in important parts. Basically, the presented vehicles provide huge possibilities for investigations and research, and the mentioned details focus on enabling novel approaches or demonstrate the performance of the architecture and the vehicles using an example application.

Toolchain

The mentioned toolchain enables the proposed vehicle level design approach. Essentially, it supports easy evaluation of algorithms and electronics operating at vehicle level in a real vehicle at early development stages. Therefore, several key aspects are covered:

- Virtual testing is facilitated by a simulation environment including vehicle dynamics models and a virtual driver that can easily be adapted to drive various vehicles with different actuator set-ups.
- The algorithms developed in simulation can quickly be ported onto microcontrollers or onboard computers on experimental vehicles. Suitable operating systems for the microcontrollers and a link to the Mathworks Simulink environment are provided. Both a scaled and a full-scale experimental vehicle are available, which support safe stepwise testing of safety critical algorithms.
- To visualize data in the vehicles, a server-client based system facilitates distributed access to all vehicle data from within and outside the experimental vehicle. The system supports online diagnostics and allows the user to individually configure the look of the dashboard.

This toolchain assists the developer during quick iterations on higher hierarchical levels of the V-Model that are so far little covered by existing tools. Figure 2.2 highlights the relevant steps in the V-Model for mechatronic components. Front-loading of component and integration tests under real driving conditions (❷, Fig. 2.2) is supported. For example, an electric drive unit and its integration with other completed parts can be investigated in the experimental vehicle before the remaining vehicle exists. Novel architectural approaches can be evaluated due to the modularity and reconfigurability of the experimental vehicle. Another special field of application targets early evaluation of how well customer needs can be met by a new functionality with relevance to vehicle handling (❶, Fig. 2.2). Therefore, the powerful experimental vehicles can simulate the dynamic behavior of vehicles that do not yet exist. Thus, the longitudinal and lateral handling of virtual vehicles can be evaluated on the test track in a way that is similar to the approach by Cornelsen et al. [2011] for longitudinal dynamics. More details on the toolchain and the special contribution of the experimental vehicles will be given in Cha. 3 and Cha. 4.

A novel system architecture

As mentioned, as a part of the toolchain, the flexible experimental vehicles are themselves subject to research. Based on requirements posed by the toolchain and further constraints due to costs and availability of components, a novel architecture is introduced for the EE system of these vehicles. This architecture supports flexibility while providing the required degree of functional safety (Cha. 5). A

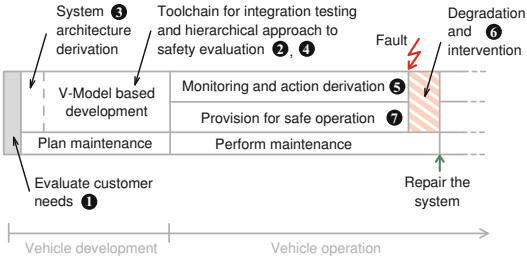


Figure 2.4.: Simplified vehicle life cycle with associated contributions of this thesis

primary objective of the architecture is to exploit functional redundancies across different types of actuators for safety purposes. Therefore, the structure of the system is introduced top-down starting from the vehicle level and relying on different views (functional, hardware, software, etc.) of the overall system. This structured approach supports system design by explicitly questioning traditional system structures in vehicles (❸, Fig. 2.2).

Mechanisms and methods

As enabling mechanisms for the proposed architecture, both preventive long-term approaches and methods for immanent intervention in case of failure are introduced. This work refers to the first group as "strategic" (Cha. 8) and to the second group as "tactical" (Cha. 7) mechanisms. Strategic measures aim to avoid safety critical situations by anticipative planning and intervention exploiting the flexibility of the vehicle. Tactical measures perform online monitoring and derive actions in case of failure so that at least degraded vehicle operation is guaranteed until a safe state can be achieved. As core mechanisms in the field of strategic measures, this work introduces an *online-optimization system* that balances load and wear among different types of actuators, and an *ability based self-representation* for the vehicle that continuously monitors the health state of the vehicle and identifies maneuvers and actions that can no longer be performed by the vehicle. This knowledge is vital for the automated decision making of the vehicle on usage of its actuators, but also as a basis for later development of autonomously driving vehicles with environmental perception. Tactical aspects covered in this thesis include an *efficient probabilistic approach* to online monitoring that supports high flexibility in the software system and a short assessment of *stability control* using four-wheel steering and torque vectoring to compensate for failures of individual actuators. For the overall system, a safety evaluation is provided (Cha. 9). Therefore, a novel method for *tailored hierarchical safety analysis* (Cha. 6) was developed that especially focuses on exploitation of functional redundancies and targeted safety evaluation.

Summary of Contributions

As stated in the objectives, the toolchain and the introduced architecture including the developed mechanisms help to close critical gaps in the development process of powerful and highly-safety critical vehicle electronics. Figure 2.4 associates the

main contributions of this thesis to a simplified vehicle life cycle, with a focus on the introduced aspects. The proposed toolchain can assist in evaluating customer benefits from novel functions (❶, Fig. 2.4). If a function is found suitable, the introduced architecture for flexible vehicles (❸, Fig. 2.4) or individual aspects of it may serve as an input for the development of the EE system of a vehicle. Thus, the reconsideration of existing domain-oriented system architectures can be triggered. During system development, the toolchain assists by enabling early testing during iteration loops at the vehicle/system/subsystem level, which are currently not supported sufficiently by available tools (❷, Fig. 2.4). The hierarchical approach (❹, Fig. 2.4) to safety analysis provides an estimate of the functional safety of the vehicle based on the first development steps, and can provide increasingly detailed results if the inputs of the safety analysis are continuously complemented in the following steps. During vehicle life, tactical safety measures, such as the monitoring and action derivation algorithm (❺, Fig. 2.4), ensure cost efficient detection and treatment of failures that occur while driving. If a failure is detected, control algorithms for vehicle dynamics contribute to the degradation concept (❻, Fig. 2.4). First research results on cross-actuator failure compensation are considered and provide an outlook on what could be possible in future. Strategic mechanisms (❼, Fig. 2.4) continuously operate while driving and reduce the probability of the occurrence of risky situations that might result in safety critical failures. Therefore, online optimization unburdens overloaded actuators, and a skill-based self-representation, e.g., prevents execution of maneuvers that are no longer regarded as safe, judging from the current vehicle state. The benefits of the individual outlined aspects will be revisited with the example of the constructed experimental vehicle "MOBILE". As a graphical guideline, Fig. 2.5 summarizes the structure of the thesis.



2.3. Project Background and Constraints

For a better understanding of decisions made in this work, a brief outline of the general conditions under which the MOBILE project presented in this thesis was carried out concludes the introduction. One of the main influencing factors is the "university only" character of the project. The project was not primarily funded by any partner from industry, which led to great freedom in decisions and design but also very definite financial limits. The main goals of the project, apart from scientific aspects, were (a) to build up know-how in various fields related to vehicle electronics, (b) to introduce a vehicle level perspective into electronics design driven by challenges observed in the projects with industry, and (c) to provide a basis for future research in these fields. The decision to construct the fully custom-built vehicle MOBILE for that purpose was inspired by the positive experiences with the vehicles "X1" and "P1" built by Gerdes at the Dynamic Design Lab (Stanford University, USA). Building the vehicle forces intense consideration of all relevant aspects from the component level up to the vehicle level ("We will learn something

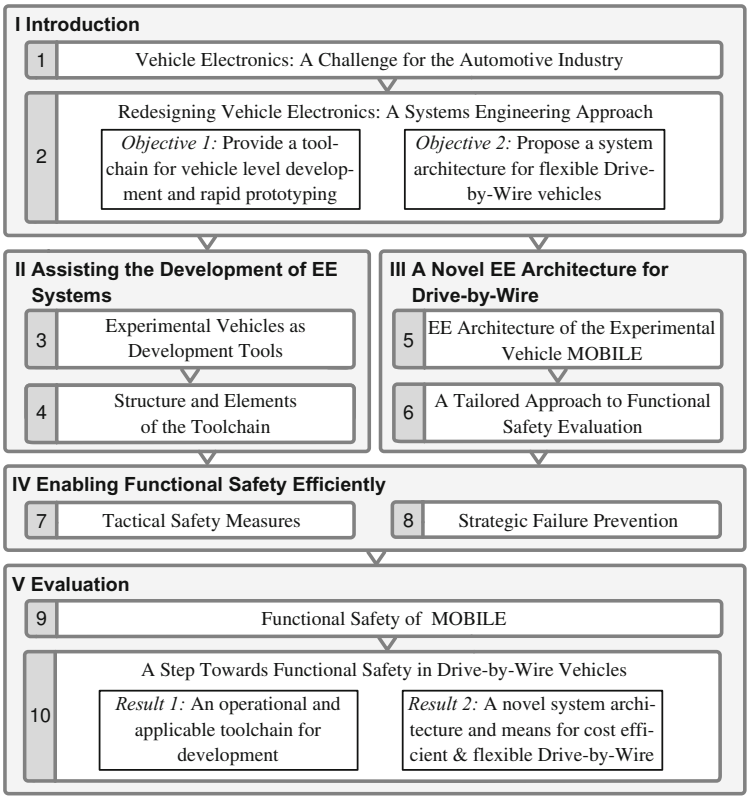


Figure 2.5.: Graphical table of contents

from it", Gerdes).

The educational aspect of the project results in multiple self-designed systems. This facilitates full accessibility for students and researchers, and supports the accumulation of critical know-how in novel fields, such as Drive-by-Wire and electromobility, at the university. Accordingly, the project was hugely supported by numerous students writing their bachelor's or master's theses (see bibliography), which were combined into an overall operational system. In summary, the university driven character of the project facilitates "out-of-the-box" thinking and novel approaches but also guides decisions on whether to purchase or design components.

http://www.springer.com/978-3-319-17484-6

Towards Functional Safety in Drive-by-Wire Vehicles

Bergmiller, P.

2015, XIV, 233 p. 82 illus., Hardcover
ISBN: 978-3-319-17484-6