SafeAdapt - Safe Adaptive Software for Fully Electric Vehicles

Philipp Schleiss, Marc Zeller, Gereon Weiss, Dirk Eilers
Fraunhofer Institute for Embedded Systems and Communication Technologies ESK
Munich, Germany
Email: {name.surname}@esk.fraunhofer.de

***Abstract*—The promising advent of *Fully Electric Vehicles (FEVs)* also induces a shift towards fully electronic control of existing and new vehicle functions. Hereby, critical functions, such as Brake- and Steer-by-Wire, require sophisticated redundancy solutions to ensure safety. As a result, the overall electric/electronic (E/E) architecture of a vehicle is becoming even more complex and costly. To address the need for safety, reliability and cost efficiency in future FEVs, the development of a novel adaptive architecture to manage complexity through generic, adaptive, and system-wide fault handling is essential. Moreover, to enable this transition, design simplicity, cost efficiency, and energy consumption are especially important elements. Consequently, the SafeAdapt project seeks a holistic approach by comprising the methods, tools, and building blocks needed to design, develop and certify such safety-critical systems for the e-vehicle domain. In detail, a platform core encapsulating the basic adaptation mechanisms for relocating and updating functionalities is developed on basis of AUTOSAR. It serves as foundation for an interoperable and standardised solution for adaptation and fault handling in upcoming automotive networked control systems. In particular, emphasis is laid on functional safety with respect to the ISO26262 standard, wherefore an integrated approach ranging from tool chain support, reference architectures, modelling of system design and networking, up to early validation and verification is derived. To realistically validate these adaptation and redundancy concepts, an e-vehicle prototype with different and partly redundant applications is being developed. Moreover, the presented work outlines the motivation and challenges of future E/E architectures and contributes a technical strategy to overcome those hindrances.**

I. Introduction

With the advent of electric drive-trains, the dream of zero emission transportation turns more tangible. Trying to transform this vision into reality however introduces a multitude of new technologies, such as, wheel-hub drives, energy recuperating brakes, body control, and Brake- and Steer-by-Wire systems, replacing well-established mechanic and hydraulic systems. In turn, these new safety critical subsystems must be controlled in a manner that compensates for failures gracefully and at least maintains a level of safety currently experienced.

Initially, mechanical fall-back mechanisms that are able to mitigate the risk of electronic system failures may ease this transition, but when inspected more closely, this coexistence of mechanical and software-based control systems introduces a cost and weight overhead that is in the long-run not bearable for a unit cost driven industry. Unfortunately, abandoning these mechanical backups in federated Electric and Electronic (E/E) vehicle architectures that consist of single purpose units only shifts these effort towards the formation of dedicated backup systems.

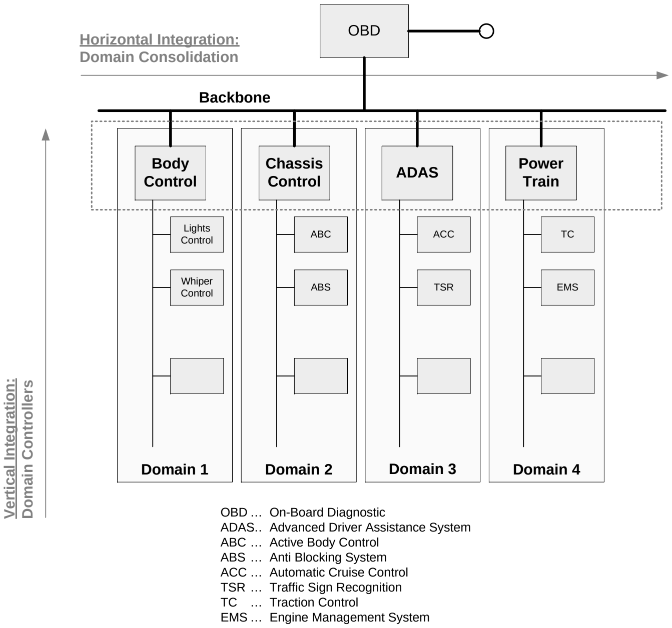

Fig. 1. Today's automotive E/E architecture and sub-systems

Regardless, in light of the emerging trend towards software-defined cars, the interconnection of presently isolated subsystems plays a major role in implementing new functions in modern vehicles (cf. Fig. 1). For instance, *Advanced Driver Assistance Systems (ADAS)* that have to interact with brake, drive train, steering systems, and other optional sensors such as cameras, radar, and accelerometer are not feasible without access to elementary data. In addition, the vision of autonomous driving, which according to large car manufacturers can be available in within the next decade [1], prerequisites an even more intertwined system, to be able to control the entire vehicle digitally. Considering that high-end automotive E/E architectures already consist of up to 100 *Electronic Control Units (ECUs)* [2], which are interconnected by multiple bus systems and provide up to 3,000 atomic software-based functions [3], the implementation of all features required for a Fully Electric Vehicle (FEV) will undoubtedly complicate and therethrough cripple current design practice. In order to implement the increasing number of functions in FEVs by software in a safe and cost-efficient way, a new and substantially revised E/E architecture is needed.

In the pursuit of finding a tangible E/E architecture for future FEVs with better safety characteristics, a manageable form of complexity, and higher cost efficiency, adaptive concepts pose as a promising alternative. More precisely, the aspects of adaptivity focusing on flexible system reconfiguration are beneficial to abolishing dedicated backup control systems safely. Therefore, the SafeAdapt project incorporates and extends these approaches while cherishing past advances in E/E architecture design. Thus, SafeAdapt sets out to create a substantial revised blueprint for flexible, but at the same time safe, E/E architectures compliant to the AUTOSAR standard [4].

The SafeAdapt approach intends to (i) considerably reduce the number of ECUs by combining multiple functions onto generic platforms, (ii) increase safety and availability by an universal failure handling method able of relocating application onto other devices after failure of an ECU, (iii) reduce development cost trough simplified E/E design, integration, certification, and maintenance, (iv) improve energy efficiency by limiting the number of active devices and communication links, therethrough reducing weight and enabling more sophisticated utilisation techniques, and (v) facilitate the abolishment of mechanical fall-back solutions. In addition, the developed concept will not only be grounded in theory but also evaluated through the creation of a prototype e-vehicle. Subsequentially, an induced failure of safety-critical control functions, such as Brake-by-Wire, will demonstrate the system's robustness.

Therefore, first of all relevant related work in the area of E/E architectures and adaptive embedded systems is presented (see Section II). Thereafter, the three main pillars of the SafeAdapt approach to realise safe adaptation in future automotive E/E systems are outlined in Section III. Finally, the paper is concluded in Section IV, leading to an outlook on future work.

II. Related Work

Today, the vehicles' functions are grouped in several subdomains of different criticality, ranging from low critical infotainment systems with typically soft real-time constraints, up to the safety-critical control software with hard real-time constraints as for instance Steer-by-Wire or Brake-by-Wire systems. Each of these domains is typically hosted on a different set of ECUs. The control units of each domain are connected by various networks and buses, tailored for the requirements of the domain, thereby forming a so-called networked embedded system.

To address the challenges of increasing E/E system complexity, recent development aims at consolidating functions on ECUs. One approach are so-called *single domain controllers*, which integrate different functions of a vehicle sub-domain by means of *vertical integration* (cf. Fig. 1). Furthermore, so-called *multi-domain controllers* are under development to consolidate the vehicle architecture through *horizontal integration* (cf. Figure 1), and could be used to reduce the overall functional safety overhead of E/E architectures by handling critical functions centrally [5]. However, an architecture with multi-domain controllers does not provide any intrinsic form of hardware redundancy within the distributed embedded system, which affects the availability of functions or alternatively necessitates a duplication of ECUs. Consequently, upcoming functions of future FEVs, such as, X-by-Wire or autonomous driving, which need to be fully fault tolerant and *fail-operational*, can not purely be implemented on current *fail-passive* multi-domain controllers without adding further hardware redundancy.

In the aerospace domain, hot redundant Fly-by-Wire control systems with dissimilar design patterns have already replaced traditional hydraulic and mechanical forms of control through the advent of so-called *Integrated Modular Avionics (IMA)* architectures [6]. In turn, this effort towards redundancy and fault containment considerably raises complexity and the need for electronic control units. For the aerospace domain this investment is justifiable, since safety-critical functions need to be fully fault tolerant and fail-operational. In contrast, the unit cost driven automotive industry with less stringent need for fail-operational behaviour, may still profit from the technical solutions found the aerospace domain, even though implementations in avionics are more complex. This simply results from the fact that an aircraft cannot be stopped during flight in case of failure. However, as soon as E/E systems substitute mechanical solutions, similar requirements will arise in the automotive industry. To ensure that a vehicle will safely be able to stop after a system impairment, a reduced set of most critical functions has to always remain operational. A full reflection of solutions originating from aerospace onto the automotive industry is however not directly possible or desired due to cost reasons. For instance, there is no need to have dual or triple redundancy or dissimilar systems in the same complex manner. An approach suitable for automotive E/E systems should copy the principal ideas of redundant systems but optimise the number of ECUs, as well as the amount of replicated functions, to attain cost effectiveness, which is in turn crucial for mass market production processes.

Therefore, adaptation poses as a viable solution to increase the reliability of highly safety-critical applications without relying on mechanical fall-back solutions. However, current software architectures only consider static reconfiguration with a fixed set of modes that build on static safety validation, as for instance seen in *AUTOSAR mode management* [7]). Obviously, this does not address redundancy and fault tolerance effectively.

As such, there are already several research projects focusing on aspects of adaptive embedded systems. For instance, the FP7 project ACTORS (Adaptivity and Control of Resources in Embedded Systems) [8] addresses the design of complex embedded systems and aims to provide adaptive resource management during run-time based on feedback control. However, the adaptation of the entire networked embedded system is not considered in this project. In order to increase the reliability of FEVs the HEMIS (electrical power-train Health Monitoring for Increased Safety in FEVs) project [9] develops a prognostic health monitoring system that monitors the electric powertrain of the vehicle and provides a fail-safe state. Furthermore, DySCAS (Dynamically Self Configuring Automotive Systems), a project funded by the European Commission (FP6), focused on dynamic reconfiguration in automobiles and proposed a middleware supporting dynamic reconfiguration and context awareness [10] [11]. Another project focusing on dynamic systems is iLand (mIddLewAre for deterministic dynamically reconfigurable NetworkeD embedded systems) [12] that is in pursuit of improving system flexibility, scalability, and composability through the development of a modular component-based middleware for deterministic dynamic functional composition and reconfiguration. Since all these projects on adaptivity and reconfiguration aspire to develop novel middleware-based approaches, the resulting solutions cannot comply with current standards in the automotive domain such as AUTOSAR and ISO26262 [13]. In sum, none of these projects address the special issues of safety-critical applications for e-vehicles.

On the contrary, the redesign of E/E architecture in the context of FEVs is also part of active inquiries. For example, the POLLUX project [14] investigates and develops architectural concepts for e-vehicles. However, POLLUX does not consider run-time adaptation or reconfiguration in automotive E/E architectures as required for safety-critical applications where redundancy concepts are mandatory. Then again, within the RACE (Robust and Reliable System Architecture for Future eCars) project [15] an integrated and open ECU platform for safety-critical functions with sophisticated redundancy concepts is developed. Hereby, fail-operational behaviour is achieved through a dual-duplex architecture, for instance by composing two fail-silent nodes to one fail-operational platform. Additionally, respect is paid to clearly layering and separating the sensor and actor level, vehicle data level, and function level. Furthermore, the extensibility of the system at run-time through Plug&Play techniques allows new components and functions to be added at a later point in time. Despite this, compliance to industry standards, such as AUTOSAR, and support for dissimilar design are not within the scope of these projects.

Moreover, there are several projects aspiring to enhance the development process of automotive E/E systems through model-based approaches. First of all, the ATESST2 (Advancing Traffic Efficiency and Safety through Software Technology) project [16] and the MAENAD (Model-based Analysis & Engineering of Novel Architectures for Dependable Electric Vehicles) project [17] are developing a modelling language for the specific needs of automotive electronic and software systems. To validate the correct timing behaviour of a networked system, the ITEA2 project TIMMO (Timing Model) [18] and the FP7 project ALL-TIMES (Integrating European Timing Analysis Technology) [19] are dedicated towards establishing timing analysis methods for the automotive domain and other industrial domains. However, none of these approaches enable the modelling of adaptivity.

III. Safe Adaptation in FEVs

In contrast to conventional combustion engine vehicles, FEVs distinguish themselves by a special set of safety requirements. For example, vehicles with multiple electrical wheel motors have abandoned the mechanical clutch, which separates the drive train from the motor. Consequently, a software-based control function is indispensable for substituting the mechanical solution and consequently must fulfil high safety standards in order to guarantee fail-operational behaviour and remain controllable in case of failure. Focusing on the issue of rising E/E architecture complexity in upcoming FEVs the SafeAdapt project develops a novel architecture concept based on adaptation to master this challenge, thereby paying particular respect to safety aspects. More precisely, the approach shall enable failure handling and extendability by dynamic function reallocation, run-time adaptation and re-configuration [20] [21] across heterogeneous controllers in systems with high functional safety requirements.

To successfully realise this ambiguous vision, multiple aspects must be addressed (see Figure 2). First of all, in order to preserve functional safety, enhance robustness and availability, and safeguard predictable system-level behaviour even in reconfiguration scenarios, reliable techniques for controlling the adaptation of the system during run-time are needed (see Section III-A). These techniques must safeguard functional and non-functional requirements of dynamic system behaviour that were previously specified during the design phase. During the system development process, a possibility to model the degree of adaptation is desirable (see Section III-C). Therefore, guidelines and methods for developing and analysing adaptive systems, for example, through simulation or formal verification, are obligatory. Furthermore, the essential parameters required for dynamic reconfigurations in safety-critical systems must be determined. During run-time, these predefined properties have to be preserved internally to guarantee the quality of safety-critical applications and prevent unwanted or uncontrolled behaviour. Thus, adherence to a predefined quality of safety-critical applications permits a graceful reaction to unforeseen situations. Moreover, safety issues and certification demands cannot be neglected (see Section III-B) in order to make adaptation and the process of dynamic function reallocation practical for the use in future FEVs.

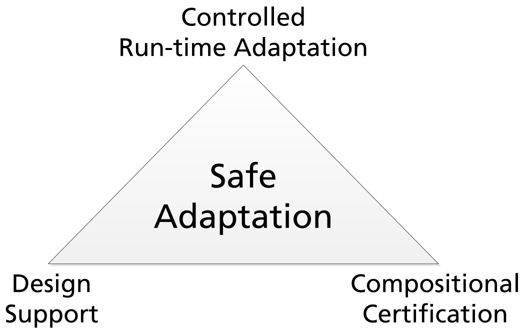

Fig. 2. The three cornerstones of the SafeAdapt approach

A. Controlled Adaptation for Safety-Critical Applications

Dynamic systems with adaptation capabilities create a promising opportunity to improve availability and reliability of safety-critical functionalities during run-time. Therefore, the run-time control system must be able to influence all components. As such, a generic run-time control, which supports controlled adaptation to reliably host safety-critical functions, is important to increase development speed of networked embedded systems and flexible use of components in the e-vehicle domain. However, a central issue concerning future dynamic systems is the efficient utilisation of available resources, as for instance, CPU time slots, power, or external devices.

Therefore, the so-called *SafeAdapt Platform Core* is designed modularly to distribute these resources freely according to the demands of each individual application. In turn, this flexibility not only allows local rearrangement of resource access patterns, but also enables software to be relocated and scheduled on other ECUs (see Figure 3). Based on this concept of application mobility, more elaborate strategies for adaptation are realised to empower the E/E system to reconfigure itself according to the needs of the FEV.

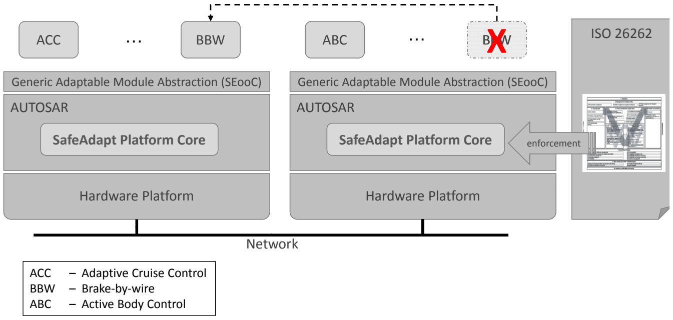

Fig. 3. SafeAdapt Platform Core providing fault tolerance

As Figure 3 shows, in case an application, such as *Brake-by-Wire (BBW)*, fails, the SafeAdapt Platform Core automatically switches the context to a redundantly operated BBW application on another ECU without endangering the correct functioning of the brakes. However, as opposed to the triple modular redundancy concept used in aerospace, there is no need for duplicating each ECU to achieve fault tolerance and reach fail-operational or fail-safe states in the SafeAdapt architecture. Therefore, the SafeAdapt run-time core enables to reduce the amount of ECUs while also providing fault tolerance.

In modern automotive embedded systems the software components interact via a static middleware, such as in AUTOSAR. This middleware, in collaboration with a real-time communication network and the operating systems, takes care of routing inter-component messages to their intended destination. A challenging aspect of this is to allow modifications at run-time while guaranteeing consistency and real-time constraints.

In the context of adaptive systems, a connection failure would occur after an application was relocated onto anther ECU because any other software component previously communicating with that application is unaware of its new physical location. To prevent such potentially disastrous scenarios, a method to uphold communication links between software without breaching any deadlines after a reconfiguration occurred is compulsory. The SafeAdapt core over-satisfies this constraint by following the principle of *Reliability*, *Availability*, *Maintainability*, and *Safety (RAMS)*. It also introduces a concept for transparent addressing, which relieves application developers from the burden of implementing own concepts to ensure correct communications. More precisely, the AUTOSAR standard already describes how requests are routed from one component to another without directly defining its physical location in every application. However, the standard prohibits any changes to this routing at run-time, wherefore the concept must be extended to attain the desired level of flexibility. Regardless, to route messages from any source to any endpoint without running the risk of interference because of different communication priorities, as for instance observed with the currently popular *Controller Area Network (CAN)* bus arbitration [22], a deterministic time-triggered network is expected to ease the realisation. Consequently, to establish a flexible addressability scheme, sensors and actuators are preferably connected directly to the network and not grouped within a domain network as typically done today.

Moreover, applications must be independent from hardware specific solutions in order to enable dynamic function reallocation. In addition, failure handling is currently platform specific and in turn necessitates considerable effort during system development and degrades reusability of software components. Due to this, applications are currently designed for a specific vehicle model, thus hindering the reuse of those components in other models. Consequently, a generic failure and adaptation handling approach is expected to decouple the application logic from the failure handling, thereby significantly improving reusability. More precisely, since the AUTOSAR standard already focuses on interoperability between devices through standardising communication interfaces, it is well suited to be further evolved into a system architecture capable of seamlessly exchanging functionality between different platforms. Hence, it enables the integration on any kind of AUTOSAR-based platform. Furthermore, this approach paves the way for the integration of dissimilar solutions, thus mitigating the risk of common-mode failures by independent designs, without elevating complexity or doubling the number of ECUs. Moreover, redundancy concepts that do not need identically replicated backup ECUs or even utilise triple redundancy to achieve a sufficient level of safety, as for instance seen in the aerospace domain, will be tailored for the specific safety regulations in the automotive sector. For the realisation of such kind of run-time control in e-vehicles, the mode management mechanisms specified in the AUTOSAR standard [7] can be utilised and enhanced.

In addition, adaptive behaviour exhibits the inherent problem of ensuring timing and functional safety requirements for every application even in reconfiguration scenarios [23]. In order to always guarantee predictable system-level behaviour, reliable techniques for controlling the adaptation of the system during run-time are needed [24]–[28]. These techniques must preserve the functional and non-functional requirements specified for the dynamic system behaviour during design time (see Section III-C). During run-time, the predefined properties of the system must be preserved by the run-time control to guarantee the quality of safety-critical applications and prevent unwanted or uncontrolled behaviour. In return, the system is able to gracefully handle unforeseen situations and guarantee the predefined quality of safety-critical applications. Furthermore, these new capabilities foster the parallel integration of safety-critical and non-safety-critical functions, thus leading to a higher system efficiency. All this is achieved by deriving the core blueprints from existing concepts for multi-domain controllers in order to provide an interoperable approach that is compliant to the existing standards for functional safety in the automotive domain, as for example ISO26262 [13], which is described in the next section.

B. Compositional Certification

Safety issues and certification demands must be addressed in order to make adaptation and the process of dynamic function reallocation practical for the use in the automotive domain. The dependability of the system must be ensured to guarantee predictable behaviour of safety-critical applications, such as X-by-Wire systems. With respect to adaptivity, suitable methods and techniques are needed to evaluate the dependability of the new modular run-time control system (see Section III-A). In order to enable certification of adaptive automotive systems, compliance with the domain-specific safety standards is mandatory, and should be achieved through compositional certification to pay respect to the modular nature of the system.

Regarding the relevant standards more closely, IEC61508 is a generic and domain-independent standard that separates safety functions from normal functions. This standard relies on providing as many separate safety protection as needed for reducing the risk to a tolerable level while also considering the system as a whole through the concept of *Equipment Under Control (EUC)*. The need to adopt a specific standard for vehicle E/E systems, where normal functions cannot be separated from safety functions, led to the standard for functional safety named ISO26262 [13]. Nowadays, ISO26262 covers the functional safety assessment for the automotive domain, replacing the IEC61508 standard. The ISO26262 imposes a new life-cycle on the development process of a vehicle's safety-critical features. This requirement is quite remarkable, since traditional certification methods only specify the produced evidence. ISO26262 also supports a modular certification strategy [29] called *Safety Element out-of Context (SEooC)* (ISO26262 Clause 10.8). The SEooC enables modular certification of components or sub-systems even though not all components of the finally deployed system exist during development. This concept of *safety elements* is a key factor for the automotive industry in the pursuit of coping with its multi-tier supplier structure and model variants. Additionally, it promises a massive reduction of certification costs through the modularisation and reuse of certification arguments.

In the aerospace domain, modular architectures allow the composition of pre-certified components with limited re-testing and re-certification effort for the complete system. The DO297 standard [30] supports the integration of context-independent modules into an aircraft system. It defines requirements that support integration of parts of a system also after a roll-out, for instance, in case of a system update, without requiring retesting of the entire resulting system. Following these interference prohibiting requirements guarantees that the newly integrated components do not have an adverse effect on the rest of system. Industrial initiatives, as those driven by the *Avionics Systems Standardisation Committee (ASSC)*, already take advantage of this flexibility in *Integrated Modular Avionics (IMA)* architectures [6].

One of the challenges that arise in applying ISO26262 on FEV development is that there is no previous experience in defining the possible hazards that can arise during runtime, which is however needed for defining countermeasures. SafeAdapt will consider the underlying processes and requirements of certification and qualification standards for the upcoming development and therethrough allow seamless advancement after the prototype implementation is completed. For this, all configuration files and other certification relevant artifacts will be saved for later use in a potential filing for certification and qualification. Therefore, the design path from prototypes towards products that are ready for mass market production will substantially benefit from this prototype design strategy. However, SafeAdapt does not endeavour to certify developed software or hardware, as filing for certification would exceed the scope of project. However, precaution will be taken to collect all required information and to foresee any potential interferences.

In sum, SafeAdapt plans to follow ISO26262 SEooC and adopt an ISO26262-guided life-cycle that will ensure compliance to this standard. This includes hazard identification for FEV and classification of safety levels, while taking into account that all systems are powered from a single energy source. Furthermore, this combination of AUTOSAR, SEooC, and adhering to design principles for safety, reliability and robustness allows the creation of standard, modular and generic-purpose items. Moreover, SafeAdapt leverages this to create an architecture consisting of modular items that can be reconfigured during run-time to enable the reallocation of functions and applications.

C. Design Support for Adaptive Systems

In order to successfully create systems based on a new adaptive run-time control, the development process must also embrace adaptivity. More precisely, guidelines and methods for modelling, developing, and analysing adaptive systems must safely embody the new degrees of freedom.

Therefore, a modelling and evaluation environment is developed that addresses the safety assessment, impact analysis, and Quality-of-Service (QoS) perspective. In detail, for safe run-time adaptation, applications need to express the value of different modes of operation and configuration to facilitate automatic selection, and make this information available in a self-descriptive way [31]. Such an adaptation specification includes the application logic for switching between modes and expresses the requirements for the mode switching process at run-time, as for instance, maximum switching delays, consistency checks, or fall-back configurations. Therefore, safe adaptation will be modelled iteratively on different levels of abstraction during the design process based on pre-existing languages, such as, UML for general purpose modelling [32], MARTE for timing specific aspects [33], EAST-ADL for automotive industry specific hardware abstraction [34], and AUTOSAR for the design flow, as it describes the E/E system at higher levels of abstraction, thus enabling the use of an off-the-shelf AUTOSAR tool-chain in combination with the described design method (see Figure 4). While SafeAdapt specifies adaptive behaviour on system and component level, on implementation level pre-existing AUTOSAR tools shall be used for the software implementation.

Figure 4 describes an overview of the development cycle and the SafeAdapt design process based on the standard "V" cycle. A major disadvantage of the latter is that it demands a fully implemented system before allowing component and integration tests. Consequently, design faults are only detected at a late stage and can accordingly only be corrected at high costs and with project delays. Therefore, the model is extend

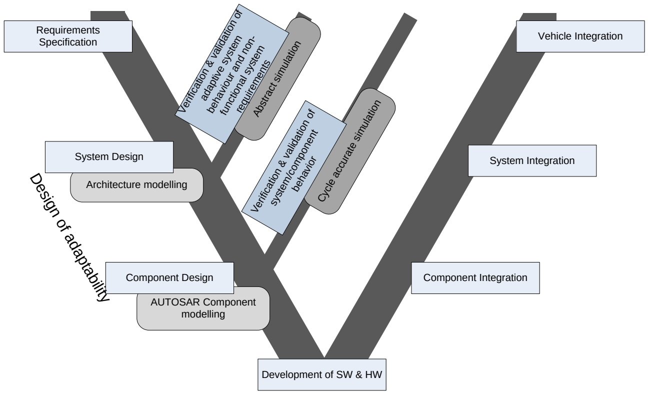
Requirements Specification
Verification & validation of adaptive system behaviour and non-functional system requirements
Abstract simulation
Vehicle Integration
System Design
Architecture modelling
Verification & validation of system/component behavior
Cycle accurate simulation
System Integration
Design of adaptability
Component Design
AUTOSAR Component modelling
Component Integration
Development of SW & HW

Fig. 4. SafeAdapt design flow based on an extended V-model approach

to provide early feedback by means of simulations at different levels of abstraction, illustrated by the additional *legs* in Figure 4.

In detail, the left leg depicts the development phases reaching for requirements engineering to detailed software and hardware implementations. The system and component design is based, on the one hand, on UML and its extensions profiles, such as EAST-ADL. On the other hand, it utilises ARText [35], which is the textual modelling language used by AUTOSAR. Further, to model complementary aspects of a system, the strengths of different modelling language are exploited. For example, UML is better suited to model the overall architecture, whereas ARText is the language of choice to model AUTOSAR specific aspects. Similarly, there is a strong motivation to use different tools for component design. For instance, some components have a strong algorithmic aspect that can be modelled via MATLAB/Simulink [36], while architectural aspects might be modelled directly with UML tools. Consequently, the different tools and languages need to be integrated within the SafeAdapt approach in a manner that facilitates an automated synchronisation between tools.

The additional legs in Figure 4 specify the early verification and validation during the design process of the safe adaptive system. Currently, the focus of system validation is usually on statically configured systems. Especially in safety-critical systems where dynamic reconfiguration might impair safety, the verification and validation throughout the design process is a notable challenge. Functional, non-functional, and trustworthiness properties have to be ensured even during reconfiguration transitions. Therefore, the correct system behaviour in reconfiguration scenarios needs to be verified and validated during the design process. Simulations at different levels of abstractions enable an early feedback whether time and resource constraints are met by a system. In early design stages, abstract simulation of the networked embedded system, for example by using the ERNEST simulation framework [37], enables the analysis of non-functional properties as well as adaptive behaviour on a system-wide level. In later design stages, specific components of sub-systems can be verified by cycle-accurate simulations with tools such as UNISIM [38]. Another complementary validation approach is the use of architectural patterns, for example by applying proven architectural solutions for a certain safety requirement. Moreover, it is important to keep trace that a certain pattern has been applied in order to execute validation rules that come with that pattern. In turn, this enables the certifiability of adaptive embedded systems in the automotive industry with special focus on FEVs regarding ISO26262. Therefore, a concept for the safety analysis of adaptive networked embedded systems during the specification as well as concepts for safety validation and assessment will be derived during the project.

IV. Conclusion and Future Work

SafeAdapt addresses the issue of unmanageably complex E/E architecture in FEVs through an extensive re-design. Thereby, a run-time adaptation system is established to provide availability and efficient, safe, and cost effective robustness. In detail, by enhancing existing platforms with the ability of dynamic function reallocation across heterogeneous controllers, the robustness and availability can be increased without costly and complex redundant dissimilar systems. Furthermore, SafeAdapt will develop a so-called *SafeAdapt Platform Core*, which provides scalable methods and techniques for controlled adaptation and reconfiguration (see Section III-A). Thereby, networked embedded systems for FEVs are enhanced with generic failure handling and adaptive communication concepts that are tailored towards automotive industry budgets but still satisfy the needs of highly safety-critical systems. Moreover, SafeAdapt plans to adopt an ISO26262-guided life-cycle that will ensure compliance with the standard for functional safety in the automotive domain during the entire development phase (see Section III-B). In addition, existing tool chains and development methods are evolved to enable the effective design and early verification and validation of highly critical systems, which are capable of generic failure handling and adaptation (see Section III-C).

In summary, this approach shall substantially improve system complexity and development efforts, thereby also reducing the bill of materials, assembly times, and maintenance efforts. Consequently, the approach leads to higher energy efficiency while also establishing more resilient systems that are capable of withstanding more severe failures. In order to evaluate the results of the project in a realistic setting, SafeAdapt will integrate the resulting E/E architectural concept into a full-scale prototype e-vehicle to assess and verify its characteristics and appropriateness in practice. For evaluation purposes different hardware platforms will be connected via a reconfigurable deterministic network and integrated into the prototype. Further, the advantages of the SafeAdapt approach will be demonstrated using different kinds of safety-critical e-vehicle applications, such as Advanced Driver Assistance Systems and X-by-Wire features.

The SafeAdapt approach currently focuses on Fully Electric Vehicles (FEV). However, it will also be possible to use the results of the project in other domains relying on distributed embedded systems, such as industrial automation or railway, by adopting the concept with respect to domain-specific standards and regulations.

Acknowledgment

This work was funded by the European Commission within the Seventh Framework Programme as part of the SafeAdapt project under grant number 608945.

References

[1] automotiveIT International, “VW’s Hackenberg says autonomous driving feasible by 2028.” http://www.automotiveit.com/vws-hackenberg-says-autonomous-driving-feasible-by-2028/news/id-00129 [Online 27.01.2014], 2011.

[2] A. Pretschner, M. Broy, I. Kruger, and T. Stauner, “Software engineering for automotive systems: A roadmap,” in *Future of Software Engineering (FOSE ’07)*, pp. 55–71, 2007.

[3] K. Venkatesh Prasad, M. Broy, and I. Krueger, “Scanning advances in aerospace & automobile software technology,” *Proceedings of the IEEE*, vol. 98, no. 4, pp. 510–514, 2010.

[4] AUTOSAR Consortium, “Automotive Open System Architecture (AUTOSAR) 4.0 specification,” 2009.

[5] S. Gandhi and S. Brewerton, “Techniques and measures for improving domain controller availability while maintaining functional safety in mixed criticality automotive safety systems,” tech. rep., SAE Technical Paper 2013-01-0198, 2013.

[6] Industrial Avionics Working Group Avionics Systems Standardisation Committee (ASSC), “Modular software safety case process,” 2010.

[7] AUTOSAR Consortium, “Guide to Modemanagement, V1.0,” 2011.

[8] ACTORS Project. http://www.actors-project.eu [Online 27.01.2014].

[9] HEMIS Project. http://www.hemis-eu.org/ [Online 27.01.2014].

[10] D. Chen, R. Anthony, M. Persson, S. Scholle, V. Friesen, G. de Boer, A. Rettberg, and C. Ekelin, “An architectural approach to autonomics and self-management of automotive embedded electronic systems,” in *4th European Congress ERTS: Embedded Real Time Software 2008*, 2008.

[11] R. Anthony, A. Rettberg, D.-J. Chen, I. Jahnich, G. de Boer, and C. Ekelin, “Towards a dynamically reconfigurable automotive control system architecture,” in *Embedded System Design: Topics, Techniques and Trends* (A. Rettberg, M. C. Zanella, R. Dömer, A. Gerstlauer, and F. Rammig, eds.), no. 231 in IFIP The International Federation for Information Processing, pp. 71–84, Springer US, 2007.

[12] iLand Project. http://www.artemis-ia.eu/project/index/view?project=10 [Online 27.01.2014].

[13] International Organization for Standardization (ISO), “ISO/DIS 26262: Road vehicles - functional safety,” 2011.

[14] POLLUX Project. http://www.artemis-pollux.eu/ [Online 27.01.2014].

[15] RACE Project. http://www.projekt-race.de/ [Online 27.01.2014].

[16] ATESST2 Project. http://www.atesst.org/ [Online 28.01.2014].

[17] MAENAD Project. http://www.maenad.eu/ [Online 28.01.2014].

[18] TIMMO Project. http://timmo-2-use.org/timmo/index.htm [Online 28.01.2014].

[19] ALL-TIMES Project. http://www.mrtc.mdh.se/projects/all-times/ [Online 28.01.2014].

[20] P. McKinley, S. Sadjadi, E. Kasten, and B. H. C. Cheng, “Composing adaptive software,” *Computer*, vol. 37, no. 7, pp. 56–64, 2004.

[21] P. Oreizy, M. Gorlick, R. Taylor, D. Heimhigner, G. Johnson, N. Medvidovic, A. Quilici, D. Rosenblum, and A. Wolf, “An architecture-based approach to self-adaptive software,” *IEEE Intelligent Systems and their Applications*, vol. 14, no. 3, pp. 54–62, 1999.

[22] Robert Bosch GmbH, “Controller Area Network (CAN) Specification - Version 2.0,” 1991. http://www.semiconductors.bosch.de/media/pdf/canliteratur/can2spec.pdf.

[23] M. Zeller, G. Weiss, D. Eilers, and R. Knorr, “An approach for providing dependable self-adaptation in distributed embedded systems,” in *Proceedings of the 2011 ACM Symposium on Applied Computing*, SAC ’11, pp. 236–237, ACM, 2011.

[24] G. Weiss, M. Zeller, D. Eilers, and R. Knorr, “Towards self-organization in automotive embedded systems,” in *6th International Conference on Autonomic and Trusted Computing*, ATC ’09, pp. 32–46, Springer-Verlag, 2009.

[25] M. Zeller, C. Prehofer, G. Weiss, D. Eilers, and R. Knorr, “Towards self-adaptation in real-time, networked systems: Efficient solving of system constraints for automotive embedded systems,” in *Proceedings of the 5th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, pp. 79–88, 2011.

[26] M. Zeller and C. Prehofer, “Timing constraints for runtime adaptation in real-time, networked embedded systems,” in *Proceedings of the 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS ’12)*, pp. 73–82, 2012.

[27] M. Zeller and C. Prehofer, “A multi-layered control approach for self-adaptation in automotive embedded systems,” *Advances in Software Engineering*, vol. 2012, p. 15, 2012. Article ID 547157.

[28] M. Zeller and C. Prehofer, “Modeling and efficient solving of extra-functional properties for adaptation in networked embedded real-time systems,” *Elsevier Journal of Systems Architecture (JSA): Special Issue on Embedded Systems Software Architecture*, vol. 59, no. 10, Part C, pp. 1067–1082, 2013.

[29] J. Rushby, *Modular Certification*. 2001.

[30] Radio Technical Commission for Aeronautics Inc. (RTCA), “DO-297: Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations,” 2005.

[31] G. Weiss, K. Becker, A. Radermacher, and S. Gerard, “RT-Describe: self-describing components for self-adaptive distributed embedded systems,” in *3rd Workshop on Adaptive and Reconfigurable Embedded Systems (APRES ’11)*, 2011.

[32] OMG, “Unified Modeling Language (UML), V2.4.1.” http://www.omg.org/spec/UML/2.4.1/ [Online 28.01.2014].

[33] OMG, “The UML profile for MARTE: Modeling and analysis of real-time and embedded system.” http://www.omg.org/spec/MARTE/ [Online 28.01.2014].

[34] EAST-ADL. http://www.east-adl.info/ [Online 28.01.2014].

[35] ARText. www.artop.org/artext/ [Online 29.01.2014].

[36] The Mathworks Inc., “MATLAB/SIMULINK.” http://www.mathworks.com/.

[37] ERNEST - framework for the EaRly verification and validation of Networked Embedded SysTems. http://www.esk.fraunhofer.de/ernest [Online 29.01.2014].

[38] UNISIM Virtual Platforms. http://unisim-vp.org/ [29.01.2014].