

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: fname.surnameg@esk.fraunhofer.de

Schleiss P, Zeller M, Weiss G, et al. SafeAdapt-Safe Adaptive Software for Fully Electric Vehicles[C]//3rd Conference on Future Automotive Technology (CoFAT). 2014.

SafeAdapt - Safe Adaptive Software for Fully Electric Vehicles (FP7)




Marc Zeller

Institutions: Siemens

Goal:

The main idea of SafeAdapt is to develop novel architecture concepts based on adaptation to address the needs of a new E/E architecture for FEVs regarding safety, reliability and cost-efficiency. This will reduce the complexity of the system and the interactions by generic, system-wide fault and adaptation handling. It also enables extended reliability despite failures, improvements of active safety, and optimized resources. This is especially important for increasing reliability and efficiency regarding energy consumption, costs and design simplicity.

SafeAdapt follows a holistic approach for building adaptable systems in safety-critical environments that comprises methods, tools, and building blocks for safe adaptation. This also includes certification support of safety-critical systems in the e-vehicle domain. The technical approach builds on a SafeAdapt Platform Core, encapsulating the basic adaptation mechanisms for re-allocating and updating functionalities in the networked, automotive control systems. This will be the basis for an interoperable and standardized solution for adaptation and fault handling in AUTOSAR. The SafeAdapt approach also considers functional safety with respect to the ISO 26262 standard.

SafeAdapt provides an integrated approach for engineering such adaptive, complex and safe systems, ranging from tool chain support, reference architectures, modelling of system design and networking, up to early validation and verification. For realistic validation of the adaptation and redundancy concepts, an actual vehicle prototype with different and partly redundant applications is developed. 

弗劳恩霍夫通信系统ESK研究所

This work was funded by the [European Commission](#) within the Seventh Framework Programme as part of the [SafeAdapt project](#) under [grant number 608945](#)

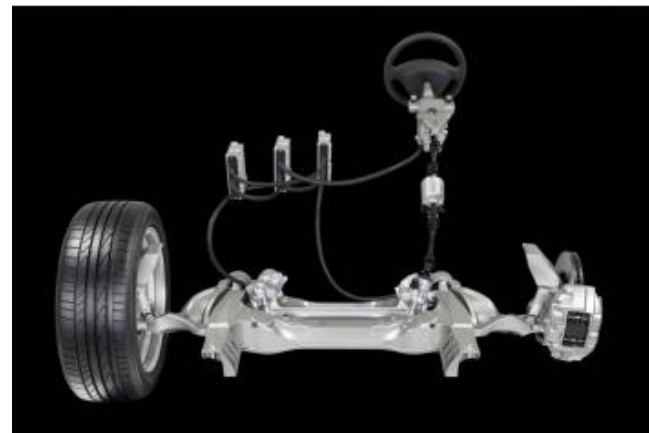
- 上次汇报的：“Zeller M, Prehofer C, Weiss G, et al. Towards self-adaptation in real-time, networked systems: Efficient solving of system constraints for automotive embedded systems[C]//Self-Adaptive and Self-Organizing Systems (SASO), 2011 Fifth IEEE International Conference on. IEEE, 2011: 79-88.”
解决的是运行时重配置的问题，抽象、转化成为NP完全问题，最后用启发式解决，主要贡献在于建立了有效且可解的系统模型。
- 本次论文其实是SafeAdapt项目的一个概述，这个项目想解决的问题比较大、偏汽车软件工程

SafeAdapt Project

- funded by the [European Commission](#)
- 关键词：全电动汽车 + 安全关键(ISO26262)
- 目标：holistic approach
- e-vehicle prototype
- 特点：工程化、标准、汽车软件工程；理论+原型系统

SafeAdapt 的主要想法是开发一套新的基于自适应的体系结构概念，以解决全电动汽车的E/E架构的一些方面的问题，这些方面包括：安全性、可靠、cost-efficiency. 这将降低系统的复杂性，以及通用的、系统级的错误及自适应的处理。

纯电动汽车



- 不采用机械液压结构(比如没有离合器, 把传动系统和马达分开)
- software-based control function取代机械解决方案
- 但机械液压结构本来运行缓慢 可以减缓减弱电子系统的电子系统失效的冒险;
- so纯电动汽车几乎全部依靠X-by-Wire, 所以安全是个问题
 - 高安全性要求,要求guarantee fail-operational behaviour and remain controllable in case of failure
 - ?若全舍弃机械, 那要开发专用的备份系统?
- 同时, 软件定义汽车->新需求出现-->相对独立的子系统之间的相互连接会多==新功能的出现使子系统交互变多->FEV的电子系统的功能越累来越复杂



= 需要一种新的E/E架构

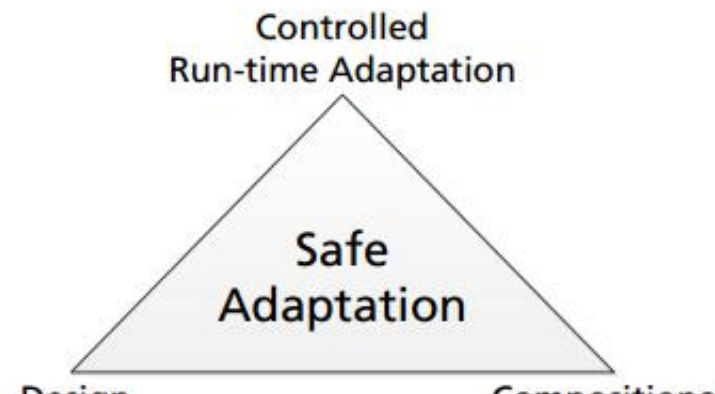
? 怎样的E/E架构能满足better safety characteristics, a manageable form of complexity, and higher cost efficiency

: Adaptive concept: 有能灵活重配置的系统, 就能废除专用的备份系统

++: Safeadapt着手于建立一个有很大改进的灵活的蓝图, 同时兼容AUTOSAR标准。

SafeAdapt intends to

- 1: 大量减少ECU的数目by将多种function结合到一般平台上
- 2: 增加safety和availability by 一种统一的错误处理方法: 一个ECU失效后将application重配置到别的devices上实现
- 3: 降低开发成本 <= 简化EE设计、集成、验证、维护
- 4: 提高能源有效性by限制活跃的devices数量及通信链路数量, 借此降低重量及使能更复杂的技术
- 5: 促进低效运行的机械技术的废除。。。。



SafeAdapt

- A. Controlled Adaptation for Safety-Critical Applications

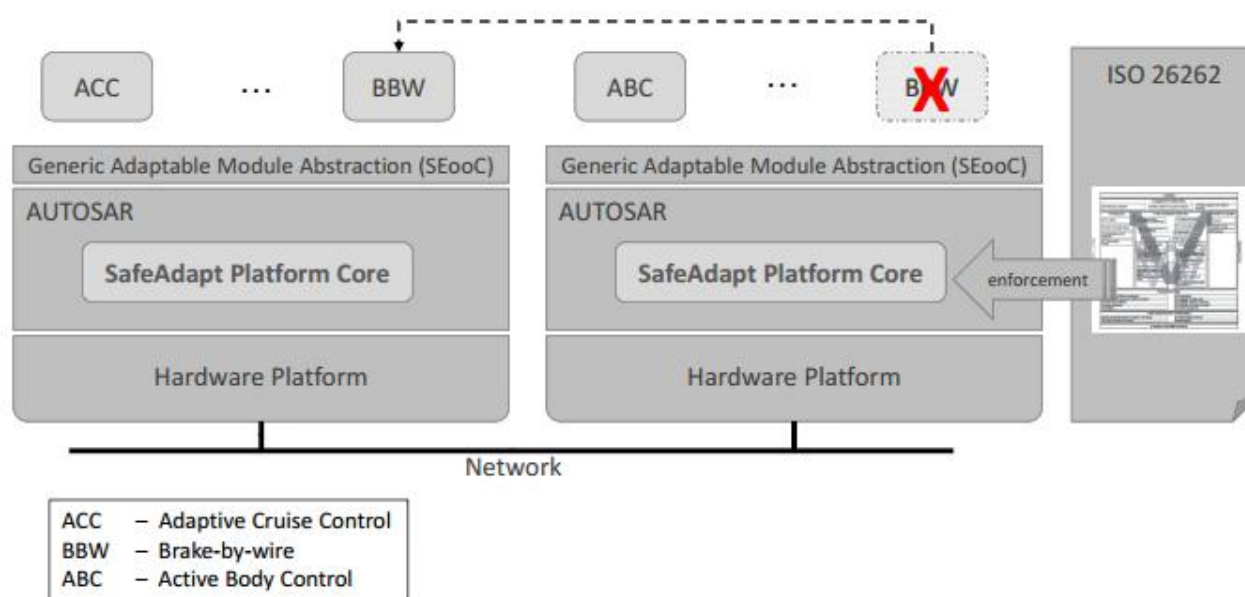


Fig. 3. SafeAdapt Platform Core providing fault tolerance

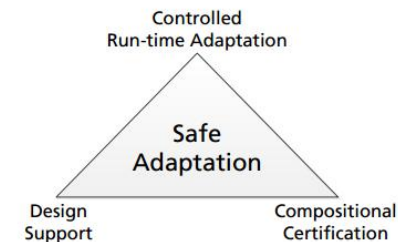


Fig. 2. The three cornerstones of the SafeAdapt approach

- application可以relocate, 在一个ECU上出错可以转移到另一个ECU上运行=>就不需要对每一个ECU进行备份来做容错=>减少ECU的数量
- 以前软件组件之间通过静态中间件->改变--uphold 软件组件之间的通信连接(防止relocate时 connection failure)
- application与hardware解绑 以支持relocate
- failure handling由platform specific变为generic, 逻辑上将application 和 failure handling解绑, 以提高软件组件的重用性
- ensuring timing and functional safety requirements for every application even in reconfiguration scenarios

SafeAdapt

- B. Compositional Certification

- Safety issues and certification demands
- plans to follow ISO26262
- hazard identification for FEV and classification of safety levels （难点，冒险、安全级别在电动汽车里目前没有定义）

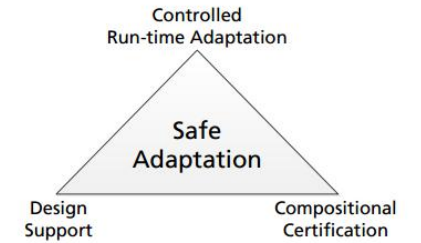


Fig. 2. The three cornerstones of the SafeAdapt approach

SafeAdapt

- C. Design Support for Adaptive Systems

- a modelling and evaluation environment is developed
- existing tool chains and development methods are evolved to enable the effective design and early verification and validation of highly critical systems

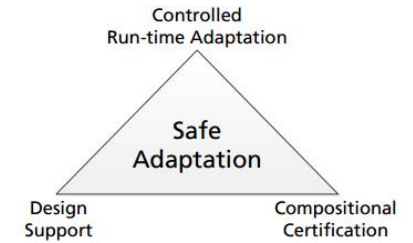


Fig. 2. The three cornerstones of the SafeAdapt approach

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

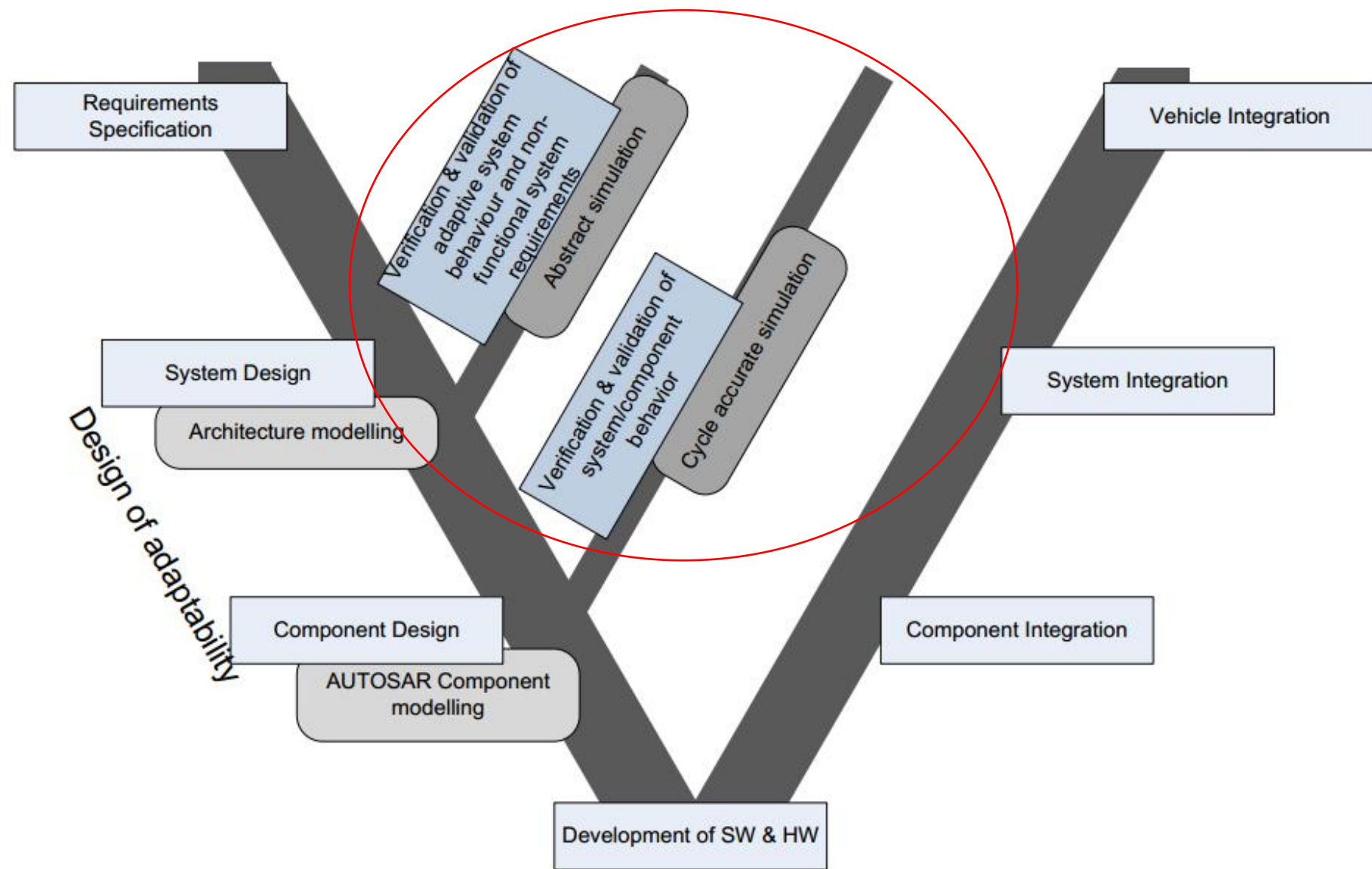


Fig. 4. SafeAdapt design flow based on an extended V-model approach

全电动汽车需要很复杂的冗余方案来保证关键功能的安全性 (e. g. Brake-, Steer-by-Wire)



整体的汽车E/E架构会变得更复杂和高成本

SafeAdapt 的主要想法是开发一套新的基于自适应的体系结构概念，以解决全电动汽车的E/E架构的一些方面的问题，这些方面包括：安全性、可靠、cost-efficiency. 这将降低系统的复杂性，以及通用的、系统级的错误及自适应的处理。

相关项目

- DySCAS (Dynamically Self Configuring Automotive Systems)
 - European Commission,08~
 - dynamic reconfiguration/middleware supporting dynamic reconfiguration/context awareness
- ACTORS (Adaptivity and Control of Resources in Embedded Systems)
 - 2014
 - design of complex embedded systems
 - aims to provide adaptive resource management during run-time based on feedback control

thinking

- 这篇材料的意义在于指出了几个有依据的 可以做文章的点
 - 未来的车用情况下，ECU虽然仍异构，但专有性降低，
 - application 重新放置的问题=>比如上一篇就通过合理建模转变为布尔逻辑可满足性问题
 - 能源有效利用的问题=>比如几个休眠几个活跃？
 - 冗余数量的问题=>冗余多少合适？
 - 全电动汽车和ISO26262结合的问题=>怎样定义和26262中相对应的冒险行为？安全级别？（电动车特有结构特点）

安全关键约束、时间约束

- 1: 大量减少ECU的数目 by 将多种function结合到一般平台上
- 2: 增加safety和availability by 一种统一的错误处理方法：一个ECU失效后将application重配置到别的devices上实现
- 3: 降低开发成本 by 简化EE设计、集成、验证、维护
- 4: 提高能源有效性 by 限制活跃的devices数量及通信链路数量，借此降低重量及使能更复杂的技术
- 5: 促进低效运行的机械技术的废除。。。？

Thank you~