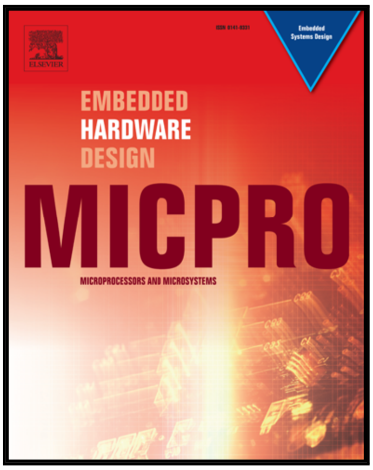

Safe Adaptation of Vehicle Software Systems

Mahmoud Hussein , Reda Nouacer , Ansgar Radermacher

PII:	S0141-9331(16)30417-3
DOI:	10.1016/j.micpro.2017.06.014
Reference:	MICPRO 2584
To appear in:	*Microprocessors and Microsystems*
Received date:	9 January 2017
Revised date:	11 May 2017
Accepted date:	16 June 2017

Please cite this article as: Mahmoud Hussein , Reda Nouacer , Ansgar Radermacher , Safe Adaptation of Vehicle Software Systems, *Microprocessors and Microsystems* (2017), doi: 10.1016/j.micpro.2017.06.014

Safe Adaptation of Vehicle Software Systems

Mahmoud Hussein[1, 3], Reda Nouacer[2], Ansgar Radermacher[1]
[1]CEA, LIST, Laboratory of Model Driven Engineering for Embedded Systems,
[2]CEA, LIST, Software Reliability and Security Laboratory
P.C. 174, Gif-sur-Yvette, 91191, France
[3]Faculty of Computers and Information, Menofia University, Egypt
{mahmoud.hussein, reda.nouacer, and ansgar.radermacher}@cea.fr, mahmoud.hussein@ci.menofia.edu.eg

***Abstract*- The promising advent of Fully Electric Vehicles (FEVs) also means a shift towards fully electrical control of the existing and new vehicle functions. In particular, critical X-by-wire functions require sophisticated redundancy solutions. As a result, the overall Electric/Electronic (E/E) architecture of a vehicle is becoming even more complex and costly. The SafeAdapt project provides an integrated approach for engineering such adaptive, complex and safe systems, ranging from tool chain support, reference architectures, system modelling and networking, up to early validation and verification. In this paper, we give an overview of the SafeAdapt project methodology. We also describe a particular aspect of the project which is the validation of the system adaptive behavior. To validate the adaptive behavior of a vehicle system, an architecture description language for automotive embedded systems (i.e. EAST-ADL) is used for designing the system. The system design model is then used for generating the embedded software. To ensure that the system behaves correctly at runtime, its adaptive behavior is analyzed using fault injection and monitoring techniques on a virtual platform.**

Keywords— Fully Electric Vehicles; Adaptive Software Systems; Safety; Virtual Platform; Model-driven Development.

1. Introduction

It is largely recognized that the architectures of embedded systems are becoming more and more complex both at hardware and software components. Thanks to the constant advances in micro-electronics, embedded system engineers are now able to integrate more system functions on a powerful System-on-Chips (SoCs) [1]. The automotive industry also benefits from these advances in micro-electronics and the engineers are now able to integrate advanced vehicle functions on high performance electronic control units (ECUs). Due to the integration level, the clock frequency and the functioning conditions (e.g. temperature, magnetic fields, etc.), the circuit failure rate increases by approximately √2 in an eighteen month period [2]. Therefore, the issue of robustness and reliability becomes crucial in the design phase.

The automotive industry faces an era of rapid change with the advent of electric drives. Fully electric drive trains promise to reduce exhaust emissions or even achieve the “Zero Emission” dream in case of Fully Electric Vehicles (FEVs) [3]. The trend towards electric vehicles also means a shift towards fully electrical control of existing and new functions. This requires a dramatic change of the system architecture of vehicles. Highly integrated subsystems, like wheel-hub drives, brake-by-wire systems, steer-by-wire systems, active body control etc. must be coordinated and controlled by novel hardware approaches and software implementations since they provide highly safety relevant applications [4]. Due to this, redundant, systems are acting as a fall-back system in case of failure. Initially, these were designed as mechanical fall-backs to electrical systems.

As a result of the above, new trend, the overall Electric/Electronic (E/E) architecture of a vehicle is becoming extremely complex [5]. This accelerates the existing trend of growing complexity of the E/E architecture in current vehicles (see Fig. 1). Today, the functions of the vehicles are provided in several sub-domains with different criticalities, ranging from low critical infotainment systems with typically soft real-time constraints, up to the very safety-critical control software with hard real-time constraints (e.g. steer-by-wire or brake-by-wire). Each of these domains is typically hosted on a different set of Electronic Control Units (ECUs). The control units of each domain are connected by various networks and busses, tailored for the domain requirements, forming a networked embedded system.

The number of networks and ECUs of the E/E architecture are permanently growing to fulfil the increasing demand for more automated functions and electronic controls (see Fig. 1). Nowadays, up to 90% of the innovations in the automotive industry are realized by hardware and software [6], resulting in between 2000 and 3000 atomic functions realized in a software distributed over up to 100 electronic control units (ECUs) in modern high-end cars [7]. In addition, applications like brake-by-wire have another need to replace mechanical systems by E/E systems. In this case, the recuperation of energy is another reason to abandon mechanical systems.

The trend towards fully electric vehicles significantly increases the amount of highly complex safety-critical functionality. It is expected that mechanical back-up systems will be replaced by full X-by-wire in the near future since having mechanically and electrically/electronically controlled systems operating in parallel is too costly and adds too much weight and complexity. In addition, more and more systems, like advanced driving assistance require electric/electronic control of systems such as brakes, drive train, or steering. The vision of “autonomous driving”, which according to major OEMs such as VW can be possible by 2028 [8], clearly needs fully electric/electronically controlled systems in order to be implemented in a safe and cost-efficient way.

This work was funded by the European Commission within the 7th Framework Program as part of the SafeAdapt project under grant number 608945.