SafeAdapt - Safe Adaptive Software for Fully Electric Vehicles

Advance Engineering UK
Birmingham 4-5 November 2015

Sandro Morero
Pininfarina - Italy
Overview & Outlook

- **SafeAdapt - Safe Adaptive Software for Fully Electric Vehicles**
  - Project Duration: July 2013 – End June 2016
  - Consortium: 9 Partners from 6 EU countries
  - Budget: Total costs: € 9.3 million, EU funding: € 5.5 million

- Final e-vehicle prototype for evaluation of SafeAdapt results expected in 2016
<table>
<thead>
<tr>
<th>No</th>
<th>Participant organisation name</th>
<th>Main Role and Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fraunhofer-Gesellschaft e.V.</td>
<td>Modeling and runtime for adaptation, system concepts and design, Coordination</td>
</tr>
<tr>
<td>2</td>
<td>TTTech Computertechnik AG</td>
<td>Networking and ECU provider, safety concepts</td>
</tr>
<tr>
<td>3</td>
<td>Fico Mirrors S.A.</td>
<td>Component (Battery management) and driver assistance applications, prototyping</td>
</tr>
<tr>
<td>4</td>
<td>Fundación Tecnalia Research Innovation</td>
<td>Safety analysis, system concepts</td>
</tr>
<tr>
<td>5</td>
<td>CEA LIST</td>
<td>Modeling of Adaptation, Design and Validation Tools</td>
</tr>
<tr>
<td>6</td>
<td>Siemens AG</td>
<td>System concepts, X-by-wire system, failure concepts, Technical manager</td>
</tr>
<tr>
<td>7</td>
<td>PININFARINA S.P.A.</td>
<td>FEV Manufacturer, overall system design &amp; requirements</td>
</tr>
<tr>
<td>8</td>
<td>DuraCar</td>
<td>FEV Integrator, evaluation, requirements</td>
</tr>
<tr>
<td>9</td>
<td>Delphi</td>
<td>ECU Platform, active driver assistance applications, prototyping</td>
</tr>
</tbody>
</table>
SafeAdapt: Motivation

- Strong need for a new software architecture for safety-critical systems in green vehicles, improving robustness and energy consumption.

- Adaptation is essential for a new architecture to optimize the vehicle’s functionality due to changing environments, failures and new users.

- However, adaptation is challenging in safety-critical industrial application systems due to safety concerns.

- Safe and controlled adaptation is hence a key success factor for the complex, networked control systems in electrical vehicles.
  - Enables to ensure reliability despite failures.
  - Essential for optimizing energy-efficiency (e.g. energy consumption).
Key Concepts of SafeAdapt

- **Enhanced software platforms** in FEVs based on a Safe adaptation core, which encapsulates the basic adaptation mechanisms.

- Generic failure handling mechanisms, with a focus on Autosar platform.

- Provides a fall-back that delimits manufacturers’ liabilities and enables open and evolving systems.

- SafeAdapt provides an integrated approach for engineering adaptive, complex and safe systems.

- Comprises methods, tools, and building blocks to create safe adaptation and to support certification of safe adaptation in FEVs.

- Facilitating the reuse of components.
Objectives

Main Objective: Novel architecture concepts and tools for adaptive systems to enhance the functional safety, flexibility and efficiency of safety-critical systems and active safety features in the green vehicle domain

- **Objective 1:** Reducing the development costs (time-to-market & testing costs) in future FEVs by providing a generic failure and extension management mechanism based on a safe adaptation core

  Based on the adaptation mechanisms, failures can be handled, as well as extensions and updates can be handled by a generic mechanism in the run time platform, particularly focusing on Autosar. The concrete objective is to reduce the development costs up to 20%, as failure handling, and extendibility are require considerable effort for systems with high functional safety requirements. In particular, failure handling will be simplified as it is handled in a generic way, which also enables easier reuse and migration of software.
Objectives (cont’)

- **Objective 2:** Increasing safety by the ability to handle complex failures by the safe adaptation core, especially failures where current systems do not degrade gracefully.

  - By adaptation mechanisms, functionality in a vehicle can be moved to different ECUs in case of failures. In this way, failures of critical, but non-redundant features can be addressed. For instance, the ESP control can be moved to some other ECU in case of a failure of the ECU or the network. Furthermore, gradual degradation of the functionality is possible by adapting to a different mode with a different software configuration. For instance, in case of an HMI failure, the vehicle may only be allowed to drive slowly.
Objectives (cont’)

- **Objective 3:** Reducing bill of material by optimizing the need for redundant ECUs for safety-critical functions (e.g. break-by-wire etc.) by providing a generic failure management based on the safe adaptation core.
  
  Since failure management is handled in run-time platform and not by each software function individually, the necessary amount of redundant hardware can be optimized on a system-based level. Thus, the number of redundant ECUs can be reduced eventually, which results in a reduction of the bill of material as well a decrease weight and energy consumption.

- **Objective 4:** Increasing energy efficiency by reducing number of ECUs and by enabling different driving modes by context-aware adaptation
  
  Deactivation of comfort functions in low energy situations
Controlled Adaptation through SafeAdapt Platform Core

- **Controlled Adaptation for Safety-Critical Applications**
  - SafeAdapt Platform Core, responsible for controlled self-adaptation (generic, system-wide fault and adaptation handling)
Hardware Architecture

AGG  Aggregate ICT Information and Communication Technology
CCC  Central ICT Computing Core
CSCC Central ICT Sub Computing
GWB  General Safety Board
GUI  Graphic User Interface
GW  Gateway / General Safety Board
TMDP Trusted Multi Domain Platform
Expected Benefits

- Enhancement of the **reliability, flexibility and energy efficiency** of safety-critical systems in the electric vehicle domain (e.g. the electric power train)
- Novel software architecture for FEVs based on the safe adaptation core
- Reducing the bill of materials by fail-safe concepts in software
- Reliable engineering methodology for safe adaptive networked embedded systems

- Reduced **development costs** and **time-to-market** due to generic failure handling concept, easier reuse of modules, and development tools

- **Validation** in a joint e-vehicle prototype including X-by-wire applications and active driver assistance applications based on SafeAdapt technology
Expected Technical Results

- Enhanced software architecture for electronics in fully electric vehicles (based on AUTOSAR)
- Update and re-organize the in-vehicle software at run-time
- SafeAdapt Platform Core, which encapsulates the basic adaptation mechanisms
  - Implementation of the ISO26262 Safety-Element-out-of-Context (SEooC) concept
  - Combination of architectural design tools & AUTOSAR

Project website: www.safeadapt.eu
THANK YOU FOR YOUR TIME AND ATTENTION!

Website:  http://www.safeadapt.eu
Project Coordinator: Fraunhofer ESK - safeadapt-coordinator@esk.fraunhofer.de
Sandro Morero – Pininfarina:  s.morero@pininfarina.it