Project acronym:	*SafeAdapt*
Project title:	*Safe Adaptive Software for Fully Electric Vehicles*
Grant Agreement number:	608945
Coordinator:	*Dr.-Ing. Dirk Eilers*
Funding Scheme:	*FP7-2013-ICT-GC*

Deliverable 5.2

Use cases prototypes

Due date of deliverable:	31.12.2015
Actual submission Date:	04.04.2016
Lead beneficiary for this deliverable:	Siemens

Dissemination level

PU	**Public**	**X**
PP	**Restricted to other programme participants (including the Commission Services)**	
RE	**Restricted to a group specified by the consortium (including the Commission Services)**	
CO	**Confidential, only for members of the consortium (including the Commission Services)**	

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013)

Document Information	
Title	Documentation for Deliverable 5.2 – Use cases prototypes
Creator	Fraunhofer ESK
Description	The document contains an overview of the use cases prototypes developed in the SafeAdapt project.
Publisher	Members of the SafeAdapt Consortium
Contributors	Fraunhofer: Annette Paulic, Christian Drabek, Philipp Schleiss, Gereon Weiss TTTech: Andreas Eckel Ficosa: Andrea Saccagno Tecnalia: Alejandra Ruiz, Mª Carmen Palacios, Josu Albizu, Garazi Juez, Maite Alvarez, Maite Alvarez CEA: Ansgar Rademacher, Mahmoud Hussein Siemens: Cornel Klein, Jan Sawallisch, Andre Marek, Konrad Schwarz, Matthias Scheffel, Andreas Zirkler, Meik Felser Pininfarina: Elena Cischino Duracar: Ken Lam Delphi: Thorsten Rosenthal, Olaf Benninghaus, Martin Lange
Language	en-GB
Creation date	01.12.2015
Version number	1.1
Version date	30.06.2016
Audience	□ internal ☒ public □ restricted

Table of Contents

List of Figures

Executive Summary

For proofing the researched concepts and for evaluation purposes, different prototypes have been developed within the scope of the SafeAdapt project, highlighting selective results and use cases. This document briefly gives an overview of these individual prototypes. It represents and documents the finalisation of the developed prototypes only.

1 Overview of Use Cases Prototypes

The prototypes developed in the project comprise a full-scale e-vehicle, a driver-in-the loop simulator, an AUTOSAR model-car, a prototype for evaluating the frozen-standby concepts, and software tool-chain prototypes.

Technical details on the different prototypes and their evaluation can also be found in the respective project deliverables D5.1 [1] and D5.3 [2].

1.1 Full-Scale E-Vehicle Prototype

The full-scale e-vehicle prototype has been enhanced with the SafeAdapt concepts showcasing fail-operational behaviour through exploiting the Safe Adaptation Platform Core (SAPC).

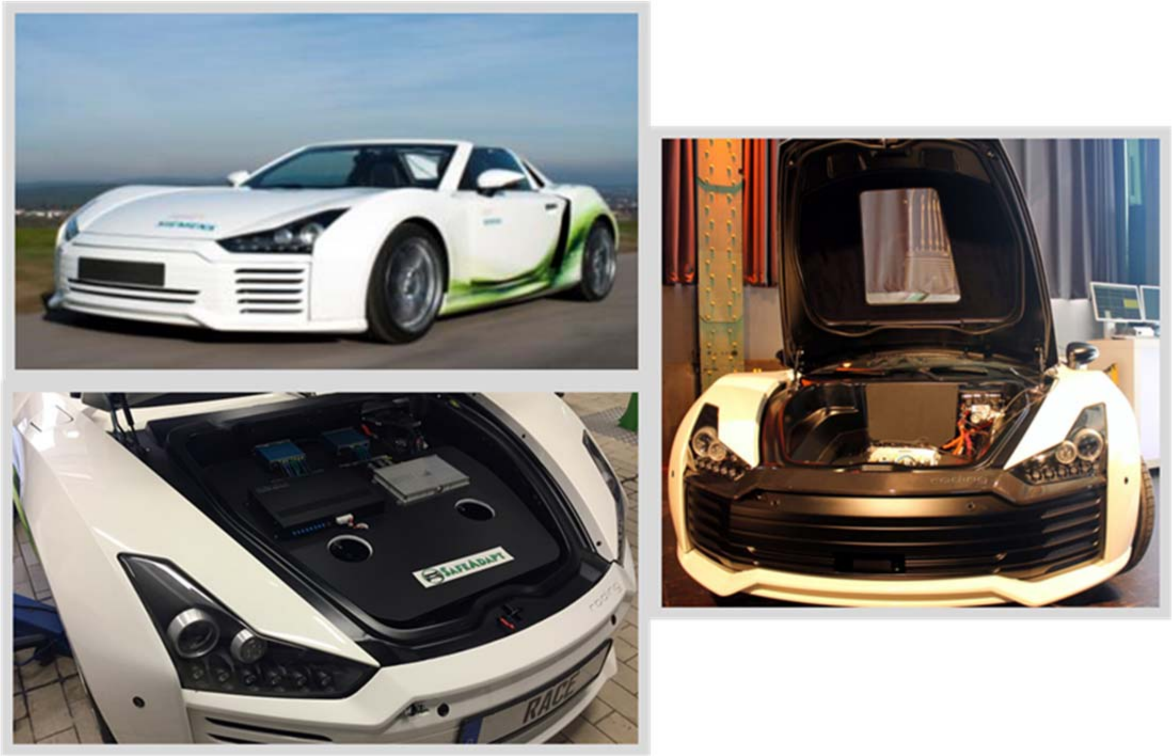

Figure 1: The developed e-vehicle prototype

In Figure 1 the respective developed prototype is depicted. The SafeAdapt enhancements are shown in more detail in Figure 2 with the SafeAdapt central computing core consisting of the TMDP, RACE DCC, and Time-Triggered Ethernet. With this, the fail-operational functionality of the SAPC is evaluated and demonstrated by the example of a Steer-by-Wire application. Even though one core node (RACE or TMDP) or application fails, the steering of the prototype is still functioning.

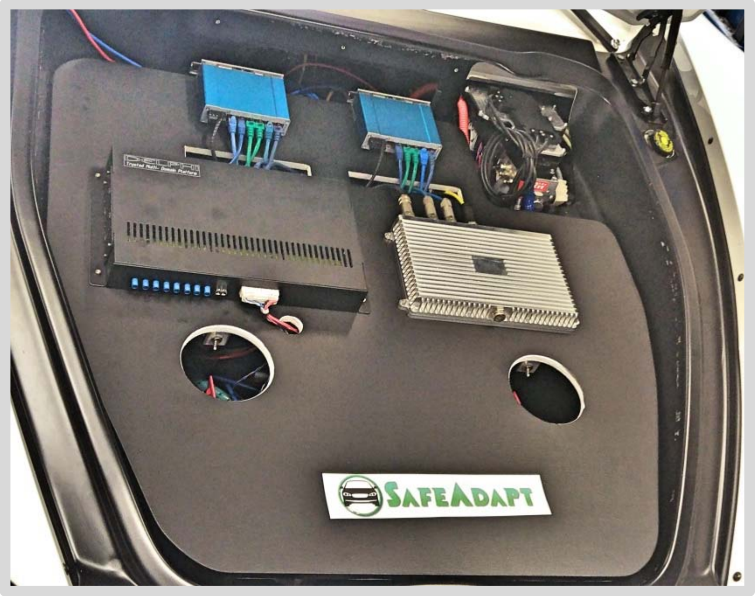

Figure 2: The integrated SafeAdapt central computing core

Detailed information on the prototype and its evaluation can be found in Deliverable D5.3 [2], Section 3.2.

1.2 Driver-in-the-Loop Simulation Prototype

For driver-in-the-loop studies and evaluation the Dynacar simulator has been extended.

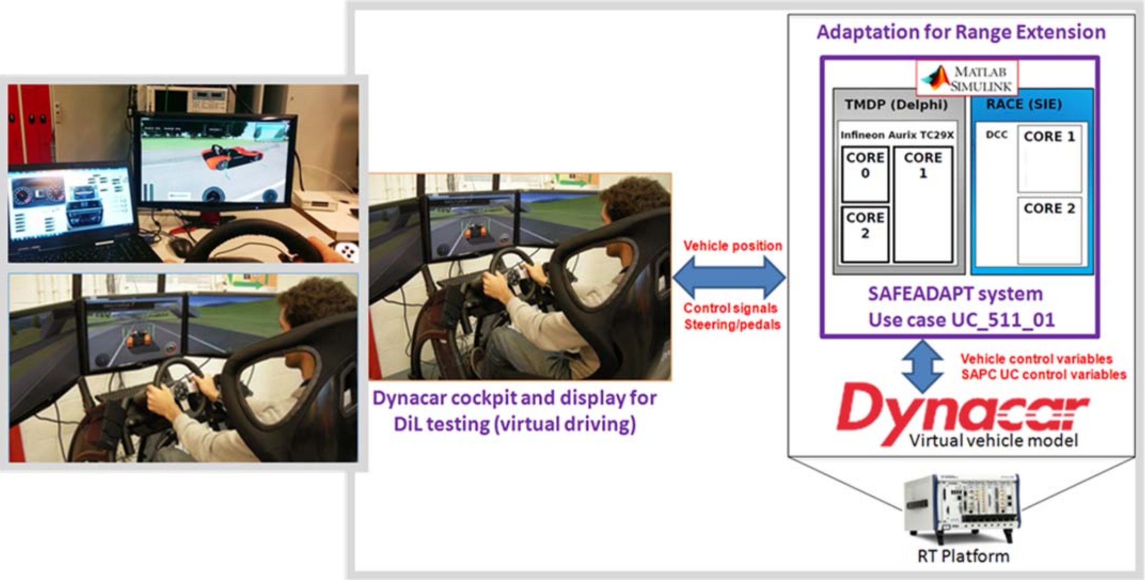

Figure 3: Driver-in-the-loop simulator

A model of the Full-Scale E-Vehicle Prototype (cf. Section 1.1) and the SafeAdapt concepts have been integrated, so that different use cases can be evaluated. For example, in case of the Steer-by-Wire application, the maximum acceptable delay of the SAPC safety mechanism, i.e., the time in which a function remains unavailable, was examined through driver studies. Thus the maximum failover time of the system is evaluated by means of several fault injection tests so that a safe adaptation functionality is ensured without losing the controllability of the vehicle. These evidences are appropriately linked within the modular safety cases related to the safety goals of the SAPC and managed by OpenCert [3] [2].

Moreover, optimisation with respect to energy-efficiency could be safely evaluated in this driver-in-the-loop simulation with the NEDC (New European Driving Cycle) in a straight line. Since the lateral dynamics do not need to be taken in account, the energy consumption is measured in an autonomous driving mode. In the considered scenario, the drowsiness detection SomnoAlert has been integrated as an exemplary non safety-critical application, which can be shutdown to reduce energy consumption and thus, leading to an increased range of an e-vehicle.

More information on this prototype is provided in Deliverable D5.3 [2], Section 3.3.

1.3 Model-Car Prototype

Through a model-car the interoperability of the SafeAdapt concepts with AUTOSAR [4] is shown.

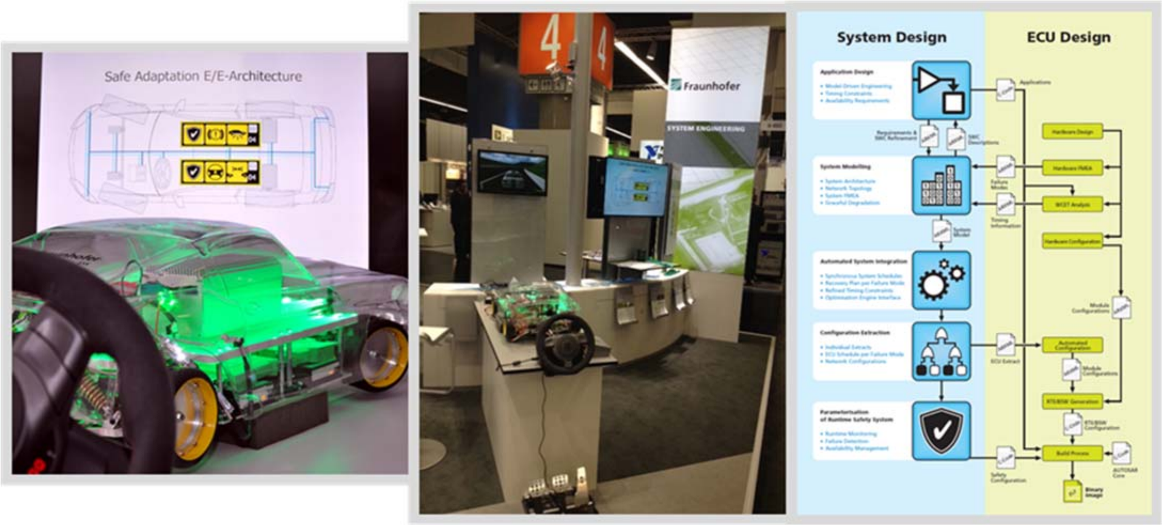

Figure 4: Overview of the model-car prototype

The prototype includes two ECUs (Electronic Control Units) incorporating a current AUTOSAR system with the SafeAdapt enhancements. Thus, the SAPC has been integrated as AUTOSAR Software-Component. The system development has been integrated with AUTOSAR and its tool-flow. On the right hand side of Figure 4 this design integration is depicted abstractly. In the other photos of Figure 4 the prototype demonstration setup is shown.

Overall, this prototype setup consists of a steering wheel and pedal, the model car with two AUTOSAR ECUs, a driving simulation, and a status screen with information on the present system architecture. The steering wheel and pedals are connected through the model car’s ECUs to the driving simulator. It showcases that the failure of a single ECU can be compensated by graceful degradation (cf. [5], Section 4.1), i.e., in this case, infotainment functionality is removed so that steering and accelerating applications can be still provided.

Detailed information on the prototype and its evaluation can be found in Deliverable D5.3 [2], in Section 3.5.

1.4 Frozen-Standby Evaluation Prototype

This prototype represents a SafeAdapt system, in which standby applications are stored in a repository (here called Application Database, see Figure 5) and are loaded to and executed on a distinct ECU when needed, e.g. in case of an ECU breakdown. This scenario is called frozen-standby. The main difference to a cold-standby scenario is the additional upload step from the repository to an ECU.

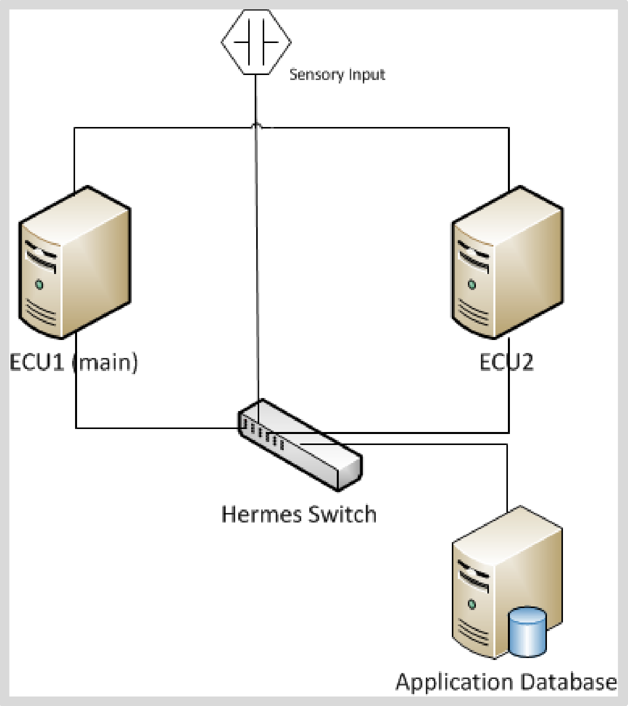

Figure 5: Frozen-standby demonstrator setup

The reasoning for the separate demonstrator on reconfiguration is as follows: The frozen-standby demonstrator was not planned initially. The idea rather was to integrate that into the main SafeAdapt full-scale e-vehicle prototype set-up (cf. Section 1.1). During the work with the architecture of the e-vehicle prototype demonstrator it turned out that generating the reconfiguration between the RACE platform and the TMDP platform with all the gateways, switches, and other interfaces (including the ring architecture involved) would deteriorate the research results to be evaluated.

Apart from other reconfiguration approaches, such as from aerospace (3 redundant, dissimilar units running in hot redundancy with voting) or automotive approaches (using only two hot redundant ECUs like evaluated in DREAMS [6] or the CRYSTAL [7] approach to use a simulation on a significantly cheaper computer compared to i.e. an ASIL D ECU), the SafeAdapt reconfiguration mechanism investigates an “old Airbus Dream”. Aerospace applications also suffer from the high effort in hardware implemented by the triple redundant solution. Thus, having one redundant ECU replaced by a reconfiguration making use of the immense not used computing power in a safety-related system is worth considering.

The setup for the frozen-standby prototype (see Figure 6) consists of:

- ECU1: All applications considered are running on this ECU
- ECU2: A redundant ECU that can run the gracefully degraded functions (after reconfiguration)
- Sensory Input: Sensor simulation for the “test use case”
- Application Database: All applications / functions resident and running on ECU 1 are also stored in this unit, including the “gracefully degraded” versions
- Hermes Switch: This is the network switching unit that allows connecting all network components accordingly

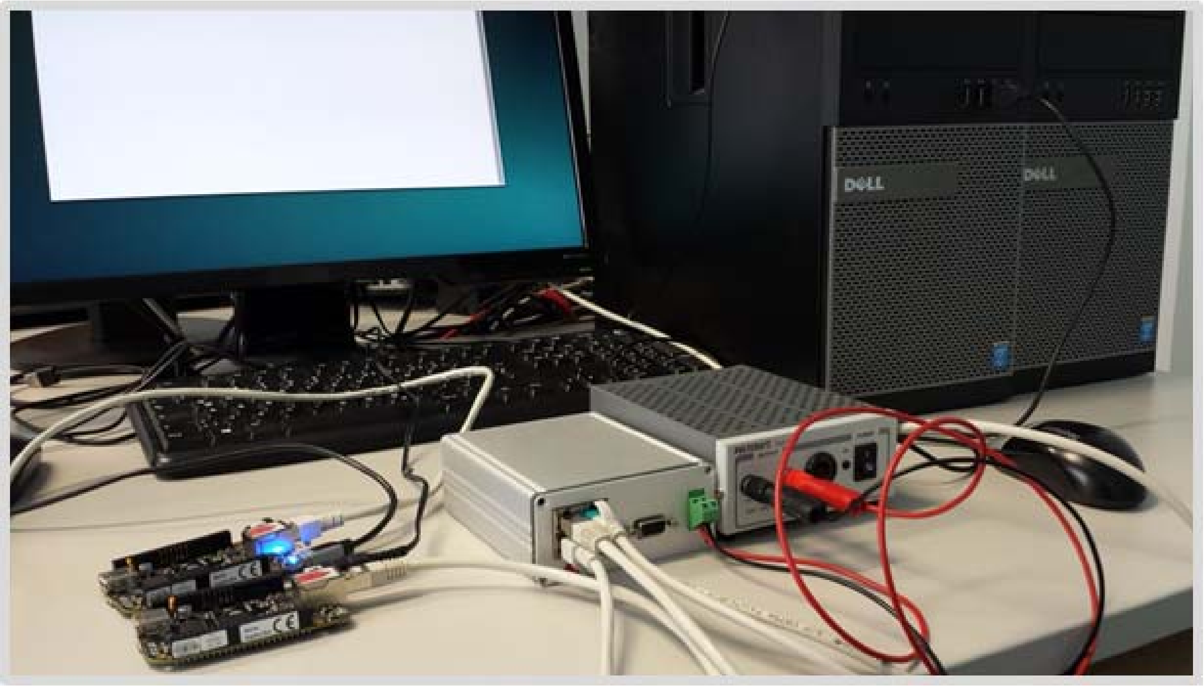

Figure 6: Frozen-standby demonstrator with two ECUs, Hermes Switch & two beaglebones

For the measurements time stamps were introduced in the demonstrator software in order to recognise how many “heartbeats” (1 heartbeat corresponds to 1 millisecond) are used for conducting the subject operation. This is how the individual operation steps were evaluated.

The results are described in detail in the Deliverable D5.3 [2], Section 3.4. A basic video about the demonstration is available and can be shown at the final review on request.

1.5 Tool-Chain Prototypes

The software tools, which have been enhanced and developed within the course of the SafeAdapt project, are described in more detail in Deliverable D5.3 [2], Section 4.1, and distinctly in the project Deliverable “*D4.3 – Prototype tool chain for the design as well as the verification & validation of dynamic system behaviour during the design process*” [8].

Bibliography

[1] SafeAdapt, "D5.1 Evaluation Methodology for the SafeAdapt Results," Project Deliverable, 2015.

[2] SafeAdapt, "D5.3 Evaluation results of the specified use cases and scenarios," Project Deliverable, 2016.

[3] SafeAdapt, "D3.3 Specification of ISO 26262 safety goal for self-adaptation scenarios," Project Deliverable, 2015.

[4] AUTOSAR. (last access June 20, 2016) AUTomotive Open System Architecture. [Online]. http://www.autosar.org

[5] SafeAdapt, "D3.1 Concept for Enforcing Safe Adaptation during Runtime," Project Deliverable, 2015.

[6] Project DREAMS. (last access June 20, 2016) Distributed REal-time Architecture for Mixed Criticality. [Online]. www.dreams-project.eu

[7] Project CRYSTAL. (last access June 20, 2016) CRitical sYSTem engineering AcceLeration. [Online]. www.crystal-artemis.eu

[8] SafeAdapt, "D4.3 Prototype tool chain for the design as well as the verification & validation of dynamic system behaviour during the design process," Project Deliverable, 2016.

List of Abbreviations

Abbreviation	Definition
ACC	Adaptive Cruise Control
AEB	Automatic Emergency Brake
APP	Application
ASIL	Automotive Safety Integrity Level
BbW	Brake-by-Wire
BMS	Battery Management System
CCC	Central Computing Core
CDD	Complex Device Driver
CFT	Component Fault Tree
Cn	Core Node
DCC	Duplex Control Computer
DiL	Driver-in-the-Loop
EBC	Emergency Brake Control
ECU	Electronic Control Unit
E/E	Electric / Electronic
FEV	Fully Electric Vehicles
GW	Gateway
HiL	Hardware-in-the-Loop
HW	Hardware
I/O	Input / Output
IWM	In-Wheel-Motor
MiL	Model-in-the-Loop
NEDC	New European Driving Cycle
RACE	Robust and reliable Automotive Computing Environment
RTE	Runtime Environment
SAPC	Safe Adaptation Platform Core
SbW	Steer-by-Wire
SOC	State Of Charge
TMDP	Trusted Multi Domain Platform
TT	Time-Triggered
TTE	Time-Triggered Ethernet