HAVEit

Highly automated vehicles for intelligent transport

7th Framework programme
ICT-2007.6.1
ICT for intelligent vehicles and mobility services
Grant agreement no.: 212154

The future of driving.

Deliverable D21.2
Software- and Configuration-Process-Concept Available

Version number	Version 1.0
Dissemination level	CO / public version
Lead contractor	Continental Automotive GmbH
Due date	31.07.2009
Date of preparation	31.07.2009

Authors

Michael Gutknecht, USTUTT

Philipp Luithardt, USTUTT

Sergej Bahnmüller, USTUTT

Torsten Schmidt, Continental Automotive GmbH

Project Manager

Prof. Dr. Alfred Hoess

Project Co-ordinator

Dr. Reiner Hoeger

Continental Automotive GmbH, STA EG

Siemensstrasse 12

93055 Regensburg

Germany

Phone +49 941 790 3673

Fax +49 941 790 13 3673

e-mail reiner.hoeger@continental-corporation.com

Executive summary

The consortium confidential deliverable D21.2 provides an overview over the applied software concept for each of the ECUs being used in HAVEit (CSC and XCC, see D21.1). Furthermore, the configuration process concepts are presented, which not only simplify the overall development-process, but also reduce the amount of potential errors during the development and integration of safe architectures.

Background

The overall objective of the HAVEit project is to enhance the safety in road traffic. One measure to achieve this goal is the development of powerful highly automated vehicle applications supporting the driver in critical situations by performing exhaustive driving tasks or even by taking over vehicle control in order to prevent accidents. In comparison with state-of-the art assistance functions, the HAVEit applications shall provide a much higher automation level. This is not only challenging for the software developer of the application, but also for the hardware designer of the specific vehicle systems, ensuring the safe execution of the software commands.

With growing automation level the impact of a faulty application on the vehicle and its environment becomes more critical (e.g. sudden loss of the servo-steering support is much less critical than the sudden loss of an autopilot). Furthermore, it needs to be assured, that

- failures are safely detected,
- faulty components are safely passivated (preventing uncontrolled vehicle movement) and
- the driver is requested to take over vehicle control in cases the ADAS gets lost.

Consequently, measures need to be applied, which provide the required availability and integrity of the highly automated vehicle application.

From the hardware point-of-view, one measure is the appliance of redundancy. By using redundant components, faults can be detected and faulty components can be passivated in consequence (so called fail-silent behaviour). Dependent on the degree of the applied redundancy even systems can be designed which replace faulty components by non-faulty ones and therewith provide the highly automated functionality even after occurrence of a first fault (so called fail-operational behaviour). To provide both behaviours, two different ECUs will be developed within the HAVEit project: for fail-silent behaviour, the CSC-ECU – developed by CAG – constitutes the suitable solution; for fail-operational behaviour, the XCC-ECU – developed by USTUTT – is available (see D21.1 »Hardware-Deliverable«).

Each ECU needs a specific software package, providing the basic functionality of the according control computer. Namely these software packages are the very complex AUTOSAR environment for the CSC and the redundancy management (providing the fail-operational behaviour) for the XCC. For both software packages, configuration processes shall be introduced in HAVEit

- to simplify the overall handling and decrease of the development effort,
- to decrease the individual “brain-work” and therewith potential error sources by provision of approved mechanism snippets and
- to provide a systematic and easy-to-understand process to ensure that no important task will be forgotten.

Results and conclusions

The software and configuration process concepts related to XCC and CSC, respectively, have been successfully implemented.

For the CSC ECU the main focus concerning configurability lies on the AUTOSAR software. Therefore, a tool-chain was presented within this document, explaining step-by-step the implementation and configuration of the AUTOSAR environment. In addition, CAG arranged a workshop for all partners, introducing this tool-chain and the according process.

For the XCC ECU the main focus concerning the configurability lies on the redundancy management, mainly providing the fail-operational behaviour of the XCC. Therefore, the concept of an assumed tool-chain was presented, which will manage and provide the configurability of the redundancy management. This concept states the basis for implementation of the tool-chain, which will start right after.

Both presented concepts promise to satisfy the project's needs, namely:

- to simplify the software production,
- to decrease potential error sources and
- to provide a systematic guideline for the software production.

References

[1] AUTOSAR Layered Software Architecture V2.1.0, R2.1 Rev 0014

[2] AUTOSAR List of Basic Software Modules V1.1.0 R2.1 Rev0014.

[3] AUTOSAR Technical Overview V2.1.0 R2.1 Rev 0014

[4] OMG Object Management Group: Software Process Engineering Metamodel Specification, http://www.omg.org/technology/documents/modeling_spec_catalog.htm

[5] AUTOSAR Methodology V1.1.0 R2.1 Rev 0014

[6] Training slides from "CSC and AUTOSAR Training", 29-30 April 2009, Schwalbach

[7] AUTOSAR Specification of C Implementation Rules V1.0.2 R2.1 Rev 001

[8] MISRA-C:2004 Guidelines for the use of the C language in critical systems, October 2004