Evolution of Functional Safety & Security in AUTOSAR

Stefan Schmerler[1], Simon Fürst[2], Steffen Lupp[3], Demetrio Aiello[4], Frank Kirschke-Biller[5], Robert Rimkus[6], Alain Gilberg[7], Kenji Nishikawa[8], Andreas Titze[9]

[1] Daimler AG, Sindelfingen, [2] BMW AG, München, [3] Bosch GmbH, Heilbronn, [4] Continental AG, Regensburg, [5] Ford Motor Company, Köln, [6] General Motors, Detroit , [7] PSA, Paris, [8] Toyota Motor Company, Brüssel, [9] Volkswagen AG, Wolfsburg

stefan.schmerler@daimler.com

Abstract: AUTOSAR (AUTomotive Open System Architecture) is an open, international standard for the software architecture of automotive ECUs, which is commonly developed in an international consortium of several OEMs, tier1s, and software tool providers. Today, numerous series vehicles with AUTOSAR technology inside are on the road.

Within the AUTOSAR standard, several concepts and mechanisms to support safety & security were developed and included in the design of the AUTOSAR software architecture and in the corresponding functionality of the AUTOSAR basic software modules. Starting with its release 4.0 published in December 2009, AUTOSAR included enhancements with respect to safety-related applications in the automotive domain. The safety-related functionality of AUTOSAR and the functional safety standard ISO 26262 have been developed in parallel with mutual stimulation.

In relation to the described activities, an overview of the available safety & security functionality is shown and a brief description of the following concepts and specified mechanisms is provided:

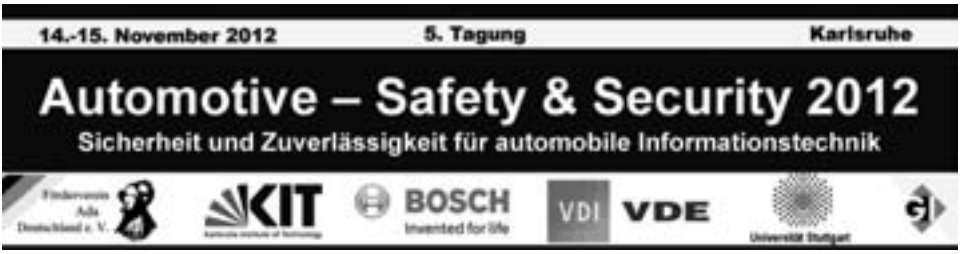
- Built-in self-test mechanisms for detecting hardware faults (testing and monitoring)
- Run-time mechanisms for detecting software execution faults, e.g. program flow monitoring
- Run-time mechanisms for preventing interference between software elements, e.g. memory partitioning for software components and time partitioning for software applications
- Run-time mechanisms for protecting communication, e.g. end-to-end (E2E) communication protection
- Run-time mechanisms for error handling
- Crypto service manager
- Crypto abstraction library

Based on market needs, AUTOSAR plans to enhance the existing safety & security mechanisms and to support new methods and features in the future. An overview of the planned concepts and a brief description of the following extensions is provided:

- Integrated end to end protection
- Hardware test manager for tests at runtime
- Guide for the utilization of crypto services

In addition to the decribed concepts in the field of software architecture, AUTOSAR also plans to introduce several process and methodology improvements, which support the development processes with respect to safety & security aspects. The major ideas of the new conecpts are discussed and a brief description of the following improvements is provided:

- Tracability within the AUTOSAR specification documents
- Safety related extensions for the AUTOSAR methodology and templates
- Signal qualifier concept


14.-15. November 2012
5. Tagung
Karlsruhe
Automotive – Safety & Security 2012
Sicherheit und Zuverlässigkeit für automobile Informationstechnik
KIT
BOSCH
Invented for life
VDI
VDE

Vorträge