AUTOSAR architecture expands safety and security applications

Stefan Bunzel, AUTOSAR - February 17, 2011

Consistent with the growing significance of safety and security for vehicle development, the development partnership AUTOSAR (AUTomotive Open System ARchitecture) published a further release of its specifications. The concepts introduced with Release 4.0 have added technical and functional improvements.

As functional safety is becoming one of the most important topics in automotive development, AUTOSAR addresses the topic of ISO DIS 26262 in Release 4.0 with a series of new features that allow both safety and non-safety applications to operate on the same controller. Additionally, AUTOSAR embeds several security-related features into its software architecture.

AUTOSAR paves the way for innovative electronic systems that further improve performance, safety, and environmental friendliness. By now AUTOSAR has become a de-facto standard for embedded automotive software architecture, but in its previous specification releases there was no explicit focus on safety and security applications. Thus AUTOSAR Release 4.0 contains a large number of new features that were demanded by the different applications of domains the AUTOSAR standard is covering. New concepts introduced in Release 4.0 have added technical and functional improvements and extensions to the main areas including functional safety, architecture, communication stack, methodology and templates, and application interfaces.

Because of the persisting trend of the increasing number of electronically controlled functions within an automobile, the amount of software in a car increases. The automotive industry answered the challenge of functional safety with elaborating the standard ISO DIS 26262, which targets avoiding these risks by providing feasible requirements and processes. Even though the terms safety and security go hand-in-hand, it is important to distinguish them. Safety means functional safety of a system, so that it behaves as specified with absence of unreasonable risk due to hazards caused by malfunctioning behavior, whereas security means the protection of a system against undesired access or usage.

Functional safety features
With Release 4.0, AUTOSAR substantially supports building automotive safety-related applications. This is an outcome of an extensive analysis of the guidance from ISO DIS 26262, which requests the detection and handling of safety issues like hardware faults at runtime, requirements on timing and logical order of execution of applications, communication protection of applications, data corruption, and wrong service calls.
Example of faults detected by E2E protection

(View a full size image)

AUTOSAR addressed those issues noted above via the following features:

1. Memory partitioning provides a fault containment technique to separate software applications from each other in order to avoid any data corruption between applications. This feature allows safety and non safety applications to be implemented on the same ECU.

2. Defensive behavior is a solution preventing data corruption and wrong service calls in the AUTOSAR basic software on microcontrollers having no hardware support for memory partitioning. In this way, the defensive behavior of basic software modules provides a low-cost efficient way to prevent fault propagation for applications with low and medium integrity levels.

3. Support for dual microcontroller architectures targets detection of faults in the core microcontroller by a secondary unit.

4. Program flow monitoring controls the temporal and logical behavior of applications by checking, at specified points of code execution, if the timing and logical order of execution requirements are met.

5. The end-to-end communication protection library is providing a state of the art safety protocol at application level to protect applications against the effects of faults within the communication link (e.g. random hardware faults or systematic faults within the software implementing the AUTOSAR communication infrastructure).

6. Time determinism and timing constraints modeling allow modeling and implementing proper and deterministic timing behavior of applications and basic software. They include synchronized time bases (i.e. a "global time") across ECU networks, synchronized execution and deterministic timing of application software components, as well as support for controlling the timing behavior and detection of timing violations at run-time. The AUTOSAR specification of timing extensions provides means to specify timing constraints like end-to-end (e.g. sensor-to-actuator or communication) delays, minimum/maximum execution times of runnable entities, or constraints on the triggering rate of events.

7. The AUTOSAR basic software provides modules to test hardware (e.g. RAM-Test, Core-Test) and to check the integrity of stored data (e.g. EEPROM Manager).

Security

Security in the automotive domain has gained increased importance through several factors. Third party services, Internet and the connected vehicle, to mention a few innovations, made the vehicle (at least partly) exposed and "visible" to the outer world which requires a higher level of security. Future technological projections clearly show convergence between automotive electronics and
personal computers or consumer electronics technology together with usage of IT standards and protocols. This leads to higher connectivity including "always online," and therefore requires more security.

The following examples illustrate the need for security features in the automobile:

1. It is necessary to secure the programming of ECUs. Only authorized entities shall be able to program ECUs, so that the programming is only possible with original OEM approved software. The application (in the boot-loader) uses standard cryptographic routines and services, e.g. hash, signature verification, and public key encryption (asymmetric encryption).

2. An electronic immobilizer shall protect the vehicle from any unauthorized driving. Technical details are totally OEM dependent but the immobilizer application always uses a specific set of cryptographic routines and services.

3. As a means of efficient variant handling, ECU software often contains multiple functions or variants of them, but only a specific subset shall be enabled for regular usage of the car (e.g. because of national legal restrictions in the country the car is sold to, or due to what the customer has ordered). Typically this is based on special data structures with cryptographic signatures.

4. To secure diagnosis, only dedicated entities are allowed to use certain diagnostic services.

With respect to security AUTOSAR has established the framework to embed a crypto module into the basic software which is called Crypto Service Manager (CSM). This module exposes an interface for security applications to allow for a generic access to standardized cryptographic routines, which provide means to restrict the access to certain functions or their usage to authorized users or callers, and to detect the unauthorized usage or access. It is located within the system services of the service layer. The CSM is configurable and has common access to cryptographic methods. Optionally there is support for cryptographic hardware.

![AUTOSAR Software Architecture Diagram](image)

The crypto module is embedded in the AUTOSAR software architecture.

**Summary and outlook**

With Release 4.0, AUTOSAR has introduced a set of safety- and security-related features into the
standard specifications. They provide standardized means which significantly support developers in achieving the desired Automotive Safety Integrity Level (ASIL) according to ISO DIS 26262.

The availability of such standardized means will simplify the development of automotive E/E systems that require functional safety and security, but they do not turn this into a trivial task. Achieving the appropriate level of functional safety and security still is a major design task on system level that can right now benefit from the mechanisms provided by AUTOSAR Release 4.0.

While the already existing AUTOSAR releases are going to remain under maintenance, the development partnership is already working to selectively enhance the standard. About 50 new technical concepts are jointly worked out and will be implemented in AUTOSAR Release 4.1 by end of 2012.

*Stefan Bunzel* is spokesperson for AUTOSAR.