AUTOSAR Adaptive Platform – a trustable software framework for connected and autonomous driving

Dr.-Ing. Thomas Scharnhorst
AUTOSAR Spokesperson

Symposium Testen - Automatisiertes und Vernetztes Fahren
Braunschweig, September 4th 2018
Topics

› AUTOSAR Introduction

› Challenges and Use Cases

› Developing the Adaptive Platform

› Roadmap, Achievements
AUTomotive Open System ARchitecture

is a worldwide development partnership of car manufacturers, suppliers and other companies from the electronics, semiconductor and software industry.
AUTOSAR – Core Partners and Partners

9 Core Partners

BMW Group  Bosch  Continental  Ford  DAIMLER  PSA GROUP  GM  TOYOTA  VOLKSWAGEN AG

53 Premium Partners

General OEM

VOLVO TRUCKS  HONDA  TATA MOTORS  HYUNDAI  VOLVO  RENAULT  NISSAN  Great Wall

Generic Tier 1

Autoliv  QN  HELLA  dSPACE  DENSO  JTEKT  LEAR

Standard Software

MathWorks  KPI  KPS  TASS  VECtor  SCSK

Tools and Services

altran  ETRI  itk  L&T Technology Services  Deloitte  Green Hills  sodius

Semiconductors

ARC CORE  Fraunhofer  Infineon  RENESAS  NXP

38 Development Partners

ANSYS  Advanced Telematic  PROQA

avelabs  avelabs  Bizarware  E.S.R.LABS

Inchron  rti  Timesys  VOCUS

itemis  SPIRIT  EasyCore  Freescale

OPENSYNERGY  Lauterbach  OSB TTech

SYMTA VISION  NORDSYS  VALIDAS

127 Associate Partners

21 Attendees

© AUTOSAR
Why do we rely on standards?

- Share efforts on non-differentiating parts
- Compete on innovative functions with increased design flexibility
- Reduce costs on overall software development
- Distribute development among suppliers
- Simplify software and system integration
- Enable cooperation
- Create markets and enable new business models
- Enable cooperation
What makes standardization successful?

**Yesterday**

Paper standards with specifications only

**Today**

Joint implementation based on specifications
Automotive software standardization at its best

Optimal sector for standardization in the automotive domain

Specifications

Implementation

Classic AUTOSAR

Adaptive AUTOSAR

OSS Projects

ISO
Advantages of AUTOSAR’s licensing model

**AUTOSAR**

- **Licensing**
  - All contributed IP of any partner is royalty free for all partners
  - Source code and specifications are covered

- **Liability**
  - Minimized for all partners

**Open Source Software**

- **Licensing**
  - Only contributed IP of specific partner is royalty free

- **Open Innovation Network**
  - All complements licensing for Linux

- **Liability**
  - Excluded
Key factors to make AUTOSAR Adaptive Platform a success

- Short development cycles
- Frontloading of validation
- Precision and quality of the standard
- Early availability of exemplary implementation
- Interoperability and increased quality
Flexible implementation of AUTOSAR Adaptive Platform

Feature hub

2017  2018  2019  2020

AP17-03  AP17-10  AP18-03  AP18-10  AP19-03  AP19-10  AP20-03

Implementation of OEM

SOP
AUTOSAR Adaptive Platform
Making the series product

AUTOSAR AP Specification and Source Code + Validation + Maintenance + Documentation + HW Adaption + Configuration + Liability + Testing = Total effort to create a product
Besides all technical advantages

AUTOSAR partners form a strong community

Collaboration, exchange of experiences, discussions…

...with companies you would never have met!
AUTOSAR standardizes two software platforms – Classic and Adaptive
Topics

› AUTOSAR Introduction

› Challenges and Use Cases

› Developing the Adaptive Platform

› Roadmap, Achievements
Game changer for AUTOSAR – selected main drivers

Main drivers for new automotive software systems have been determined.

▷ Highly automated driving
Main drivers for new automotive software systems have been determined.

- Car-2-X applications
- Internet of Things and cloud services
Game changer for AUTOSAR – selected main drivers

Main drivers for new automotive software systems have been determined.

- Increasing data rates
Game changer for AUTOSAR – selected main drivers

Main drivers for new automotive software systems have been determined.

- New processor technologies
Autonomous vehicle: It’s all about trust!

The basis of autonomous driving is **Trustability**. Trustability means **Reliability** at any instance of operation. Reliability is based on **Availability, Safety and Security**.

(Basic Picture: Volkswagen Concept Car Sedric, Geneva Car Salon 2018)
Timeline to full automation

Level 3 automated driving - Conditional automation:
Trustworthy software platform enables developers by safety and security measures do develop onboard software for automated driving.

Level 4 highly automated driving:
E/E Systems cope with all situations automatically in defined use cases. SW platform provides the framework to cope with sensor and data fusion. Perception supports algorithm processing.

The Future: Level 5 full automation
Localization and backend systems providing filtering, data mining and data provision capabilities to support E/E onboard system development.
Topics

› AUTOSAR Introduction

› Challenges and Use Cases

› Developing the Adaptive Platform

› Roadmap, Achievements
AUTOSAR Adaptive Platform – emerging from deeply embedded systems

**Application framework**
- Support for run-time configuration
- Service-oriented communication
- Partial update, system update and upgrade capabilities

**Formats for design data**
- Configuring of dynamic behavior (e.g. constraints for scheduling and communication)
- Consider automotive specific cooperation scenarios
- Support integration with existing systems (Classic Platform)

**Reference architecture**
- Reuse existing (non-automotive) standards
- Ease software development
- Support automotive use-cases and protocols
- Reference Implementation

… and many more
AUTOSAR runtime for adaptive applications – logical architecture

<table>
<thead>
<tr>
<th>AUTOSAR Runtime for Adaptive Applications (ARA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution Management</td>
</tr>
<tr>
<td>Identity Access Management</td>
</tr>
<tr>
<td>Time Synchronisation</td>
</tr>
<tr>
<td>Update and Configuration Management</td>
</tr>
<tr>
<td>Diagnostics</td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>Communication Management</td>
</tr>
<tr>
<td>Persistency</td>
</tr>
<tr>
<td>Signal 2 Service Mapping</td>
</tr>
<tr>
<td>Network Management</td>
</tr>
<tr>
<td>Bootloader</td>
</tr>
<tr>
<td>Platform Health Management</td>
</tr>
<tr>
<td>Logging and Tracing</td>
</tr>
<tr>
<td>Cryptography</td>
</tr>
<tr>
<td>REST</td>
</tr>
</tbody>
</table>

ARA includes POSIX profile PSE51. Additional APIs are extended by the functional clusters.

Not part of AUTOSAR standardization.
# Classic Platform vs. Adaptive Platform

## Technical characteristics

<table>
<thead>
<tr>
<th>Classic Platform</th>
<th>Adaptive Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on OSEK</td>
<td>Based on POSIX</td>
</tr>
<tr>
<td>Execution of code directly from ROM</td>
<td>App. is loaded from persistent memory into RAM</td>
</tr>
<tr>
<td>Same address space for all applications (MPU support for safety)</td>
<td>Each application has its own (virtual) address space (MMU support)</td>
</tr>
<tr>
<td>Optimized for signal-based communication (CAN, FlexRay)</td>
<td>Service-oriented communication</td>
</tr>
<tr>
<td>Fixed task configuration</td>
<td>Support of multiple (dynamic) scheduling strategies</td>
</tr>
<tr>
<td>Specification</td>
<td>Specification and code</td>
</tr>
</tbody>
</table>
Safety expectations, where do they come from?

- ISO 26262 Standards
- HAD
- Centralized E/E architectures

- System architectures capable up to ASIL D
- Reliable system architectures

Supported by Autosar Adaptive Platform:
- Architectural decisions
- Features
- ...
Features and architectural constraints

Examples for safety support

Safe communication:  
→ check sums

Persistant data storage: safety rel. data

Isolation of applications wrt. data and memory → FOI

Configuration of resource budgeting → FOI

Mechanisms to bind individual processes to CPU cores → FOI

Configuration of memory budgeting → FOI

Evaluation of health channels: memory check ok?

Supervision of sw entities → logical sequence of prog execution within time limits?

State dependant behaviour → exec. of error corrections

Secure data access and exchange → implicizt support for safety

Evaluation of health channels:

POSIX PSE51 / C++ STL
Operating System

AUTOSAR Runtime for Adaptive Applications

User Applications

Legend

Legend

© AUTOSAR
Safety approach

➢ Definition of Safety mechanisms integrated into the Layered Architecture
➢ Possibility to tailor Safety mechanisms to project needs
➢ SEooC approach applicable

➢ Definition of Safety mechanisms integrated into the service oriented approach
➢ Possibility to tailor Safety mechanisms to project needs
➢ Definition of the Platform Health Manager

➔ Interoperability between Classic and Adaptive Platform on bus level (e.g. E2E communication)
Security

AUTOSAR goals

- Support the development of secure systems through the two standards
- To provide layered automotive security approach, to define measures at specific layers:
  - Individual ECU
  - In vehicle network
  - E/E architecture
  - Connected vehicle
- Provide und support Coexistence and Interoperability of Security measures between CP and AP

Adaptive Platform Security Feature Team

- Responsible for providing features that enable the development of a secure system
- Provide security controls to platform functional clusters and for secure deployment of adaptive platform application
### Classic Platform vs. Adaptive Platform

**Technical characteristics – additional security features**

<table>
<thead>
<tr>
<th>Classic Platform</th>
<th>Adaptive Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based on OSEK</td>
<td>Based on POSIX</td>
</tr>
<tr>
<td>Execution of code directly from ROM</td>
<td>App. is loaded from persistent memory into RAM</td>
</tr>
<tr>
<td>Same address space for all applications (MPU support for safety)</td>
<td>Each application has its own (virtual) address space (MMU support)</td>
</tr>
<tr>
<td>Optimized for signal-based communication (CAN, FlexRay)</td>
<td>Service-oriented communication</td>
</tr>
<tr>
<td>Fixed task configuration</td>
<td>Support of multiple (dynamic) scheduling strategies</td>
</tr>
<tr>
<td>Specification</td>
<td>Specification and code</td>
</tr>
</tbody>
</table>

- POSIX compliant OS security features
- Applications must be authenticated
- Individual process tree / no awareness of other processes
- Secure communication channels (TLS, IPsec)
- Access control to services
- Predefined quota of memory allocation and fair distribution of processor time
Features and architectural constraints

**security support**

- Secure Communication channels
- Access Control to Service Oriented Communication
- Secure Storage
- Access control framework
- Authentication of applications

Inter-process separation
Process-system separation
Protection against Memory Corruption Attacks

Legend

- SERVICE Non-PF Service
- SERVICE Func. Cluster
- API Func. Cluster

User Applications

- User Applications
  - Adaptive Application
  - Adaptive Application
  - Adaptive Application

Legend

- IPC (local)
- DDS

Legend

- POSIX PSE51 / C++ STL
- Operating System

Legend

- Identity Access Mgmt.
- Persistence
- Time Synchronization
- Platform Health Mgmt.
- RESTful
- State Management
- Diagnostics
- Signal to Service Mapping
- Network Management
- Update and Configuration Management
- Cryptography
- Logging & Tracing
- Execution Mgmt.
- Communication Mgmt.
- Core Types
Intelligence functionality within the vehicle should run on a trusted platform based on safety and security.
Specification of test cases intending to validate the behavior of an AUTOSAR implementation with AUTOSAR application software components or within one vehicle network.
Verification & Validation

- AUTOSAR Platforms via Acceptence Tests are straight due to supplied test cases.
- AI input increases complexity because of non deterministic behaviour.
- UoA applications need to supply diagnostic functionality for safety by themselves w.r.t. required diagnostic coverage.
- V&V needs to be tailored to criticality, requirement maturity and complexity of application → Efficiency of V&V.
Features of Adaptive Platform Release 18-03.

**METHODOLOGY**
- Methodology Extensions for Adaptive
- Service to signal modeling

**EXECUTION MANAGEMENT**
- Resource Management
- Parallel Processing by HWA
- Recovery action framework

**COMMUNICATION**
- Support of RESTful
- Network Management Ethernet

**DIAGNOSTICS**
- Maintenance and Improvements

**PERSISTENCY**
- Data Storage
- Safe Data Storage
- Persistent Data Encryption

**SAFETY**
- Platform Health Management
- Safety concept for AP
- E2E for non periodic communication

**SECURITY**
- Crypto API
- Authentication & Certificates
- Key Management
- Secure Communication
- Support of trusted platform

**LOGGING / TRACING**
- Maintenance and Improvements

**SW-CONFIGURATION MGNT**
- Package Management
- Installation routine

© AUTOSAR
Joint development of AUTOSAR specifications and exemplary software implementations for the AUTOSAR Adaptive Platform

Development in AUTOSAR Work Packages

- ** validate **
- ** improve **

** AUTOSAR Specifications **
Licensing for exploitation

** AUTOSAR Software Implementations **
Providing for product development

› Usage by AUTOSAR partners
Transparent to other standards

Open to connect with others
Identifying / monitoring open source projects
Topics

› AUTOSAR Introduction

› Challenges and Use Cases

› Developing the Adaptive Platform

› Roadmap, Achievements
AUTOSAR Platform Roadmap

Acceptance Tests
- R1.2.0
- Review of open RFCs

Adaptive Platform
- R17-03
- R17-10
- R18-03
- R18-10

Classic Platform
- R4.3.0
- R4.3.1
- R17-10
- R18-03

Foundation
- R1.1.0
- R1.2.0
- R1.4.0

Q1/17 Q2/17 Q3/17 Q4/17 Q1/18 Q2/18 Q3/18 Q4/18
- new contracts

Life Cycle
- released
- planned
- on demand
- development
- evolution
- maintenance
The AUTOSAR Core Partners are fully committed to the standardization of the AUTOSAR Adaptive Platform

- Number-crunching algorithms and high interconnectivity are the demands of future technologies. The Adaptive Platform is exactly what we need.
- AUTOSAR is one of the key enablers for autonomous driving cars.
- AUTOSAR is our standard of choice for realizing new technologies such as autonomous driving and interconnectivity.
11th AUTOSAR

Open Conference and Networking Reception

Networking Reception
Tuesday, November 6th, 2018
7:00 pm – 10:00 pm

Conference
Wednesday, November 7th, 2018
All-day

Venue:
The Portman Ritz-Carlton Shanghai
1376 Nanjing Xi Lu, Shanghai 2000-40, China

Further information:
https://www.autosar.org/news-events/
Further information on AUTOSAR

For more information on AUTOSAR:

- Working results
- User Experiences
- Exploitation

You are welcome to have a look at AUTOSAR’s publications available at the AUTOSAR website www.autosar.org.
© 2017 by AUTOSAR
All rights reserved.
Confidential and proprietary document.

This document and all information contained herein is the sole property of AUTOSAR. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of AUTOSAR. This document and its content shall not be used for any purpose other than that for which it is supplied.

The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, AUTOSAR will be pleased to explain the basis thereof.

Picture Credits – iStock