Software Architectures for Advanced Driver Assistance Systems (ADAS)

Robert Leibinger
July 7th, 2015
Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
About Elektrobit (EB) Automotive

EB’S TECHNICAL CORE COMPETENCES ARE:
Automotive-grade software
System and software architectures

OVER 1300 EMPLOYEES

GLOBAL PRESENCE:
development and business offices in Austria, China, Finland, France, Germany, Japan, Romania and USA

2014 NET SALES* OF MEUR 171.4, up 24%

LISTED ON NASDAQ OMX HELSINKI: EBC1V

Over 70 million vehicles on the road and 1 billion embedded devices

* including 51% of e.solutions
Our solutions for the automotive world

**Infotainment software and services**
- Connected navigation software
- HMI tools for in-dash, digital instrument clusters and head-up displays
- Global software integration and engineering services

**Connected services**
- Connected experiences around urbanization and electrification
- Online diagnostics
- Software and content updates

**Car Infrastructure software and services**
- EB tresos – integrated ECU software and tools, based on AUTOSAR standards
- Complete solutions for: basic software, functional safety, automotive security
- Test & Analyzing solutions
- Functional Safety consulting

**Driver Assistance software and services**
- Software development for driver assistance functions
- Electronic horizon and test drive recording solutions
- Driver Assistance modules and algorithms
Delivering unique experiences year over year

- **1997**: Establishing the idea of embedded systems control via Internet technologies
- **2003**: Providing navigation for the first fully connected solution (Daimler A-class and smart)
- **2004**: Pioneering the separation of HMI software by rest of the vehicle (Audi A6)
- **2008**: e.solutions is formed, a joint venture between EB and Audi Electronics Venture GmbH (AEV)
- **2010**: EB, the first company to take AUTOSAR 4.0 to the road across the globe (all BMW carline)
- **2012**: Strategic partnership of Daimler and EB centered around driver assistance software development
- **2014**: Expanded innovation focus: Automated Driving, Car as a Sensor, Connected Everything

OSPERT Leibinger | 2015-07-07 | © Elektrobit Automotive GmbH 2015. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Software Architectures for Advanced Driver Assistance Systems (ADAS)

EB at the forefront of automotive technology

Paving the way to automated driving

Automated Driving
- EB’s electronic horizon information is playing a major role for predictive driving
- Connected Navigation in combination with Driver Assistance is the lever for highly automated driving

Car as a Sensor
- Delivering ADAS and navigation data (electronic horizon) to enable future driving experiences
- Long-standing experience with connected services in safety- and security-critical environments

Connected Everything
- Know-how in OBD with experience in mission critical client/server systems
- Secure back-end infrastructure to enable OTA data and service updates.
- Always up-to-date maps validated by EB via vehicle sensor data to provide the highest quality maps
Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
History and Roadmap for Accident-Free Driving

- **2015 – 2016:**
  - ACC
  - Longitudinal/lateral
  - Traffic Jam Assistant (highway)
  - Lateral Collision Avoidance
  - Emergency Steering Assistant

- **2020:**
  - Highway Assist
  - Stop & Go, Cruising, 0-130km/h

- **2025:**
  - Construction Site (highly automated)
  - City Stop & Go
  - Inter-Urban

- **2025+:**
  - Highway (highly automated)

Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
Confidence
Software Architectures for Advanced Driver Assistance Systems (ADAS)

Who was this woman?

Taken from wikipedia.org
Bridget Driscoll

• Bridget Driscoll received instant notoriety when she stepped off the kerb and into the history books on August 17th 1896.

• Mrs Driscoll, a 44 year old housewife, who was travelling from Old Town, Croydon to a folk-dancing display in Crystal Palace, became the first pedestrian in the UK to be killed by a car.

• Mrs Driscoll, a resident of Croydon, was hit by a demonstration car travelling at 4mph. She died within minutes of receiving a head injury.
The Case

• Witnesses said that the car, driven by Arthur Edsel, was travelling at a reckless pace, in fact: “like a fire engine”.

• Mr Edsel claimed that he had only been doing 4 mph and that he had rung his bell as a warning.

• The jury took six hours to reach a verdict that Mrs. Driscoll had died of accidental death.

• At Mrs Driscoll’s inquest, Coroner William Percy Morrison said he hoped that “such a thing would never happen again” and was the first to apply the term “accident” to violence caused by speed. Coroners across the country have followed his example ever since.
Today...

WERK IN BAUNATAL

Roboter tötet VW-Mitarbeiter!

Baunatal (Hessen) – Horror-Unfall im Volkswagenwerk Baunatal: Ein Mitarbeiter ist von einem Roboter getötet worden.

Der 22-Jährige war am Montag bei einer neuen Produktionslinie der Elektromotorenfertigung mit dem Einrichten des Roboters beschäftigt, als dieser ihn erfasste und gegen eine Metallplatte drückte. Das teilte ein Sprecher des VW-Werks am Mittwoch mit.

Der Mitarbeiter einer Firma aus Sachsen erlebt schwere Schmerzen im
Complexity
Complexity - Callgraph of an Engine Control Unit
Complexity - Callgraph of an integration platform

- 150 software components
- 14 of them are safety-relevant according to ASIL B
- Over 1000 assembly connectors
- Multiple n:m edges between SWCs
Rising amount of OEM application software at Volkswagen

Standardized software architectures necessary. AUTOSAR is the first step to handle this complexity.
Computing Power
BMW i8 and i3 – Figures and Facts

Already large number of ECUs
Where to get the computing power for ADAS?
Power Consumption within BMW cars

Max. power consumption limits the number of ECUs
Automotive Multicore Microcontroller

Simon Fürst, BMW, EMCC2015 Munich
Rising Quota of Multicore deliveries at Volkswagen

Multicore usage ramps up (e.g. Powertrain). ADAS will speed this up.
Next level of Functional Safety
There is a very basic and helpful definition for a safe system:

“You know what the system does”
Current Systems (usually fail-safe)

Failure Detected?

- Deactivate / degrade function → Safe State
- Inform the driver
- Report a diagnostic error

Standard approach in many safety relevant systems:
- Airbag, ESP, air conditioning, battery charging, ...
- Driver assistant functions such as adaptive cruise control, lane assist, ...

Some functions provide a degraded mode, sometimes limited in time:
- Electronic Power Steering
- Braking
Software Architectures for Advanced Driver Assistance Systems (ADAS)

FULLY AUTOMATED
- Monitoring of the system not required
- Driver does not need to be able to take over the driving task

Example: Highway driving up to 130 km/h

HIGHLY AUTOMATED
- Monitoring of the system not required
- Driver needs to be able to take over the driving task with lead time

Example: Stop-and-go (highway)

PARTIALLY AUTOMATED
- Monitoring of the system required
- Driver needs to be able to take over the driving task at any moment

Example: Stop-and-go up to 30 km/h

Wolfgang Schäfer, Continental, May 19, 2015
Levels of Autonomous Driving (AD)

<table>
<thead>
<tr>
<th>driver in the loop</th>
<th>yes (required)</th>
<th>not required</th>
</tr>
</thead>
<tbody>
<tr>
<td>time to take control</td>
<td>~ 1s</td>
<td>several seconds</td>
</tr>
<tr>
<td>back</td>
<td></td>
<td></td>
</tr>
<tr>
<td>other activities</td>
<td>not allowed</td>
<td>specific</td>
</tr>
<tr>
<td>while driving</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>examples</th>
<th>FCW, LDW</th>
<th>ACC, LKA</th>
<th>Traffic Jam Assistant</th>
<th>Highway Chauffeur</th>
<th>Valet Parking</th>
<th>Robot car</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCW ... Forward Collision Warning</td>
<td>ACC ... Adaptive Cruise Control</td>
<td>LKA ... Lane Keeping Assistant</td>
<td></td>
<td></td>
<td></td>
<td>Source: SAE, NHTSA, VDA</td>
</tr>
</tbody>
</table>
Goal: Autonomous driving

Safe State means:

• Continue driving until driver is in the loop
  – approx. 7-15s for conditional autonomous driving
  – Several minutes for high and full autonomous driving

• Perform an autonomous „safe-stop“ (stand-still at a non-hazardous place)
  – Main issue is to get the driver attention focused on the situation
  – Several minutes, depending on the situation
Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
Approach: 2 channels with comparison

Two ECUs working on the input data, outputs are compared.

A 2 channels with comparison system is simply fail-safe and since you cannot distinguish between “ECU1 not ok” and “ECU2 not ok”.

The safe state is a complete system shutdown.
Approach: 2oo3 Systems

If one of the ECUs fails the system can continue with the remaining two ECUs.

Failures in the input data can be detected by an “Input-Voter”.

This pattern is well established.
2003 Systems and automotive

Applicable for automotive?

- More ECUs
- More wiring
- More weight
- More power consumption
- Higher complexity to manage

Will we as a customer accept that?

- Different opinions and market studies
- Referring to several studies, customer will pay 1500 - 3000 € more for autonomous driving car (mid-size car).

• High diagnostic coverage needed to detect failures in one channel
• IF component fails in one of the two channels, the system does not shut down but continues to operate with one channel

Common sense:
*The best policy is not to operate on a single channel, or not for a long period of time.*
→ See above: only some seconds may be needed.
Diagnostics in software in autonomous driving systems

Integrity mechanism
- Memory Partitioning
- Temporal Monitoring
- Data protection

Infrastructure
- Fault tolerant Ethernet
- Service Orientated communication

Software Engineering
- Plausibility checks
- Functional monitoring
- Defensive programming
- Dynamic analysis

**Safety OS**
- Data Protection
- Stack Protection
- Context Protection
- OS Protection
- Hardware Error management

**Safety E2E Protection**
- Safe communication

**Safety TimE Protection**
- Alive supervision
- Deadline Monitoring
- Control flow monitoring

**OSPERT Leibinger | 2015-07-07 | © Elektrobit Automotive GmbH 2015. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.**
Outlook: Reconfiguration for rebuilding 1oo2D

1oo2D
- Normal operation

1 channel
- Still Operational
- Handover to driver
- Failure recovery
- Internal recovery

< 10s

1oo2D*
- Rebuilding 2 channel system
- Disabling of comfort functions
1oo2D - Normal operation

1oo2D system

ECU1
- Func1
- Func2
- Func3

Diagnose

ECU2
- Func1
- Func2
- Func3

Diagnose

ECU3
- Func1
- Func4
- Func5
- Func6

Fault tolerant Ethernet

Sensors /Actuators

disabled

critical

non-critical
1oo2D – 1 channel

1oo2D system

ECU1
- Func1
- Func2
- Func3

Diagnostics

ECU2
- Func2
- Func3

Diagnostics

ECU3
- Func4
- Func5
- Func6

Fault tolerant Ethernet

Sensors /Actuators

disabled

critical

non-critical
Requirements for Reconfiguration

- Req. 1: Functions can be dynamically relocated
- Req. 2: Sensor/Actuators are redundant or accessible via network
Dynamic Reconfiguration

Req. 1: Functions can be dynamically relocated
- Application information based on AUTOSAR xml description available
- Runtime environment (RTE) supporting reconfigurable software components
- Threads can started/stopped in EB tresos Safety OS

Req. 2: Sensor/Actuators are redundant or accessible via network
- Service orientated communication
- Multi-cast fault-tolerant Ethernet
Agenda

Short overview of Elektrobit automotive

The road to Advanced Driver Assistance Systems

Challenges for ADAS

System Architecture

ECU Software Architecture
Overview of different architecture approaches
Full AUTOSAR architecture

- Safety Microcontroller
- AUTOSAR Multi-Core Safety OS
- ADAS algorithms as SWC
- Advanced hardware drivers integration as Complex Device Drivers
  - e.g. OpenCL, AVB
  - Proprietary video bus systems

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy integration into OEM/T1 AUTOSAR process</td>
<td>Advanced hardware support needs AUTOSAR complex device drivers</td>
</tr>
<tr>
<td>One System</td>
<td>High Performance Safety Microcontroller necessary</td>
</tr>
</tbody>
</table>
Microcontroller partitioning architecture

- Partitioning in Safety and Performance Microcontroller
- Separated applications treated as different ECUs during development
- Private Network for communication

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalable (combine two or more Microcontroller)</td>
<td>Additional hardware costs</td>
</tr>
<tr>
<td>Suitable Microcontroller already available</td>
<td>Need for private communication link</td>
</tr>
<tr>
<td></td>
<td>Complex Flashloader and Startup</td>
</tr>
</tbody>
</table>

All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Core partitioning architecture

- One Microcontroller with several performance cores and one safety core (typically Lockstep)

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>No need for private network hardware</td>
<td>No suitable Microcontroller available today</td>
</tr>
<tr>
<td>Performance and Safety in one Micro</td>
<td></td>
</tr>
</tbody>
</table>
Hypervisor architecture

- Host OS with AUTOSAR guest system on one Microcontroller
- Hypervisor could be part of Guest OS

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor as Gateway between different OS</td>
<td>Limited realtime capabilities</td>
</tr>
<tr>
<td>Hypervisor as Security Gateway between car and cloud</td>
<td>Limited Performance</td>
</tr>
</tbody>
</table>
Compare and contrast each architecture

Full AUTOSAR

Microcontroller Partitioning

Core Partitioning

Hypervisor

Safety or Performance

Safety & Performance

Safety & Performance optimized

Security Architecture

Software Architectures define next generation Microcontroller Architectures

AUTOSAR is part of each architecture as a common standard for
- Basic Software, Safety and Security in ECUs
- Synchronized development process between OEM and T1
Summary

• Re-use of available integrity mechanisms from fail-safe systems is the basis for building fail-operational systems.

• Software systems that are designed to achieve a high diagnostic coverage are available today.

• Fault tolerant Automotive Ethernet is available today.

• Established concepts for fail-operational system are available and can be reused in automotive systems with cost constraints.
Let’s build the next generation software systems for autonomous driving!