A systematic approach based on STPA
for developing a dependable architecture for fully automated driving

ESW 2016, Zürich, September 24th 2016
Daniel Lammering and Asim Abdulkhaleq
Automated Driving Architecture

Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. Results
5. Conclusion & Future Work
Motivation
Current and upcoming challenges

Software and architecture complexity

<table>
<thead>
<tr>
<th>Million Lines of Code</th>
<th>Number of ECUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODERN CAR</td>
<td>100</td>
</tr>
<tr>
<td>FACEBOOK</td>
<td>61</td>
</tr>
<tr>
<td>WINDOWS 7</td>
<td>40</td>
</tr>
<tr>
<td>BOEING 787</td>
<td>14</td>
</tr>
<tr>
<td>ANDROID</td>
<td>12</td>
</tr>
<tr>
<td>LINUX KERNEL 2.60</td>
<td>5</td>
</tr>
</tbody>
</table>

Numbers from 2014
Safety-driven Design

Why paradigm change?

› Old approaches becoming less effective (FTA / FMEA focus on component failures)

› New causes of accidents not handled (interaction accidents / complex software errors)

Component reliability (component failures)

Systems thinking (holistic View)

e.g. Automated Driving

› Many parallel interactions between components!

Data Fusion  Environment Modell  Driving Strategy  Trajectory Planning

› Accidents happen with no component failures (Component Interaction Accidents)

› Complex, Software-intensive Systems (New Hazards: System functional but Process/Event is unsafe)
Automated Driving Architecture

Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. Results
5. Conclusion & Future Work
Automated Driving
A revolutionary approach in evolutionary steps

> 2025
FULLY AUTOMATED
- Monitoring of the system not required
- Driver does not need to be able to take over the driving task

2020
HIGHLY AUTOMATED
- Monitoring of the system not required
- Driver needs to be able to take over the driving task with lead time

2016
PARTIALLY AUTOMATED
- Monitoring of the system required
- Driver needs to be able to take over the driving task at any moment

September 24, 2016
Lammering & Abdulkhaleq © Continental AG
# Automated and Autonomous Driving

## SAE Definitions on Automation Levels

<table>
<thead>
<tr>
<th>SAE level</th>
<th>SAE name</th>
<th>SAE narrative definition</th>
<th>Execution of steering and acceleration/deceleration</th>
<th>Monitoring of driving environment</th>
<th>Fallback performance of dynamic driving task</th>
<th>System capability (driving modes)</th>
<th>BASL level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
<td>the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Human driver</td>
<td>n/a</td>
<td>Driver only</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>Human driver and system</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>Assisted</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
<td>the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>System</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>Partially automated</td>
</tr>
</tbody>
</table>

### Automated Driving

- **3** Conditional Automation: the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene.
- **4** High Automation: the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene.

### Autonomous Driving

- **5** Full Automation: the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.
The future of in-vehicle data management
Automotive part of the network

Vehicle E/E – Architecture needs a holistic approach:

› Service Oriented Architectures
› Secure Connections
› Cloud services / Backend
› Software Update over the Air
A System View on Autonomous Driving
Functional Architecture

SENSE
- Sensors
  - Sensor 1: e.g. stereo camera
  - Sensor 2: e.g. long range radar, lidar
  - Sensor 3: e.g. Backend/HD Map
  - Sensor N: e.g. ...
- Data Interpretation
  - Data Fusion
  - Environment Model
  - Localization
  - Vehicle Model
- Object Abstraction

PLAN
- Driving Strategy
  - Behaviour Planning
  - Maneuver Planning
- Trajectory Planning

ACT
- Motion Control
  - Lateral Controller
  - Longitudinal Controller
- Actuators
  - Actuator 1: e.g. steering system
  - Actuator 2: e.g. brake system
  - Actuator 3: e.g. engine system
  - Actuator M: e.g. ...

System Views
- HMI, Safety, Security, I&V, Backend, ...

University of Stuttgart
Germany
A System View on Automated Driving
Closer Look on Driving Functions

Driving Functions

Environment Model
› Road Data
› Dynamic Objects
› Grid
› Map
› Situation

Vehicle Model
› Ego pose
› Ego dynamics
› Localization

Driving Strategy
Trajectory Planning

Reference
Maneuvers, Intentions, Predicted Trajectories
Dynamic Predictions

Object Prediction

Collision Check

Trajectory
Future Architecture Challenges
Growing Complexity – leads into stepwise change

Today
Component orientation

Distributed Architecture
Component Approach

Feature Update Rates
once a year [dealer’s garage]

System orientation
Future

Domain Architecture
Multi Domain Approach

Feature Update Rates
monthly, weekly

Future Mobility Architectures
System Approach

Feature Update Rates
every time, everywhere

› Impact on customers and suppliers
  › Impact on processes

› Impact on organizations
  › Impact on business models…
Automated Driving Architecture

Agenda

1 Motivation
2 Challenges: Fully Automated Driving
3 Proposed Approach
4 Results
5 Conclusion & Future Work
Operational Safety of The Fully Automated Vehicle
Ensuring a high level of operational safety of the fully automated vehicle

Confidential

Space for Sender Information

Operational Safety of The Fully Automated Vehicle
Ensuring a high level of operational safety of the fully automated vehicle

Functional safety
[absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems]

Safety of the intended functionality
[absence of unreasonably hazardous functionality]

Safety in use
[absence of hazards due to human error]

Safety
[absence of unreasonable risk]

Reliability
[continuing for correct service]

Availability
[readiness of a correct service]

Roadworthiness
(Operational Safety)
[property or ability of a car, bus, truck or any kind of automobile to be in a suitable operating condition or meeting acceptable standards for safe driving and transport of people, baggage or cargo in roads or streets]

Security

Continental

University of Stuttgart
Germany
Safety of the intended functionality
A new aspect in safety of road vehicles

Definition
[absence of unreasonably hazardous functionality, e.g. false-positive of sensor performance to detect a real object in the lane]
working document at Continental AG, 2016
STPA-based Assessment Approach
Developing a dependable Architecture

› Myth  It’s software—we can fix it later (add safety, security, other “-ilities”)
› Fact  “-ilities” must be architected in, and can’t be easily added later

Our Approach
1. Decompose the architecture of fully automated driving
2. Apply STPA at each architecture levels
3. Develop an operational safety concept for fully automated driving
4. Generate test cases to evaluate the architectural design
5. Develop/Assign design patterns for dependable critical software systems

[Boehm et al., 2002]
STPA-based Assessment Approach
Detailed View of the Proposed Approach
Automated Driving Architecture

Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. Results
5. Conclusion & Future Work
### Operational Safety and Design Constraints

High Level Constraints for Fully Automated Driving Function

- We apply STPA to the autonomous vehicular level (Architectural level 0)
- We identify the operational safety and design constraints

<table>
<thead>
<tr>
<th>ID</th>
<th>Operational Safety and Design Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR0.1</td>
<td>The AD vehicle shall be functional all the time, while it is active <em>(Reliability)</em></td>
</tr>
<tr>
<td>SR0.2</td>
<td>The AD vehicle and its network shall be secured during driving task <em>(Security)</em></td>
</tr>
<tr>
<td>SR0.3</td>
<td>The AD vehicle shall communicate with backend on a highly secure channel. <em>(Security)</em></td>
</tr>
<tr>
<td>SR0.4</td>
<td>The AD vehicle data on the vehicle and backend should be available only to authorized personality <em>(Security)</em></td>
</tr>
<tr>
<td>SR0.5</td>
<td>The AD vehicle shall drive safely and jerk optimized on the road <em>(Functional safety)</em></td>
</tr>
<tr>
<td>SR0.6</td>
<td>The AD vehicle should react in all situations correct <em>(Safety of the intended functionality)</em></td>
</tr>
<tr>
<td>SR0.7</td>
<td>The AD vehicle and its autonomous driving functions shall be ready for usage all the time <em>(Availability)</em></td>
</tr>
</tbody>
</table>
Accidents
High Level Accidents which fully automated driving can lead to

› We identify 26 accidents which fully automated driving vehicle can lead to
› We assign the relevant operational safety attributes to each accidents

<table>
<thead>
<tr>
<th>ID</th>
<th>Accident Description</th>
<th>Relevant Attributes**</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC0.1</td>
<td>AD vehicle lost steering control and crashed into an object moving in front.</td>
<td>Sa, Su, Re</td>
</tr>
<tr>
<td>ACC0.2</td>
<td>AD vehicle lost steering control and crashed in the ego lane.</td>
<td>Sa, Su, Re, SIF</td>
</tr>
<tr>
<td>ACC0.3</td>
<td>AD vehicle made an accident while an object suddenly appeared in its lane in front.</td>
<td>Sa, Av, Re</td>
</tr>
<tr>
<td>ACC0.4</td>
<td>AD vehicle suddenly lost the steering/braking control while the vehicle moving up the hill and made an accident.</td>
<td>Sa, Re, Av</td>
</tr>
<tr>
<td>ACC0.5</td>
<td>AD vehicle made an accident due to fake data of sensors manipulated by an anonymous person.</td>
<td>Se</td>
</tr>
<tr>
<td>ACC0.6</td>
<td>AD vehicle made an accident due to loss of the communication signals from the Backend</td>
<td>Av, Se</td>
</tr>
</tbody>
</table>

**Sa**: Functional safety, **Su**: Safety in use, **Re**: Reliability, **SIF**: Safety of intended functionality, **Av**: Availability, **Se**: Security.
Hazard Categories of fully Automated Driving

› We identify 9 hazard categories at the Autonomous Vehicular level to facilitate developing operational safety concepts
› We identify 176 hazards which are grouped into the nine hazard categories

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard Categories</th>
<th>Operational Safety Attributes *</th>
<th>No. of Hazard</th>
<th>Linked Accidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>HG1</td>
<td>Road Surface Detection</td>
<td>Sa, Re, SIF, Av</td>
<td>4</td>
<td>1-12, 16-19</td>
</tr>
<tr>
<td>HG2</td>
<td>Object Detection</td>
<td>Sa, Re, Av, SIF</td>
<td>23</td>
<td>1-13, 15-20</td>
</tr>
<tr>
<td>HG3</td>
<td>Control Hazard</td>
<td>Sa, Su, Re</td>
<td>47</td>
<td>1, 2, 12, 15, 24-26</td>
</tr>
<tr>
<td>HG4</td>
<td>Localization &amp; Mapping</td>
<td>Sa, Se, Av</td>
<td>8</td>
<td>1-21, 24-26</td>
</tr>
<tr>
<td>HG5</td>
<td>Environmental Model Hazards</td>
<td>Sa, Av, Se, SIF</td>
<td>34</td>
<td>1-13, 14-21</td>
</tr>
<tr>
<td>HG6</td>
<td>Decision Making Hazards</td>
<td>Sa</td>
<td>30</td>
<td>1-21</td>
</tr>
<tr>
<td>HG7</td>
<td>Data Communication Hazards</td>
<td>Se, Av</td>
<td>10</td>
<td>1-19, 21</td>
</tr>
<tr>
<td>HG8</td>
<td>Individual ECU Defect</td>
<td>Re</td>
<td>5</td>
<td>1-19</td>
</tr>
<tr>
<td>HG9</td>
<td>Security Hazards</td>
<td>Se</td>
<td>15</td>
<td>20-23</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>176</td>
<td></td>
</tr>
</tbody>
</table>
Safety Control Structure Diagram at Level 0
Developing Operational Safety Concepts

› We evaluate each control actions to determine the hazardous events
› We identify 29 hazardous control actions

HCA-0.1{Sa, Av, Re, SIF, Su}
The AD function platform does not provide a valid trajectory to motion control while the AD vehicle is approaching too fast in the lane ➔ [H-31, H-46, H-54], Hazard Category: control hazards

Control Hazard
loss of steering or braking or acceleration

Operational Safety Requirements
OSR 0.1: The AD function platform shall always provide a trajectory to motion control

Operational Safety Concept
OSC 0.1: Unintended absence of a vehicle trajectory shall be avoided
Refine Operational Safety Concepts

› We identify the process model variables of the fully automated driving at the level 0
Refine Operational Safety Concepts

› We use XSTAMPP to generate the context table and provide a minimal set of combination between the process model variable and refine hazardous control actions and operational safety concepts
› We identify 229 hazardous scenarios
› We identify the accident causes (STPA Step 2) for each hazardous control action

---

**Operational Safety Requirements**

OSR 0.1: The AD function platform shall always provide a trajectory to motion control

---

**Refine Operational Safety Requirements**

ROS 0.1: the AD function platform shall always provide the trajectory to enable motion control to adjust throttle and apply brake friction when the vehicle is moving and there is traffic ahead to avoid the potential collision

---

**Refine Operational Safety Concept**

ROSC 0.1: Unintended absence of a vehicle trajectory shall be avoided when the vehicle is moving and there is traffic ahead.
Automated Driving Architecture

Agenda

1. Motivation
2. Challenges: Fully Automated Driving
3. Proposed Approach
4. Results
5. Conclusion & Future Work
A systematic approach based on STPA

Conclusion

› We used STPA approach as a risk assessment approach of functional architecture of fully automated driving function.

› We applied STPA to complex functional architecture of fully automated driving at early stage of development process.

› We provide a systematic guidance on deriving operational safety requirements and develop operational safety concepts.

› We address different attributes to develop operational safety concepts.

› Ensuring completeness of hazards list.

› Linking between different control structure diagram at multiple levels of functional architecture.

› XSTAMPP does not support multi-levels of control structure diagram and multi-STPA process for one project.

› Directly mapping between our results to the safety standard like ISO 26262.
A systematic approach based on STPA
Future Work

› We plan to apply STPA to other levels (level 1 and level 2) to identify the hazardous scenarios of each system or component

› We plan to generate the test cases based on the results of STPA to test the prototype of the fully automated driving (STPA SwISs approach)

› We plan to explore the use of STPA approach in compliance with ISO 26262

› We plan to use CAST approach to analyse the accidents which are occurred during the simulation phase to get a better understanding why these accidents occurred

› We plan to link between XSTAMPP platform which is an extensible safety engineering platform with architectural tool such PREEVision to link the results of STPA safety analysis directly to the architecture element
Thank you for your attention

Q&A

Joint work with:
Prof. Dr. Stefan Wagner, University of Stuttgart, Stuttgart, Germany
Jürgen Röder, Norbert Balbierer and Ludwig Ramsauer, Continental AG, Regensburg, Germany
Thomas Raste and Hagen Boehmert, Continental Teves AG & Co. oHG, Frankfurt am Main, Germany