Using STPA in Compliance with ISO26262
for developing a Safe Architecture for Fully Automated Vehicles

STAMP Workshop MIT, March 27th 2017
Asim Abdulkaleq, Pierre Blueher, Daniel Lammering

www.continental-automotive.com
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. Usage of STPA in the ISO26262 Lifecycle
4. Methodology & Results
5. Conclusion & Future Work
Motivation
Architecture trend analysis

Continuously growing complexity, number of functions and networked ECUs results in:

› Requirements for new technologies and modules
› Major redesign of E/E architecture at most worldwide OEMs
› New design criteria required for future E/E architectures
Motivation
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!
› Accidents happen with no component failures (Component Interaction Accidents)
› Complex, Software-intensive Systems (New Hazards: System functional but Process/Event is unsafe)
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. Usage of STPA in the ISO26262 Lifecycle
4. Methodology & Results
5. Conclusion & Future Work
Vehicle E/E – Architecture needs a holistic approach
e.g. Service Oriented Architectures, Cloud services, Update over the air

› Safety & system architecture/interface must be defined together

› Safety, reliability and availability has important implications for analyzing

› **Fail Operational Behavior** – fail silent may not be suitable any longer
Operational Safety in Automotive Domain
Ensuring a high level of operational safety

Safety
[absence of unreasonable risk]

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]

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]

Availability
[readiness of a correct service]

Reliability
[continuing for correct service]

Security
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. Usage of STPA in the ISO26262 Lifecycle
4. Methodology & Results
5. Conclusion & Future Work
## Usage of STPA in the ISO26262 Lifecycle

Road Vehicles Functional Safety

### 1. Glossary

- [ISO26262](ISO26262)

### 2. Management of functional safety

- 2.4 Management during complete safety lifecycle
- 2.5 Safety management during development
- 2.6 Safety management activities after SOP

### 3. Concept phase

- 3.4 Item definition
- 3.5 Initiation of safety lifecycle (modification and derivates)
- 3.6 Hazard analysis and risk assessment
- 3.7 Functional safety concept

### 4. Product development system

- 4.4 Initiation of product development system
- 4.5 Specification of technical safety concept
- 4.6 System design
- 4.7 Integration
- 4.8 Safety validation
- 4.9 Functional safety assessment
- 4.10 Product release

### 5. Product development H/W

- 5.4 HW requirements analysis
- 5.5 HW architecture design
- 5.6 Quantitative requirements for random HW failures
- 5.7 Measures for avoidance and control of systematic HW failures
- 5.8 Safety HW integration and verification
- 5.9 Qualification of parts and components
- 5.10 Overall requirements for HW-SW interface

### 6. Product development S/W

- 6.4 Initiating SW development
- 6.5 SW safety requirements specification
- 6.6 SW architecture and design
- 6.7 SW implementation
- 6.8 SW unit test
- 6.9 SW integration and test
- 6.10 SW safety acceptance test

### 7. Production and operation

- 7.4 Production
- 7.5 Operation, service and decommissioning

### 8. Supporting processes

- 8.4 Interfaces within distributed developments
- 8.5 Overall management of safety requirements
- 8.6 Configuration management
- 8.7 Change management
- 8.8 Safety analysis
- 8.9 Analysis of CCE, CME, cascading failures
- 8.10 Verification activities
- 8.11 Documentation
- 8.12 Overall quality management
- 8.13 Qualification of software tools
- 8.14 Qualification of software libraries
- 8.15 Proven in use argumentation

[ISO26262]
Usage of STPA in the ISO26262 Lifecycle
Concept Phase (ISO 26262-part 3)

- **3-5 Item Definition**: Item (subject) is defined
- **3-6 Initiation of the safety lifecycle**: Functions, operating modes and system states are known
- **3-7 Hazard Analysis and Risk Assessment (HARA)**: Hazard analysis and risk assessment are completed
- **3-8 Specification of functional safety concept**: Safety concept for “item” is defined

Concept phase
Product development

- **4-6 Specification of technical safety requirements: System Level**: Technical requirements are defined
- **5-6 Specification of hardware safety requirements**
- **6-6 Specification of software safety requirements**: Safety requirements for hardware and software are defined on a detailed level
Usage of STPA in the ISO26262 Lifecycle
Hazard Analysis and Risk Assessment (HARA)

3-5: Item Definition
3-7: Hazard Analysis and Risk Assessment

Situation Analysis
- Operational Situations
- Operating Modes

Hazard Classification
- Hazards Classification: Severity (S), Exposure (E), and Controllability (C)
- Determine the hazardous events

ASIL Determination
- ASIL Determination (A to D)
- Quality Management (QM)

Safety Goal formulation
- Determine the safety goal for each hazardous events

3-8 Build Functional Safety Concept
- 3-8 System Functional Safety Concept
- 3-8 System Functional Safety Requirements
Usage of STPA in the ISO26262 Lifecycle

ISO 26262 challenges for autonomous vehicles

- ISO 26262 has no recommended method for the item definition
- ISO 26262 recommends various hazard analysis techniques (e.g. FTA, FMEA, HARA)
- ISO 26262 is not established for fully automated driving vehicles (autonomous vehicles)
- No controllability assessment method for the hazardous events of fully automated vehicle (no driver in loop, SAE level 5)
Usage of STPA in the ISO26262 Lifecycle
STPA vs HARA

HARA Safety Scope

Malfunctioning behaviour caused by:

• Component failure

STPA Safety Scope

Inadequate controls caused by:

• Human error
• Interaction failure
• Environmental error
• Software failure

• Inadequate control in absence of failure

ISO 26262

Operational Safety
Usage of STPA in the ISO26262 Lifecycle
STPA vs HARA

HARA Terminologies

- Harm
- Hazardous events
- Malfunctioning Behaviour
- Operation Situation
- Functional Safety Requirements
- Operating Mode
- Item

STPA Terminologies

- Accidents
- Unsafe Control Action
- Causal Factors
- Corresponding safety constraints
- Process Model
- Safety Constraints
- ASIL
- Hazard

Corresponding terms:
- No corresponding term
- Somehow match
- Partially match
- Exactly match

Abdulkhaleq, Lammering, Blueher© Continental AG
March 27, 2017
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. Usage of STPA in the ISO26262 Lifecycle
4. Methodology & Results
5. Conclusion & Future Work
Methodology & Results

STPA Methodology

**Input**
System specification and design models

**STPA Process**

1. **Start**
   - Define Analysis Scope
   - Develop Control Structure Diagram

2. **STPA Step 1**: Identify unsafe control actions
   - STPA Step 2: Identify how each unsafe control action could occur

3. **STPA Result**
   - System-Level Accidents, related hazards, design and safety constraints

**Results**

- Fundamentals
- STPA Safety Analysis Report
- New/Refined Safety Constraints
- Causal Scenarios
- Unsafe Control Actions
- Corresponding Safety Constraints
- Hierarchical Control Structure Diagram
- Hierarchical Control Structure with process model

[Abdulkhaleq 2017]
Methodology & Results
STPA in ISO 26262

STPA Step 0
- Safety-critical components
  - Accidents, Hazards, linking between hazards and accidents, system safety constraints

STPA Step 1
- Hazardous events, safety goals, situations and modes
  - STPA Step 2
    - Causal Scenarios and safety constraints

3-5: Item Definition
3-7: Hazard Analysis and Risk Assessment

Situation Analysis
- Operational Situations
- Operating Modes

Hazard Classification
- Hazards Classification: Severity (S), Exposure (E), and Controllability (C)
- Determine the hazardous events

ASIL Determination
- ASIL Determination (A to D)
- Quality Management (QM)

Safety Goal formulation
- Determine the safety goal for each hazardous events

3-8 Build Functional Safety Concept
- 3-8 System Functional Safety Concept
- 3-8 System Functional Safety Requirements
Methodology & Results
Example: Autonomous Vehicle

Conceptual Architecture

Functional Architecture

Automated Vehicle

Plan
Trajectory Planning
Maneuver Planning
Driving Strategy

Act
Motion Control
Lateral Controller
Actuator 1 (e.g. Steering System)
Actuator 2 (e.g. Brake System)
Actuator 3 (e.g. Engine System)

Longitudinal Controller

Sense
Data Interpretation
Data Fusion
Env. Model
Vehicle Model / Localization

Sensor 1 (e.g. Stereo Camera)
Sensor 2 (e.g. Long Range Radar)
Sensor 3 (e.g. Backend / HD Map)
Methodology & Results
STPA Step 0: Safety Control Structure Diagram

ISO 26262

Item Definition

- item description
- its boundaries
- its interfaces

- Enable/Disable
- SeatBelt
- DoorSwitch
- Route Selection

- Warnings/
  messages/
  notifications
  haptic/audible/
  visual

- Feedback

- Road data,
  vehicle position

- Situation data,
  sensors data

- Environmental data,
  central gateway
  data, vehicle data

- Motion Control
  (Actuator)

- Timestamp
- Curvature rate
- Curvature
- Tangent/track angle
- Velocity
- Acceleration
- Jerk

- Controlled Process

- Fully automated Vehicle

- AD Configurations

- HMI

- Bakend

- AD Sensors

- By XSTAMPP
Methodology & Results
STPA Step 0: Accidents & Hazards

› We identify 26 accidents which fully automated driving vehicle can lead to
› We identify 176 hazards which are grouped into the 9 hazard categories

STPA
Step 0

Accident AC-1: The fully automated vehicle collided into an object moving in front on a highway

Hazard HA-1: The fully automated vehicle lost steering control because it received wrong ego longitudinal torque

Safety Constraint SC-1: The fully automated vehicle must receive correct data all the time while driving on a road

HARA

Operational Situation OS-1: Crashing on a highway
Operating Mode OM-1: Driving
We estimated the severity and exposure of each hazard identified in STPA Step 0.

We identified the hazardous events for each hazard and estimated its controllability.

**STPA Step 0**

<table>
<thead>
<tr>
<th>Hazard HA-1: The fully automated vehicle lost steering control because it received wrong ego longitudinal torque.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity</strong> of HA-1 is: S3 (Life-threatening injuries or fatal injuries)</td>
</tr>
<tr>
<td><strong>Exposure</strong> of HA-1 is: E3 (Medium probability)</td>
</tr>
<tr>
<td><strong>Hazardous event</strong> HE-1: The fully automated vehicle lost control steering while driving on a highway</td>
</tr>
<tr>
<td><strong>Controllability</strong> of HE-1 is: C3 (difficult to control)</td>
</tr>
<tr>
<td><strong>ASIL</strong> of HE-1 is: ASIL C (difficult to control)</td>
</tr>
<tr>
<td><strong>A safety goal of</strong> HE-1 is: The fully automated vehicle must not lose the steering control while driving on a highway</td>
</tr>
</tbody>
</table>

Driver is not expected to take control at any time.
Methodology & Results
STPA Step 0: Accidents & Hazards

› We identify the unsafe control actions of the fully automated driving platform
› We translate each unsafe control action into a corresponding safety constraint

**Safety-critical control action** CA-1: Trajectory

**Unsafe control action** UCA-1: The fully automated driving function platform does not provide a valid trajectory to motion control while driving too fast on a highway [HA-1]

**Corresponding safety constraint** SC-1: The fully automated driving function platform must always provide a valid trajectory to motion control while driving too fast on a highway
Methodology & Results
STPA Step 0: Accidents & Hazards

- We use the results of the situation analysis to determine the process model of AD
- We identify the causal factors and scenarios of each unsafe control action

**Process Model Variables** PMV: road_type (highway, parking, intersection, mountain, city, urban) throttle position, brake friction, etc.

**Unsafe control action** UCA-1: The fully automated driving function platform does not provide a valid trajectory to motion control while driving too fast on a highway [HA-1]

**Causal Factor:** Lack of Communication

**Causal Scenario** CS-1: The fully automated driving function platform receives wrong signals from backend due to the lack of communication while driving too fast on a highway

**Safety Constraint** SC-1: The fully automated driving function platform must always provide the trajectory to enable motion control to adjust the throttle position and apply brake friction when the vehicle is moving and there is traffic ahead to avoid a potential collision not provide a valid trajectory to motion control while driving too fast on a highway.
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. Usage of STPA in the ISO26262 Lifecycle
4. Methodology & Results
5. Conclusion & Future Work
STPA in compliance with ISO 26262

Conclusion

› We used STPA as a assessment approach for the functional architecture of automated driving vehicle.

› We show how to use STPA in compliance with ISO 26262 to extend the safety scope of ISO 26262

› We provide a guidance on how use the STPA into the ISO 26262 lifecycle.

› We found that STPA and HARA can be applied with a little bit knowledge about the detailed design of the system at early stage of development.

› STPA and HARA have different base assumptions.

› The integration of STPA into HARA activities still needs modification in the assumptions and terms of both STPA and HARA to directly map the results of STPA into HARA

› ISO 26262 has no systematic way to define the item.

› STPA has no guidance on how to define the process model and its variables.

› XSTAMPP does not support the HARA activities
STPA in compliance with ISO 26262
Future Work

› Use of STPA as a qualitative analysis in an advanced development project (e.g. fully automated driving vehicle)

› We plan to explore the use of STPA approach in compliance with ISO 26262 at different levels of the fully automated driving architecture (e.g. software level) to develop detailed safety requirements.

› We plan to develop an extension to XSTAMPP to support the HARA activities.

› We plan to conduct empirical case study evaluating our proposed concept with functional safety engineers at Continental to understand the benefits and limitations.
Thank you for your attention

Q & A

Joint work with
- Prof. Dr. Stefan Wagner, University of Stuttgart, Stuttgart, Germany
- Hagen Boehmert, Continental Teves AG & Co. oHG, Frankfurt am Main, Germany