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

Automotive-Safety and Security 2017, Mai 31th 2017
Asim Abdulkhaleq, Daniel Lammering

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

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. HARA & ISO26262 Lifecycle
4. Introduction to STAMP/STPA
5. STPA in ISO 26262 & Results
6. 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. HARA & ISO26262 Lifecycle
4. Introduction to STAMP/STPA
5. STPA in ISO 26262 & Results
6. Conclusion & Future Work
Operational Safety in Automotive Domain

Architecture Challenges

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

- **Availability**: readiness of a correct service

- **Reliability**: continuing for correct service

- **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

- **Security**

**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

[Abdulkhaleq, Lammering et al., 2016]
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. HARA & ISO26262 Lifecycle
4. Introduction to STAMP/STPA
5. STPA in ISO 26262 & Results
6. Conclusion & Future Work
**HARA & ISO26262 Lifecycle**

**Road Vehicles Functional Safety**

1. Glossary

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

5. Product development HW
   - 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 SW
   - 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 CCF, CMF, cascading failures

---

[ISO26262]
HARA & ISO 26262 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

4-6  Specification of technical safety requirements: System Level
Concept phase
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
HARA & ISO 26262 Lifecycle
Hazard Analysis and Risk Assessment (HARA)

3-5: Item Definition

3-7: Hazard Analysis and Risk Assessment

- 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 Functional Safety Concept
- 3-8 Functional Safety Requirements
ISO 26262 challenges for autonomous vehicles

- ISO 26262 has no recommended method for the item definition
- ISO 26262 recommends various 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)
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. HARA & ISO26262 Lifecycle
4. Introduction to STAMP/STPA
5. STPA in ISO 26262 & Results
6. Conclusion & Future Work

Mai, 31, 2017
Abdulkhaleq, Lammering © Continental AG
Introduction to STAMP/STPA Assessment Methodologies

Technical Systems

- Decomposition works for technical systems, because they have been designed.
- They can be described bottom-up in terms of components and subsystems.
- Risks and failures can therefore be analysed relative to individual components and events.

Socio-Technical Systems

- Decomposition does not work for socio-technical systems, because they are emergent.
- Must be described top-down in terms of functions and objectives.
- Risks and failures must therefore be described relative to functional wholes.

Introduction to STAMP/STPA

Limitation of traditional accident models

› Technology is changing faster than the engineering techniques

› Changing nature of accidents.

› New types of hazards (e.g. unacceptable physical, scientific, or financial losses)

› Decreasing tolerance for single accidents

› Increasing complexity and coupling

› More complex relationships between human and automation

› Changing regulations and public view of safety

[Leveson 2004, A new Accident Model for Engineering Safer Systems]
Introduction to STAMP/STPA
STAMP New Accident Model

**STAMP** (Systems-Theoretic Accident Model and Processes)

is an accident causality model based on system theory and system thinking

› Developed by Nancy Leveson, MIT in 2004
› Accidents are more than a chain of events, they involve **complex dynamic processes**.
› Treat accidents as a **control problem**, not a failure problem
› Prevent accidents by enforcing constraints on component behaviour and **interactions**.
› Capture **more causes** of accidents:
  › Component failure accidents.
  › Unsafe interactions among components
  › Complex human, software behaviour
  › Design errors
  › Software-related accidents

Introduction to STAMP/STPA Methodology

**STPA (System-Theoretic Process Analysis)**

Technique based on systems thinking by a STAMP model

- Based on system theory rather than reliability theory
- Integrates safety into system engineering and can also analyze hazards in existing design
- Drive the earliest design decisions (Safety by Design)
- Identify unexpected accident scenarios
- In systems theory, instead of breaking systems into interacting components, systems are viewed (modeled) as a hierarchy of organizational levels.

Introduction to STAMP/STPA

Safety Analysis Approach

Input

System specification and design models

STPA Process

Start

Define Analysis Scope

Develop Control Structure Diagram

Hierarchical Control Structure Diagram

STPA Step 1: Identify unsafe control actions

STPA Step 2: Identify how each unsafe control action could occur

(Causal Factors)

Causal Scenarios

Unsafe Control Actions

Hierarchical Control Structure with process model

Corresponding Safety Constraints

New/Refined Safety Constraints

Results

System-Level Accidents, related hazards, design and safety constraints

Fundamentals

Safety Analysis Report

[Abdulkhaleq 2017]
Introduction to STAMP/STPA
Causal Factors Analysis (Qualitative Analysis)

STPA Step 2:
Identify how each unsafe control action could occur

Using STPA in Compliance with ISO26262

Agenda

<table>
<thead>
<tr>
<th></th>
<th>Motivation – Automated Driving</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Operational Safety - Roadworthiness</td>
</tr>
<tr>
<td>3</td>
<td>HARA &amp; ISO26262 Lifecycle</td>
</tr>
<tr>
<td>4</td>
<td>Introduction to STAMP/STPA</td>
</tr>
<tr>
<td>5</td>
<td>STPA in ISO 26262 &amp; Results</td>
</tr>
<tr>
<td>6</td>
<td>Conclusion &amp; Future Work</td>
</tr>
</tbody>
</table>

Mai, 31, 2017
Abdulkhaleq, Lammering © Continental AG
Methodology & Results
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
Methodology & Results
STPA vs HARA

HARA Terminologies
- Item
- Harm
- Hazardous events
- Malfunctioning behaviour
- Operation situation
- Functional safety requirements
- Operating mode
- ASIL

STPA Terminologies
- Accident
- System goals
- Unsafe control action
- Causal factors
- Corresponding safety constraints
- Process model
- Safety constraints

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

Mai, 31, 2017
Abdulkhaleq, Lammering © Continental AG
Methodology & Results
STPA in ISO 26262

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

STPA Step 1
- Hazardous events, safety goals, situations and modes

STPA Step 2
- Causal Scenarios and safety constraints

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 event

3-8 Build Functional Safety Concept
- 3-8 System Functional Safety Concept
- 3-8 System Functional Safety Requirements

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

Mai, 31, 2017
Abdulkhaleq, Lammering © Continental AG
Methodology & Results
Example: Autonomous Vehicle

Conceptual Architecture

Functional Architecture

Automated Vehicle
Methodology & Results
STPA Step 0: Safety Control Structure Diagram

ISO 26262
Item Definition
item description, Its boundaries, Its interfaces

Motion Control (Actuator)
Steering, braking, engine data

timestamp
curvature rate
curvature
tangent/track angle
velocity
acceleration
jerk

Enable/Disable
SeatBelt
DoorSwitch
Route Selection

Warnings/
messages/
notifications
haptic/audible/
visual

HMI
AD Configurations
Feedback

Bakend
Road data,
vehicle position

Situation data,
sensors data

AD Sensors

Environmental data,
Central gateway
data, vehicle data

Fully automated Vehicle
Controller Process

Passenger

By XSTAMPP

Mai, 31, 2017
Abdulkaleq, Lammering © Continental AG
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

- **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
- **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.

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

**Severity** of HA-1 is: S3 (Life-threatening injuries or fatal injuries)

**Exposure** of HA-1 is: E3 (Medium probability)

**Hazardous event** HE-1: The fully automated vehicle lost control steering while driving on a highway

**Controllability** of HE-1 is: C3 (difficult to control)

**ASIL** of HE-1 is: ASIL C

**A safety goal of** HE-1 is: The fully automated vehicle must not lose the steering control while driving on a highway

Driver is not expected to take control at any time.
Methodology & Results
STPA Step 1: Unsafe Control Actions

 › 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 2: Causal Factors and Scenarios

› 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 driving too fast on a highway and there is traffic ahead to avoid a potential collision.
XSTAMPP Tool Support (www.xstampp.de)
XSTAMPP for Safety Engineering based on STAMP

› We used an open source tool called XSTAMPP which we developed to support the STAMP methodologies and its extensions to other applications such as security, privacy.
Using STPA in Compliance with ISO26262

Agenda

1. Motivation – Automated Driving
2. Operational Safety - Roadworthiness
3. HARA & ISO26262 Lifecycle
4. Introduction to STAMP/STPA
5. STPA in ISO 26262 & Results
6. 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

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

› Our tool support XSTAMPP does not support the HARA activities

STPA will be recommended in the next version of ISO 26262 (2018)
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 our tool 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.

To download our tool: www.xstampp.de
Thank you
for your attention

Q & A

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

Mai, 31, 2017
Abdulkhaleq, Lammering © Continental AG