



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

STAMP Workshop MIT, March 29<sup>th</sup> 2017  
Asim Abdulkhaleq, Pierre Blueher, Daniel Lammering



University of Stuttgart  
Germany

# Using STPA in Compliance with ISO26262

## Agenda



**1** | Motivation – Automated Driving

**2** | Operational Safety - Roadworthiness

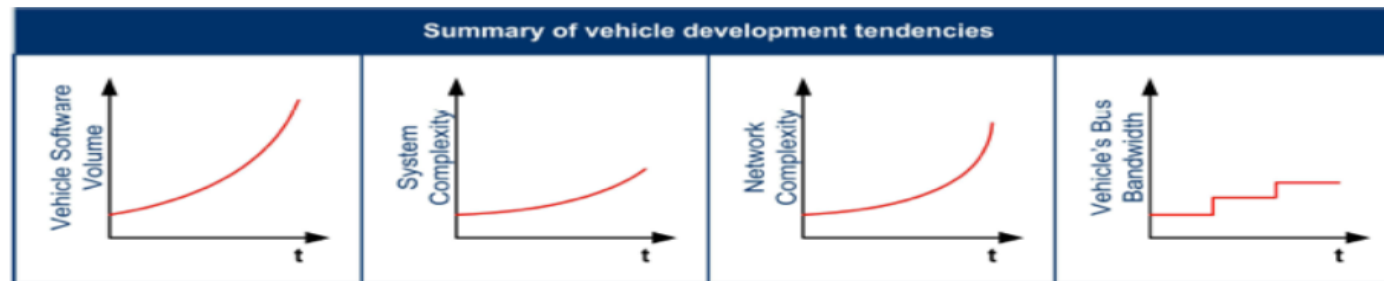
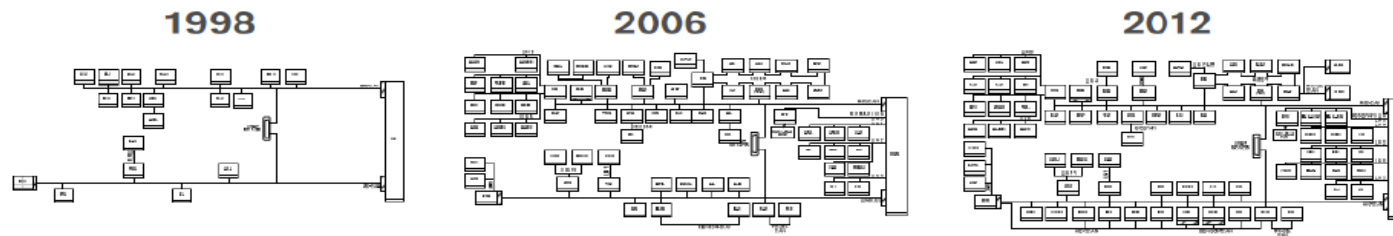
**3** | Usage of STPA in the ISO26262 Lifecycle

**4** | Methodology & Results

**5** | Conclusion & Future Work

# Motivation

## Architecture trend analysis



Source: WRC Market Report E/E Architecture 2013



**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



# Architecture Challenges

## Automotive part of the network

### Vehicle E/E – Architecture needs a holistic approach

e.g Service Oriented Architectures, Cloud services, Update over the air

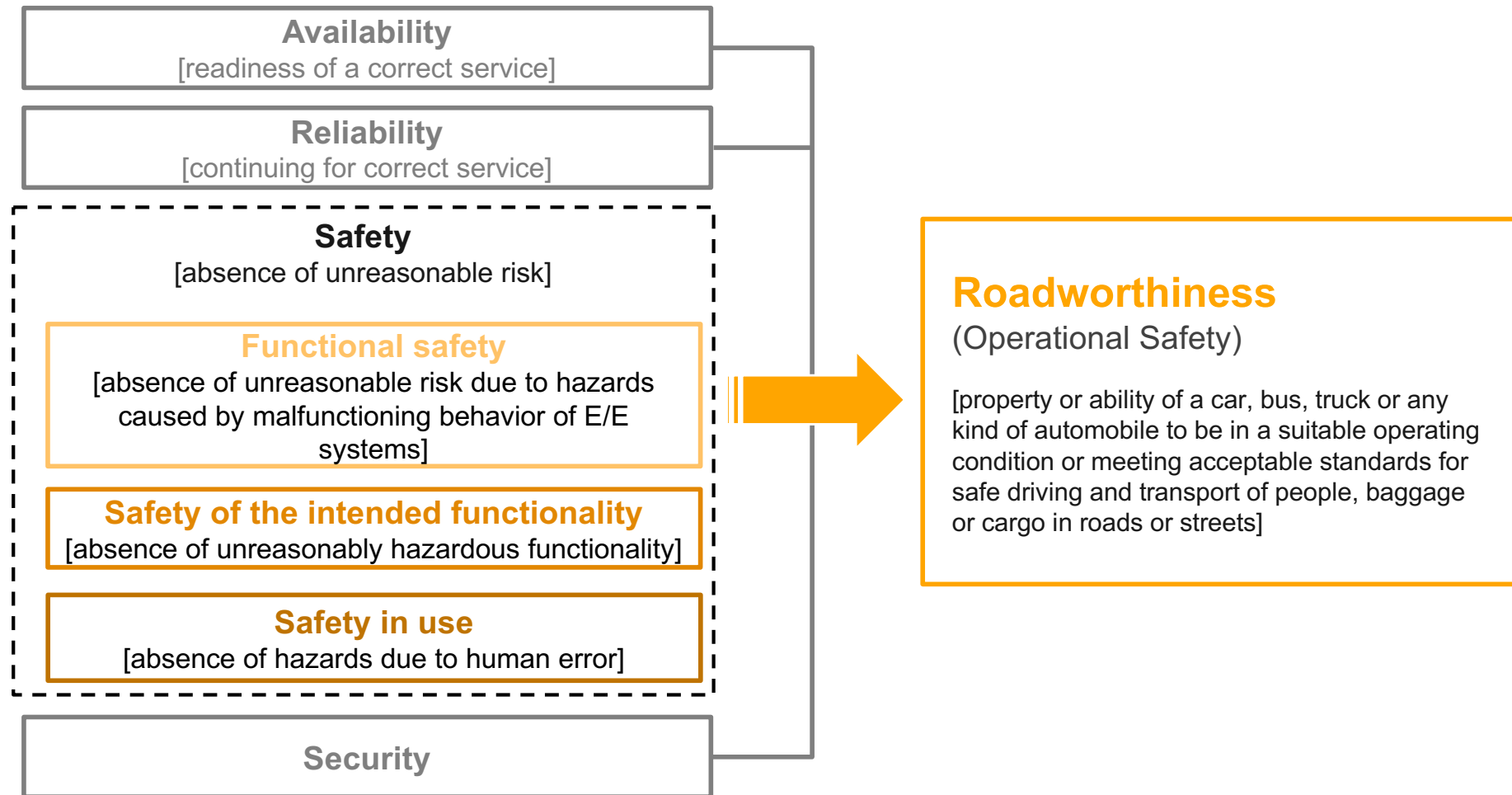
---



- › 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



[Abdulkhaleq, Lammering et al., 2016]

# Using STPA in Compliance with ISO26262

## Agenda



**1** | Motivation – Automated Driving

**2** | Operational Safety - Roadworthiness

**3** | Usage of STPA in the ISO26262 Lifecycle

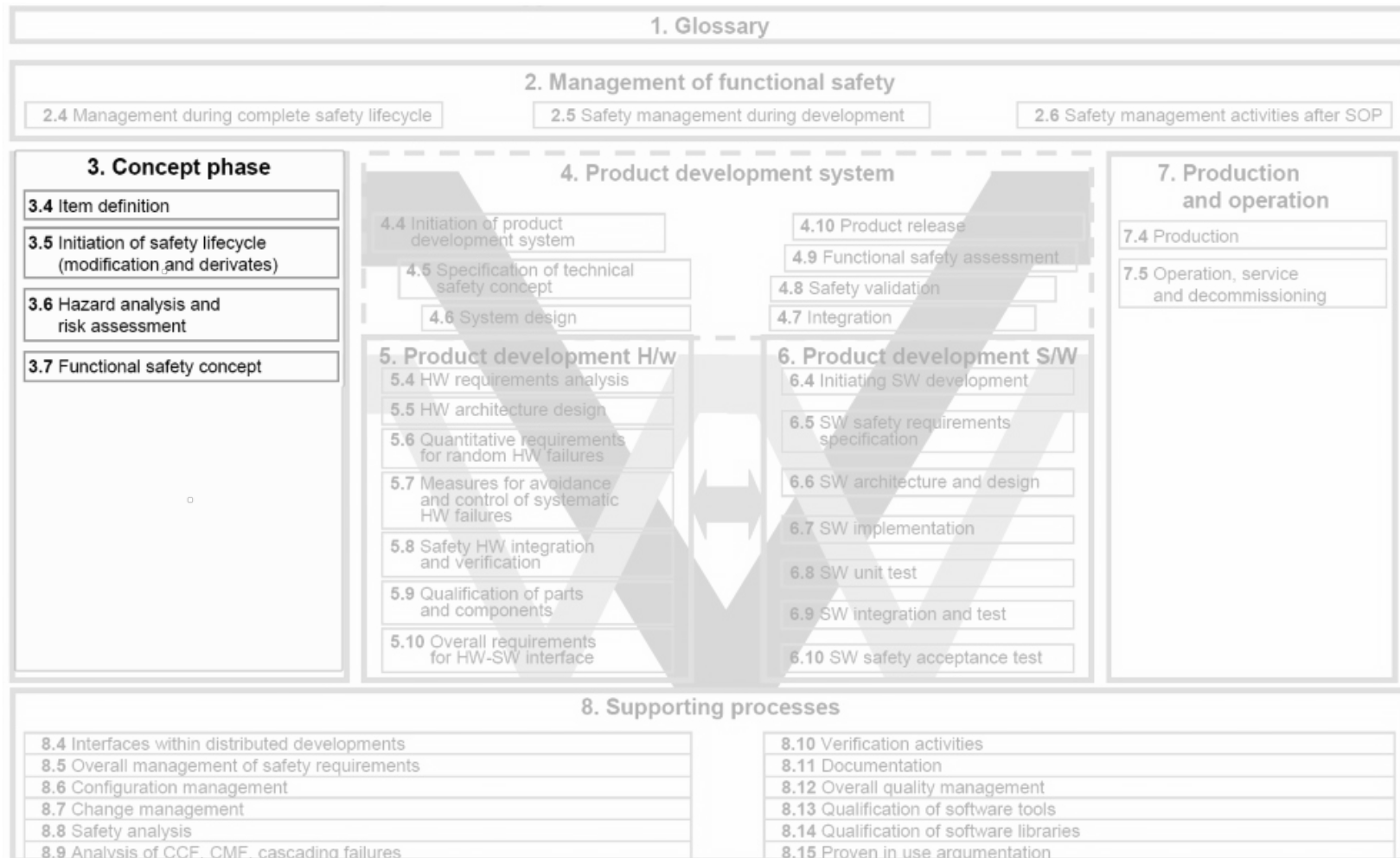
**4** | Methodology & Results

**5** | Conclusion & Future Work



# Usage of STPA in the ISO26262 Lifecycle

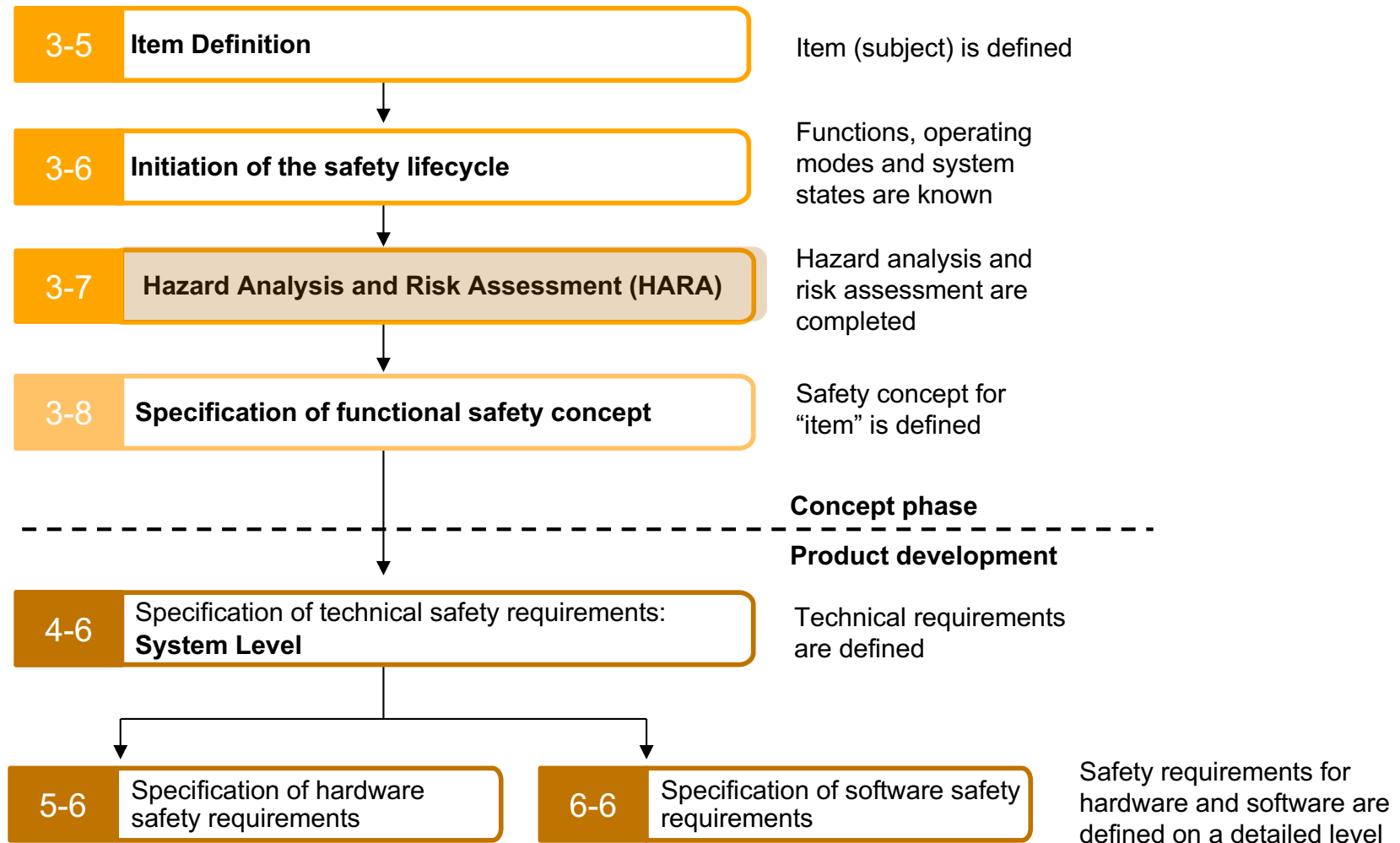
## Road Vehicles Functional Safety



[ISO26262]

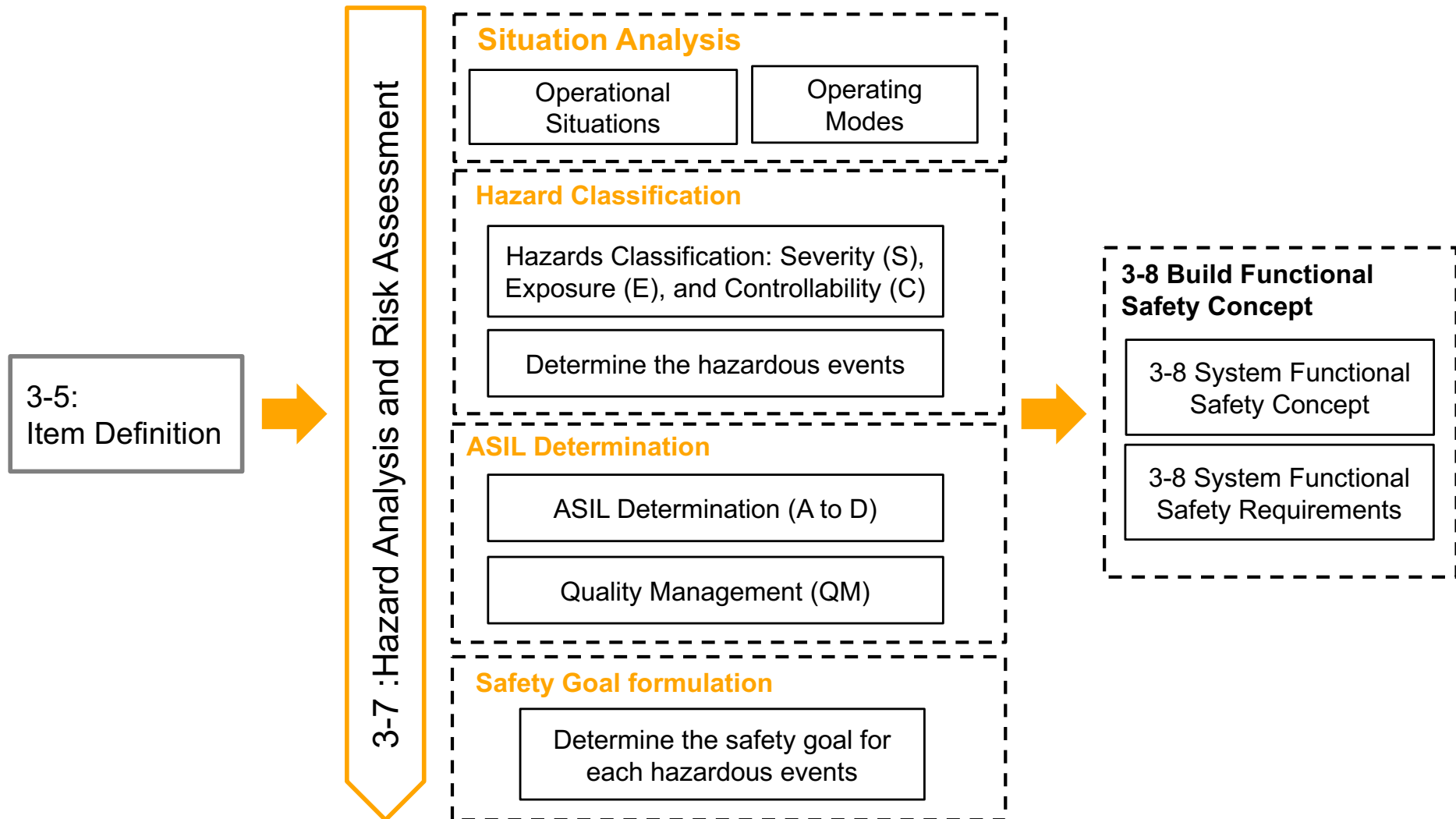
# Usage of STPA in the ISO26262 Lifecycle

## Concept Phase (ISO 26262-part 3)



# Usage of STPA in the ISO26262 Lifecycle

## Hazard Analysis and Risk Assessment (HARA)



# Usage of STPA in the ISO26262 Lifecycle

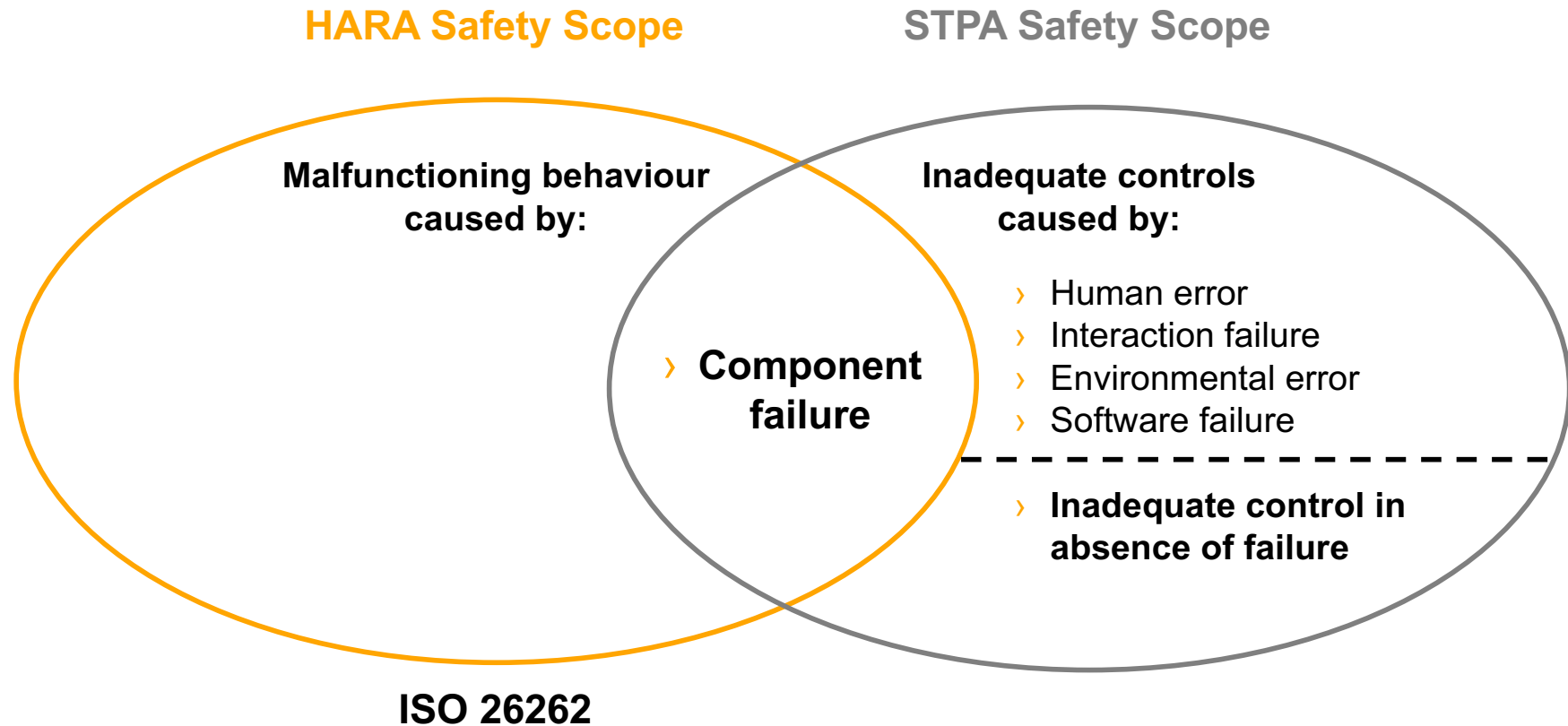
## ISO 26262 challenges for autonomous vehicles



- › 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

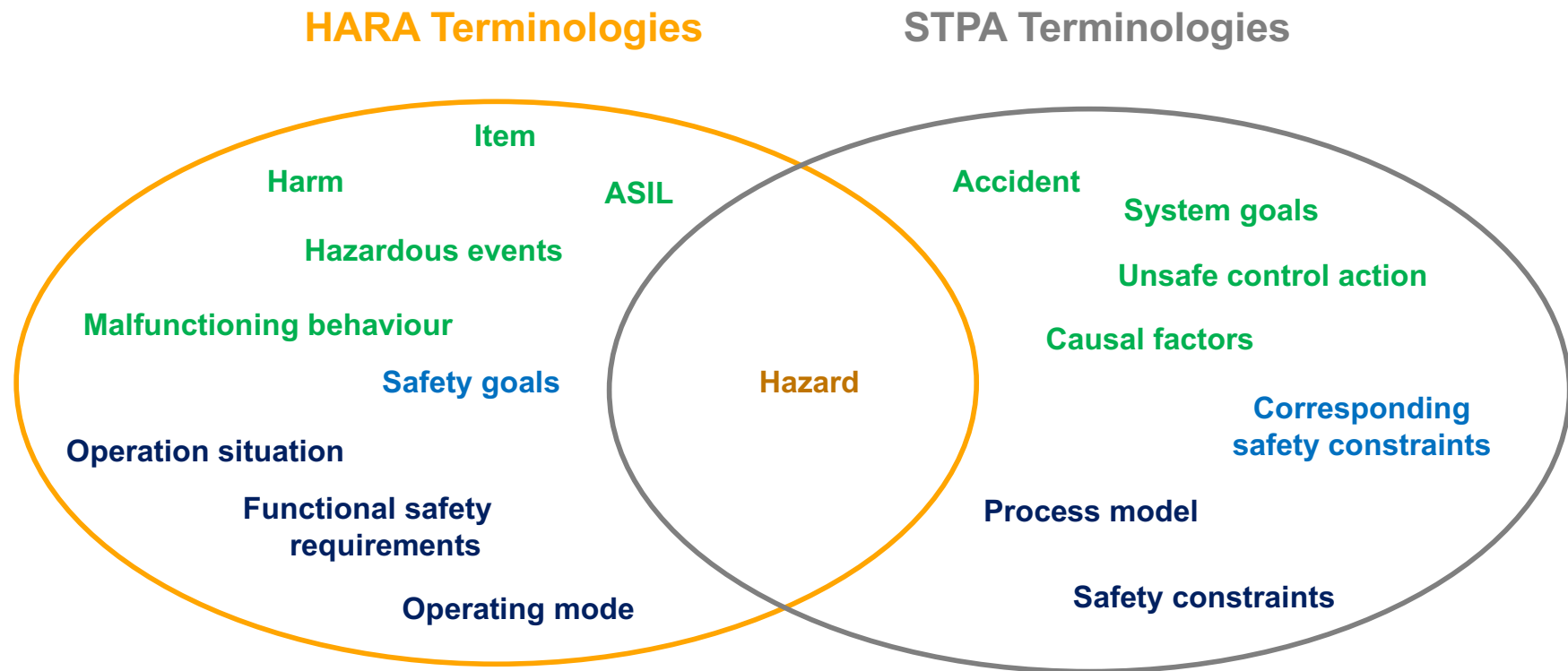


## Operational Safety



# Usage of STPA in the ISO26262 Lifecycle

## STPA vs HARA



- No corresponding term
- Somehow match
- Partially match
- Exactly match

# Using STPA in Compliance with ISO26262

## Agenda



**1** | Motivation – Automated Driving

**2** | Operational Safety - Roadworthiness

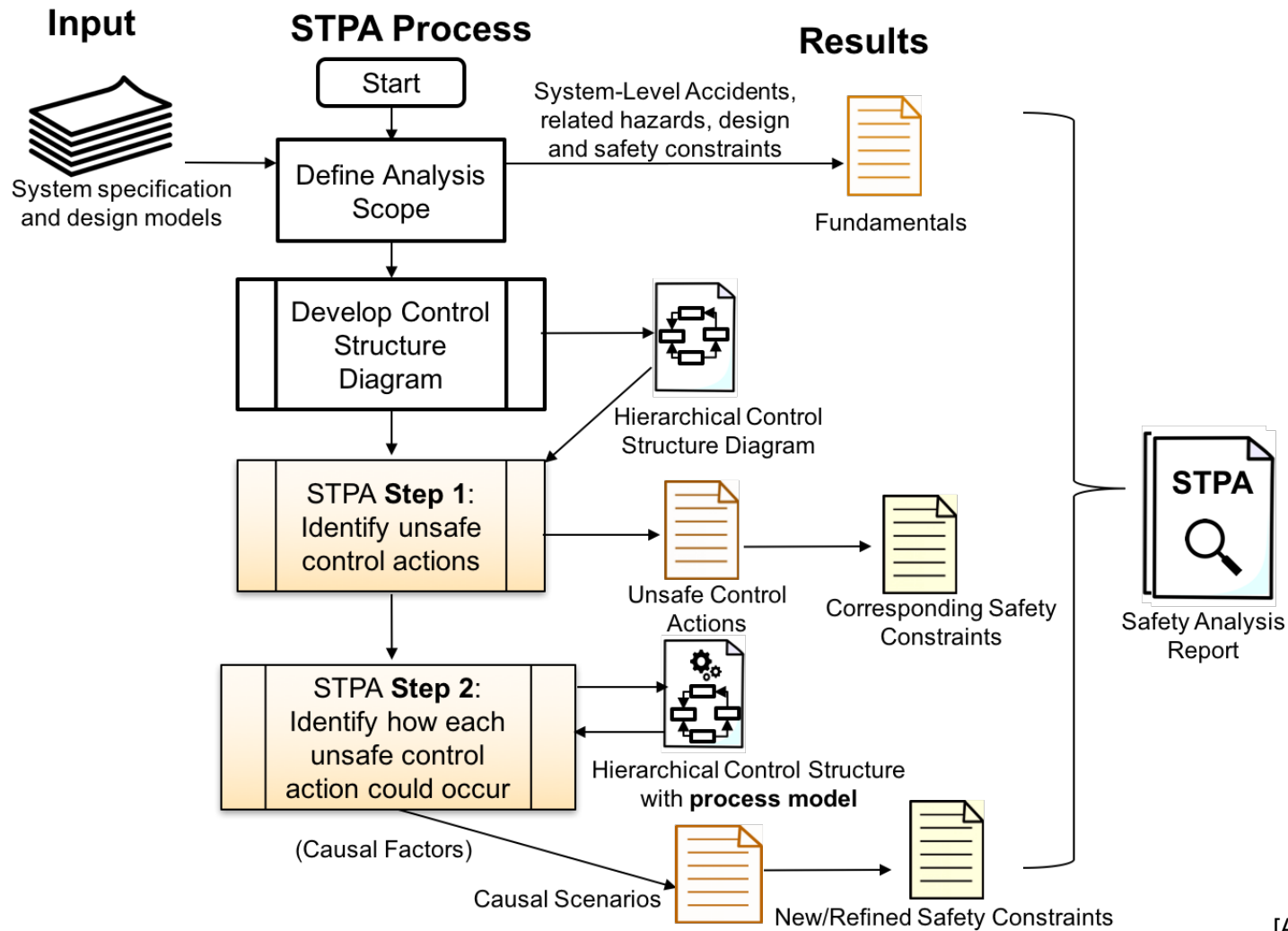
**3** | Usage of STPA in the ISO26262 Lifecycle

**4** | Methodology & Results

**5** | Conclusion & Future Work

# Methodology & Results

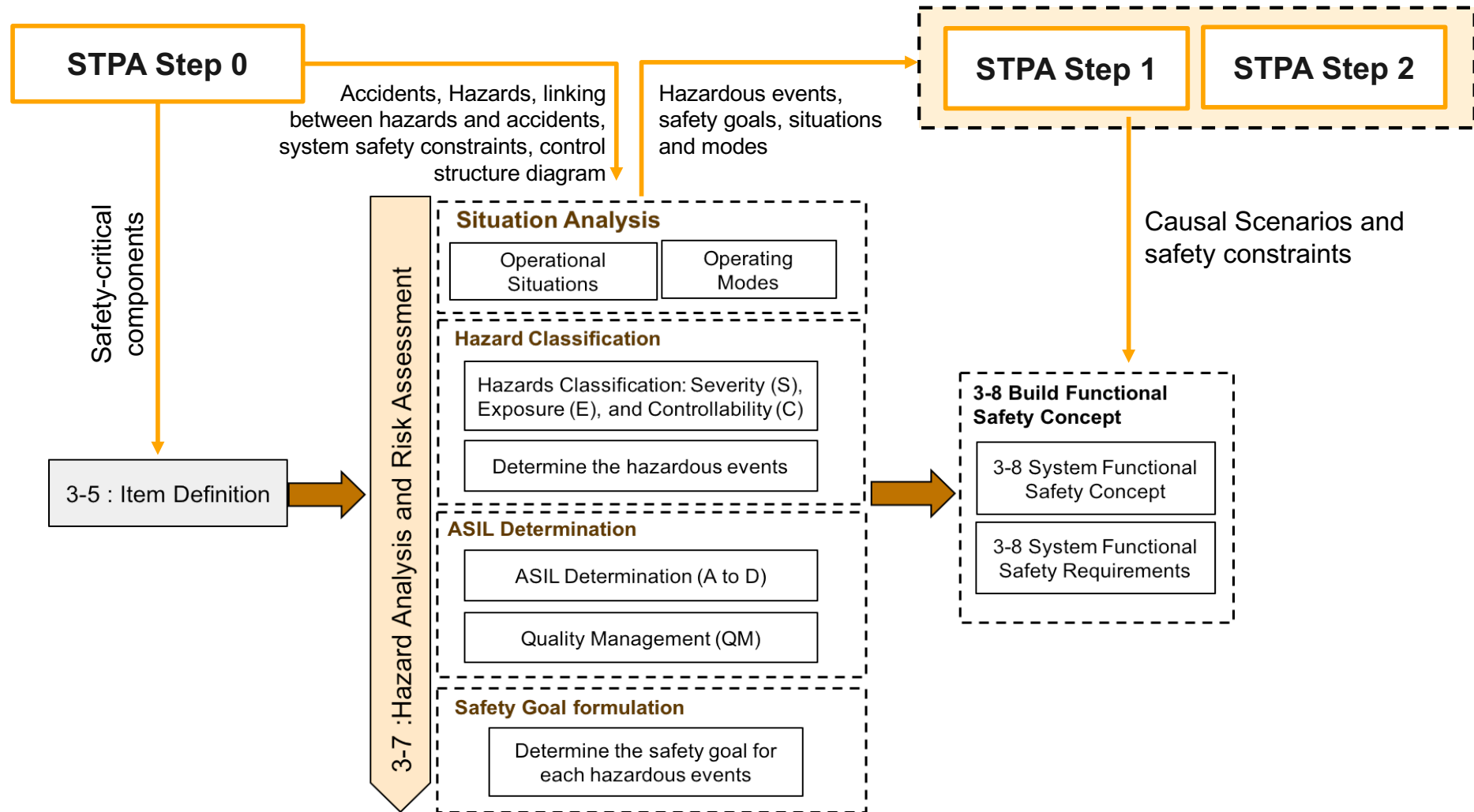
## STPA Methodology



[Abdulkhaleq 2017]

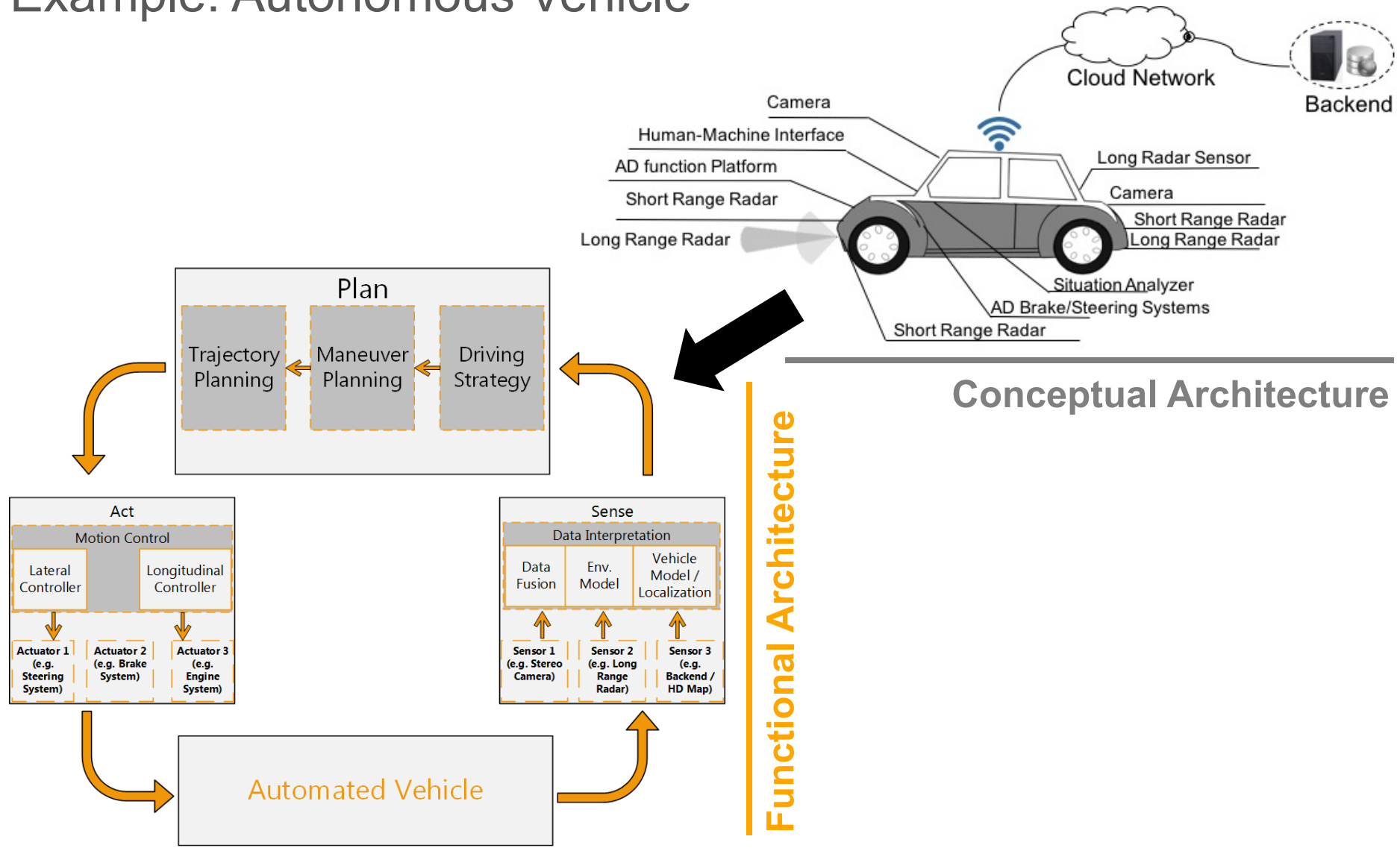
# Methodology & Results

## STPA in ISO 26262



# Methodology & Results

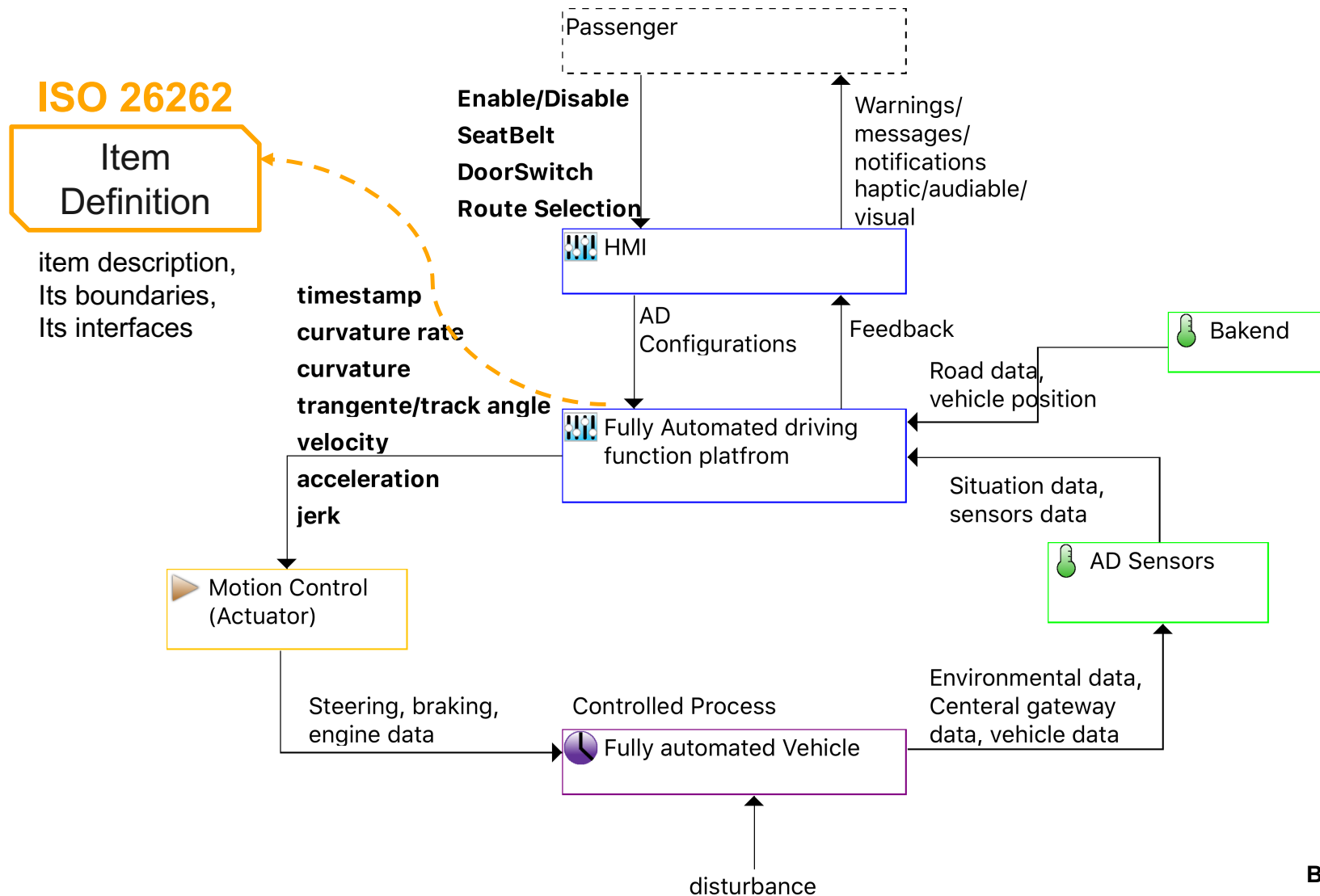
## Example: Autonomous Vehicle





# Methodology & Results

## STPA Step 0: Safety Control Structure Diagram

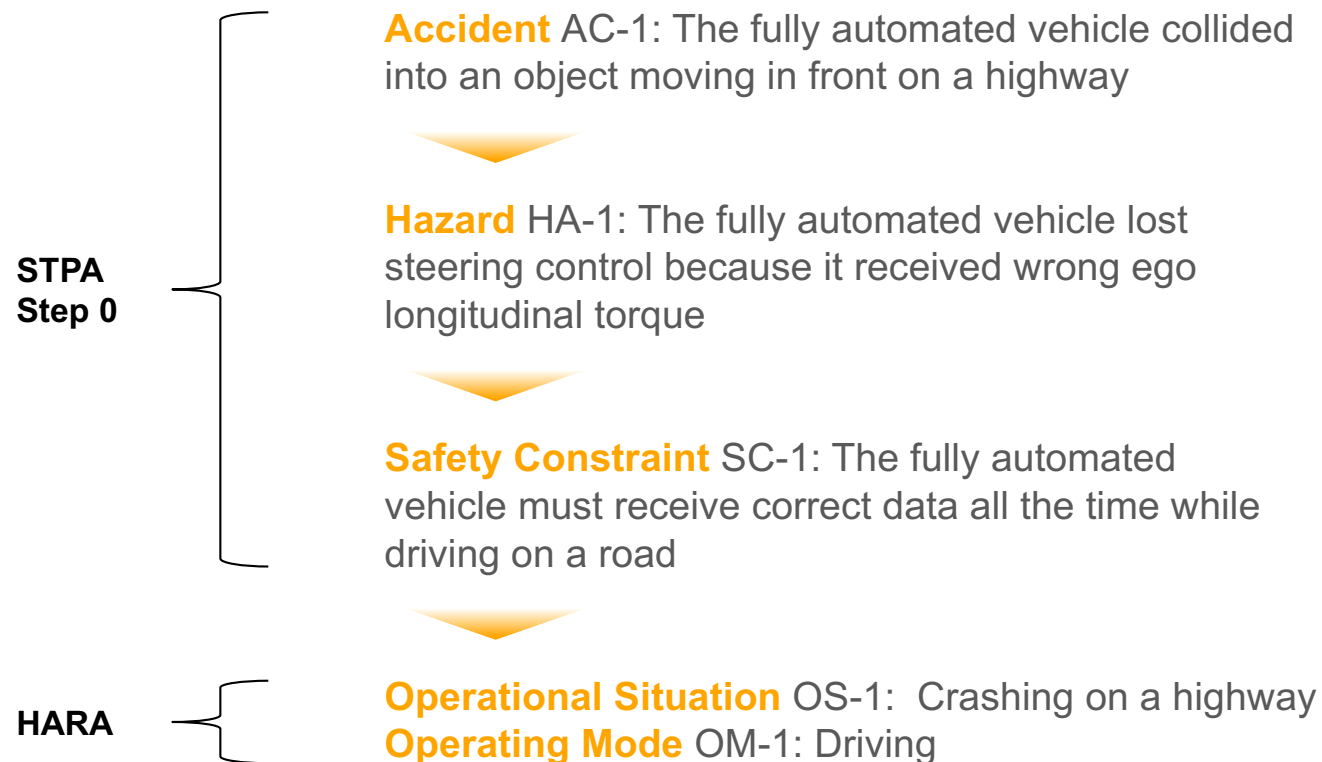


By XSTAMPP

# 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
- 



# Methodology & Results

## Risk Assessment & Hazards Classification

- › 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**

**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)

Driver is not expected to take control at any time

**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

**HARA**

# 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



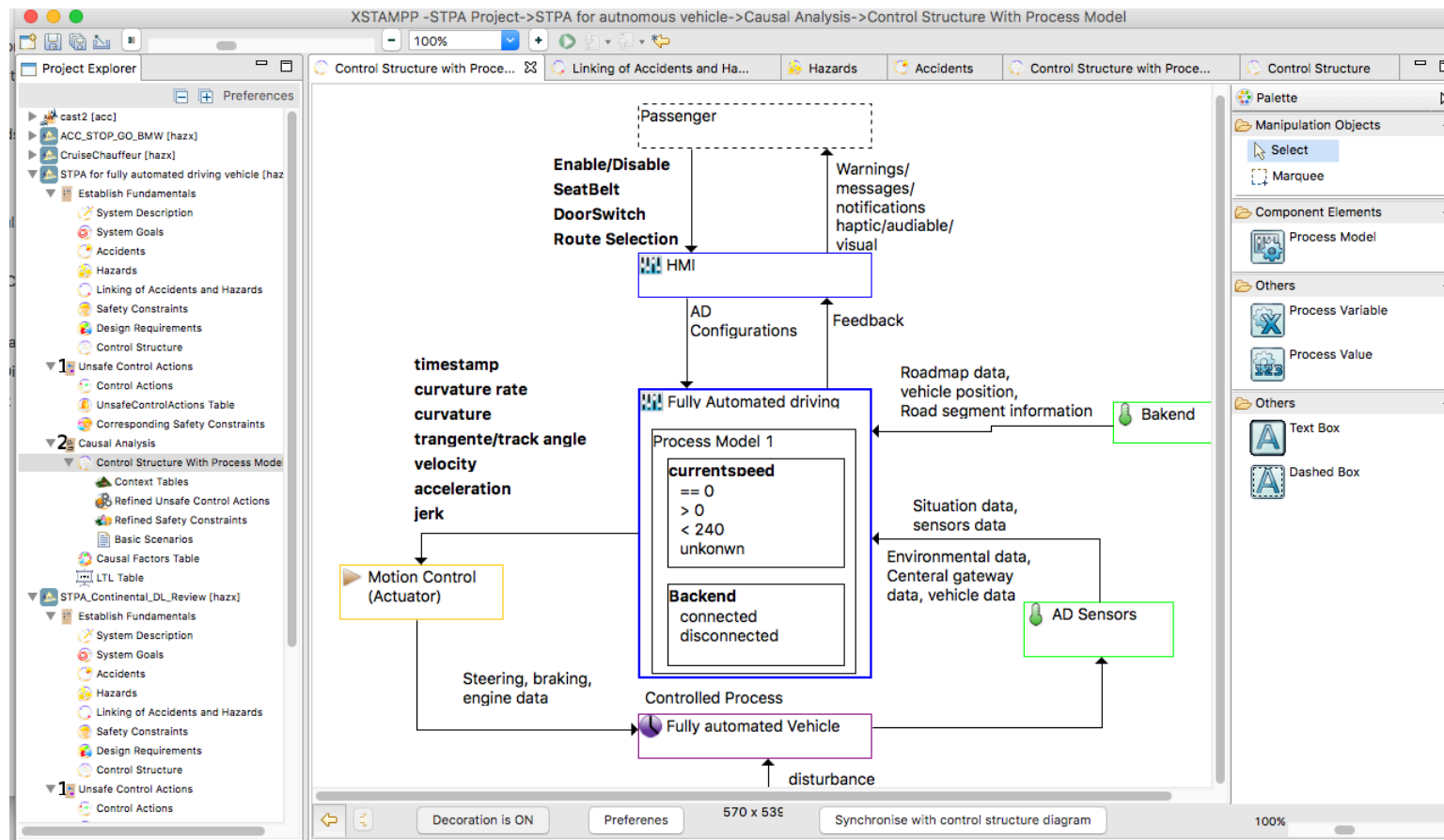
**Safety Constraint** SC-1: The fully automated driving function platform must always provide the trajectory to enable motion control to adjust the throttle position and apply brake friction when the vehicle is driving too fast on a highway and there is traffic ahead to avoid a potential collision.



# XSTAMPP Tool Support ([www.xstamp.de](http://www.xstamp.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** | 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
- › 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