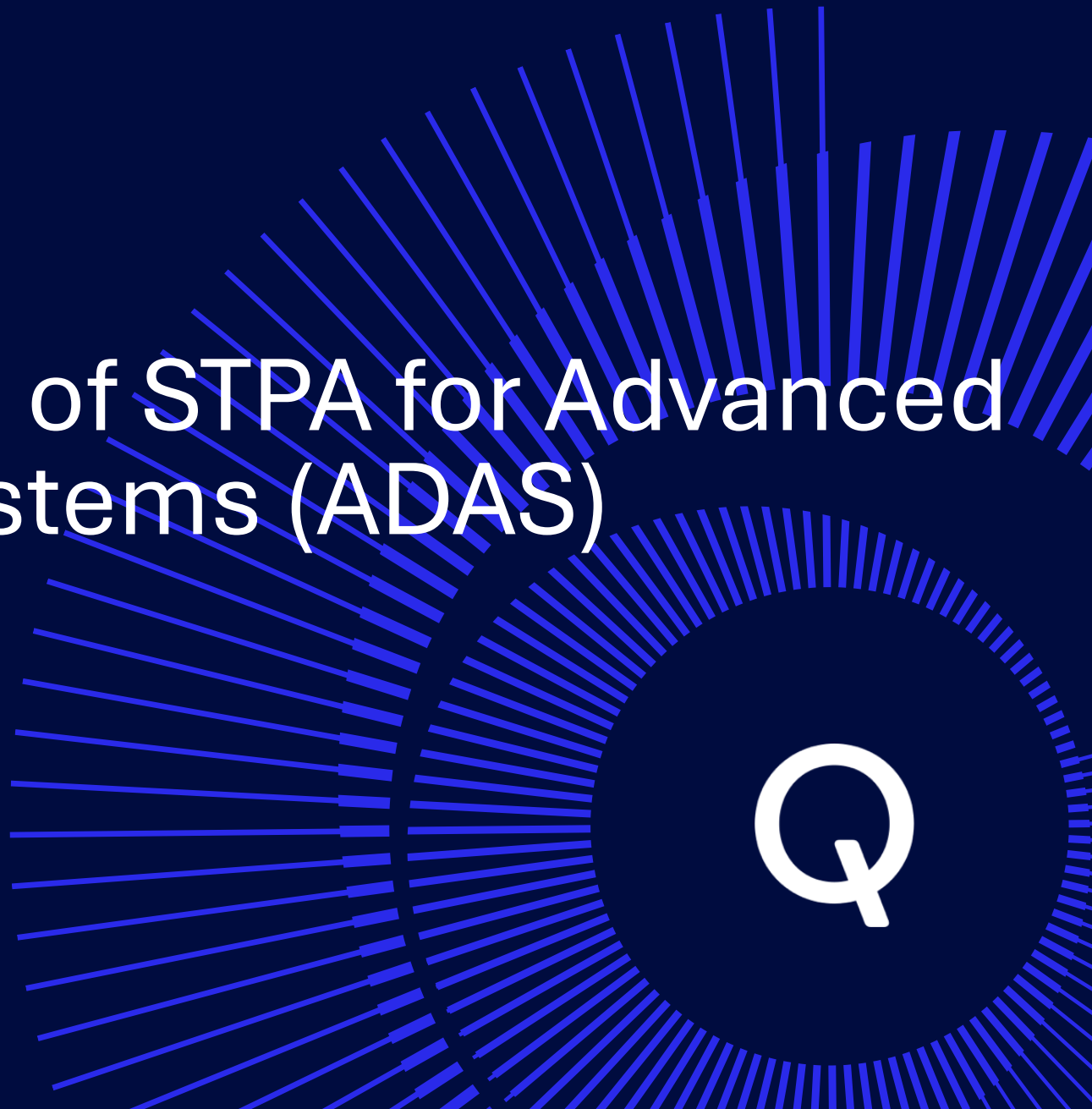
Qualcomm

OEM & Suppliers Use of STPA for Advanced Driver-Assistance Systems (ADAS)

Kilian Zwirglmaier[1], Jeff Stafford[2], Shabin Mahadevan[3] and Ali Abbaspour[2]

[1]Arriver Software GmbH, [2] Qualcomm Technologies, Inc., [3]Arriver Software LLC

@qualcomm



Snapdragon Ride

Complete AD Stack

Modular Architecture
- Perception, Maps, Localization,
- Advanced AI Predictor and planner

5th Gen CV / perception product
- Advanced 360° camera CV (3D)
- Low level Multi-modal perception

SoCs, BSP & Middleware

AD Cloud & Workbench
- Data simulation factory
- Reprocessing / GT / Data
- ML Ops

Apps

ADAS/AD feature bundles

Core Technology

Environment Model

Localization & Maps

Vehicle Guidance (prediction & planner)

Vision / Perception

SoCs, BSP & Middleware

Backend Infrastructure and Services

Map

Shadow Mode and Active Learning

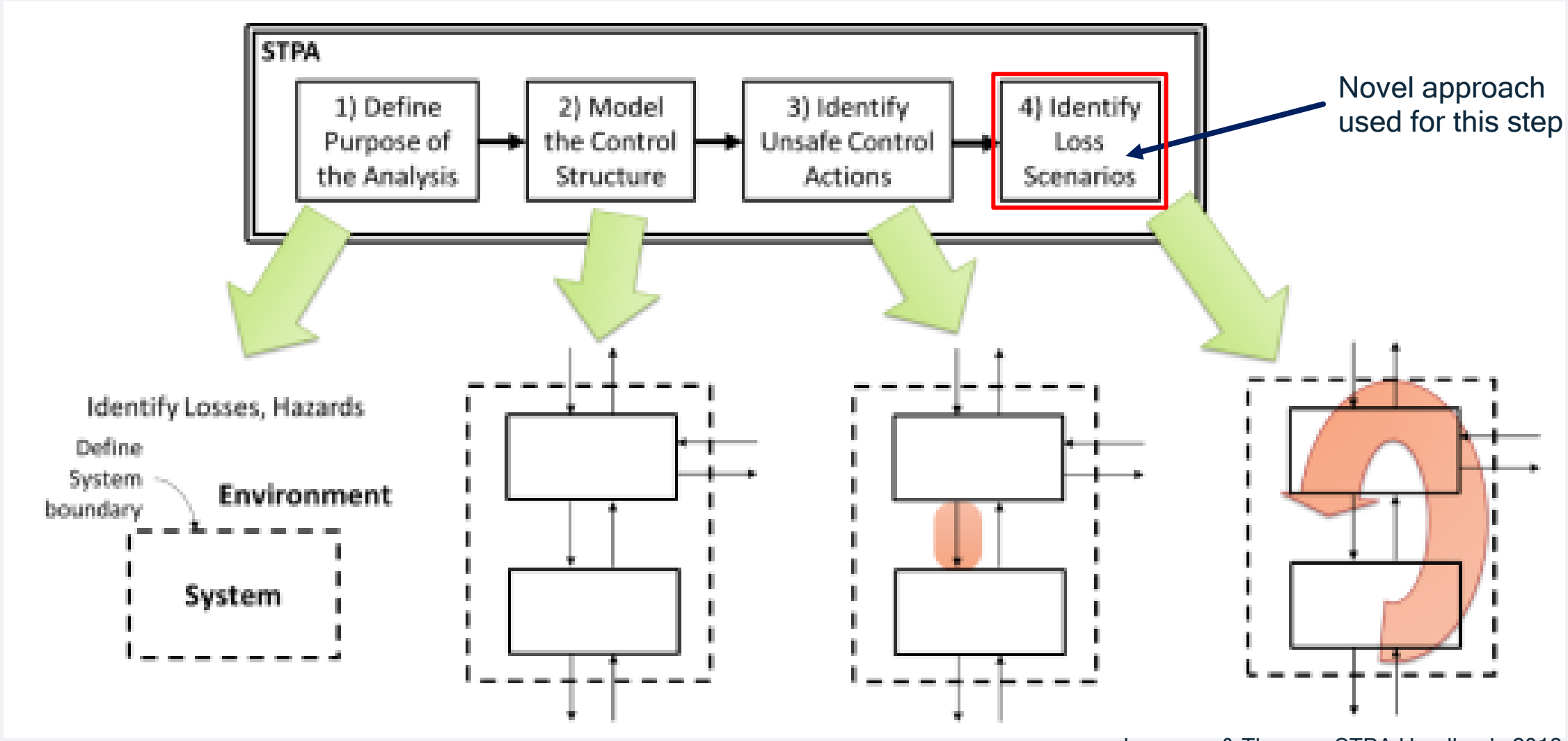
Data-Centric AI Framework (Ground Truth 2.0 & Auto Annotation)

Data and Simulation Factory

Problem statement

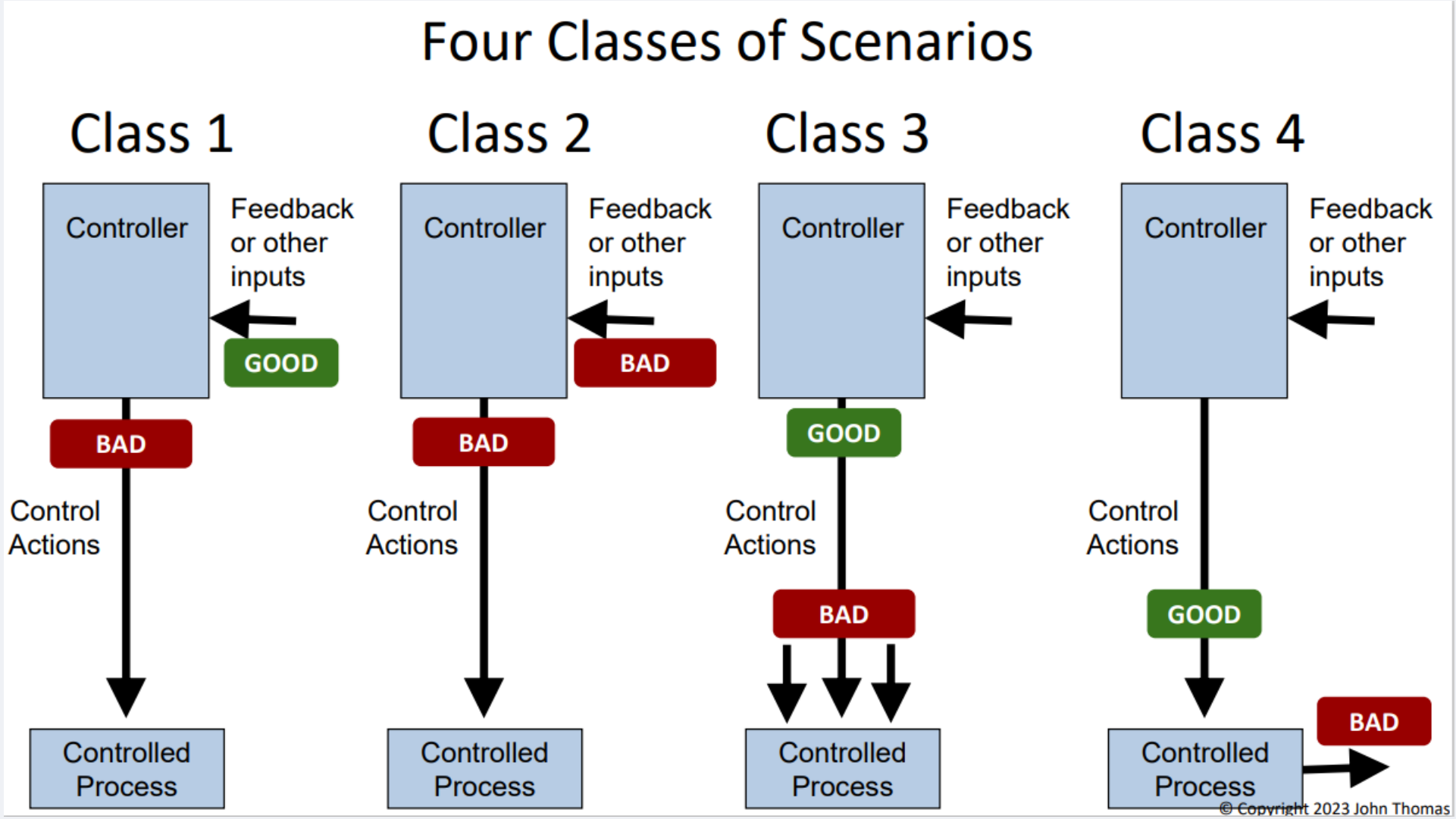
- **ADAS systems** are highly complex due to their interaction with the open world through sensing systems and related algorithms, integrating ADAS systems (SEooC) with multiple OEMs adds to this complexity.
- **Additional complexity through SEooC**:
  - Systems developed as Safety Elements out of Context (SEooC) introduce additional complexity.
  - Integration of an ADAS system into various OEM contexts can lead to additional hazardous scenarios.
  - STPA is used to identify these additional hazardous scenarios introduced by the integration of the SEooC.
  - STPA, as a tool for communication, helps bridge the gap between the assumptions made by the ADAS supplier and the OEM's context.
- **Safety standards**:
  - In particular, Safety of the Intended Functionality (SOTIF), ISO 21448, requires iterative identification of previously unknown hazardous scenarios.
  - STPA is well-suited for fulfilling this purpose.
- **STPA:**
  - A state-of-the-art, non-proprietary system analysis method for identifying hazardous scenarios in complex systems.
  - SOTIF is not replacing hazard analysis methods stated in ISO 26262 but used to complement these moreover it's an additional method (besides DFMEA, FTA, HAZOP) as mentioned in ISO 21448.

STPA



Leverson & Thomas, STPA Handbook, 2018

STPA – Basic scenarios



Automotive Safety of the Intended Functionality (SOTIF)

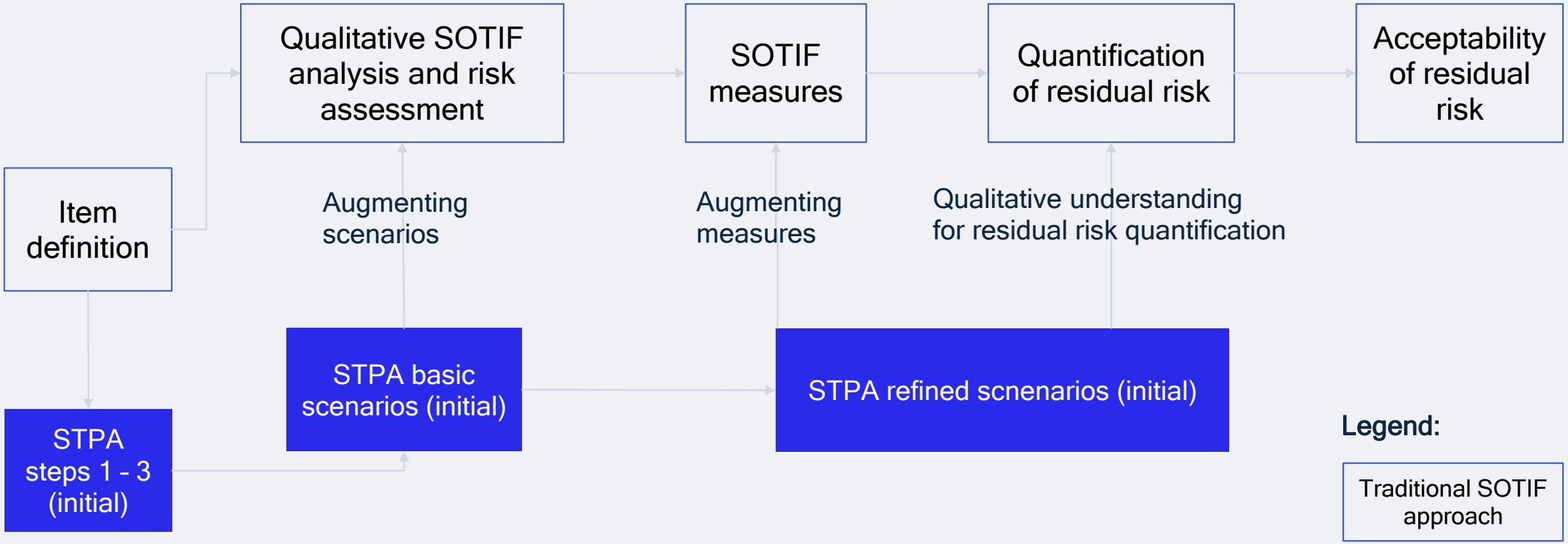
ISO 21448

- Focus on System Safety Risks:
  - leading to the injuries or loss of life (Losses)
  - resulting from functional insufficiencies
- In brief:
  1. Identify and evaluate potential hazardous scenarios
  2. Identify and implement modifications to address the potential hazardous scenarios and their associated functional insufficiencies and triggering conditions
  3. Show that the residual risk that cannot be fully mitigated is acceptably low according to a defined risk acceptance criterion

There is a strong argument for using STPA - in combination with other methodologies (e.g., FTAs) - to satisfy these safety objectives

Adding STPA to an existing SOTIF process

STPA can be used as a gap analysis tool to enhance an existing SOTIF process

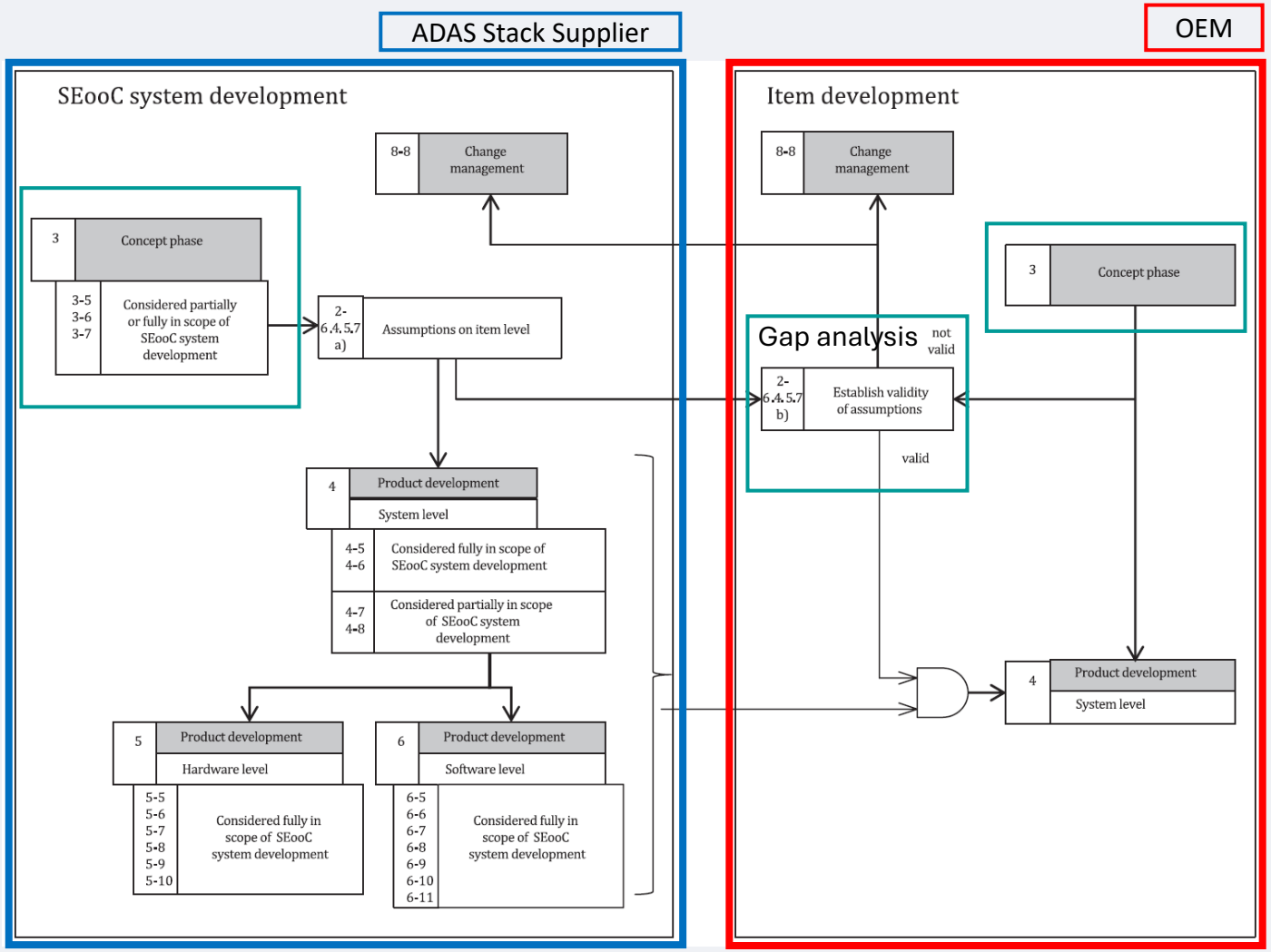


Note: STPA is always performed in context of the OEM's vehicle platform. In case of a new OEM‘s context the analysis is refined.

SEooC validity of assumptions – Potentially new Hazards

Common language of STPA between OEM and supplier

- The ADAS stack supplier performs a safety analysis for an assumed vehicle context - e.g. by abstracting from an SEiC development
- The ADAS stack supplier delivers Assumptions of use (AoUs) to an integrating OEM
- The integrating OEM takes responsibility for the safety analyses for their in-context system
- Need for **gap analysis** between the assumed context of the SEooC and the context of the integrating OEM.
- How to support the integrating OEM beyond that? → STPA



ISO 26262-10:2018(E) , Figure 22 — SEooC system development

AoU: Assumption of Use
ADAS: Advanced Driver-Assistance Systems
Item: System at the vehicle level
SEiC: Safety Element in Context
SEooC: Safety Element out of Context

Initial STPA work products are provided together with AoUs to the integrating OEM to support their SOTIF analysis.

STPA enables OEM and Supplier Collaboration in Concept Phase

STPA provides guidance on responsibility and supporting roles in collaboration

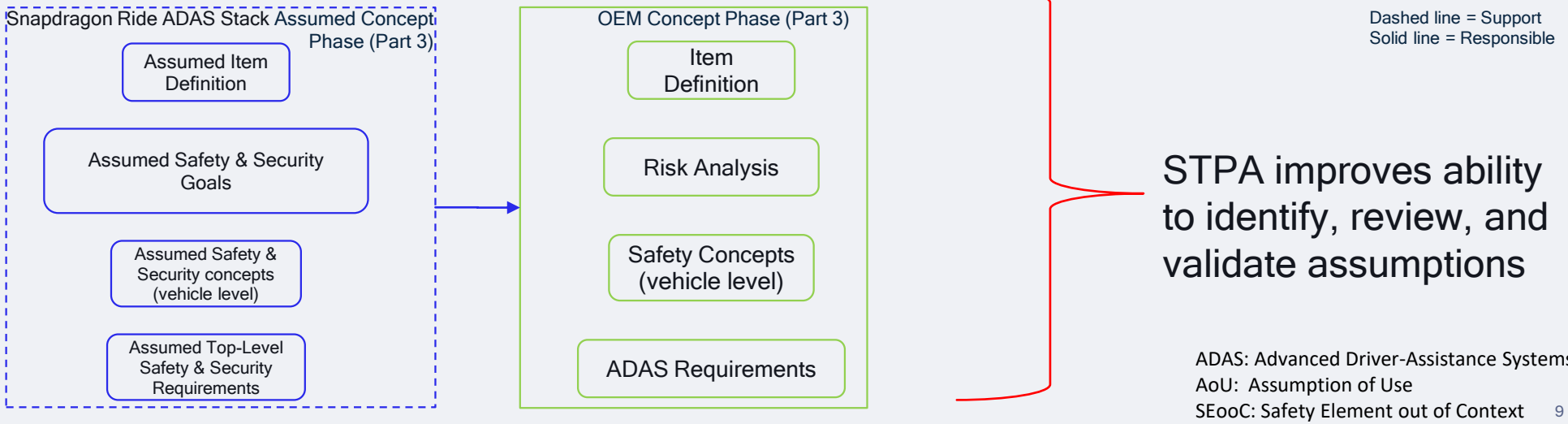
SEooC Supplier Role

- Delivers assumptions of use (AoUs)
- Provides initial draft STPA draft control structure with assumed vehicle context (item level)
- Provides initial STPA UCAs
- Provides initial STPA scenarios

OEM Role

- Uses AoU inputs and initial STPA work products for their own safety analysis

STPA supports OEM's gap analysis in their Concept Phase

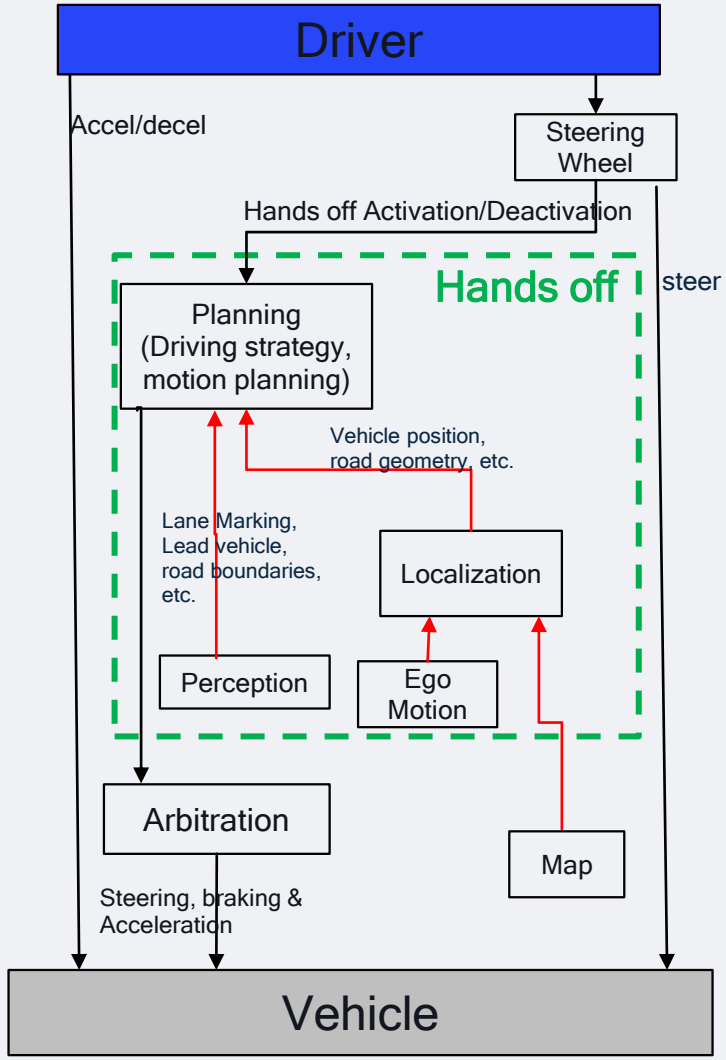


STPA improves ability to identify, review, and validate assumptions

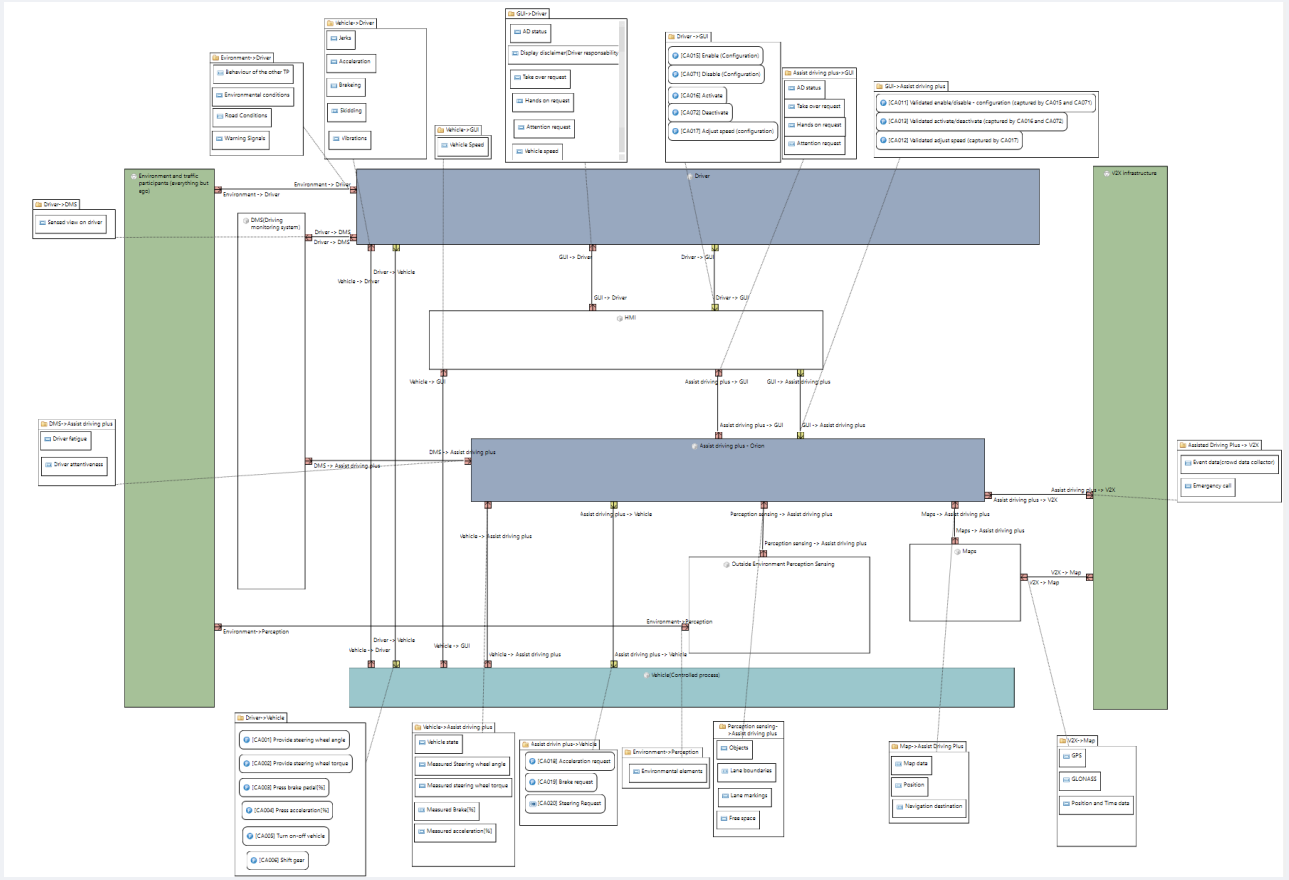
ADAS: Advanced Driver-Assistance Systems
AoU: Assumption of Use
SEooC: Safety Element out of Context
UCA: Unsafe control action

Case study – STPA control structure

SAE L2 customer function that allows hands off driving but only in appropriate conditions.



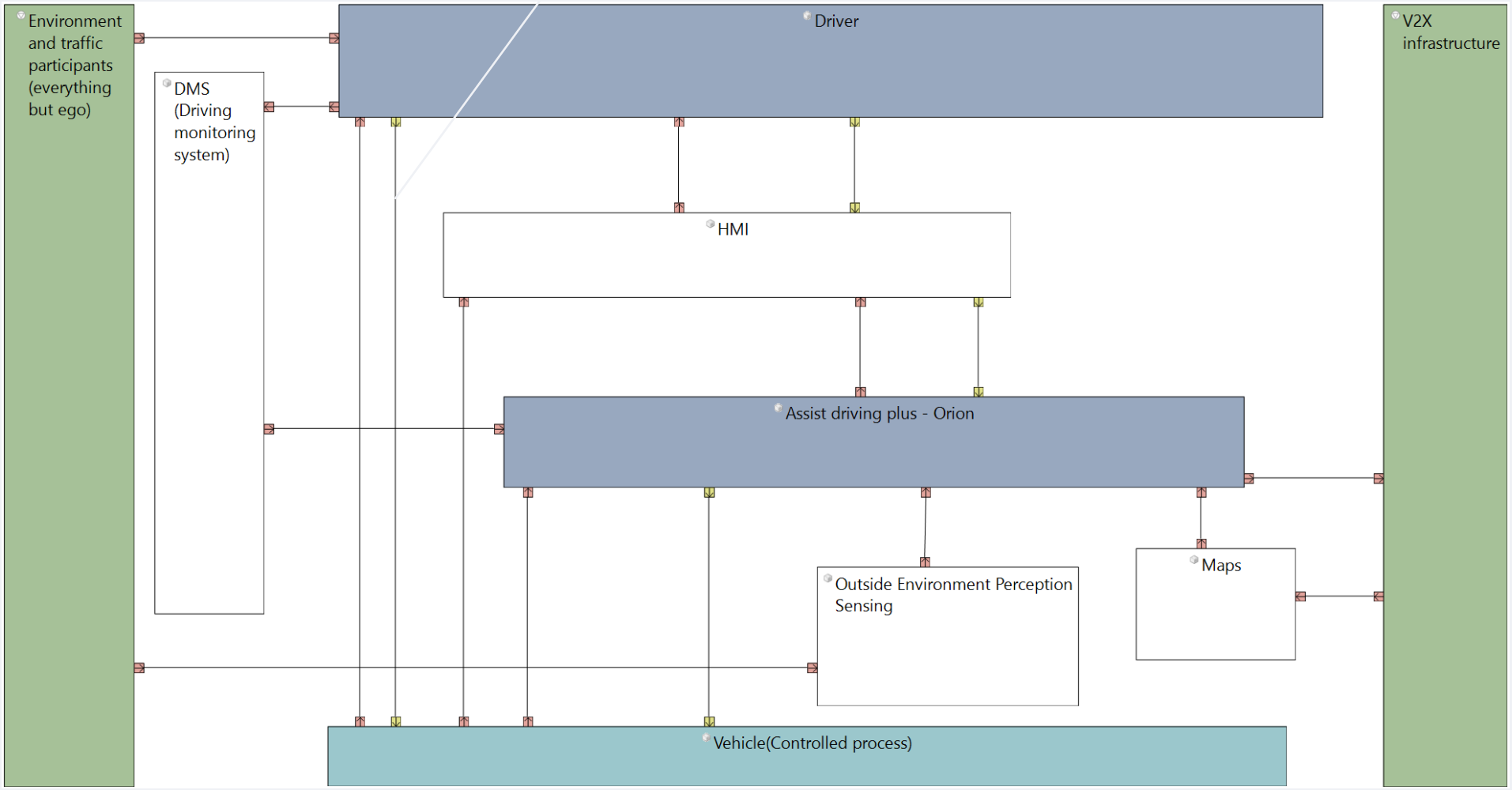
Compare to the STPA control structure using the MEDINI tool.
Notice that tools can make the control structure harder to read.



STPA analysis Level 1

Control structure

Control action:
CA1 Provide steering wheel angle



Findings I

Unsafe control action (UCA):

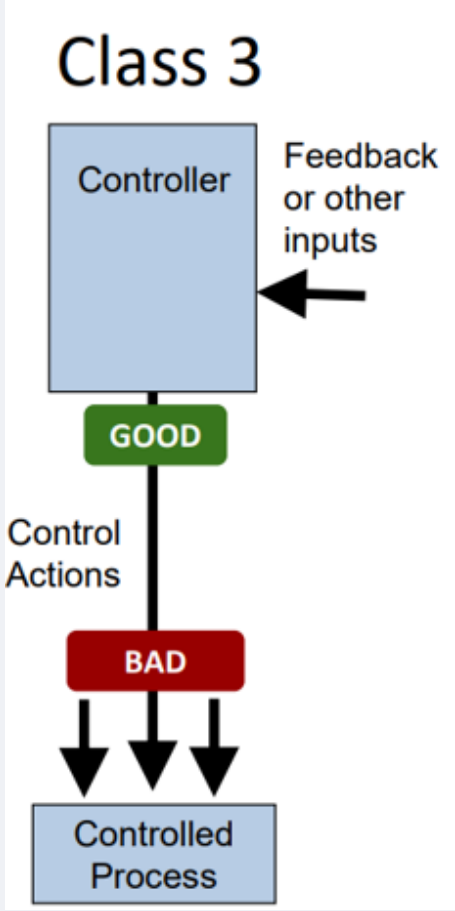
Driver provides steering wheel angle when the new steering angle results in leaving the allowed travel area.

Scenario Class 3 (Unsafe Control path):

1) Driver does not provide steering to leave the safe travel area
2) Vehicle received steering command to leave the safe travel area

Refined scenario(s):

Emergency Steering Support (ESS) amplifies/dampens the drivers steering command.



Findings II

Unsafe control action (UCA):

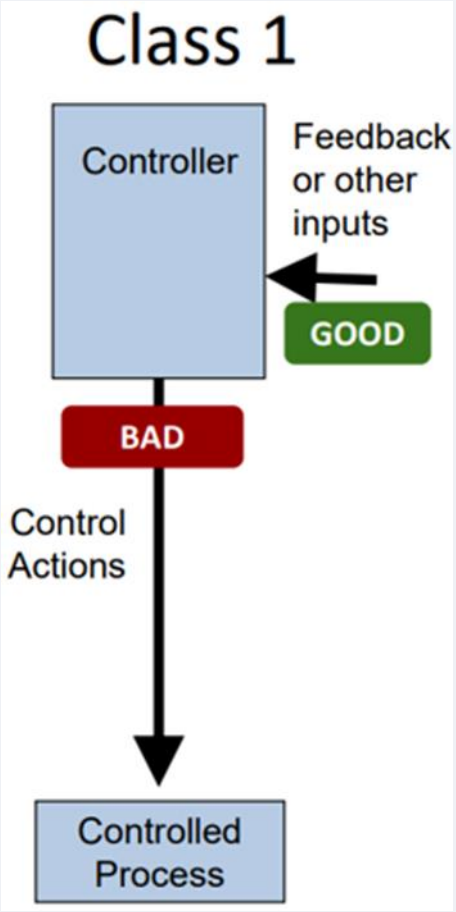
Driver Continues providing steering wheel angle too long after collision is avoided.

Scenario Class 1 (Unsafe Controller behavior):

1) Driver provides steering wheel command for too long
2) Driver received feedback by vehicle that indicated the steering command is on time

Refined scenario(s):

- Driver tests out the capabilities of the system
- Driver is distracted
- Driver underestimates the steering wheel reaction to the commanded steering input



Concluding remarks

STPA

- Identification of gaps in existing sets of potentially hazardous scenarios
- Develop a common safety focused understanding of the system between OEM and suppliers

STPA basic scenarios

- Well structured approach
- Basic scenarios can be refined by different domain expert teams
- Good basis for collaboration between OEM and suppliers

Prioritization of results:

- There are scenarios for which a residual risk remains
- The acceptability of the resiudal risk can be evaluated using the STPA results
- STPA scenarios can support prioritization as a qualitative basis

Thank you

Follow us on:

For more information, visit us at qualcomm.com & qualcomm.com/blog