STPA in Support of Next-Gen Automotive E/E Architecture Development

2021 MIT STAMP Workshop

Sandro Nüesch (sandro.nueesch@huawei.com)
Christoph Ainhauser

Gereon Hinz (gereon.hinz@sttech.de)
Odysseas Papanikolaou
Diego Ortiz
Outline

2. Approach: Findings from Highway Pilot example
Motivation: Automotive E/E Architecture (EEA) Consolidation

ECU-based EEA

Domain-based EEA

Software-Defined Vehicle (SDV)

Established

Upcoming

Next Generation

• Existing EEA reach a complexity limit.
• Not suited to satisfy needs of the future vehicles:
  • Frequent software updates
  • Automated driving
  • Customer individualization
  • V2X, AI, teleoperation, etc.

 ➢ Vehicle-centralized
 ➢ Most business logic in central compute
 ➢ Scalable, open, flexible
 ➢ More resource efficient
SDV In-Vehicle Platform

Idea: Use STPA to identify potential safety-critical weaknesses of the EEA early in the development.

EEA optimization objectives:
- Scalable (e.g. from entry-level to luxury vehicles)
- Profitable
- Safe!
- Etc.

Central compute
Bus aggregation
5G & other radios
Infotainment compute

VIU: Vehicle Integration Unit
DMS: Driver Monitoring System
CPD: Child Presence Detection
Challenges when using STPA for EEA Design

• Typical EEA development has a strong focus on concrete technologies.  

versus

• Typical application of STPA follows top-down paradigm, starting from a high-level, technology-agnostic perspective.

Variables:
• Architectural patterns (ring, star, etc.)
• Communication technologies (Ethernet, PCIe, LIN, CAN, etc.)
• Number of gateways?
• Which communication links need to be redundant?
• Which components require safety integrity (ASIL)?
• Etc.

How can a technology provider such as Huawei leverage STPA to develop the next-gen EEA?
Challenges when using STPA for EEA Design

**EEA needs to be applicable for various features and functions**

Netflix  Night Vision  Driver Monitoring  Adaptive Cruise Control  Highway Pilot  Urban Pilot
Augmented Reality  Child Presence Detection  Lane-Keep Assist  Valet Parking

• Ideally, architecture is developed out of context (function-independent).
• Then applied to an OEM (specific system designs and sets of features and functions of mixed criticality)

“Ensure every UCA specifies the context that makes the control action unsafe.” [STPA Handbook, 2018]

How do we analyze the safety of an architecture which is developed out of context?
Our Approach in 4 Steps

- Feature assumption for context
- Perform STPA on feature
- Map control loop onto EEA
- Identify EEA weaknesses
Assumed Feature: Highway Pilot

**SAE J3016™ LEVELS OF DRIVING AUTOMATION**

- **No automation**
  - You are driving and are In control of the vehicle at all times.
  - No automated driving tasks.

- **Shared responsibility**
  - Driver and system share responsibility.
  - Allows ~10s response time to driver take over request (TOR).

- **Full automation**
  - No human intervention.
  - System performs all driving tasks.

### Automated Driving feature of SAE Level 3

- Shared responsibility between driver and system

### Responsibility of the system:

- Performs all driving tasks
- Provides driver take over request (TOR) if it cannot execute the function anymore.
- Allows ~10s for driver to respond to TOR, otherwise slows down or stops.

### Responsibility of the driver:

- Does not have to pay constant attention.
- Needs to be ready to take over control within ~10s of TOR.

---

Highway Pilot (HWP) allows automated, high-speed highway driving

[Safety First for Automated Driving, 2019]
Responsibility of the system:
- Performs all driving tasks
- Provides driver take over request (TOR) if it cannot execute the function anymore.
- Allows ~10s for driver to respond to TOR, otherwise slows down or stops.

Responsibility of the driver:
- Does not have to pay constant attention.
- Needs to be ready to take over control within ~10s of TOR.

Common approach: Dual Channel System

Assumed Feature: Highway Pilot

(In Automotive considered “fail-safe” or “fail-silent”)

Detect

Inform driver

Disable

Safe state

Safety-critical fault

Try to continue

Continue operation

Detect

Inform driver

Disable

Safe state

Safety-critical fault

Try to continue

Continue operation

Detect

Inform driver

Disable

Safe state

Safety-critical fault

Try to continue

Continue operation

Common approach: Dual Channel System

(In Automotive considered “fail-operational”)

Responsibility of the system:
- Performs all driving tasks
- Provides driver take over request (TOR) if it cannot execute the function anymore.
- Allows ~10s for driver to respond to TOR, otherwise slows down or stops.

Responsibility of the driver:
- Does not have to pay constant attention.
- Needs to be ready to take over control within ~10s of TOR.
Control Structure

Prior work focuses on key elements of function pipeline (e.g. perception, localization, path planning, etc.).
We took a complementary approach: Focus on analysis of the two channels.
Unsafe Control Actions

Example: Fail-Degraded Channel:

Note: Based on its responsibility, the FDC should only provide a braking and steering request if the NC is for some reason incapacitated.

UCA-1: The Fail-Degraded Channel does not provide the FDC Steering Request when HWP is enabled, the NC is inactive and the vehicle is about to enter a curve.
Loss Scenarios

<<Unsafe Control Action>>
UCA-1: The **Fail-Degraded Channel** does not provide the FDC Steering Request when HWP is enabled, the NC is inactive and the vehicle is about to enter a curve.

<<Loss Scenario>>
LS-1-1: HWP is enabled, the NC is inactive and the vehicle is about to enter a curve.

The FDC does not receive relevant camera image data to perceive the curve.

Therefore the FDC does not provide the FDC Steering Request.

Challenge: Need engineering judgement to focus on loss scenarios most relevant for EEA (e.g. related to communication, power supply, computation, etc.)
Map Control Loop onto EEA

Map control loop related to Loss Scenario onto the EEA. → Analysis re-usable for many EEAs.

Disclaimer: This slide depicts only an illustration of the EEA mapping, not the full-detail version.

– Huawei Public –
Identify EEA Weaknesses

<<Unsafe Control Action>>
UCA-1: The Fail-Degraded Channel does not provide the FDC Steering Request when HWP is enabled, the NC is inactive and the vehicle is about to enter a curve.

<<Loss Scenario>>
LS-1-1: HWP is enabled, the NC is inactive and the vehicle is about to enter a curve. The FDC does not receive relevant camera image data to perceive the curve. Therefore the FDC does not provide the FDC Steering Request.

<<Requirement>>
The EEA shall provide independent power supplies for the front camera and the NC.

<<Requirement>>
The EEA shall provide a connection from front camera to FDC independent of NC.

<<Requirement>>
The EEA shall provide FDC access to front camera data independent of NC access to lidar data.

<<Causal Factor>>
CF-1-1-1: NC is inactive due to a power supply failure. Front camera uses same power supply as NC. Camera is therefore also inactive and does not provide camera data.

<<Causal Factor>>
CF-1-1-2: NC loses access to lidar data and becomes inactive. Due to the same reason, FDC also loses access to front camera data.

<<Causal Factor>>
CF-1-1-3: Front camera data reaches Central Compute Platform but needs to pass through inactive NC to reach FDC. Therefore FDC does not receive required front camera data.
Summary

• Successfully applied STPA on assumed HWP to systematically derive safety requirements for SDV Next-Gen EEA.

• Requirements only based on a single feature.
  ➢ To derive comprehensive set of requirements need to expand to large set of features incl. their combinations.
Thank you!

Are you interested in collaborating with us? Contact us!

Sandro Nüesch, sandro.nueesch@huawei.com

- Have you already solved a similar problem (maybe outside of automotive)?
- Do you have feedback regarding our approach?
- Do you know of a smart and scalable tooling solution for STPA?