Using STPA to address challenges in achieving SOTIF

6/29/2021

Amardeep Sidhu

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and does not reflect the official policy or position of Arriver Inc.

Agenda

- What is SOTIF?
- Why this work?
- Observations

What is SOTIF?

- SOTIF- safety of the intended functionality and is defined[1] as the absence of unreasonable risk due to hazard caused by-
  - the insufficiencies of specification of the intended functionality at the vehicle level, or
  - the insufficiencies of specification or performance limitations in the implementation of E/E elements in the system

- Example
  - An object detection algorithm detecting and reporting a road sign resembling image on a truck in the vicinity of the ego vehicle as a true road sign.
  - Inadvertent or erroneous deactivation of the feature by the driver.

[1] ISO/DIS 21448: Road vehicles -- Safety of the intended functionality. Geneva, Switzerland: International Organization for Standardization, 2021.

Why this work?

- Learn from applying STPA to achieve objectives listed under clauses 6 and 7 of ISO/DIS 21448.
- The standard already has guidance on the use of STPA.
  - Deriving SOTIF related misuse scenarios using STPA.
  - STPA applied on a simplified SAE L3 feature to run SOTIF analysis for Clause 6 and 7.

Observations

- Specification and design from clause 5 (functional and system specifications) are a natural input to STPA steps 1 (defining the purpose of the analysis) and 2 (Modeling the control structure).
- Hazards and consequences of hazardous events identified during the functional safety analysis of the item could be reused in STPA step 1 for SOTIF analysis if they meet the requirements in the STPA handbook.
- SOTIF driven (performance of sensing the environment, planning (through decision algorithms) and actuation) selection of control loops and UCAs is okay as a start but it is best to eventually cover the entire control structure.

Observations

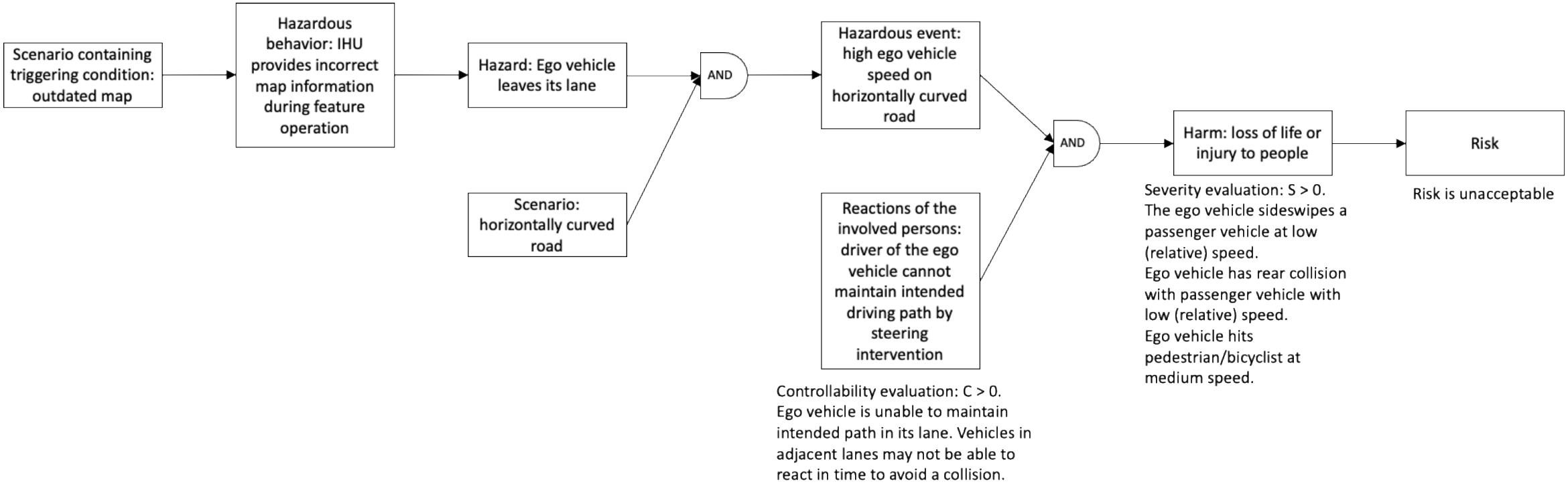
- Different category of causal scenarios will be generated (SOTIF, functional safety, etc.) and hence filtering is required.
- A scenario generated from STPA can be parsed and mapped to the various elements of a hazardous event relevant to SOTIF.

Causal scenario from STPA	Hazardous behavior (UCA)	Hazard	Scenario	Reactions of the involved persons	Harm
Scenario 3 for UCA-6: correct map file is uploaded onto the infotainment head unit (IHU) but with time it becomes outdated. Incorrect map information is reported by the IHU when outdated map is queried using correct GNSS input [UCA-6]. As a result, incorrect acceleration commands may be provided when navigating challenging scenery, for example horizontally curved road [H-1].	UCA-6: IHU provides incorrect map information during feature operation [H-1, H-2, H-3, H-4].	Ego vehicle leaves its lane.	Curved road.	Driver senses the high speed of the ego vehicle when navigating a tight turn, but is unable to prevent lane departure and subsequent rollover.	Loss of life or injury to people. Loss or damage to ego vehicle Loss of reputation (OEM and/or supplier) Loss of driver comfort.

- Each associated hazard could result in a new scenario.

Observations

- Another way to view the mapping of unsafe scenarios from STPA to the various elements of a hazardous event relevant to SOTIF.



Motivated by *Figure 7- An illustration of common elements of hazard analysis in the ISO 26262 series and in this document,* ISO/DIS 21448:2021.

Observations

- A causal scenario can be parsed to identify one or more functional insufficiency and a trigger condition.

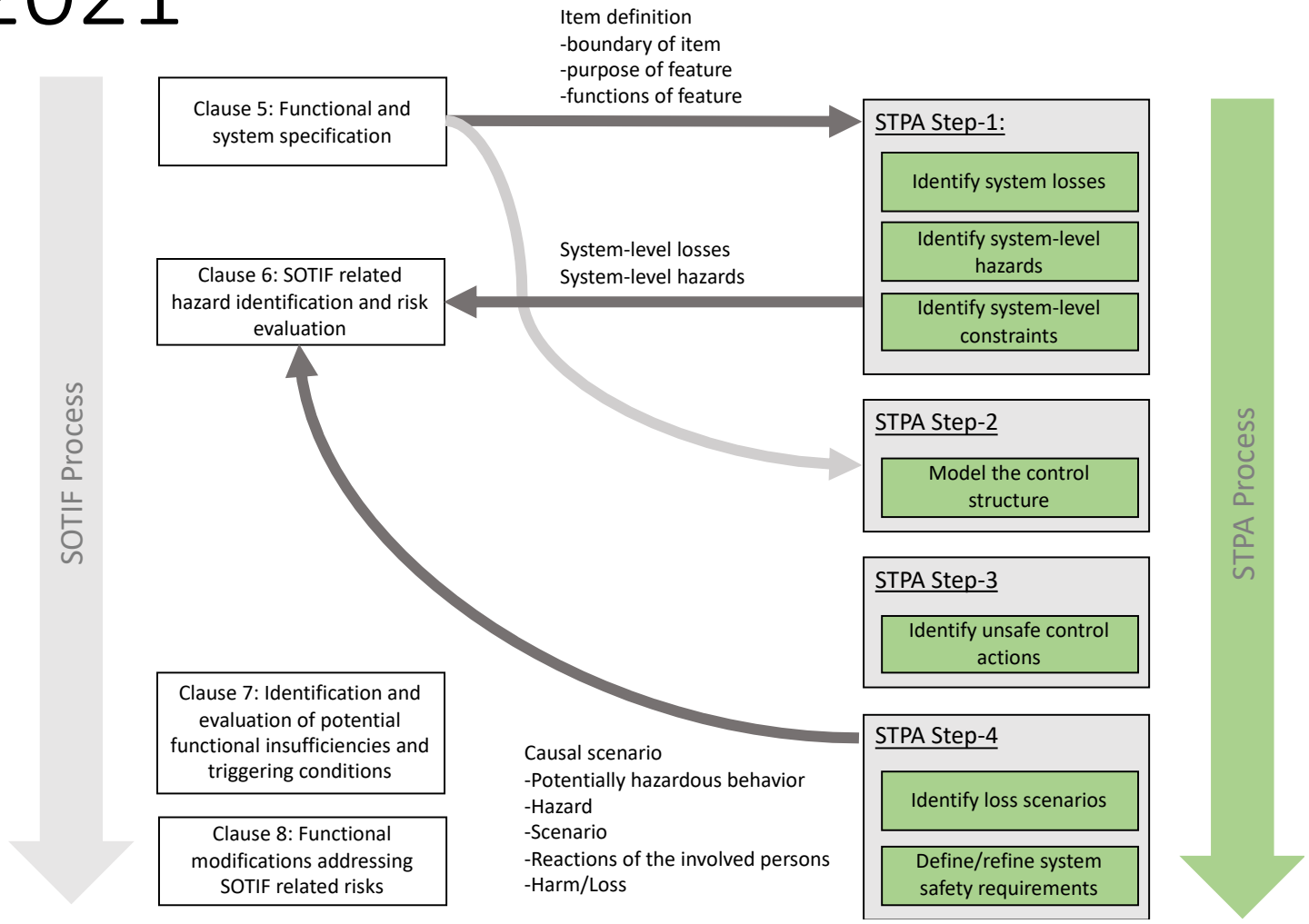
Scenario	Functional insufficiency	Triggering condition
Scenario 3 for UCA-6: correct map file is uploaded onto the infotainment head unit (IHU) but with time it becomes outdated. Incorrect map information is reported by the IHU when outdated map is queried using correct GNSS input [UCA-6]. As a result, incorrect acceleration commands may be provided when navigating challenging scenery, for example horizontally curved road [H-1].	FI-2: Outdated map file on the IHU.	TC-2: The outdated map file is queried.

Thank you!

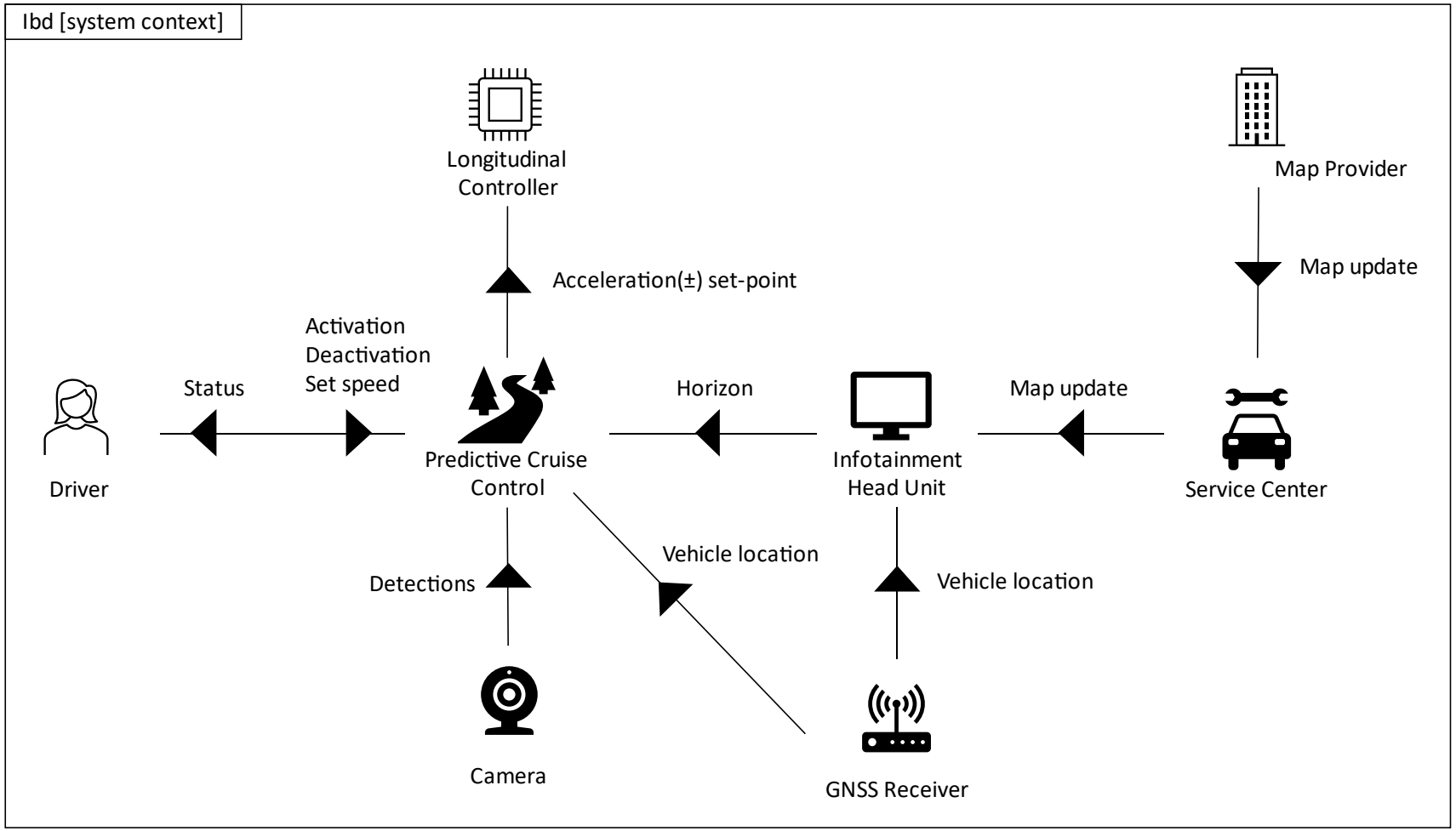
Contact
asidhu@alum.mit.edu

Extra/Backup

Mapping between STPA and ISO/DIS 21448:2021



Predictive cruise control feature CONOPS



The system under analysis is a driver assistance feature called predictive cruise control (PCC). PCC provides brake/acceleration and steering support to the driver using short range onboard sensors and long-range scenery information reported by the map to ensure safe vehicle behavior.

Assumptions

1. PCC is an SAE level 2 feature (lateral and longitudinal control) conceived for the purpose of this study.
2. Long range scenery information used by the feature includes speed limits on level, inclined, and curved roads.
3. The feature does not work under 25 km/hr.
4. The driver is always in control of the vehicle and is required to always keep his/her hands on the steering wheel.
5. Lack of hands-on steering wheel for prolonged duration results in feature deactivation.
6. The feature is usable anywhere and does not have any scene restrictions such as lane networks, weather etc.
7. If map information is not available at any time, then the feature will automatically scope down to rely only on the camera input.
8. The driver is responsible for keeping the map current by taking the vehicle in for service at predefined intervals throughout the life of the vehicle.
9. Ego vehicle speed at the time of feature engagement is accepted by the system as the set speed.
10. The driver can resume the feature operation to the last set speed.
11. Set speed can be changed by the driver at any time using dedicated control buttons.

STPA step-1: define the purpose of the analysis

Losses

L-1: loss of life or injury to people.

L-2: loss or damage to ego vehicle.

L-3: loss of reputation (OEM and/or supplier).

L-4: loss of driver comfort.

System-level hazards

H-1: Ego vehicle leaves its lane [L-1, L-2, L-3, L-4].

H-2: Ego vehicle applies hard braking [L-1, L-2, L-4].

H-3: Ego vehicle applies insufficient braking [L-1, L-2, L-3].

H-4: Ego vehicle applies hard acceleration [L-2, L-4].

Derived system-level constraints

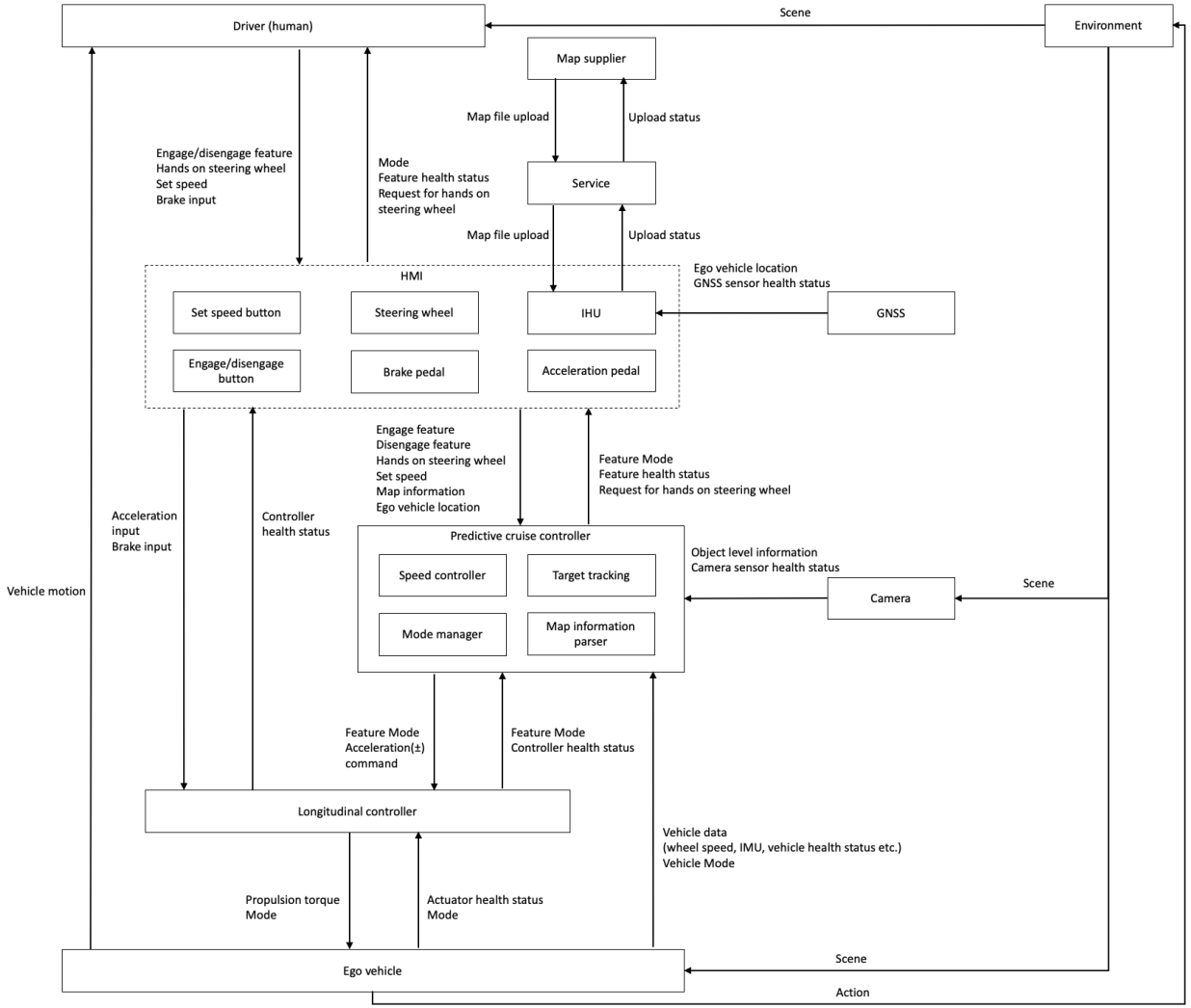
SC-1: Ego vehicle must not leave the lane unless desired by the driver [H-1].

SC-2: Ego vehicle must not decelerate at rates greater than 4 m/s^2 [H-2].

SC-3: Ego vehicle must decelerate at rates greater than 0.9 m/s^2 [H-3].

SC-4: Ego vehicle must not accelerate at rates greater than 1 m/s^2 [H-4].

STPA step-2: model the control structure



STPA step-3: identify unsafe control actions

Control action (CA)	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
CA-1: Engage feature (by driver).	N/A	UCA-1: Driver provides feature engagement command during controlled deceleration under driver's control [H-3, H-4].	N/A	N/A
CA-2: Disengage feature (by driver).	N/A	UCA-2: Driver provides feature disengagement command during controlled deceleration under feature control [H-1, H-3]. UCA-3: Driver provides feature disengagement command while the vehicle is navigating a turn under feature control [H-1].	N/A	N/A
CA-3: Hands-on steering wheel (by driver).	UCA-4: Driver does not provide hands-on steering wheel command during operation under feature control [H-1].	N/A	N/A	N/A
CA-4: Set speed (by driver).	N/A	UCA-5: Driver provides a high set speed during operation under feature control [H-4].	N/A	N/A
CA-5: Map Information (by IHU).	N/A	UCA-6: IHU provides incorrect map information during feature operation [H-1, H-2, H-3, H-4].	N/A	N/A
CA-6: Ego vehicle Location (by GNSS).	UCA-7: GNSS does not provide ego vehicle location during operation [H-1, H-2, H-3, H-4].	UCA-8: IHU provides incorrect ego vehicle location during operation [H-1, H-2, H-3, H-4].	N/A	N/A

STPA step-3: identify unsafe control actions

Unsafe control actions (UCA)	**Controller constraints (CC)**
UCA-1: Driver provides feature engagement command during controlled deceleration under driver's control [H-3, H-4].	CC-1: Driver must be ready to take over control of the ego vehicle when feature engagement command is issues during controlled deceleration under driver's control [UCA-1].
UCA-2: Driver provides feature disengagement command during controlled deceleration under feature control [H-1, H-3].	CC-3: Driver must be ready to take over the longitudinal control of the ego vehicle when feature is disengaged while the vehicle is in controlled deceleration under feature control [UCA-2].
UCA-3: Driver provides feature disengagement command while the vehicle is navigating a turn under feature control [H-1].	CC-3: Driver must be ready to take over the lateral control of the ego vehicle when feature is disengaged while the vehicle is navigating a turn under feature control [UCA-3].
UCA-4: Driver does not provide hands-on steering wheel command during operation under feature control [H-1].	CC-4: Driver must provide hands-on steering wheel command during vehicle operation under feature control [UCA-4].
UCA-5: Driver provides a high set speed during operation under feature control [H-4].	CC-5: Driver must not provide a high delta set speed during operation under feature control [UCA-5].
UCA-6: IHU provides incorrect map information during feature operation [H-1, H-2, H-3, H-4].	CC-6: IHU must provide correct map information during feature operation [UCA-6].
UCA-7: GNSS does not provide ego vehicle location during operation [H-1, H-2, H-3, H-4].	CC-7: IHU must provide ego vehicle location during feature operation [UCA-7].
UCA-8: IHU provides incorrect ego vehicle location during operation [H-1, H-2, H-3, H-4].	UCA-8: IHU must provide ego vehicle location within TBD tolerance during feature operation [UCA-8].

STPA step-4: identify loss scenarios

UCA-3: Driver provides feature disengagement command while the vehicle is navigating a turn under feature control [H-1].

Scenario 1 for UCA-3: The driver attempts to tune the radio using controls on the steering wheel. S/he inadvertently provides feature disengagement command while the vehicle is navigating a turn under feature control [UCA-3]. As a result, the ego vehicle leaves its lane [H-1].

UCA-6: IHU provides incorrect map information during feature operation [H-1, H-2, H-3, H-4].

Scenario 3 for UCA-6: correct map file is uploaded onto the infotainment head unit (IHU) but with time it becomes outdated. Incorrect map information is reported by the IHU when outdated map is queried using correct GNSS input [UCA-6]. As a result, incorrect acceleration commands may be provided when navigating challenging scenery, for example horizontally curved road [H-1].

CA-3: Hands on steering wheel.

Scenario 7 for CA-3: The driver sends hands on steering wheel command by placing his/her hands on the steering wheel, but the predictive cruise controller does not continuously detect driver's hands on the steering wheel because the sensor data is outside the calibrated sensor range. As a result, the feature may deactivate when the ego vehicle is navigating a horizontally curved road [H-1].

Parsing of select causal scenarios to identify elements of the SOTIF hazard analysis (ISO/DIS 21448:2021 clause 6)

Causal scenario from STPA	Hazardous behavior (UCA)	Hazard	Scenario	Reactions of the involved persons	Harm
Scenario 1 for UCA-3: The driver attempts to tune the radio using controls on the steering wheel. S/he inadvertently provides feature disengagement command while the vehicle is navigating a turn under feature control [UCA-3]. As a result, the ego vehicle leaves its lane [H-1].	UCA-3: Driver provides feature disengagement command while the vehicle is navigating a turn under feature control [H-1].	Ego vehicle leaves its lane.	Curved road.	Driver of the ego vehicle reacts to the lane departure by turning the steering wheel but is unable to prevent lane departure and subsequent rollover.	Loss of life or injury to people. Loss or damage to ego vehicle. Loss of reputation (OEM and/or supplier). Loss of driver comfort.
Scenario 3 for UCA-6: correct map file is uploaded onto the infotainment head unit (IHU) but with time it becomes outdated. Incorrect map information is reported by the IHU when outdated map is queried using correct GNSS input [UCA-6]. As a result, incorrect acceleration commands may be provided when navigating challenging scenery, for example horizontally curved road [H-1].	UCA-6: IHU provides incorrect map information during feature operation [H-1, H-2, H-3, H-4].	Ego vehicle leaves its lane.	Curved road.	Driver senses the high speed of the ego vehicle when navigating a tight turn but is unable to prevent lane departure and subsequent rollover.	Loss of life or injury to people. Loss or damage to ego vehicle. Loss of reputation (OEM and/or supplier). Loss of driver comfort.

Parsing of select control path scenario to identify elements of the SOTIF hazard analysis (ISO/DIS 21448:2021 clause 6)

Control path scenario from STPA	**Hazardous behavior**	**Hazard**	**Scenario**	**Reactions of the involved persons**	**Harm**
Scenario 7 for CA-3: The driver sends hands on steering wheel command by placing his/her hands on the steering wheel, but the system does not continuously detect driver's hands on the steering wheel because the sensor data is outside the calibrated sensor range. As a result, the feature may deactivate when the ego vehicle is navigating a horizontally curved road [H-1].	The hands-on steering wheel command from the driver is rejected.	Ego vehicle leaves its lane.	Curved road.	Driver of the ego vehicle reacts to the lane departure by turning the steering wheel but is unable to prevent lane departure and subsequent rollover.	Loss of life or injury to people. Loss or damage to ego vehicle. Loss of reputation (OEM and/or supplier). Loss of driver comfort.

Parsing of the STPA scenarios to identify functional insufficiency and triggering conditions (ISO/DIS 21448:2021 clause 7)

Scenario	Functional insufficiency	Triggering condition
Scenario 1 for UCA-3: The driver attempts to tune the radio using controls on the steering wheel. S/he inadvertently provides feature disengagement command while the vehicle is navigating a turn under feature control [UCA-3]. As a result, the ego vehicle leaves its lane [H-1].	FI-1: There is low differentiation between PCC feature deactivation control on the steering wheel and other functions also controlled through the steering wheel, for example radio tuning function.	TC-1: Different buttons on the steering wheel look the same to the driver.
Scenario 3 for UCA-6: correct map file is uploaded onto the infotainment head unit (IHU) but with time it becomes outdated. Incorrect map information is reported by the IHU when outdated map is queried using correct GNSS input [UCA-6]. As a result, incorrect acceleration commands may be provided when navigating challenging scenery, for example horizontally curved road [H-1].	FI-2: Outdated map file on the IHU.	TC-2: The outdated map file is queried.
Scenario 7 for CA-3: The driver sends hands on steering wheel command by placing his/her hands on the steering wheel, but the predictive cruise controller does not continuously detect driver's hands on the steering wheel because the sensor data is outside the calibrated sensor range. As a result, the feature may deactivate when the ego vehicle is navigating a horizontally curved road [H-1].	FI-3: Calibrated sensor range programmed in the predictive cruise controller is narrow and does not cover all user profiles.	TC-3: Driver places his/her on the steering wheel.