# STPA Analysis Report of Automatic Emergency Braking (AEB) system

Date: December 24, 2024

Generated by: SafeChatbot

Prepared by: Asim Abdulkhaleq

# System Identification

Description: The Automatic Emergency Braking (AEB) system is a critical vehicle safety feature designed to detect potential collisions and automatically apply the brakes to mitigate or prevent an accident. Below is a detailed design and description of the AEB system, including its components, functionality, and interactions.  
  
\*\*System Overview\*\*  
The AEB system employs a combination of sensors, processors (ECU), actuators, and a Human-Machine Interface (HMI) to monitor the vehicle's surroundings, identify potential collision risks, and automatically apply braking pressure when necessary. The system operates in several phases:  
  
1. \*\*Detection\*\*: Identify potential obstacles or hazards through various sensor inputs.  
2. \*\*Risk Assessment\*\*: Analyze the sensor data to predict the likelihood of a collision.  
3. \*\*Warning\*\*: Alert the driver of an imminent collision.  
4. \*\*Action\*\*: Apply brakes automatically if the driver does not respond in time.  
5. \*\*Post-Event Analysis\*\*: Log data for diagnostics and system improvement.  
  
\*\*System Components\*\*  
  
\*\*1. Human Controller:\*\*  
 - \*\*Role\*\*: The vehicle driver who is responsible for controlling the vehicle and may respond to warnings provided by the AEB system, their actions will influence the overall system operation.  
 - \*\*Key Features\*\*: Can override or react to system warnings.  
 - \*\*Connections\*\*: Receives visual, auditory, and haptic feedback from the HMI, their control action could affect the controlled process such as braking or steering if the human respond to the warnings.  
 - \*\*Example Contribution\*\*: If the driver brakes in response to an alert, the system assists in applying optimal braking force.  
  
\*\*2. Controller (Electronic Control Unit - ECU):\*\*  
 - \*\*Role\*\*: The central processing unit of the AEB system. Integrates data from all sensors, analyzes the environment using algorithms, and decides when to activate the brakes. It also sends a control command to the braking actuator and warnings to the HMI.  
 - \*\*Key Features\*\*: Utilizes machine learning and advanced signal processing for object recognition and decision-making. Implements collision prediction algorithms and braking force modulation.  
 - \*\*Connections\*\*: Receives data from radar, camera, LIDAR (optional), ultrasonic, wheel speed, yaw rate, and acceleration sensors. Sends control actions to the braking actuator and warnings to the HMI. It could also receives feedback from the braking actuator.  
 - \*\*Example Contribution\*\*: Processes data from multiple sensors to determine if a vehicle is approaching too quickly and initiates braking or the HMI warnings.  
  
\*\*3. Sensors:\*\*  
 - \*\*Role\*\*: Provide data about the vehicle's surroundings and motion.  
 - \*\*Key Features\*\*: Multiple sensors for redundancy and accuracy under different conditions.  
 - \*\*Connections\*\*: Provide data to the ECU.  
 - \*\*Radar Sensors\*\*:   
 - Mounted at the front of the vehicle to detect objects and measure their distance and speed relative to the vehicle.  
 - \*\*Camera Sensors\*\*:   
 - Typically located near the rearview mirror to capture visual data for object recognition.  
 - Examples of data include: vehicles, pedestrians, cyclists.  
 - \*\*LIDAR Sensors (optional)\*\*:   
 - Provide high-resolution 3D mapping of the environment for precise object detection.  
 - \*\*Ultrasonic Sensors\*\*:   
 - Used for close-range detection, often in low-speed scenarios.  
 - \*\*Wheel Speed Sensors\*\*:   
 - Monitor the speed of each wheel to ensure accurate braking response.   
 - \*\*Yaw Rate and Acceleration Sensors\*\*:   
 - Measure the vehicle's motion dynamics to improve stability during braking.   
 - \*\*Example Contribution\*\*: Radar detects the distance to the car ahead, while the camera identifies objects as a pedestrian.  
  
\*\*4. Actuator (Braking Actuator):\*\*  
 - \*\*Role\*\*: Implements the braking force as directed by the ECU, by either applying hydraulic braking force or using an electric brake booster  
 - \*\*Key Features\*\*: Provides rapid and precise brake response. Includes hydraulic and electrical components to provide redundancy, could include feedback to ECU about the execution.  
 - \*\*Connections\*\*: Receives control action signals from the ECU and send execution signal to the controlled process (Vehicle Braking System) or send feedback to the ECU  
 - \*\*Example Contribution\*\*: Applies the necessary braking force to slow down or stop the vehicle to avoid a collision.  
  
\*\*5. Controlled Process (Vehicle):\*\*  
 - \*\*Role\*\*: The physical vehicle that is being controlled by the system, which includes the braking system.  
 - \*\*Key Features\*\*: Includes the physical breaking system and the car motion dynamics  
 - \*\*Connections\*\*: Receives braking force command from the actuator and has a state of car motion that is used by the sensors.  
 - \*\*Example Contribution\*\*: The braking system applies friction to slow the car motion based on the actuator output  
  
\*\*6. Human-Machine Interface (HMI):\*\*  
 - \*\*Role\*\*: Provides feedback and warnings to the driver.  
 - \*\*Key Features\*\*: Multimodal feedback through auditory, visual, and haptic signals.  
 - \*\*Connections\*\*: Receives control commands from the ECU and delivers information to the human controller. It is also part of the controlled process since it is part of the vehicle.  
 - \*\*Example Contribution\*\*: Provides a warning beep and displays a visual alert on the dashboard to indicate a potential collision.   
  
\*\*7. Communication Modules:\*\*  
 - \*\*Role:\*\* Enables communication with external sources for enhanced situational awareness.  
 - \*\*Key Features:\*\* V2X communication capabilities  
 - \*\*Connections:\*\* Receives data from other vehicles or infrastructure, enhancing collision avoidance and providing additional data to the ECU for decision making, but it does not affect braking directly and does not send control action, thus it is more part of the sensor.  
 - \*\*Example Contribution:\*\* Receives data about traffic conditions that help improve collision prediction accuracy.  
  
\*\*System Functionality (Detailed)\*\*  
  
1. \*\*Detection and Monitoring:\*\* The system continuously scans the road using radar, cameras, and other sensors. The ECU processes the sensor data to identify objects, calculate their distance, relative speed, and predict their trajectory.  
2. \*\*Risk Assessment:\*\* The collision prediction algorithms calculate the probability of an impact based on vehicle speed, distance to the obstacle, and driver behavior. If a potential collision is detected, the system evaluates whether it can be avoided through braking or steering.  
3. \*\*Driver Warning:\*\* When a potential collision is identified, the system first alerts the driver using visual, auditory, or haptic warnings. If the driver responds by braking or steering, the system assists as needed. The HMI also provide feedback about the system state or faults.  
4. \*\*Autonomous Braking:\*\* If the driver does not respond, the system automatically applies the brakes. The braking force is modulated to either avoid the collision entirely or reduce its severity.  
5. \*\*Post-Event Analysis:\*\* After an AEB event, the system logs data for diagnostic and feedback purposes, enabling continuous improvement.  
  
\*\*Key Design Considerations\*\*  
  
- \*\*Redundancy:\*\* Multiple sensors (e.g., radar and cameras) ensure reliability even if one sensor fails or is obstructed.  
- \*\*Latency:\*\* The system must process sensor data and activate the brakes within milliseconds to be effective.  
- \*\*Environmental Adaptability:\*\* Sensors must function in various conditions, including rain, fog, snow, and low light.  
- \*\*Fail-Safe Mechanisms:\*\* Backup power and fail-safe modes ensure the system operates reliably in emergencies.  
- \*\*Integration with Other Systems:\*\* The AEB system is often integrated with adaptive cruise control (ACC), lane-keeping assist (LKA), and electronic stability control (ESC).  
  
\*\*Connections\*\*  
  
- [Radar Sensors] --> [ECU]: radar data  
- [Camera Sensors] --> [ECU]: camera data  
- [LIDAR Sensors] --> [ECU]: lidar data  
- [Ultrasonic Sensors] --> [ECU]: ultrasonic data  
- [Wheel Speed Sensors] --> [ECU]: wheel speed data  
- [Yaw Rate and Acceleration Sensors] --> [ECU]: vehicle motion data  
- [ECU] --> [Braking Actuator]: braking control  
- [Braking Actuator] --> [Vehicle]: braking command  
- [ECU] --> [HMI]: warning control  
- [HMI] --> [Human Controller]: warning info  
- [Communication Modules] --> [ECU]: external data

Boundary: The system boundary includes the vehicle's sensors, the ECU, the braking actuator, the braking system, the HMI, the driver, the vehicle motion and their interactions. It also involves external environment such as the road conditions and other vehicles, and the interaction with the external system is done by communication module and is a part of the system and the sensor. The system does not include the road, other vehicles or external weather conditions.

# Purpose

The purpose of the analysis is to identify potential safety hazards associated with the AEB system and to develop safety constraints to mitigate these hazards, preventing accidents, loss of life or injury and to improve overall performance of the system.

# System Goals

* To prevent or mitigate vehicle collisions.
* To reduce the severity of unavoidable accidents.
* To ensure the safety of the vehicle occupants and other road users.

# Accidents

|  |  |
| --- | --- |
| id | description |
| A1 | Collision between the vehicle and another vehicle, pedestrian, cyclist, or object. |
| A2 | Loss of control of the vehicle leading to an accident. |
| A3 | Injury to vehicle occupants or other road users |
| A4 | Property damage |

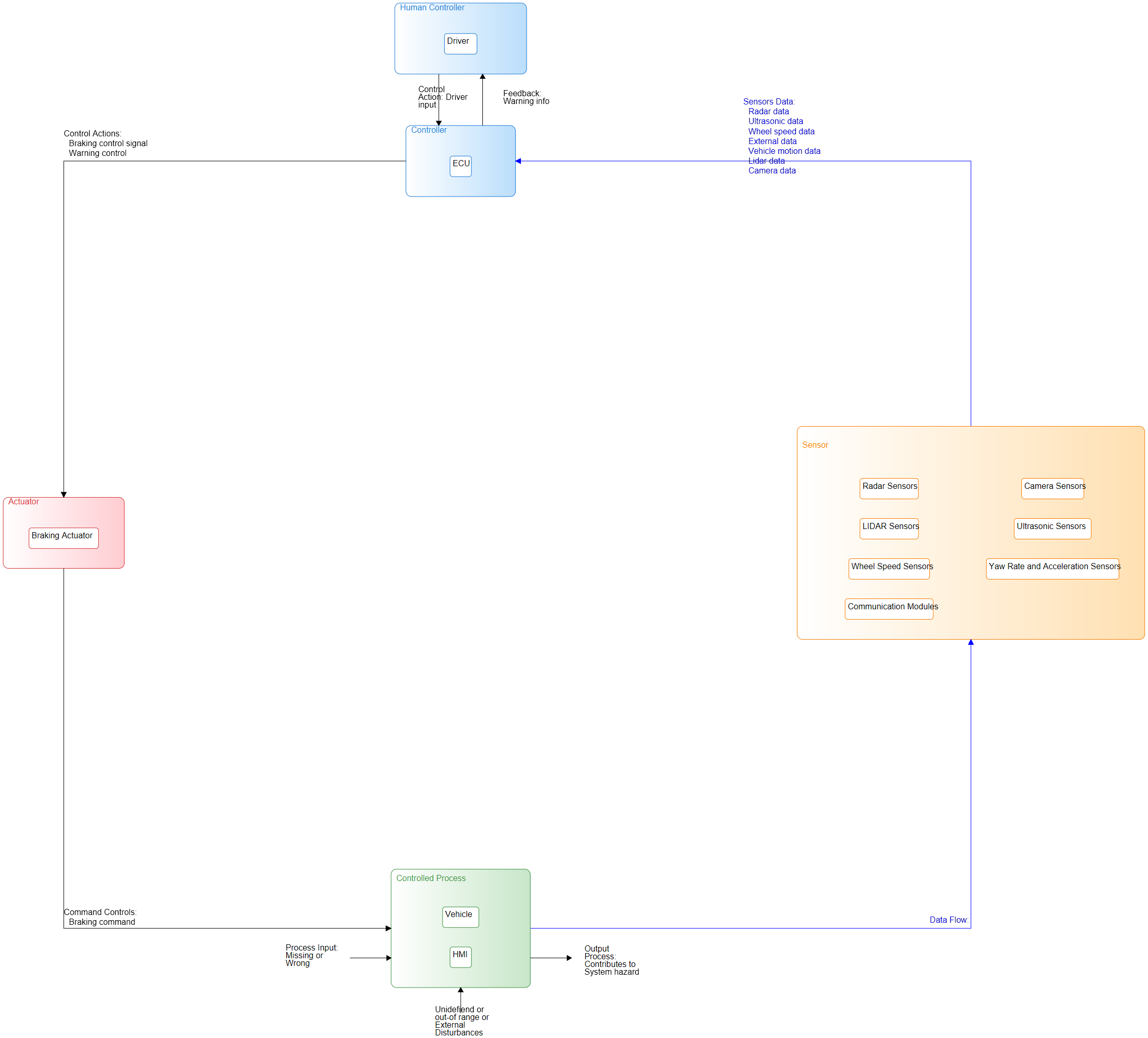
# Hazards

|  |  |  |
| --- | --- | --- |
| id | description | linked\_accidents |
| H1 | AEB fails to activate when a collision is imminent. | ['A1', 'A2', 'A3', 'A4'] |
| H2 | AEB activates unnecessarily causing a sudden stop and potential rear end collision. | ['A1', 'A2', 'A3', 'A4'] |
| H3 | AEB activation is delayed such that a collision is not mitigated | ['A1', 'A2', 'A3', 'A4'] |
| H4 | AEB activation is too strong or too weak, leading to loss of control or a collision that is not prevented. | ['A1', 'A2', 'A3', 'A4'] |
| H5 | AEB system does not provide adequate warning to the human driver, leading to an accident. | ['A1', 'A2', 'A3', 'A4'] |

# System Constraints

|  |  |  |
| --- | --- | --- |
| id | description | linked\_Hazard |
| SC1 | If a collision is imminent, then the AEB system must activate to mitigate a collision. | ['H1'] |
| SC2 | If no collision is imminent, then the AEB system must not activate and cause unnecessary braking. | ['H2'] |
| SC3 | If a collision is imminent, then the AEB system must activate with minimal delay to mitigate a collision. | ['H3'] |
| SC4 | If a collision is imminent, then the AEB system must apply the appropriate braking force and modulation to prevent a collision or reduce its severity. | ['H4'] |
| SC5 | If a collision is imminent, the AEB system must provide clear and timely warnings to the human driver. | ['H5'] |

# Control Structure



## Components

|  |  |
| --- | --- |
| name | type |
| Driver | Human Controller |
| ECU | Controller |
| Radar Sensors | Sensor |
| Camera Sensors | Sensor |
| LIDAR Sensors | Sensor |
| Ultrasonic Sensors | Sensor |
| Wheel Speed Sensors | Sensor |
| Yaw Rate and Acceleration Sensors | Sensor |
| Communication Modules | Sensor |
| Braking Actuator | Actuator |
| Vehicle | Controlled Process |
| HMI | Controlled Process |

## Connections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| label | source | target | description | connection\_type |
| radar data | Radar Sensors | ECU | Radar sensor provides the distance and speed data of the objects |  |
| camera data | Camera Sensors | ECU | Camera sensor provides the visual data of the objects |  |
| lidar data | LIDAR Sensors | ECU | Lidar sensor provides 3D mapping data of the environment. |  |
| ultrasonic data | Ultrasonic Sensors | ECU | Ultrasonic sensor provides close-range detection data. |  |
| wheel speed data | Wheel Speed Sensors | ECU | Wheel speed sensors provide the speed of each wheel. |  |
| vehicle motion data | Yaw Rate and Acceleration Sensors | ECU | Yaw rate and acceleration sensor provide the vehicle motion data. |  |
| External data | Communication Modules | ECU | Communication module sends data from other vehicles or infrastructure. |  |
| braking control | ECU | Braking Actuator | ECU sends command to braking actuator for braking operation |  |
| braking command | Braking Actuator | Vehicle | Braking Actuator applies braking force to vehicle breaking system |  |
| warning control | ECU | HMI | ECU sends command to HMI for warning delivery. |  |
| warning info | HMI | Driver | HMI provide warning about collision to the driver. |  |

# Unsafe Control Actions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Control Action** | **Not providing causes hazard** | **Providing causes hazard** | **Too early, too late, out of order** | **Stopped too soon, applied too long** |
| *1* | *braking control* | UCA1: The ECU does not send a braking control action to the braking actuator when a collision is imminent. | UCA2: The ECU sends a braking control action to the braking actuator when there is no imminent collision. | UCA3: The ECU sends braking control action to braking actuator too late after a collision was identified. | UCA4: The ECU sends a braking control action that is too strong/weak leading to a collision. |
| *UCA1: ['H1']* | *UCA2: ['H2']* | *UCA3: ['H3']* | *UCA4: ['H4']* |
| *2* | *warning control* | UCA5: The ECU does not send warning control action to HMI when a collision is imminent |  | UCA6: The ECU sends warning control action to HMI too late after a collision was identified |  |
| *UCA5: ['H5']* |  | *UCA6: ['H5']* |  |

# Controller Constraints

|  |  |  |
| --- | --- | --- |
| id | controller constrain | Linked Unsafe control\_action |
| C1 | The ECU must provide braking control action to the braking actuator when a collision is imminent. | ['UCA1'] |
| C2 | The ECU must not provide braking control action to braking actuator when there is no imminent collision. | ['UCA2'] |
| C3 | The ECU must provide braking control action to braking actuator with minimal delay after a collision is identified | ['UCA3'] |
| C4 | The ECU must provide the appropriate braking control action that is not too strong or too weak for the braking actuator to prevent a collision or minimize its impact. | ['UCA4'] |
| C5 | The ECU must provide warning control action to HMI when a collision is imminent | ['UCA5'] |
| C6 | The ECU must provide warning control action to HMI with minimal delay after a collision was identified. | ['UCA6'] |

# Loss Scenarios

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | uca | Linked Unsafe control\_action | type | scenario |
| L\_S\_1 | braking control | ['UCA1'] | controller failure | The ECU fails due to a hardware or software malfunction, causing it not to send a braking control action to the braking actuator when a collision is imminent. The sensors sends correct feedback to the controller but the controller does not respond or not process the information due to controller failure. |
| L\_S\_2 | braking control | ['UCA2'] | controller malfunction | The ECU misinterprets sensor data or due to a software bug incorrectly determines a collision risk and sends a braking control action when no collision is imminent. |
| L\_S\_3 | braking control | ['UCA3'] | controller algorithm fault | The collision prediction algorithm is flawed in the ECU, leading to a delayed braking control action, even when a collision is detected. |
| L\_S\_4 | braking control | ['UCA4'] | controller process model failure | The ECU applies incorrect braking force due to inaccurate process model or miscalculating the braking force needed to mitigate the collision and results in insufficient or too strong braking force, leading to loss of control and ineffective collision prevention. |
| L\_S\_5 | warning control | ['UCA5'] | controller failure | The ECU fails to send warning signal to HMI due to malfunction, causing a hazard due to no warning or delayed warning. |
| L\_S\_6 | warning control | ['UCA6'] | controller algorithm fault | The collision prediction algorithm in the ECU is flawed, causing a delayed warning signal to HMI and leading to the human driver not having enough time to response to avoid the collision. |

# Safety Constraints

|  |  |  |
| --- | --- | --- |
| id | Safety constraint | Linked\_loss\_scenarios |
| SF\_1 | The ECU must undergo regular self-testing and error handling mechanisms to ensure its reliability in critical situations. | ['L\_S\_1', 'L\_S\_2', 'L\_S\_5'] |
| SF\_2 | The collision prediction algorithm and braking control logic in the ECU must be rigorously validated and tested to ensure accurate collision detection and response. | ['L\_S\_2', 'L\_S\_3', 'L\_S\_4', 'L\_S\_6'] |
| SF\_3 | The system must have a backup power source and fail-safe mode to continue functioning in case of a power failure. | ['L\_S\_1', 'L\_S\_5'] |
| SF\_4 | The system must ensure sufficient warning time is provided to the human driver by considering various factors such as speed of the vehicle, time to collision and human reaction time | ['L\_S\_6'] |