# STPA Analysis Report of Adaptive Cruise Control (ACC)

Date: December 24, 2024

Generated by: SafeChatbot

Prepared by: Asim Abdulkhaleq

# System Identification

Description: Adaptive Cruise Control (ACC) is a cutting-edge driver assistance system designed to improve driving safety and convenience by automating speed control and maintaining a safe following distance. The system's design involves a seamless integration of sensors, control units, and actuators, working together to ensure optimal performance in real-world driving conditions. The ACC system aims to reduce driver fatigue by automating the longitudinal movement of the vehicle, which includes speed maintenance and distance keeping from lead vehicles.  
  
System Architecture and Components  
The ACC system comprises several key components, each playing a critical role in its operation:  
  
Human Controller (Driver)  
  
 Scope and Definition: The human driver sets the target speed and following distance and can override the system at any time by steering, braking, or accelerating. The human controller monitors the system's operation and remains in ultimate control of the vehicle, responsible for monitoring the operational environment and ensuring the safety.  
 Key Features: The ability to set speed and distance, receive system status via HMI, and override the system, as well as being able to take over the system at any time when unexpected situations occur, ensuring that the human driver remains the ultimate authority  
 Connections: The driver provides input via the Human-Machine Interface (HMI) to set the system parameters and monitor the system status.  
 Example: The driver uses the HMI to set the desired speed and following distance before initiating the ACC, also receives warnings through the HMI when ACC is not operating correctly, and they can disengage ACC by pressing brake or accelerator pedal.  
  
Sensor Suite  
  
Radar Sensors:  
  
 Scope and Definition: These sensors detect the relative speed, distance, and position of vehicles ahead using radar technology. They are mounted on the front grille or bumper.  
 Key Features: Real-time object tracking, effectiveness in diverse weather conditions.  
 Connections: The sensors send radar data to the Central Control Unit (ACC Controller).  
 Example: Radar sensors track a vehicle 30 meters ahead, providing data on its speed and distance for the ACC to adjust the host vehicle's speed.  
  
Video Cameras:  
  
 Scope and Definition: Positioned near the windshield, video cameras detect lane markings, vehicles, and obstacles using image processing technologies.  
 Key Features: Object recognition, lane detection, and classification capabilities.  
 Connections: These cameras send video data to the Central Control Unit (ACC Controller).  
 Example: Cameras detect that the host vehicle is drifting out of its lane and provide the lane data to the controller to adjust the vehicle to ensure lane keeping, complementing the radar data for more accurate object tracking.  
  
Ultrasonic Sensors (Optional):  
  
 Scope and Definition: These sensors assist in low-speed scenarios by detecting nearby objects through ultrasonic waves.  
 Key Features: Precise close-range detection, ideal for traffic jams and parking situations.  
 Connections: They send ultrasonic data to the Central Control Unit (ACC Controller) when activated.  
 Example: In stop-and-go traffic, ultrasonic sensors provide precise distance information to the car ahead, preventing small collisions in close range traffic situations.  
  
Central Control Unit (ACC Controller)  
  
 Scope and Definition: This unit processes input from the sensor suite using advanced algorithms to calculate the optimal speed and following distance. It is the core decision-making component of the system. The ACC Controller will determine the target vehicle speed and generate the command for the actuator to perform the necessary action to adjust the vehicle to the desired speed  
 Key Features: Predictive modeling, adaptive filtering, integration of driver preferences, and real-time adaptation to traffic conditions, ensure compliance with safety constraints.  
 Connections: Receives sensor data, receives input from the HMI through the driver input and sends control commands to the actuation system.  
 Example: The controller receives data that the vehicle ahead is slowing down; it calculates the required deceleration and sends command to the actuators to adjust speed accordingly.  
  
Actuation System  
  
Throttle Actuator:  
  
 Scope and Definition: Adjusts the engine power to increase or decrease speed as directed by the ACC Controller.  
 Key Features: Accurate adjustment of engine output to maintain desired vehicle speed  
 Connections: Receives commands from the Central Control Unit and adjusts engine power accordingly, sending the execution data to the vehicle engine or process.   
 Example: When the ACC controller calculates that more speed is needed, the throttle actuator increases engine power, to accelerate the vehicle.  
  
Brake Actuator:  
  
 Scope and Definition: Applies braking force to reduce speed or bring the vehicle to a complete stop as needed or directed by the ACC Controller.  
 Key Features: Precise braking force application for speed reduction or stopping.  
 Connections: Receives commands from the Central Control Unit and applies the brake force accordingly, sending the brake execution data to the vehicle wheel or controlled process.  
 Example: When a lead vehicle slows down, the brake actuator applies brake force to reduce speed.  
  
Transmission Interface:  
 Scope and Definition: Ensures smooth gear transitions during acceleration or deceleration, particularly in vehicles with automatic transmissions, sending the execution command to the vehicle transmission.  
 Key Features: Smooth gear changes to ensure stable acceleration/deceleration.  
 Connections: Receives commands from the ACC controller and adjusts the gear smoothly, sending the data execution to the vehicle gear system.  
 Example: During deceleration, the transmission interface ensures that the vehicle changes down a gear smoothly for the vehicle to be more responsive to the brake system.  
  
Controlled Process  
  
Vehicle (including Engine, Brakes, and Transmission):  
  
 Scope and Definition: The physical vehicle including its engine, brakes, and transmission responds to the actuator actions to achieve the desired speed and following distance.  
 Key Features: Physical movement of the vehicle, speed adjustment and distance keeping.  
 Connections: Receives command from the actuators such as throttle, brake and transmission interfaces, outputs vehicle speed and distance to the radar sensors, camera and ultrasonic sensor.  
 Example: The car moves forward, increases or decreases its speed, and maintains its position in the lane.  
  
Human-Machine Interface (HMI)  
  
 Scope and Definition: The HMI allows the driver to interact with the ACC system, setting parameters and monitoring its status. it is a part of the vehicle and allows communication between the driver and the system.  
 Key Features: Display of system status, alerts, input interface for driver preferences.  
 Connections: Receives input from the human controller (driver) to set system parameters and communicates system status to the driver, it receives driver set system speed and distance preference  
 Example: The display shows the target speed and the current status of the ACC system, when an error is detected, an error messages will be showed to the driver, when the ACC system detects an event that may require a driver intervention, the ACC will display a warning message to the driver.  
  
System Workflow  
  
Environment Sensing  
The radar, camera, and ultrasonic sensors continuously scan the road ahead, capturing data on vehicle positions, speeds, and lane boundaries.  
  
Data Processing  
The sensor data is fused and analyzed by the ACC controller to create a comprehensive situational model. Algorithms calculate the safe following distance using parameters such as relative speed, vehicle dynamics, and road conditions.  
  
Control Decision  
Based on the calculated safe distance, driver inputs, and system status, the controller determines the required acceleration or deceleration. In traffic scenarios, the system can bring the vehicle to a complete stop and resume driving when the traffic clears (stop-and-go functionality).  
  
Actuation  
The controller sends commands to the throttle, brake, and transmission actuators to adjust the vehicle's speed seamlessly. Feedback loops ensure real-time adjustments to maintain stability and comfort.  
  
Design Considerations  
  
Safety and Redundancy  
Redundant sensors and fail-safe mechanisms ensure system reliability in the event of a component failure. Emergency braking functionality is integrated to prevent collisions in critical situations.  
  
Environmental Adaptability  
The system is designed to operate effectively in diverse conditions, including rain, fog, and low-light scenarios, by leveraging sensor fusion techniques.  
  
Driver Override  
The driver retains full control and can override the ACC system at any time via braking, acceleration, or steering inputs.  
  
Scalability  
ACC can be integrated with other advanced systems, such as lane-keeping assist (LKA) and autonomous emergency braking (AEB), to provide a comprehensive driver assistance package.  
  
Operational Scenarios  
  
Highway Driving: ACC maintains a consistent cruising speed and adjusts for varying traffic flow.  
Stop-and-Go Traffic: The system handles frequent stops and starts, reducing driver fatigue in congested conditions.  
Curved Roads: Advanced algorithms and lane detection assist in maintaining safe distances even on winding roads.

Boundary: The system boundary includes the vehicle with ACC system, including driver inputs via HMI, the vehicle with all the sensors, the control units, the actuators and the vehicle including engine, brake, transmission, and the Human-Machine Interface (HMI). External entities are the environment, surrounding vehicles, road conditions, and external objects.

# Purpose

The purpose of this analysis is to identify potential safety hazards and unsafe control actions of the Adaptive Cruise Control (ACC) system to prevent accidents, ensuring passenger safety and system reliability and reduce driver fatigue.

# System Goals

* Maintain safe following distance from lead vehicles.
* Automate speed control to reduce driver fatigue.
* Ensure safe operation in diverse driving conditions.
* Provide a smooth and comfortable driving experience.
* Ensure that the driver retains full control of the vehicle.
* Prevent collisions with other vehicles or obstacles.

# Accidents

|  |  |
| --- | --- |
| id | description |
| A1 | Collision with a lead vehicle. |
| A2 | Collision with an obstacle on the road. |
| A3 | Loss of control of the vehicle |
| A4 | Injury to the driver or passengers. |

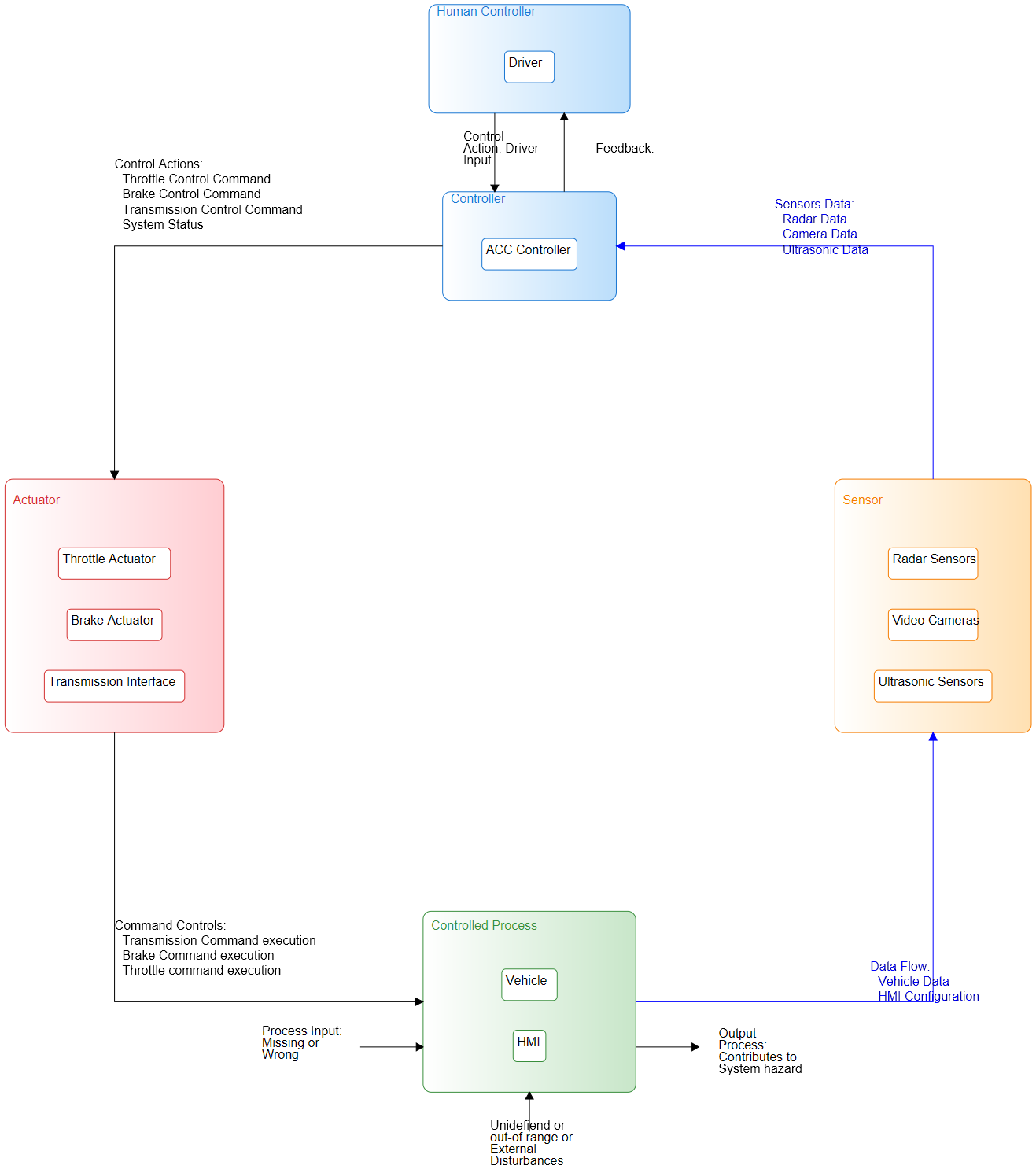
# Hazards

|  |  |  |
| --- | --- | --- |
| id | description | linked\_accidents |
| H1 | Vehicle following too closely behind the lead vehicle. | ['A1', 'A2', 'A4'] |
| H2 | Unintended acceleration or deceleration of the vehicle. | ['A1', 'A2', 'A3', 'A4'] |
| H3 | Failure to brake when needed, leading to collision. | ['A1', 'A2', 'A4'] |
| H4 | ACC system fails to detect a lead vehicle or an obstacle. | ['A1', 'A2', 'A4'] |
| H5 | System provides false information or warnings to the driver. | ['A4'] |

# System Constraints

|  |  |  |
| --- | --- | --- |
| id | description | linked\_Hazard |
| SC1 | If the vehicle gets too close to the lead vehicle, then the system must increase the distance between the vehicles by applying break or reducing the throttle [H1] | ['H1'] |
| SC2 | If unintended acceleration or deceleration is detected, the system must revert to normal operation and provide visual and audible warnings to the driver [H2] | ['H2'] |
| SC3 | If a collision is detected, the system must apply braking to prevent or mitigate the crash [H3] | ['H3'] |
| SC4 | If the ACC system fails to detect an object or lead vehicle, the system must revert to normal operation and provide visual and audible warnings to the driver [H4] | ['H4'] |
| SC5 | If the system provides false warnings or informations to the driver, the system must correct the error immediately and display a warning to the driver [H5] | ['H5'] |

# Control Structure



## Components

|  |  |
| --- | --- |
| name | type |
| Driver | Human Controller |
| ACC Controller | Controller |
| Radar Sensors | Sensor |
| Video Cameras | Sensor |
| Ultrasonic Sensors | Sensor |
| Throttle Actuator | Actuator |
| Brake Actuator | Actuator |
| Transmission Interface | Actuator |
| Vehicle | Controlled Process |
| HMI | Controlled Process |

## Connections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| label | source | target | description | connection\_type |
| Driver Inputs | Driver | ACC Controller | The driver inputs the desired speed and following distance and system status monitoring to the ACC controller through HMI |  |
| Radar Data | Radar Sensors | ACC Controller | Radar sensors send data on distance, speed of lead vehicles to ACC controller |  |
| Camera Data | Video Cameras | ACC Controller | Video Cameras send data on lane markings, objects and road conditions to ACC Controller |  |
| Ultrasonic Data | Ultrasonic Sensors | ACC Controller | Ultrasonic sensors send data on nearby objects and distance to ACC Controller |  |
| Throttle Control | ACC Controller | Throttle Actuator | ACC Controller sends control command to the throttle actuator to adjust the engine power |  |
| Brake Control | ACC Controller | Brake Actuator | ACC Controller sends control command to the brake actuator to apply braking force |  |
| Transmission Control | ACC Controller | Transmission Interface | ACC Controller sends command to the Transmission interface to adjust the gear. |  |
| Throttle Command | Throttle Actuator | Vehicle | Throttle Actuator adjust the engine power of the vehicle |  |
| Brake Command | Brake Actuator | Vehicle | Brake Actuator applies brake force to the vehicle |  |
| Transmission Command | Transmission Interface | Vehicle | Transmission interface adjusts the gear of the vehicle. |  |
| Vehicle data for radar | Vehicle | Radar Sensors | Vehicle provides speed and position data to the radar sensors |  |
| Vehicle data for Camera | Vehicle | Video Cameras | Vehicle provides data on lane markings and road condition to the video cameras. |  |
| Vehicle data for Ultrasonic | Vehicle | Ultrasonic Sensors | Vehicle provides data on nearby objects to the Ultrasonic sensors |  |
| Vehicle data to HMI | Vehicle | HMI | Vehicle system provides current speed and system status to the HMI |  |
| HMI Configuration | HMI | Driver | HMI provides system status, and warning messages 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* | *Throttle Control* | UCA1: ACC controller does not provide the command to the throttle actuator to accelerate the vehicle when the lead vehicle moves away and a safe distance needs to be maintained, causing the vehicle to maintain its current speed and become too close to the lead vehicle or slow down below the set speed. | UCA2: ACC controller incorrectly provides throttle command when there is no lead vehicle or when the lead vehicle is slowing down leading to a hazard of unwanted acceleration. This causes the vehicle to accelerate at an unsafe time, potentially causing a collision or loss of control. | UCA3: ACC controller provides the throttle command to accelerate too late when the lead vehicle has already started moving, resulting in the following vehicle not maintaining a safe distance and potentially colliding with the lead vehicle. | UCA4: ACC controller stops providing the command to the throttle actuator too soon before achieving the target speed, leading to the system driving at lower speed or stopping when it was not intended |
| *UCA1: ['H1', 'H2', 'H4']* | *UCA2: ['H1', 'H2']* | *UCA3: ['H1', 'H2', 'H3']* | *UCA4: ['H1', 'H2']* |
| *2* | *Brake Control* | UCA5: ACC controller does not provide the command to the brake actuator to decelerate or stop the vehicle when the lead vehicle decelerates or stops or when an object is detected on the road, resulting in the following vehicle crashing into the lead vehicle or the object. | UCA6: ACC controller provides the command to the brake actuator to decelerate or stop the vehicle incorrectly (when there is no obstruction) resulting in a sudden deceleration and causing a rear-end collision. | UCA7: ACC controller provides the command to the brake actuator too late after the lead vehicle has already started decelerating resulting in insufficient brake force being applied to the vehicle, leading to a collision with the lead vehicle. | UCA8: ACC controller stops providing command to the brake actuator too early, before achieving a safe stopping distance or desired speed, leading to a rear-end collision with the lead vehicle or object or overshooting the desired speed, also applies brake for too long when it should be releasing the brake which will lead to unnecessary deceleration or total stop of the vehicle. |
| *UCA5: ['H1', 'H2', 'H3', 'H4']* | *UCA6: ['H1', 'H2', 'H3']* | *UCA7: ['H1', 'H2', 'H3']* | *UCA8: ['H1', 'H2', 'H3']* |
| *3* | *Transmission Control* | UCA9: ACC controller does not provide the necessary command to the transmission interface to change gears during acceleration or deceleration, resulting in the vehicle not accelerating or decelerating smoothly, making it unstable, and potentially unsafe. | UCA10: ACC controller incorrectly provides the command to the transmission interface to change gear, resulting in the wrong gear being selected and the vehicle becoming unstable during acceleration or deceleration, thus leading to an unsafe situation. | UCA11: ACC controller provides the command to change gears too early or too late leading to an unstable condition in the vehicle and potential loss of control. | UCA12: ACC controller stops providing the command to the transmission interface too early or too late, resulting in the wrong gear for the situation and the vehicle not accelerating or decelerating as needed, leading to the car being unsafe. |
| *UCA9: ['H2', 'H3', 'H4']* | *UCA10: ['H2', 'H3', 'H4']* | *UCA11: ['H2', 'H3', 'H4']* | *UCA12: ['H2', 'H3', 'H4']* |

# Controller Constraints

|  |  |  |
| --- | --- | --- |
| id | controller constrain | Linked Unsafe control\_action |
| C1 | ACC controller must provide the command to the throttle actuator to accelerate the vehicle when the lead vehicle moves away and a safe distance needs to be maintained | ['UCA1'] |
| C2 | ACC controller must not provide throttle command when there is no lead vehicle or when the lead vehicle is slowing down. | ['UCA2'] |
| C3 | ACC controller must provide the throttle command to accelerate in time when the lead vehicle has already started moving to maintain a safe distance | ['UCA3'] |
| C4 | ACC controller must not stop providing the command to the throttle actuator before achieving the target speed | ['UCA4'] |
| C5 | ACC controller must provide the command to the brake actuator to decelerate or stop the vehicle when the lead vehicle decelerates or stops or when an object is detected on the road. | ['UCA5'] |
| C6 | ACC controller must not provide the command to the brake actuator to decelerate or stop the vehicle incorrectly (when there is no obstruction). | ['UCA6'] |
| C7 | ACC controller must provide the command to the brake actuator at the right time (not too late or early) after the lead vehicle has already started decelerating so that sufficient brake force is applied to the vehicle. | ['UCA7'] |
| C8 | ACC controller must not stop providing command to the brake actuator too early or applying the brake for too long which can result in a collision or overshooting the desired speed and must not apply brake for too long when it should be releasing the brake | ['UCA8'] |
| C9 | ACC controller must provide the necessary command to the transmission interface to change gears during acceleration or deceleration, to ensure smooth operation. | ['UCA9'] |
| C10 | ACC controller must not incorrectly provide the command to the transmission interface to change gear. | ['UCA10'] |
| C11 | ACC controller must not provide command to change gear too early or too late. | ['UCA11'] |
| C12 | ACC controller must not stop providing the command to the transmission interface too early or too late. | ['UCA12'] |

# Loss Scenarios

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| id | uca | Linked Unsafe control\_action | type | scenario |
| L\_S\_1 | Throttle Control | ['UCA1'] | Controller Failure | ACC controller fails to detect the lead vehicle's movement or the need for increased speed due to internal software malfunction, preventing the throttle command from being sent, causing the vehicle to maintain its current speed or slow down, becoming too close to the lead vehicle and potentially resulting in a collision. |
| L\_S\_2 | Throttle Control | ['UCA2'] | Sensor Malfunction | Radar sensors or video cameras malfunction or provide inaccurate data about the environment leading the ACC controller to incorrectly provide command for unwanted acceleration, causing an unsafe condition that might lead to a collision or loss of control. |
| L\_S\_3 | Throttle Control | ['UCA3'] | Control Algorithm Flaw | The control algorithm fails to process the sensor data correctly or provides delay in its calculation, causing the controller to respond too late by providing the throttle command to accelerate, causing unsafe following distance and increasing the risk of an accident. |
| L\_S\_4 | Throttle Control | ['UCA4'] | Process Model Inaccuracy | The ACC controller has an incorrect process model regarding the required acceleration time and cuts off the throttle command too soon, before the desired speed is attained, thus leading to a unsafe condition such as the vehicle driving at an unsafe lower speed, or stopping unexpectedly which can lead to a collision. |
| L\_S\_5 | Brake Control | ['UCA5'] | Controller Failure | ACC controller fails to calculate the required braking force or fails to send the brake command due to an internal hardware or software malfunction, resulting in a collision with the lead vehicle or object because the vehicle does not decelerate or stop. |
| L\_S\_6 | Brake Control | ['UCA6'] | Inadequate Control Algorithm | The ACC controller misinterprets sensor data and applies brakes incorrectly when there is no obstruction or any need for deceleration, thus leading to a sudden deceleration and causing a rear-end collision. |
| L\_S\_7 | Brake Control | ['UCA7'] | Process Model Inaccuracy | The ACC controller has inaccurate information about the lead vehicle's speed or deceleration rate and provides the brake command too late after the lead vehicle has already started decelerating leading to the vehicle not braking in time and colliding with the lead vehicle. |
| L\_S\_8 | Brake Control | ['UCA8'] | Controller Failure | ACC controller malfunctions and stops providing brake command too early, before achieving a safe distance or desired speed, leading to a rear-end collision or overshooting, or also if it applies the brake for too long thus leading to unnecessary and unwanted deceleration or stopping. |
| L\_S\_9 | Transmission Control | ['UCA9'] | Actuator Failure | Transmission interface failure during acceleration or deceleration, causing the ACC controller command to not be executed and the vehicle not changing gears as it should, resulting in the vehicle not accelerating or decelerating smoothly and thus becoming unstable, and unsafe. |
| L\_S\_10 | Transmission Control | ['UCA10'] | Process Model Inaccuracy | The ACC controller misinterprets the current gear required and transmits the wrong command to the transmission interface leading to an unsafe gear and thus affecting the vehicle's stability during acceleration or deceleration. |
| L\_S\_11 | Transmission Control | ['UCA11'] | Control Input Flaw | The ACC controller provides the wrong command to the transmission due to data corruption causing the transmission gear to be changed at the wrong time which leads to unstable driving conditions |
| L\_S\_12 | Transmission Control | ['UCA12'] | Actuator Failure | The ACC controller incorrectly stops providing the command to the transmission interface too early or too late due to an internal software or hardware malfunction, leading to the vehicle being in the wrong gear for the situation and not accelerating or decelerating as needed, making it unsafe. |

# Safety Constraints

|  |  |  |
| --- | --- | --- |
| id | Safety constraint | Linked\_loss\_scenarios |
| S\_C\_1 | The ACC system must have redundancy in place so that if controller is failed or faulty, the system safely transitions to minimal risk condition or to manual operation, to avoid any accidents | ['L\_S\_1', 'L\_S\_5', 'L\_S\_8', 'L\_S\_12'] |
| S\_C\_2 | The system must ensure that any sensor malfunciton will not impact the performance of the ACC system or it will transition safely, using other redundant sensors or to manual operation by alerting the driver. | ['L\_S\_2'] |
| S\_C\_3 | The control algorithm for the controller must be validated and verified to be safe under any normal driving conditions. | ['L\_S\_3', 'L\_S\_6'] |
| S\_C\_4 | The process models used by the controllers must be accurate and reliable to prevent unsafe conditions due to inaccurate models and also data validation must be performed. | ['L\_S\_4', 'L\_S\_7', 'L\_S\_10'] |
| S\_C\_5 | The system must be designed to fail safely such that if the ACC fails, the car is brought to a safe stop. | ['L\_S\_9'] |
| S\_C\_6 | Control input from other sources to the controller must be validated and the system must prioritize safety critical data to avoid unsafe control command | ['L\_S\_11'] |