# Model-Based Software Design, A.Y. 2024/25

# Assignment #1

## Components of the working group (max 2 people)

* Federico Bena, 328197
* Michele Lauriola, 332679

Item definition (Example)

One pedal controller

# Purpose of this document

The purpose of this document is to be the input for the “Hazard Analysis and Risk Assessment” (HARA) needed to comply with the ISO26262 standard. To ensure safety, all activities of the safety life cycle have to be planned to avoid systematic failures.

Therefore, this document describes the assumption on the one pedal acceleration/braking system item you should develop.

An additional purpose of this document is to define and describe the item, its functionality, dependencies on, and interaction with, the driver, the environmental conditions, external measure, the boundary of the item and interfaces to other items as well as assumptions concerning other elements at the vehicle level. This document will handle the requirements and recommendations for establishing the definition of the item, including its functionality, interfaces, environmental conditions, legal requirements, and known hazards.

# Purpose of the item

*Please describe in this chapter the purpose of the item. Consider laws, standards, and regulations to sufficiently describe the item's purpose.*

The purpose of the item is the following:

* To allow the driver to set the torque (positive🡪acceleration, negative🡪 braking) applied on the driving wheels of a car. This system enables the driver to use only the throttle pedal for both the functions of accelerating or braking (up to a certain level) the vehicle. This system only allows use of the regenerative braking function of an electric/hybrid vehicle.
* As an assumption, the braking pedal is still inside the car, it acts directly on the hydraulic braking system, and its circuitry is independent of interferences from the “one” throttle/braking pedal. The information on whether the brake pedal is pressed is available for the considered item.

## Functional behavior

The automatic transmission selector is implemented as a by-wire (hence, no mechanical links between the transmission and the selector are present) and features, in the order, these positions: P (park), R (reverse), N (neutral), D (drive), and B (braking/one pedal). The driver can move the transmission selector at any moment, so the actually selected mode is shown on the dashboard screen. The item switches to the position chosen by the driver as soon as all related safety conditions are met.

The system can adopt two different behaviours, one when the automatic transmission selector (an independent system) is in the D position and the other in the B.

In particular:

* In D position mode, it reads the position of the throttle pedal and requires a traction torque proportional to the pedal position, as traditional in the automotive market. When the pedal is completely released, no torque is required meaning that the vehicle has its own braking force due to interaction with the air or the terrain, the internal combustion engine, or just the transmission power consumption due to internal frictions in the case of an electric vehicle. In this mode, to increase the braking torque, it is necessary to press the brake pedal and stop the vehicle completely. When the brake pedal is released in cars equipped with automatic transmissions, the vehicle starts to move slowly.
* In B (brake) position mode, the throttle pedal travel is divided into two regions:
  + regenerative braking, from the complete release up to a certain point (for example, 1/3 of the travel angle) that we can call the *neutral point*. The readout from the pedal inside this region is interpreted as a request for a braking torque, maximum when the pedal is completely released, then proportionally decreased upon the *neutral point*. When the pedal is released, the vehicle brakes up to completely stop its motion. From then on, the car remains stopped automatically regardless of the street slope. To make the vehicle moving, it is necessary to press the throttle pedal up to the acceleration region, described in the following, or to press the brake pedal and then release it.
  + Acceleration, from the neutral point up to the end of the travel (acceleration region), where the position is interpreted as a request of a traction torque proportional to the pedal position.

The behaviour can be described mathematically as follows:

where:

* is the requested torque;
* is the pedal position expressed in normalized range;
* is the maximum acceleration torque in the forward direction.

The requested torque is positive to indicate a forward acceleration action or negative to indicate a braking (or backward) acceleration action (from here, the – sign in the equation 1).

Of course, it is still possible to use the braking pedal in case of emergencies or to increase the braking torque thanks to the hydraulic brakes.

|  |  |
| --- | --- |
| Function | Operating elements |
| Determine torque request | Throttle pedal |
| Select transmission mode (behavior) | Automatic transmission selector |
| Brake pedal pressed | Data from the CAN bus regarding the status of the braking pedal |
| Driver notifications | Tell the driver the selected mode on the dashboard (between P, R, N, D, and B) and eventual faults. This is usually the one chosen by the by-wire selector |

# Functional block diagram

*Please describe the interaction with external systems or items and/or interfaces to other elements outside the boundary of your item. Please consider the combination of “sensor-logic-actuator” and choose functional names for these elements regarding your item.*



# Boundaries of the system responsibility and interfaces

*Please describe the boundary of the system responsibility, interaction with external systems or items and interfaces to other elements outside your item in combination with the block diagram above*

The system is in charge of providing the torque request (positive or negative) to the electric motor (EM) electronic control unit (ECU).

It provides this request through the vehicular Controller Area Network (CAN).

It has to compute this torque request based on the gear selector position (negative torque only for the B position).

Moreover, it has to check the vehicle speed to determine the torque effects, in particular preventing that, during the regenerative braking, the negative torque request causes the vehicle to move in the reverse direction.

Another responsibility is to keep the vehicle stopped until the throttle pedal reaches the acceleration position and to monitor when the braking pedal is pressed to make the car slowly move when it is released.

In the reverse gear, the car acts like a standard automatic transmission car, so the vehicle only stops when the braking pedal is pressed and starts to slowly move backward when it is released.

Moreover, the transition between the position N and R or D/B is accepted only when the speed of the vehicle is lower than 5 km/h (in the same motion direction) AND the brake pedal is pressed, with the only exception on the selection of the N (neutral), which can be accepted at any time and causes the vehicle to move freewheel. The transition between R and P can be accepted only with the car almost still, and the braking pedal pressed.

# Other sources of hazards, which influence the safety and reliability of the item

*Please describe other sources (not E/E) of hazards, which influence the safety and reliability of the item*

None.

# Functional requirements

*Please describe all already noted functional safety requirements, this is normally output of H&R.*

The item must determine the right torque request, that the driver is asking, considering:

* The current driving mode for the automatic transmission selector.
* The current throttle pedal position.
* The actual speed of the vehicle.

# Other requirements

*Other environmental requirements which can influence your item.*

None.

# Law, directive and standard

*List the laws, directives and standard which have to be considered*

None.

# External measure to minimizing risks

*Which external measures can be taken in order to minimize the risk:*

* The driver is required by law to have a driver license.
* The driver should always check the driving mode on the dashboard.
* The driver should always verify that the braking mode B is working properly while at low speeds.
* The driver should always rely also on the braking pedal.
* Periodic service of the car as prescribed by the manufacturer.

Hazard Analysis and Risk Assessment (Example)

One pedal controller

# Participants

|  |  |  |
| --- | --- | --- |
| **Name, department** | **Qualification** | **Experience** |
| Federico Bena, 328197 |  |  |
| Michele Lauriola, 332679 |  |  |

# Analyzes of Hazardous Situations

|  |  |
| --- | --- |
| H1 | Unintended vehicle acceleration |
| H2 | Unintended vehicle deceleration |
| H3 | Insufficient vehicle acceleration |
| H4 | Insufficient vehicle deceleration |
| H5 | Unintended vehicle motion in incorrect direction |
| H6 | Wrong system mode displayed |

## H1 Unintended vehicle acceleration: Computation of a higher positive torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the acceleration region, caused by reading a higher than actual position value (the pedal is closer to the neutral point with respect to the reeded value).

## H2 Unintended vehicle deceleration: Computation of a higher negative torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the braking region, caused by reading a lower than actual position value (the pedal is closer to the neutral point with respect to the reeded value).

H3 Insufficient vehicle acceleration: Computation of a lower positive torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the acceleration region, caused by reading a lower than actual position value (the pedal is closer to the completely pressed position with respect to the reeded value).

## H4 Insufficient vehicle deceleration: Computation of a lower negative torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the braking region, caused by reading a higher than actual position value (the pedal is closer to the completely released position with respect to the reeded value).

## H5 Unintended vehicle motion in incorrect direction: Incorrect calculation of the microcontroller for the braking region in situations where the vehicle is stationary (vehicle starts moving backwards instead of forward) or is slowing down and the negative torque request reverses the direction of motion (the vehicle does not stop at zero speed but proceeds by reversing motion).

## H6 Wrong system mode displayed: The dashboard incorrectly displays the transmission mode potentially leading the driver to misinterpret the vehicle’s operational state. This could result in inappropriate use of the pedal, potentially causing accidents.

# Analyses of situations

## Definition of possible functional failures

|  |  |
| --- | --- |
| **Failure #** | **Description** |
| F1 | throttle pedal position misreading: wrongly read or not read at all. |
| F2 | Microcontroller failure: error in the computation of the requested torque. |
| F3 | Failure in communication. |

## Driving scenarios

*Describe the possible driving situations and define the status of the vehicle you want to consider*

### Description of the possible driving situations

DS1: City road

DS2: Highway road

DS3: Parking

### Definition of the vehicle status

VS1: Medium/high speed (>50 km/h)

VS2: Low speed (<50 km/h)

VS3: Stop

## Considerations

*Describe driving situations for each status of the vehicle*

|  |  |  |
| --- | --- | --- |
| **Operational Situations #** | **Driving situation** | **Vehicle status** |
| ~~S1~~ | ~~DS1: City road~~ | ~~VS1: Medium/high speed (>50 km/h)~~ |
| S2 | DS1: City road | VS2: Low speed (<50 km/h) |
| S3 | DS1: City road | VS3: Stop |
| S4 | DS2: Highway road | VS1: Medium/high speed (>50 km/h) |
| S5 | DS2: Highway road | VS2: Low speed (<50 km/h) |
| S6 | DS2: Highway road | VS3: Stop |
| ~~S7~~ | ~~DS3: Parking~~ | ~~VS1: Medium/high speed (>50 km/h)~~ |
| S8 | DS3: Parking | VS2: Low speed (<50 km/h) |
| S9 | DS3: Parking | VS3: Stop |

Scenarios S1 and S7 will not be considered in the estimation matrix because respectively city road driving and parking environments are unfeasible for medium/high speeds.

# Analysis

## Estimation matrix

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Operational Situations** | | | | | | | | | | |
| ~~S1~~ | S2 | S3 | S4 | S5 | S6 | ~~S7~~ | S8 | S9 | **Top event (worst case)** | **ASIL[[1]](#footnote-1)** |
| **Hazards** | H1 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 4  C: 1 | S: 2  E: 3  C: 2 | S: 3  E: 4  C: 2 | S: 2  E: 3  C: 2 | S: 2  E: 1  C: 2 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 3  C:1 | S: 1  E: 4  C: 1 | S: 3  E: 4  C: 2 | C |
| H2 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 4  C: 2 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 4  C: 2 | S: 2  E: 3  C: 2 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 3  C: 1 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 4  C: 2 | B |
| H3 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 4  C: 1 | S: 1  E: 3  C: 0 | S: 2  E: 4  C: 2 | S: 1  E: 3  C: 2 | S: 1  E: 1  C: 1 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 0  E: 3  C: 1 | S: 0  E: 4  C: 0 | S: 2  E: 4  C: 2 | B |
| H4 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 4  C: 1 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 3  E: 4  C: 2 | S: 2  E: 3  C: 1 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 3  C: 1 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 3  E: 4  C: 2 | C |
| H5 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 3  C: 2 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S: 2  E: 1  C: 3 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 4  C: 1 | S: 2  E: 3  C: 2 | A |
| H6 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 4  C: 1 | S: 1  E: 3  C: 1 | S: 2  E: 4  C: 2 | S: 1  E: 3  C: 1 | S: 2  E: 1  C: 2 | ~~S:~~  ~~E:~~  ~~C:~~ | S: 1  E: 3  C: 1 | S: 1  E: 4  C: 1 | S: 2  E: 4  C: 2 | B |

Color-coding is used for higher clarity: QM, ASIL A, ASIL B, ASIL C, ASIL D

Controllability was assigned values considering that in medium/high velocity vehicle status (S4) leads to a lower available time reaction for the driver with respect to a low velocity status. Moreover, Controllability for Hazards 1 and 4 was assigned a value of 1 or 2, depending on the vehicle status, but not 3 because it has been considered the driver capable of compensating for unintended acceleration or for the lack of braking with the brake pedal present in the vehicle.

## Operational Situations – Comment of entries

*Start with the description of what happens and then assign the parameters.*

Please analyse in this way two other scenario/failure associations at your choice.

H1/S4: Unintended acceleration while driving on highway at medium/high speed (>50 km/h)

|  |  |  |
| --- | --- | --- |
| *Effect* | The driver may lose the control of the vehicle, which may lead to collision with other vehicles or environment objects | |
| *Statement S* | High speed collision on highway may lead to fatal injuries | S3 |
| *Statement E* | Driving in highway at medium/high speed (over 10% of operating time) | E4 |
| *Statement C* | Normally controllable (despite low available time reaction, most drivers should be able to notice unexpected acceleration and compensate for it by braking) | C2 |

H2/S4: Unintended deceleration while driving on highway at medium/high speed (>50 km/h)

|  |  |  |
| --- | --- | --- |
| *Effect* | The vehicle may unexpectedly decelerate, causing a collision with vehicles following behind | |
| *Statement S* | Rear-end collision at high speed (assuming the car is not stationary) may lead to severe injuries | S2 |
| *Statement E* | Driving in highway at medium/high speed (over 10% of operating time) | E4 |
| *Statement C* | Normally controllable (most drivers should be able to regain control by further accelerating) | C2 |

H4/S4: Insufficient deceleration while driving on highway at medium/high speed (>50 km/h)

|  |  |  |
| --- | --- | --- |
| *Effect* | The driver may lose the control of the vehicle, which may lead to collision with other vehicles or environment objects | |
| *Statement S* | High speed collision on highway may lead to fatal injuries | S3 |
| *Statement E* | Driving in highway at medium/high speed (over 10% of operating time) | E4 |
| *Statement C* | Normally controllable (despite low available time reaction, most drivers should be able to notice insufficient braking and compensate for it with the brake pedal) | C2 |

H5/S3: Unintended motion in incorrect direction while being parked on a city park spot (ON)

|  |  |  |
| --- | --- | --- |
| *Effect* | The vehicle starts backwards, instead of forwards, with the possibility of causing collisions or accidents with vehicles or people behind the vehicle. | |
| *Statement S* | A sudden accident with a person behind the vehicle can cause severe injuries | S2 |
| *Statement E* | Parking in a city (10% of operational time) | E3 |
| *Statement C* | Normally controllable (despite low available time reaction, most drivers should be able to notice a motion in undesired direction trying braking) | C2 |

# Safety goals

|  |  |
| --- | --- |
| SG1 | The item shall compute correctly the torque (both positive and negative) requested by the driver while the transmission mode is B, shall monitor that the transmission mode displayed is the correct one and shall transit to safe state. |
| SG2 | The item shall monitor that the transmission mode displayed is the correct one and shall transit to safe state. |
| SG3 | The item shall transit to safe state. |

## Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Failure/**  **Malfunction/**  **Hazardous situation** | **Safety goal** | **ASIL-level** | **Safe state** | **Fault tolerance time interval (FTTI)** |
| H5 | SG3 | A | Transit in transmission mode D and alert the driver through notification on the dashboard of the presence of malfunctioning. | < 500 ms |
| H2, H3, H6 | SG2 | B | Transit in transmission mode D and alert the driver through notification on the dashboard of the presence of malfunctioning. | < 300 ms |
| H1, H4 | SG1 | C | Transit in transmission mode D and alert the driver through notification on the dashboard of the presence of malfunctioning. | < 100 ms |

Hazard 6 (wrong mode displayed on the dashboard) has been considered separately since it is due to a different failure mode but its consequences are reflected into the other hazards.

## Relevant failure modes for H1

**Unintended vehicle acceleration**: Computation of a higher positive torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the acceleration region.

## Relevant failure modes for H2

**Unintended vehicle deceleration**: computation of a higher negative torque than the requested one due to malfunction of the microcontroller or due to a wrong lecture of the throttle pedal position in the braking region.

## Relevant failure modes for H5

**Unintended vehicle motion in incorrect direction**: incorrect computation of the microcontroller for the braking region in situations where the vehicle is stationary (vehicle starts moving backwards instead of forward) or is slowing down and the negative torque request reverses the direction of motion (the vehicle does not stop at zero speed but proceeds by reversing motion).

1. Remember that the ASILs are assigned to the Safety Goals and not to failures. These ASILs are reported in the table just for the reader convenience. [↑](#footnote-ref-1)