# Model-Based Software Design, A.Y. 2023/24

# Laboratory 1 Report

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

* Luca Pili s331500
* Riccardo Solazzo s331337

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*

# Functional requirements

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

# Other requirements

*Other environmental requirements which can influence your item*

# Law, directive and standard

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

# External measure to minimizing risks

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

Hazard Analysis and Risk Assessment (Example)

One pedal controller

# Participants

|  |  |  |
| --- | --- | --- |
| **Name, department** | **Qualification** | **Experience** |
| LUCA PILI |  |  |
| RICCARDO SOLAZZO |  |  |
|  |  |  |

# Analyzes of Hazards

|  |  |
| --- | --- |
| H1 | Unintended vehicle acceleration |
| H2 | Unintended vehicle braking |
| H3 | Insufficient vehicle acceleration |
| H4 | Insufficient vehicle braking |
| H5 | Unintended vehicle motion in incorrect direction |

## H1 Unintended acceleration generates an unexpected situation, to which the driver may not be ready to react.

## H2 Unintended braking generates an unexpected situation, to which the driver may not be ready to react.

## H3 The acceleration provided is not sufficient to satisfy vehicle request.

## H4 The braking provided is not sufficient to satisfy vehicle request.

## H5 Unintended motion in incorrect direction generates an unexpected situation, to which the driver may not be ready to react.

# Analyses of situations

## Definition of possible functional failures

*Functional failures are misbehavior of the considered item that can expose people inside or surrounding the vehicle to hazards.*

|  |  |
| --- | --- |
| **Failure #** | **Description** |
| F1 | The microprocessor fails in executing instructions |
| F2 | The CAN network fails |
| F3 | No pedal position measurements (unresponsive sensor) |
| F4 | Wrong pedal position measurement: the actual value of p is higher than what measured |
| F5 | Wrong pedal position measurement: the actual value of p is less than what measured |

## Driving scenarios

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

### Description of the possible driving situations

### Definition of the vehicle status

## Considerations

*Describe driving situations for each status of the vehicle*

|  |  |  |
| --- | --- | --- |
| **Scenario #** | **Driving situation** | **Vehicle status** |
| S1 | Acceleration request | Automatic transmission selector : B |
| S2 | Acceleration request | Automatic transmission selector : D |
| S3 | Braking request | Automatic transmission selector : B |
| S4 | Braking request | Automatic transmission selector : D |
| S5 | Reverse driving | Automatic transmission selector : R |
| S6 | Parked | Automatic transmission selector : P |

# Analysis

## Estimation matrix

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Scenarios** | | | | | | | | | | |
| S1 | S2 | S3 | S4 | S5 | S6 |  |  |  | **Top event (worst case)** | **ASIL[[1]](#footnote-1)** |
| **Hazards** | H1 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S:3  E:2  C:3 | ~~S:~~  ~~E:~~  ~~C:~~ | S:3  E:1  C:2 | ~~S:~~  ~~E:~~  ~~C:~~ |  |  |  | S: 3  E: 2  C: 3 | B |
| H2 | S:3  E:2  C:3 | ~~S:~~  ~~E:~~  ~~C:~~ | S:3  E:2  C:2 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ |  |  |  | S: 3  E: 2  C: 3 | B |
| H3 | S:1  E:2  C:1 | S:1  E:2  C:1 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S:1  E:2  C:1 | ~~S:~~  ~~E:~~  ~~C:~~ |  |  |  | S: 1  E: 2  C: 1 | QM |
|  | H4 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | S:3  E:2  C:3 | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ | ~~S:~~  ~~E:~~  ~~C:~~ |  |  |  | S: 3  E: 2  C: 3 | B |
|  | H5 | S:3  E:1  C:2 | S:3  E:1 C:2 | S:3  E:1  C:2 | ~~S:~~  ~~E:~~  ~~C:~~ | S:3  E:1  C:2 | ~~S:~~  ~~E:~~  ~~C:~~ |  |  |  | S: 3  E: 1  C: 2 | QM |

## Scenarios – Comment of entries

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

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

S3: Braking request, automatic transmission selector : B

F5: Wrong pedal position measurement: the actual value of p is less than what measured

|  |  |  |
| --- | --- | --- |
| *Effect* | (H1) Possible unintended vehicle acceleration | |
| *Statement S* | Possible life threatening injuries due to collision with other vehicles or pedestrians. | *S:3* |
| *Statement E* | not more than 1% of operating time | *E:2* |
| *Statement C* | Less than 90% of drivers and other participants can avoid harm | *C:3* |

S1: Acceleration request, automatic transmission selector : B

F1: The microprocessor fails in executing instructions

|  |  |  |
| --- | --- | --- |
| *Effect* | (H3) Insufficient vehicle acceleration | |
| *Statement S* | The vehicle does not accelerate as expected, this does not cause serious harm to the driver or other people. | S:1 |
| *Statement E* | not more than 1% of operating time | E:2 |
| *Statement C* | 99% or more drivers and other participants can avoid harm | C:1 |

# Safety goals

|  |  |
| --- | --- |
| SG1 | The item must warn the driver in case of malfunction |
| SG2 | The item shall provide the correct reference torque signal |
| SG3 | in case the item is not able to provide the correct reference torque signal it shall transit to the safe state |

## Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hazards** | **Safety goal** | **ASIL-level** | **Safe state** | **Fault tolerance time interval (FTTI)** |
| H1 | SG1/SG2/SG3 | B | Driver must be informed properly and the item shall be disabled | 100ms |
| H2 | SG1/SG2/SG3 | B | Driver must be informed properly and the item shall be disabled | 100ms |
| H3 | SG1/SG2/SG3 | QM | Driver must be informed properly | 100ms |
| H4 | SG1/SG2/SG3 | B | Driver must be informed properly and the item shall be disabled | 100ms |
| H5 | SG1/SG2/SG3 | QM | Driver must be informed properly | 100ms |

*Choose two hazards to be analyzed more in details.*

## Relevant functional failures for H3

FM1: The microprocessor fails in executing instructions

FM2: The CAN network fails

FM3: No pedal position measurements (unresponsive sensor)

## Relevant functional failures for H1

FM1: Wrong pedal position measurement: the actual value of p is less than what measured.

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)