Model-Based Software Design, A.Y. 2022/23

Laboratory 1 Report

Components of the working group (max 2 people)

- Simone Bergadano, S303053
- Pietro Vignini, S317465

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:

$$\begin{cases} \tau_r = -\max(\tau_a) \cdot (1 - 3p), & \text{when } 0 < p \leq \frac{1}{3} \text{ (braking region).} \quad (1) \\ \tau_r = \max(\tau_a) \cdot \frac{3}{2} \cdot \left(p - \frac{1}{3} \right), & \text{when } \frac{1}{3} < p \leq 1 \text{ (acceleration region).} \quad (2) \end{cases}$$

where:

- τ_r is the requested torque;
- p is the pedal position expressed in normalized $[0,1]$ range;
- $\max(\tau_a)$ is the maximum acceleration torque in the forward direction.

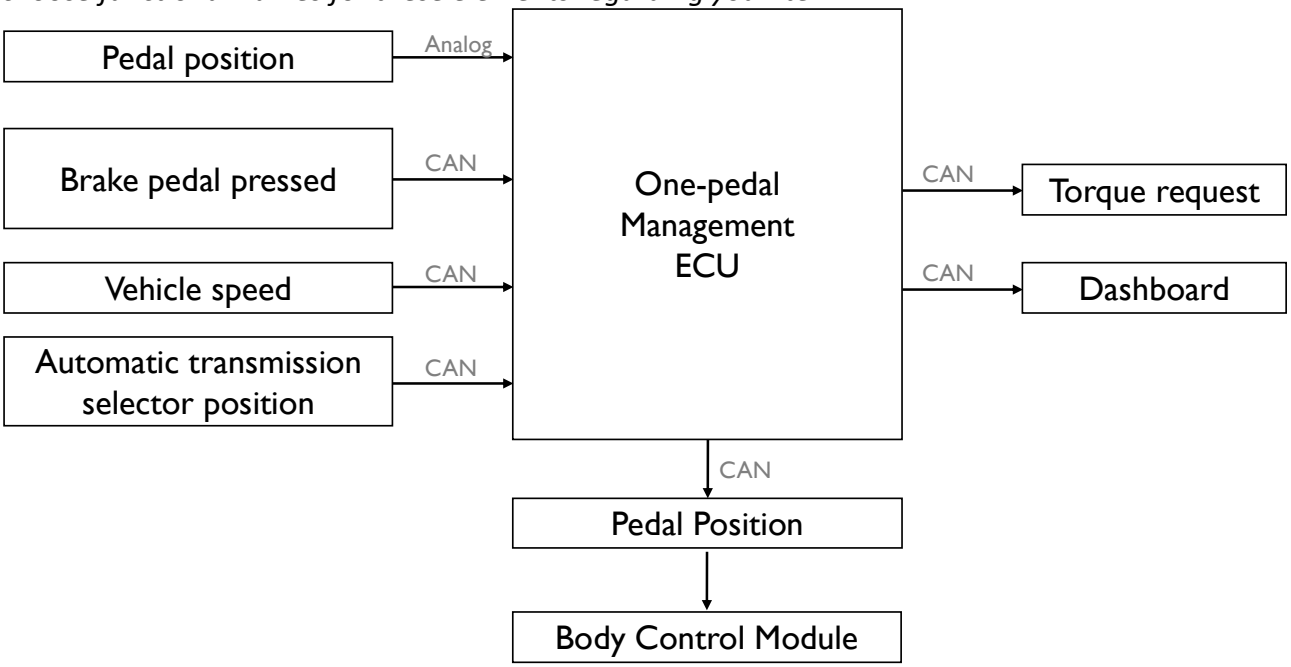
The requested torque is positive to indicate a forward acceleration action or negative to indicate a braking (or backward) acceleration action (from here, the – sign in the equation 1).

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

- The pedal mechanism no longer works properly.
- Pedal breakage (accidental or from tampering).
- Something prevents pedal movement.

Functional requirements

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

The item has to provide the torque request to the electric motor ECU considering:

- The automatic transmission selector position
- The vehicle's speed
- If the breaking pedal is pressed

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

External measure to minimizing risks

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

- Periodic check of the pedal as prescribed by the manufacturer.
- The vehicle operator is required by law to be properly trained and to obtain a driver's license, so they verifies, before start driving, that the pedal is working properly.

Hazard Analysis and Risk Assessment

One pedal controller

Participants

Name, department	Qualification	Experience
Simone Bergadano	Student	
Pietro Vignini	Student	

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

An unintended acceleration can cause the driver to lose control of the vehicle, leave the road and collide with other vehicles, pedestrians, or environmental parts.

H2

Unintentional regenerative braking can be dangerous at high speeds, when cornering and during an overtake, as it can affect the vehicle dynamics.

H3

Insufficient vehicle acceleration can pose a hazard when overtaking and when crossing an intersection as it increases the time required to complete the maneuver.

H4

Insufficient regenerative braking can cause an increase in stopping distance or can cause the vehicle to move after it has reached a stop condition due to the slope of the road, thus posing a hazard.

H5

Unintended vehicle motion in incorrect direction can cause the driver to lose control of the vehicle, leave the road and collide with other vehicles, pedestrians, or environmental parts.

Analyses of situations

Definition of possible functional failures

Failure #	Description
F1	Wrong pedal position reading.
F2	No pedal position reading.
F3	Wrong reading of the automatic transmission selector position.
F4	Wrong brake pedal position reading.
F5	No brake pedal position reading.

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 Driving in D mode
- DS2 Driving in B mode
- DS3 Parked
- DS4 Driving in Reverse gear

Definition of the vehicle status

- VS1 Medium/high speed
- VS2 Low speed
- VS3 Stopped

Considerations

Describe driving situations for each status of the vehicle

Scenario #	Driving situation	Vehicle status
S1	Driving in D mode	Driving at medium/high speed
S2	Driving in D mode	Driving at low speed
S3	Driving in D mode	Stopped
S4	Driving in B mode	Driving at medium/high speed
S5	Driving in B mode	Driving at low speed
S6	Driving in B mode	Stopped
S7	Parked	Stopped
S8	Driving in Reverse gear	Driving at low speed
S9	Driving in Reverse gear	Stopped

Analysis

Estimation matrix

		Scenarios										
		S1 *D mode High/ Medium speed*	**S2** *D mode Low speed*	**S3** *D mode Stopped*	**S4** *B mode High/ Medium speed*	**S5** *B mode Low speed*	**S6** *B mode stopped*	**S7** *Parked*	**S8** *Reverse gear low speed*	**S9** *Reverse gear stopped*	**Top event (worst case)**	**ASIL**[1]
Hazard	**H1** *Unintended vehicle acceleration*	S: 3 E: 4 C: 3	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	S: 3 E: 4 C: 3	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	S: 3 E: 4 C: 3	ASIL-D
	H2 *Unintended vehicle braking*	S: 2 E: 4 C: 2	S: 1 E: 4 C: 1	N/A	S: 2 E: 4 C: 2	S: 1 E: 4 C: 1	N/A	N/A	S: 1 E: 4 C: 1	N/A	S: 2 E: 4 C: 2	ASIL-B
	H3 *Insufficient vehicle acceleration*	S: 1 E: 4 C: 2	S: 1 E: 4 C: 1	S: 0 E: 4 C: 0	S: 1 E: 4 C: 2	S: 1 E: 4 C: 1	S: 0 E: 4 C: 0	N/A	S: 1 E: 4 C: 1	S: 0 E: 4 C: 0	S: 1 E: 4 C: 2	ASIL-A
	H4 *Insufficient vehicle braking*	N/A	N/A	N/A	S: 1 E: 4 C: 2	S: 1 E: 4 C: 2	S: 2 E: 4 C: 2	N/A	N/A	N/A	S: 2 E: 4 C: 2	ASIL-B
	H5 *Unintended vehicle motion in incorrect direction*	N/A	N/A	S: 3 E: 4 C: 2	N/A	N/A	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	N/A	S: 3 E: 4 C: 2	S: 3 E: 4 C: 2	ASIL-C

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.

H1/S1

Effect	*Unintended acceleration when driving in D mode at high speed, resulting in an unpredictable behavior of the vehicle, with possible loss of control and crash occurrence.*	
Statement S	*Life-threatening injuries (survival uncertain) or fatal injuries*	*S3*
Statement E	*>10% of average operating time / Occurs during almost every drive on average*	*E4*
Statement C	*Less than 90% of the average drivers or other traffic participants are able to avoid harm*	*C3*

H4/S6

Effect	*Insufficient vehicle breaking when the car is stopped in B mode.*

[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.3

	It can cause the vehicle to move forward or backward according to the slope of the road, with possible loss of control and accident	
Statement S	*Severe and life-threatening injuries (survival probable due to the low speed of the accident)*	*S2*
Statement E	*>10% of average operating time / Occurs during almost every drive on average*	*E4*
Statement C	*Between 90% and 99% of the average drivers or other traffic participants are able to avoid harm*	*C2*

Safety goals

SG1	Prevent unwanted vehicle accelerations
SG2	Prevent misbehavior of regenerative braking
SG3	Guarantee the correct reading of the automatic transmission selector position
SG4	Warn the driver if the correct operation of the pedal cannot be guaranteed

Results

Failure/malfunction	**Safety goal**	**ASIL-level**	**Safe state**	**Fault tolerance time interval (FTTI)**
Unintended Acceleration (H1)	SG1	D	No further increase in the torque supplied to the motor is allowed	10 ms
Wrong regenerative breaking behavior (H2, H4)	SG2	B	Make driving mode B unavailable and notify the driver that the regenerative breaking is not working.	100 ms
Unintended vehicle motion in incorrect direction (H5)	SG3	C	The vehicle goes in park mode (P)	10 ms
Insufficient acceleration (H3)	SG4	A	The driver is notified by an alarm on the dashboard	1000 ms

Relevant failure modes for H1

Relevant failure modes for H2