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

Laboratory 1 Report

Components of the working group (max 2 people)

- Cihan Yurtsever, s296824
- Alessandro Cavalli, s301494

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:

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

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.

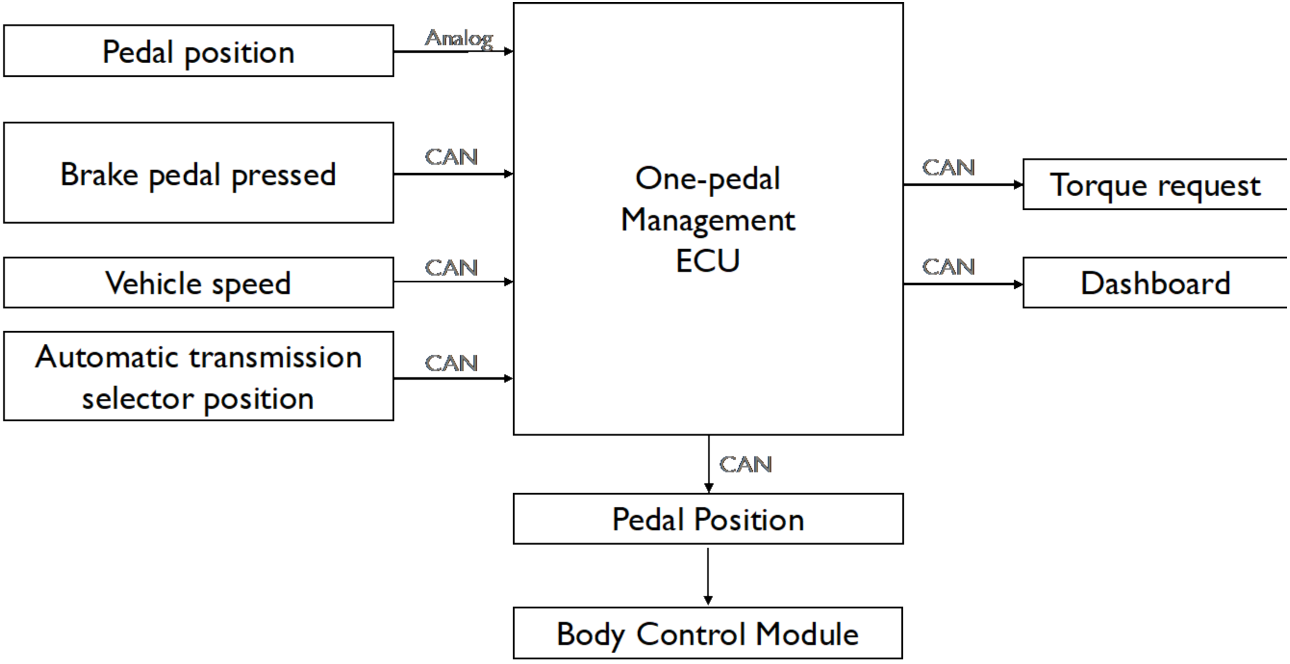
The requested torque is positive to indicate a forward acceleration action or negative to indicate a braking (or backward) acceleration action (from here, the – sign in the equation 1).

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

- Possible mechanical damages caused by external factors such as possible accidents or uneven road surfaces.
- Mechanical damages to the sensor pedal.
//- Driver error; which can be cause by wrong command on the vehicle that leads an accident.
- Out source effect; Electrical/Magnetic(external sources) power disturbance on the transmission selector mechanism.

Functional requirements

Please describe all already noted functional safety requirements, this is normally output of H&R.
The One Pedal controller allows the driver to set the torque(positive→acceleration, negative→ braking) applied on the driving wheels of a car by modifying the pedal position p.
In particular,

- The auto-trans-selector can be position on P, R, N, D, B mods.
- Driver should be able to change the transmission mod position only at very low speed.
- Driver should be informed from the dashboard screen of the currently enabled mode
- The torque request should be determined by the throttle pedal according the control law of the selected mode

- The Break pedal info should the provided through CAN bus

- Moreover the system should be adopted two different way;

When the Auto trans selector on the D position;
-reads the throttle pedal and
-requires a traction torque that is proportional to the pedal position.
-When there is no breaking force the car is equiped with the automatic transmission and starts to move slowly

When the auto-trans-select on the B mode
-reads the throttle pedal and
if the position is lower than 1/3 of the travel angle then request a regenerative braking torque proportional to that range
if the position is exactly 1/3 of the travel angle then do not apply any torque (neutral point)
if the position is strictly greater than 1/3 of the travel angle apply a forward torque proportional to that range

When the breaking is higher then
one when it is compressing in order o obtain the maximum possible stability.

Other requirements

We assume that the vehicle is working in not extreme conditions, so we will neglect external electromagnetic fields disturbances and issues due to thermal and humidity presence.

Law, directive and standard

ISO26262

External measure to minimizing risks

The vehicle operator is required by law to be properly trained and to obtain a driving license, he/she should verify, at the start of the engine, the absence of dashboard info about the position of the driving mode signaling a malfunction in the one pedal acceleration/braking system.

Hazard Analysis and Risk Assessment (Example)

One pedal controller

Participants

Name, department	Qualification	Experience
Cihan Yurtsever	Bachelor degree in Mechatronics Engineering	
Alessandro Cavalli	Bachelor degree in Informatics Engineering	

Analyzes of Hazards

H1	Unintended vehicle acceleration
H2	Unintended vehicle break
H3	Insufficient vehicle acceleration
H4	Insufficient vehicle break
H5	Unintended vehicle motion in incorrect direction

H1 This hazard potentially could cause the vehicle to speed up and a worsen handling, causing the driver to lose control of the vehicle, leave the road and collide with other vehicles, pedestrians, or environmental parts.

H2 This hazard potentially could cause the vehicle to slow down and stop handling, may stuck middle of the road and in instant occurrence of hazard may cause other drivers to crash on vehicle collide with other vehicles.

Exceptions and Boundary Conditions to H2:

This hazard does not apply in case of stopped vehicles.

H3 This hazard potentially could cause the vehicle to not speed up, causing the vehicle not behaving as expected and collide with other vehicles, pedestrians, or environmental parts.

H4 This hazard potentially could cause the vehicle to not stop properly, may cause, leave the road and collide with other vehicles, pedestrians, or environmental parts.

Exceptions and Boundary Conditions to H4:

This hazard does not apply in case of parked vehicles.

H5 This hazard potentially could cause the vehicle to not control causing the driver to not may cause, leave the road and collide with other vehicles, pedestrians, or environmental parts.

Analyses of situations

Definition of possible functional failures

Failure #	Description
F1	The ECU requests a positive torque when it should be non positive
F2	The ECU requests a negative torque when it should be non negative
F3	The produced torque is different in magnitude from the one requested by the ECU

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 city road
- DS2 Driving in a country road
- DS3 Driving in a highway

Definition of the vehicle status

VS1 Accelerating
VS2 Braking
VS3 Stopped

Considerations

Describe driving situations for each status of the vehicle

Scenario #	**Driving situation**	**Vehicle status**
S1	Driving in city road	Accelerating
S2	Driving in city road	Breaking
S3	Driving in city road	Stopped
S4	Driving in a country road	Accelerating
S5	Driving in a country road	Braking
S6	Driving in a country road	Stopped
S7	Driving in a highway	Accelerating
S8	Driving in a highway	Braking
S9	Driving in a highway	Stopped

Analysis

Estimation matrix

		Scenarios										
		S0	S2	S3	S4	S5	S6	S7	S8	~~S9~~	**Top event (worst case)**	**ASIL**[1]
Failures	H1	S:0 E:4 C:2	S:3 E:4 C:2	S:2 E:3 C:0	S:1 E:4 C:1	S:3 E:4 C:2	S:1 E:4 C:0	S:2 E:4 C:1	S:3 E:4 C:3	S: E: C:	S:3 E:4 C:3	D
	H2	S:3 E:4 C:2	S:1 E:4 C:0	S:0 E:3 C:0	S:3 E:4 C:2	S:1 E:4 C:1	S:0 E:3 C:0	S:3 E:4 C:2	S:1 E:4 C:1	S: E: C:	S:3 E:4 C:2	C
	H3	S:1 E:4 C:0	S:1 E:4 C:0	S:1 E:3 C:0	S:0 E:4 C:0	S:0 E:4 C:0	S:0 E:3 C:0	S:2 E:4 C:1	S:2 E:4 C:1	S: E: C:	S:2 E:4 C:1	A
	H4	S:2 E:4 C:1	S:1 E:4 C:0	S:0 E:3 C:0	S:2 E:4 C:0	S:1 E:4 C:0	S:0 E:3 C:0	S:2 E:4 C:2	S:1 E:4 C:1	S: E: C:	S:2 E:4 C:2	B
	H5	S:1 E:4 C:2	S:3 E:4 C:2	S:2 E:3 C:0	S:2 E:4 C:1	S:3 E:4 C:2	S:2 E:4 C:0	S:3 E:4 C:1	S:2 E:4 C:3	S: E: C:	S:3 E:4 C:3	D

[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.

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.

Effect	F3/S7: Accelerating in highway, the car starts to accelerate more than requested.	
Statement S	*In the highway the accelerating even more may be life threatening.*	*S:2*
Statement E	*In the highway, accelerating is highly probable.*	*E:4*
Statement C	*The accelerating on the vehicle that already accelerated is can simply controlable.*	*C:1*

Effect	*F3/S2: In the city, breaking even its not requested.*	
Statement S	*In the city breaking even its not requested would cause light and moderate injuries in the worst case.*	*S:1*
Statement E	*In the city, it is highly probable that vehicles break.*	*E:4*
Statement C	*The breaking in the city when already the car is breaking can be controllable in general.*	*C:0*

Safety goals

SG1	When the pedal position request is not consistent with ECU signal we should warn the driver to use the hydraulic breaking pedal and swap to neutral to avoid accelerating.
SG2	When pedal position is not in the breaking and CAN bus does not send signal and the vehicle is breaking then swap to neutral (safe state) and warn the user on the dashboard
SG3	When the pedal position request is not consistent with ECU signal we should warn the driver on the dashboard.

SG1: When the pedal position request is not consistent with the ECU signal, a warning must be produced, so that the user can use the hydraulic pedal, and the item should swap to neutral (all the previous safety goals are a reword of this concept)

Results

Failure/malfunction	Safety goal	ASIL-level	Safe state	Fault tolerance time interval (FTTI)
FM1: ECU increasing the torque regardless of pedal position.	SG1	D	Swapped to neutral position and using the hydraulic pedal.	1 s
FM2: ECU is decreasing the torque regardless of pedal position.	SG2	C	Swap to neutral	1s
FM3: ECU required torque magnitude is not consistent	SG3	B	Swap to the neutral position	1s

Relevant failure modes for H1

FM1: The ECU sends wrong signal to the electric motor that makes the vehicle perform break action in unexpected time.

Relevant failure modes for H2

FM2: The ECU sends wrong signal to the electric motor that makes the vehicle accelerate unintentionally.

Relevant failure modes for H3 and H4

FM3: The ECU sends inconsistent magnitude of the signal to the electric motor that makes the vehicle accelerate/break less then desired.