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

Assignment #1

Components of the working group (max 2 people)

- Amirhossein Ayanmanesh Motlaghmofrad, 323874

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.

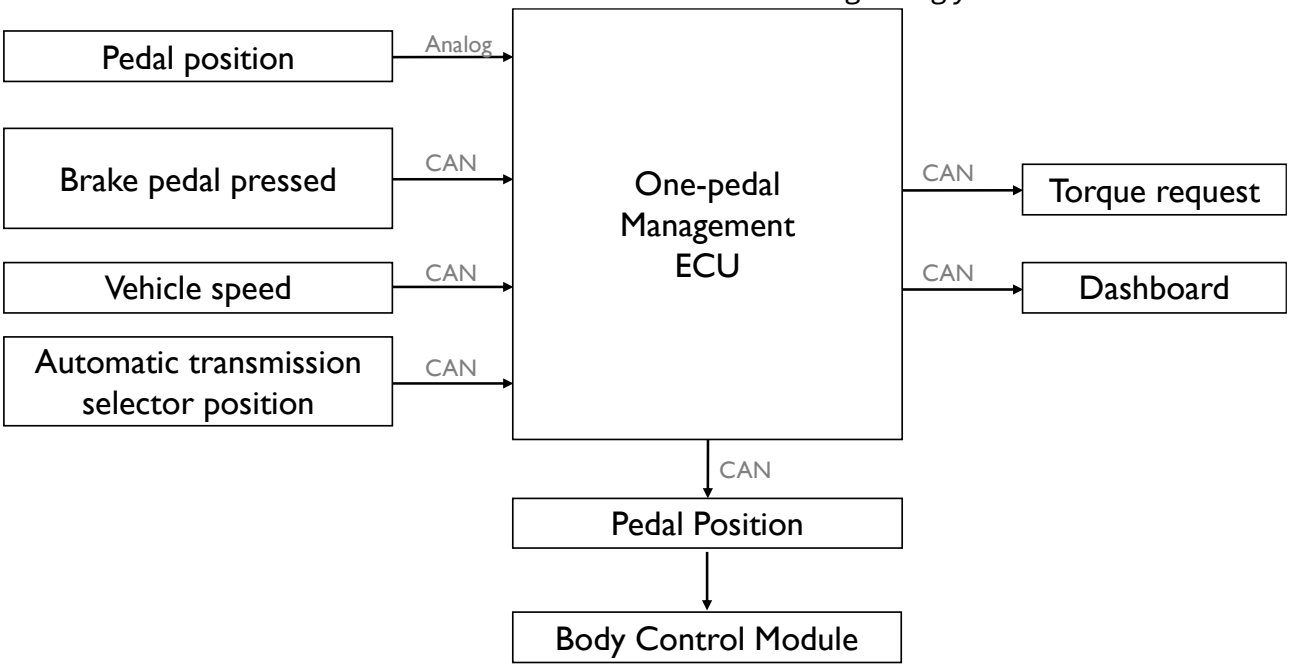
The requested torque is positive to indicate a forward acceleration action or negative to indicate a braking (or backward) acceleration action (from here, the – sign in the equation 1).

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

None

Functional requirements

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

Determine the torque to be requested according to the

- throttle pedal position
- the brake pedal information
- vehicle velocity
- the selected transmission mode

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:

A thorough explanation of the logic by which the state of transmission states changes.

Hazard Analysis and Risk Assessment (Example)

One pedal controller

Participants

Name, department	Qualification	Experience

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	Displayed transmission mode does not correspond to the selected one

H1

A higher positive torque is requested even if the position of the throttle pedal is kept fixed by the driver.

H2

A negative torque is requested even if the position of the throttle pedal is kept fixed by the driver, or while the pedal is in the 2/3 of its course in the B mode, resulting in an unintended deceleration.

H3

The torque requested is lower than the driver requested considering the course of throttle pedal.

H4

The negative torque requested by the module is lower than the one requested by the driver considering the position of the throttle pedal.

H5

The vehicle starts moving in the reverse direction, which means the velocity is low or the vehicle is stopped, and a negative torque is requested by the module, while it is not expected considering the transmission mode chosen by the driver.

H6

The mode represented on the instrument cluster does not correspond to the one used by the module to calculate the torque.

Analyses of situations

Definition of possible functional failures

Failure #	Description
F1	The throttle pedal does not send a correct analogue signal correspondent to the angle of the throttle pedal
F2	Microcontroller does not calculate the torque to be requested properly.
F3	Failure in communication

Driving scenarios

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

DS1: Driving
DS2: Stopped at a traffic light
DS3: Stopped in a parking lot

Description of the possible driving situations

Definition of the vehicle status

VS1: High speed
VS2: Low speed
VS3: Starts moving
VS4: A pedestrian is crossing the crossway.
VS5: Evasive maneuver

Considerations

Describe driving situations for each status of the vehicle

Operational Situations #	**Driving situation**	**Vehicle status**
S1	Driving (DS1)	High velocity (VS1)
S2	Driving (DS1)	Low velocity (VS2)
S3	Driving (DS1)	A person crossing the street (VS4)
S4	Driving (DS1)	Evasive maneuver (VS5)
S5	Stopped at a traffic light (DS2)	Starts moving (VS3)
S6	Stopped at a traffic light (DS2)	A person is crossing the street (VS4)
S7	Stopped in a parking lot (DS3)	Starts moving (VS3)
~~S8~~	~~Stopped in a parking lot (DS3)~~	~~A person is crossing the street~~
~~S9~~	~~Stopped in a parking lot (DS3)~~	~~Low velocity (VS2)~~
~~S10~~	~~Stopped in a parking lot (DS3)~~	~~High velocity (VS1)~~
~~S11~~	~~Stopped in a parking lot (DS3)~~	~~Evasive maneuver (VS5)~~
~~S12~~	~~Stopped at a traffic light (DS2)~~	~~Evasive maneuver (VS5)~~
~~S13~~	~~Stopped at a traffic light (DS2)~~	~~Low velocity (VS2)~~
~~S14~~	~~Stopped at a traffic light (DS2)~~	~~Higher velocity (VS1)~~
~~S15~~	~~Driving (DS1)~~	~~Starts moving (VS3)~~

Analysis

Estimation matrix

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

[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.

	H6	S:2 E:4 C:1	S:1 E:4 C:1	S:2 E:4 C:1	S:3 E:1 C:2	S:1 E:4 C:2	~~S:0~~	S:1 E:4 C:2	n.a	n.a	S:2 E:4 C:1	A

In the kit it is available the spreadsheet `Assessment Matrix.xlsx` to prepare this table.

Operational Situations – 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/OS1

Effect		
Statement S	*Crash at high velocity*	*S: 3*
Statement E	*Depending on the region, the average speed of a vehicle can be high in more than 10% of a vehicle usage. (failure is the trigger)*	*E: 4*
Statement C	*90% of the drivers should be able to react by timely pressing the brake pedal.*	*C: 2*

H2/OS1

Effect		
Statement S	*Crash at high velocity*	*S: 3*
Statement E	*Depending on the region, the average speed of a vehicle can be high in more than 10% of a vehicle usage. (failure is the trigger)*	*E: 4*
Statement C	*Since the previous car observe the safe distance and more than %99 percent of the drivers can react seeing that the vehicle ahead of them is getting closer all of a suddent.*	*C: 1*

H3/OS5 **(not safety relevant)**

Effect		
Statement S	*The driver starts to move but the vehicle does not have enough acceleration, it might cause inconvenience for the other drivers but it does not cause an injury*	*S: 0*
Statement E		~~*E:*~~
Statement C		~~*C:*~~

H4/OS3

Effect		
Statement S	*Crash with a pedestrian at low velocity*	*S: 2*
Statement E	*Very often a person is crossing the street in the cities or urban aria*	*E: 4*
Statement C	*The driver can use the brake to decelerate and more than 90% of the passenger can evade the crash by moving forward or backwards.*	*C:1*

H5/OS5

Effect		
Statement S	*Crash of vehicles at low speed*	*S: 1*
Statement E	*Very often vehicles stop at the traffic lights*	*E: 4*
Statement C	*90% of the drivers should be able to react by timely pressing the brake pedal.*	*C:2*

H6/OS6

Effect		
Statement S	*Crash of vehicles at low speed*	*S: 1*
Statement E	*Very often vehicles stop at the traffic lights*	*E: 4*
Statement C	*90% of the drivers should be able to react by timely pressing the brake pedal.*	*C:2*

Safety goals

SG1	The torque to be requested corresponds to the angle of the throttle pedal and the transmission mode selected.
SG2	When the vehicle has a velocity less than 5 Km/h, no torque in the reverse of the expected direction of motion is requested.
SG3	The correct transmission mode shall be represented on the instrument cluster.

Results

Hazardous situation	**Safety goal**	**ASIL-level**	**Safe state**	**Fault tolerance time interval (FTTI)**
H1	SG1	C	Check the course of the pedal and reduce the positive torque request. The driver will be notified about the mall function.	200ms
H2	SG1	B	Check the course of the pedal and reduce the negative torque request. The driver will be notified about the mall function.	300ms
H3	SG1	A	Check the course of the pedal and increase the positive torque request. The driver will be notified about the mall function.	500ms
H4	SG1	A	Check the course of the pedal and increase the negative torque request. The driver will be notified about the mall function.	500ms

H5	SG2	A	The brake is activated to stop the vehicle. The driver will be notified of the malfunction.	500ms
H6	SG3	A	The driver will be notified of the malfunction.	500ms

Relevant failure modes for H1

F1: the throttle pedal sends a signal which corresponds to a higher torque with respect to the torque required by the driver.

F2: The microcontroller miscalculates the torque to be requested and requests a higher value of torque or request a torque while no signal is received from the throttle pedal.

F3: One-pedal management ECU does not receive the data that the brake pedal is pressed and starts requesting torque, as if the driver left his/her foot from the brake pedal in order to initiate driving.

Relevant failure modes for H2

F1: the throttle pedal sends a signal which corresponds to a torque with a different sign with respect to the torque required by the driver. Alternatively, the throttle pedal does not send any signal even if the driver is pressing it.

F2: The microcontroller miscalculates the torque to be requested and requests a lower value of torque.