MBSD Lab #3 A.Y. 2022/23

# Purposes

* Perform some parts of the Functional and Technical Safety Concept analysis, according to ISO26262, of a “one pedal controller” for a car.
* Implement some of the safety concepts in the Simulink model of the controller developed in Laboratory #2.
* Perform unit and integration tests on the implemented safety-related functionalities.

It is available an example of a Functional Safety Concept for the item Front Light Manager (FLM).

The deliverable, composed of

* the report (the following pages of this document)
* the Simulink models on where the safety concepts have been implemented
* all the needed files to replicate the software testing results

has to be provided as a .ZIP file up to **May 28th at 23:59.** It shall also contain a brief report explaining the design of the controller using the following template.

It is sufficient that only one of the group members uploads it.

**Important hint:**

For the following analysis, consider ASIL C all the safety goals related to unintended acceleration (those leading to an increase of the vehicle’s speed modulus) and ASIL B the warnings to the driver and the unintended deceleration (those leading to a decrease of the vehicle’s speed modulus).

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

# Laboratory 3 Report

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

* Cihan Yurtsever, s296824
* Alessandro Cavalli, s301494

Functional Safety Concept

One pedal

# Functional safety architecture

Figure 1 Functional safety architecture (from the safety concept)

# Attributes of the safety goals

*Fill in the attribute/parameters of the safety goal*

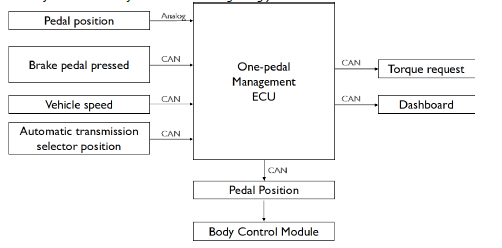
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Safety goal** | **Attributes/Parameters of the safety goal** | | | | |
| Integrity (ASIL) | Safe state | Fault tolerance time | Warning concept | Degradation concept |
| SG1 | C | Neutral and warn | 1s | Driver must be notified that OP system does not work properly. | In case of failure system swap to Neutral state. |
| SG2 | B | Neutral and warn | 1s | Driver must be notified that OP system does not work properly. | In case of failure system swap to Neutral state. |
| SG3 | B | Warn | 1s | Driver must be notified on dashboard that warning system does not working. | Disabling warning system |

# Functional (and technical) safety requirements and allocation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Define functional safety requirements** | | **Allocation of requirements on systems and elements** | |
| **Safety requirements** | **Remark** | **If applicable, allocate the safety requirements to other Items / Systems** | **If applicable, allocate the safety requirements to equipment other technologies to minimize risk.**  **That could be e.g. hydraulic, mechanical equipment** |
| **Safety goals** | **The system should not accelerate  unintentionally.** | SR1 If we are in the Driving state, Requested Torque should be constrained between 0, 80 Nm or If we are in the Reverse state Requested Torque should be constrained between -40, 0 Nm.  If we are in the Breaking and Parking, conditions we need to jump to Neutral.  Driver should be informed | No | In the Driving and Reverse state jumping to Neutral state can be let on the driver (since the an instantaneous stop would be dangerous in this cases)(?). | Hydraulic Breaking Pedal |
| **The system should not decelerate(break)  unintentionally.** | SR2 If throttle position is TP>=1/3 (since its regenerative part), and we are in the breaking transmission state jump to the Neutral state and driver should be informed.  If the AutoTransSelector is on Drive or Reverse The driver should be warned. | No | In the Driving and Reverse state jumping to Neutral state can be let on the driver (since the an instantaneous stop would be dangerous in this cases)(?). | Hydraulic Breaking Pedal |
| **The system should be able to detect when warning system is not working** | SR3 If we are not getting any CAN signal from the Automatic Transmission Selector Position.  In addition the dashboard CAN signal should be checked | The warning system is depending on the Transmission Selector | Driver can evaluate the situation(for blink and the state that he is on). | (replicate?) No. |

# ASIL preliminary architecture[[1]](#footnote-2)

B



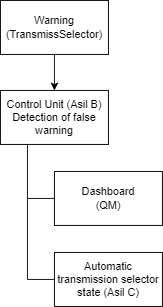
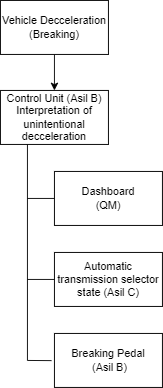
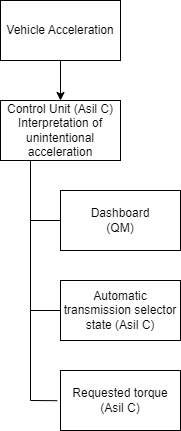
C

C

B

Figure 2 Preliminary architecture

ASIL preliminary architecture (with ASIL Decomposition)



# Implementations[[2]](#footnote-3)

## Functional redundancies

The functional safety of this item relies heavily on the warning system, so a secondary (and simpler) warning device should be implemented. In particular, in the case when the dashboard is not responding on the CAN bus or is reporting an error, a simple and independently driven indicator, such as a LED, must be turned on.

If dashboard is not responding on the CAN bus, we need to add external basic warning element(led,etc..) to make the user informed about the warning system is not functioning properly.

## Implemented plausibility checks

The inputs of this item are the following:

BrakePedalPressed, a boolean reading without any plausibility check applicable;

ThrottlePedalPosition, a floating point reading normalized between 0 and 1, we will assume that the pedal sensor in case of malfunction will return a value greater than one;

VehicleSpeed\_km\_h, a floating point reading that in correct operations must remain within the range -60, 240 km/h;

AutomaticTrasmissionSelectorState, an integer reading to be interpreted as an enumeration, we will assume that the selector will send through the CAN bus a value outside the range 0, 4 (5 for instance) if some error occur.

Torque contraint on certain level Screen shout needed….

# Software testing

## Implemented unit tests

*Describe in English the test performed to verify the correct functionality of the safety mechanism implemented.*

Since the system is very simple, the unit tests coincide with the integration test.

## Implemented integration tests

*Describe, in English, the scenarios tested at the integration level to verify the proper integration between the various units implementing the safety mechanisms.*

A suitable test harness was developed in order to stimulate all the part of the controller such that a 100% Condition Decision coverage is reached. In particular a driving scenario is simulated such that each functional logical state is reached and every functional transition is tested. For what concerns the safety logic, the triggering mechanism is based on the assumption that the sensor readings in input to the item provide an out of range value in case of malfunction. Therefore with a suitable fault injection is possible to stimulate the safety logic as well.

1. See document 02-iso26262.pdf, slides 89, 90, 91, 92, 93. [↑](#footnote-ref-2)
2. In the ISO26262 the implementations are based on a document called *Technical Safety Concept*, but for simplicity we move straight from the *Functional Safety Concept* to software implementations.

   A guideline for the implementation phase can be found in the document 02-iso26262.pdf from slide 81, in particular slide 86. [↑](#footnote-ref-3)