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)

* Name Surname, student ID

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 while driving** | SR1 If throttle position is TP<1/3, and we are in the breaking transmission state jump to the Neutral state.  Driver should be informed | No | No | Hydraulic Breaking Pedal |
| SR2 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. | No | No | Hydraulic Breaking Pedal |
| **The system should not deccelerate  unintentionally while driving** |  |  |  |  |
|  |  |  |  |
| **The system should not deccelerate  unintentionally while driving** |  |  |  |  |
|  |  |  |  |

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

Figure 2 Preliminary architecture

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

## Functional redundancies

## Implemented plausibility checks

# Software testing

## Implemented unit tests

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

## 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.*

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)