# Model-Based Software Design

# Laboratory 1 Report

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

* Alessandro Fasiello, s297276
* Alice Giordano, s304003

Item definition

Skyhook 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 be compliant 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 Skyhook controller (SHC) 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. In this document, the requirements and recommendations for establishing the definition of the item, including its functionality, interfaces, environmental conditions, legal requirements, and known hazards will be handled.

# Purpose of the item

*Please describe in this chapter the purpose of the item. Consider laws, standards and regulations in order to describe sufficiently the purpose of the item.*

The purpose of the item is the following:

* To improve the performance of a vehicle and to guarantee a better comfort of the vehicle occupants, a semi-active suspension system is adopted where a control low is used to change the Damping in relation to the suspended mass and wheel speed.

## Functional behavior

Thanks to a mechatronic system based on electro valves, the Skyhook controller changes the damping coefficient c of each of the 4 suspensions installed in the car to impose a higher damping coefficient when the suspension itself is expanding and a lower one when it is compressing. It allows to maintain the maximum possible stability for the vehicle body regardless of driving and road conditions: the system damps the vibrating body in comparison to an imaginary line in the horizon.

From a mathematical point of view, the principle is the following:

|  |  |
| --- | --- |
| Function | Operating elements |
| Measure Front Left wheel acceleration | FLA |
| Measure Front Right wheel acceleration | FRA |
| Measure Rear Left wheel acceleration | RLA |
| Measure Rear Right wheel acceleration | RRA |
| Measure chassis acceleration | CA |
| Changes the damping of the Front Left wheel shock absorber | FLEV |
| Changes the damping of the Front Right wheel shock absorber | FREV |
| Changes the damping of the Rear Left wheel shock absorber | RLEV |
| Changes the damping of the Rear Right wheel shock absorber | RREV |
| Disable the item functionality when required by the driver | BTN |
| Warn the driver when the SHC is not functioning/disabled | LED |

# 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.*

The following figure shows the assumed system architecture, including system elements like:

* Ignition Key position (KL15) (via Body Controller)
* Enable/Disable Button (BTN)
* Service request /malfunction indication LED on the instrument cluster to warn the driver (LED)
* Front Left suspension electro valve (FLEV)
* Front Left suspension accelerometer (on unsprung mass) (FLA)
* Front Right suspension electro valve (FREV)
* Front Right suspension accelerometer (on unsprung mass) (FRA)
* Rear Left suspension electro valve (RLEV)
* Rear Left suspension accelerometer (on unsprung mass) (RLA)
* Rear Right suspension electro valve (RREV)
* Rear Right suspension accelerometer (on unsprung mass) (RRA)
* Chassis accelerometer (sprung mass) (CA)
* Power supply (PSU)

The technical interfacing of system elements with FLM ECU is assumed as shown in figure and table:



|  |  |
| --- | --- |
| System element | Interface to FLM ECU |
| Ignition Key position (KL15) (via Body Controller) | CAN interface |
| Service request /malfunction indication LED on the instrument cluster to warn the driver (LED) | CAN interface |
| Front Left suspension electro valve (FLEV) | DO |
| Front Left suspension accelerometer (on unsprung mass) (FLA) | Serial Bus (e.g., SPI, I2C) |
| Front Right suspension electro valve (FREV) | DO |
| Front Right suspension accelerometer (on unsprung mass) (FRA) | Serial Bus (e.g., SPI, I2C) |
| Rear Left suspension electro valve (RLEV) | DO |
| Rear Left suspension accelerometer (on unsprung mass) (RLA) | Serial Bus (e.g., SPI, I2C) |
| Rear Right suspension electro valve (RREV) | DO |
| Rear Right suspension accelerometer (on unsprung mass) (RRA) | Serial Bus (e.g., SPI, I2C) |
| Chassis accelerometer (sprung mass) (CA) | Serial Bus (e.g., SPI, I2C) |
| Power supply (PSU) | Analog |
| Enable/Disable button (BTN) | CAN |

Assumptions:

As a starting point, the following configuration of the system is assumed:

* Implementation of SHC on one ECU
* At the vehicle powering on, the state of the SHC is Enabled.
* The electro-valves are monostable hence when the firing signal is OFF, or the ECU cannot provide it, the shock absorber remains set at the damping coefficient.
* All memories (volatile and non-volatile) is protected against reversible transient faults. It is assumed that mechanisms like ECC are available.
* Hardware means for memory partitioning, like MPU or MMU, are available.
* The microcontroller is considered a Safety Element out of Context (SEooC), hence the analysis of failure modes of the microcontroller is performed, and safety measures are defined and implemented. This analysis is based on data provided by the supplied (safety manual) and the requirements of ISO26262.

**Consider only a quarter (one wheel) of the car and not consider the external components like BTN, LED, PSU, and the KL15 signal.**

# 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 to stabilize the vehicle trough the actuation of valves that modify the dumping coefficient of the suspensions. Doing this it is in charge to the readings of the accelerometers (e.g. FRA and CA) of wheel and chassis and communication of it through the BUS.

It is in charge to send signals to the instrumental cluster in order to warn the drivers about failures.

# 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*

Accidental damage leading to mechanical damage, wrong pression of dumping fluid.

# Functional requirements

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

SHC has to be enabled when the KL15 is on, except in case of error state, during which the shock absorber remains set at the damping coefficient and a LED has to warn the driver.

When the system is active, the EVs have to be actuated in other to grant the following value of dumping:

# Other requirements

*Other environmental requirements which can influence your item*

# Law, directive and standard

*List the laws, directives and standard which have to be considered*

ISO26262

# External measure to minimizing risks

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

The vehicle operator is required by law to be properly trained and to obtain a driving license, so he/she verifies, before start driving, that there are not any warnings and errors led on.

The vehicle is required to pass periodical inspection and revisions that control the correct functionality of main security systems like suspensions.

Hazard Analysis and Risk Assessment

Skyhook controller

**Consider only a quarter (one wheel) of the car and not consider the external components like BTN, LED, PSU, and the KL15 signal.**

# Participants

|  |  |  |
| --- | --- | --- |
| **Name, department** | **Qualification** | **Experience** |
|  |  |  |
|  |  |  |
|  |  |  |

# Analyses of situations

## Definition of possible functional failures

|  |  |
| --- | --- |
| **Failure #** | **Description** |
| F1 | The electro valve modifies or left set the shock absorber damping factor at when it should be |
| F2 | The electro valve modifies or left set the shock absorber damping factor at when it should be |

## 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 Driving at high speed
* VS2 Driving at low speed
* VS3 Performing an evasive maneuver

## Considerations

*Describe driving situations for each status of the vehicle*

|  |  |  |
| --- | --- | --- |
| **Scenario #** | **Driving situation** | **Vehicle status** |
| ~~S1~~ | ~~Driving in city road (DS1)~~ | ~~Driving at high speed (VS1)~~ |
| S2 | Driving in city road (DS1) | Driving at low speed (VS2) |
| S3 | Driving in city road (DS1) | Performing an evasive maneuver (VS3) |
| S4 | Driving in a country road (DS2) | Driving at high speed (VS1) |
| S5 | Driving in a country road (DS2) | Driving at low speed (VS2) |
| S6 | Driving in a country road (DS2) | Performing an evasive maneuver (VS3) |
| S7 | Driving in a highway (DS3) | Driving at high speed (VS1) |
| S8 | Driving in a highway (DS3) | Driving at low speed (VS2) |
| S9 | Driving in a highway (DS3) | Performing an evasive maneuver (VS3) |

# Analysis

## Estimation matrix

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Scenarios** | | | | | | | | | | |
| ~~S1[[1]](#footnote-1)~~ | S2 | S3 | S4 | S5 | S6 | S7 | S8 | S9 | **Top event (worst case)** | **ASIL[[2]](#footnote-2)** |
| **Failures** | F1 | S: x  E: x  C: x | S: 2  E: 4  C: 0 | S:3  E: 2  C: 0 | S: 3  E: 2  C: 1 | S: 2  E: 4  C: 0 | S: 2  E: 2  C: 0 | S: 3  E: 4  C: 0 | S: 2  E: 2  C: 0 | S: 3  E: 3  C: 1 | S: 3  E: 3  C: 1 | A |
| F2 | S: x  E: x  C: x | S: 2  E: 4  C: 0 | S:3  E: 2  C: 0 | S: 3  E: 2  C: 1 | S: 1  E: 4  C: 0 | S: 2  E: 2  C: 0 | S: 3  E: 4  C: 0 | S: 2  E: 2  C: 0 | S: 3  E: 3  C: 1 | S: 3  E: 3  C: 1 | A |

## 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.

**(S7)** Driving in highway (DS3) at high speed (VS1) – **(F2)** The electro valve modifies or left set the shock absorber damping factor at when it should be

|  |  |  |
| --- | --- | --- |
| *Effect* | The driving experience of the vehicle worsens | |
| *Statement S* | Life-threating injuries (survival uncertain) or fatal injuries due to:   * Rear/front collision with another passenger car with high speed * Side impact with other surpassing vehicle or vehicle entering the highway from acceleration lane | *S3* |
| *Statement E* | High probability (>10% of average operating time) | *E4* |
| *Statement C* | Controllable in general | *C0* |

**(S9)** Driving in highway (DS3) performing evasive maneuver (VS3) – **(F2)** The electro valve modifies or left set the shock absorber damping factor at when it should be

|  |  |  |
| --- | --- | --- |
| *Effect* | The driving experience of the vehicle worsens | |
| *Statement S* | Life-threating injuries (survival uncertain) or fatal injuries due to:   * Rear/front collision with another passenger car with high speed * Side impact with other surpassing vehicle * Side impact with vehicle in the lane in which the driver is entering | *S3* |
| *Statement E* | Medium probability (1% to 10% of average operating time) | *E3* |
| *Statement C* | More than 99% of the average drivers or other participants are able to avoid harms | *C1* |

# Hazards

|  |  |
| --- | --- |
| H1 | The shock absorber damping factor at when it should be |
| H2 | The shock absorber damping factor at when it should be |

## H1

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

**Exceptions and Boundary Conditions to H1:**

* The effects are perceived only at high speeds travelling on curves
* On rough roads where the effect of the SHC is more useful, the driver shall reduce its speed regardless the presence of this functionality

## H2

The same as for H1

# Safety goals

|  |  |
| --- | --- |
| SG1 | H1 -> Ensure a non vibrating and stable dumping factor |
| SG2 | H2 -> Ensure a non vibrating and stable dumping factor |

## Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Failure/malfunction** | **Safety goal** | **ASIL-level** | **Safe state** | **Fault tolerance time interval (FTTI)** |
| F1 | SG1 | A | Dumping factor = | 50 ms [[3]](#footnote-3) |
| F2 | SG2 | A | Dumping factor = | 50 ms 3 |

## Relevant failure modes for H1

MF1: Failure of the electrovalves during the modification of the dumping coefficient.

MF2: Failure of the evaluation and implementation of the target value of dumping coefficient.

MF3: Failure of the detection of the acceleration values of wheels.

## Relevant failure modes for H2

*The same as for H1*

1. Driving at high speed in city roads is forbidden. [↑](#footnote-ref-1)
2. 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. [↑](#footnote-ref-2)
3. Marcelo Menezes Morato, Olivier Sename, Luc Dugard. LPV -MPC Fault Tolerant Control of Automotive Suspension Dampers. LPVS 2018 - 2nd IFAC Workshop on Linear Parameter Varying Systems, Sep 2018, Florianopolis, Brazil. pp.31-36. ffhal-01658662v2f [↑](#footnote-ref-3)