Item definition (Example)

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: (to be drown by the students)



|  |  |
| --- | --- |
| 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.**

**The solution provided below comments the complete system.**

# 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 adapting the damping factor of each 4 shock absorber composing the suspension system of a car. It manages 5 accelerometers (4 on the unsprung masses and 1 on the chassis) and 4 electro valves. Moreover, it must send an opportune status CAN message containing a signal used to turn on a service/malfunction LED on the instrumentation cluster.

In the case of a malfunction of each of its core components (accelerometer or electro valves), it should stop to provide the functionality and inform the driver.

If the status CAN massage is not generated, the instrument cluster shall assume that the SHC ECU is failed, warning the driver.

# 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*

Vibrations leading to mechanical damage, vandalic acts, collision with debris during the driving

# Functional requirements

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

SHC has to stay enabled when the KL15 is on and the driver does not press the BTN. Its state is restored to “enabled” every time the vehicle is turned on again.

It shall monitor that all the core components (accelerometers and electrical valve) are working properly.

# 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*

# 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 obtain a driving license, so he/she verifies that no malfunction is indicated in the instrument cluster during the driving.