Hazard Analysis and Risk Assessment (Example)

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:3  E:1  C:1 | S:2  E:4  C:1 | S:3  E:2  C:1 | S:3  E:4  C:0 | S:2  E:4  C:1 | S:3  E:2  C:1 | S:3  E:4  C:0 | S:2  E:4  C:0 | S:3  E:2  C:1 | S:2  E:4  C:1 | A/QM[[3]](#footnote-3) |
| F2 | S:3  E:1  C:1 | S:2  E:4  C:1 | S:3  E:2  C:1 | S:3  E:4  C:0 | S:2  E:4  C:1 | S:3  E:2  C:1 | S:3  E:4  C:1 | S:2  E:4  C:1 | S:3  E:2  C:1 | S:3  E:4  C:1 | B |

## 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.

F1/S7

|  |  |  |
| --- | --- | --- |
| *Effect* | *The suspensions are always set to , making the vehicle less comfortable. This can increase the stress of the driver, making him/her more error-prone* | |
| *Statement S* | *High speed collision in a highway* | *S3* |
| *Statement E* | *Driving in a highway* | *E4* |
| *Statement C* | *More stress on the driver, not direct effects on the driving* | *C0* |

F2/S7

|  |  |  |
| --- | --- | --- |
| *Effect* | *The suspensions are always set to , making the vehicle less stable due to increased roll and pitch movements with respect the usual one of the vehicle with properly working suspension system* | |
| *Statement S* | *High speed collision in a highway* | *S3* |
| *Statement E* | *Driving in a highway* | *E4* |
| *Statement C* | *Less control on the car at high speed due to increased movements* | *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 | Disable the SCH in the case it is not possible to guarantee its correct functionality. |

## Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Failure/malfunction** | **Safety goal** | **ASIL-level** | **Safe state** | **Fault tolerance time** |
| The SHC is cannot properly control the suspension system | SG1 | B | SHC controller disabled. | 100 ms |

## Relevant failure modes for H1

FM1: The SHC ECU sends improper commands to electro valves worsening the handling of the car.

## Relevant failure modes for H2

FM1: The SHC ECU sends improper commands to electro valves worsening the handling of the car.

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. The sum S+E+C is 7, leading to an ASIL A classification, but increased stress on the driver is not considered safety-related by the ISO26262 standard (since C0 level is not formally defined in the standard). Both the classifications are hence correct. [↑](#footnote-ref-3)