Hazard Analysis and Risk Assessment (Example)

Airbag Control Unit

# Participants

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

# Analyses of situations

## Definition of possible functional failures

For sake of simplicity, consider only the driver front airbag.

|  |  |
| --- | --- |
| **Failure #** | **Description** |
| F1 | Balloons erroneously deployed. |
| F2 | Balloons not deployed in the case of a crash. |

## 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
* DS2 Crash
* DS2 Parked

### Definition of the vehicle status

* VS1 Medium/high speed
* VS2 Low speed
* VS3 Stopped

## Considerations

*Describe driving situations for each status of the vehicle*

|  |  |  |
| --- | --- | --- |
| **Scenario #** | **Driving situation** | **Vehicle status** |
| S1 | Driving | Medium/high speed |
| S2 | Driving | Low speed |
| S3 | Driving | Stopped |
| S4 | Crash | Medium/high speed |
| S5 | Crash | Low speed |
| S6 | Crash | Stopped |
| ~~S7~~ | ~~Parked~~ | ~~N/A (balloon never deployed with parked car)~~ |

# Analysis

## Estimation matrix

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

## Scenarios – Comment of entries

*Start with the description of what happens and then assign the parameters.*

F1 / S1

|  |  |  |
| --- | --- | --- |
| *Effect* | *The driver loses control of the car* | |
| *Statement S* | *Life threatening injuries* | *3* |
| *Statement E* | *Every time the vehicle is moving* | *4* |
| *Statement C* | *Not controllable (the deployment is automatically triggered)* | *3* |

F1 / S5

|  |  |  |
| --- | --- | --- |
| *Effect* | *The airbag deploys when the seat belt is not worn…* | |
| *Statement S* | *…worsening the accident effects* | *3* |
| *Statement E* | *A crash that requires airbags to be deployed (hopefully happens less often than once per year).* | *1* |
| *Statement C* | *Not controllable (the deployment is automatically triggered)* | *3* |

F2 / S4

|  |  |  |
| --- | --- | --- |
| *Effect* | *The airbag does not protect the driver* | |
| *Statement S* | *Life-threatening injuries could have been avoided by deploying the airbag.* | *3* |
| *Statement E* | *A crash that requires airbags to be deployed (hopefully happens less often than once per year).* | *1* |
| *Statement C* | *Not controllable (the deployment is automatically triggered)* | *3* |

# Hazards

|  |  |
| --- | --- |
| H1 | Balloon explosive inflation[[3]](#footnote-3) |

## H1

An airbag deployment is a dangerous event: in case of a crash, it has been demonstrated to be less harmful compared to not having the presence of the inflated balloons, but anyway it deploys a large amount of mechanical energy against the passengers’ bodies.

Moreover, in conditions different from the optimal ones (a passenger seated and with the seat belt fastened) a person hit by the inflating balloon can report serious consequences.

# Safety goals

|  |  |
| --- | --- |
| SG1 | Prevent to wrongly deploy airbags. |
| SG2 | Warn the driver if the airbags are not available. |

## Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Failure/malfunction** | **Safety goal** | **ASIL-level** | **Safe state** | **Fault tolerance time** |
| F1 | SG1 | D | Squid-wire driver not power-supplied | Malfunctions affecting the squid wire drivers must be detected before they can trigger the explosive capsule |
| F2 | SG2 | A | The driver is notified by turning on the airbag warning lamp on the dashboard | 1000 ms |

## Relevant failure modes for H1

1. 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-1)
2. The failure effect is visible only in defined situation (in this case, if a crash happens) [↑](#footnote-ref-2)
3. In this particular case the hazard is the functionality of the item by itself, when provided at a wrong time. [↑](#footnote-ref-3)