**Appendix Z**

# **Functional Safety Assessment Plan**

Table of Contents

[**1.** **Introduction** 5](#_Toc495503926)

[1.1. Purpose 5](#_Toc495503927)

[1.2. Applicability 5](#_Toc495503928)

[1.3. Assessment Activity Description 5](#_Toc495503929)

[**2.** **Applicable Documents** 5](#_Toc495503930)

[2.1. Automotive Standard 5](#_Toc495503931)

[2.2. Additional Documents: 5](#_Toc495503932)

[2.3. System safety administrative documents 6](#_Toc495503933)

[**3.** **ABS System Overview** 6](#_Toc495503934)

[**4.** **Operational Modes** 6](#_Toc495503935)

[**5.** **System Safety Requirements** 6](#_Toc495503936)

[**6.** **Design Considerations for Safety** 7](#_Toc495503937)

[6.1. General 7](#_Toc495503938)

[6.2. Hazard Mitigation Methods 7](#_Toc495503939)

[6.2.1. General 7](#_Toc495503940)

[**7.** **Safety Analysis Process** 7](#_Toc495503941)

[7.1. Safety Analysis Process Overview 7](#_Toc495503942)

[7.2. Mishap Risk 8](#_Toc495503943)

[7.2.1. Mishap Severity 8](#_Toc495503944)

[7.2.2. Failure Conditions Probability 8](#_Toc495503945)

[7.2.3. Failure Conditions Controllability 9](#_Toc495503946)

[7.2.4. Mishap Risk Assessment 9](#_Toc495503947)

[7.2.5. Categories for Risk Level 10](#_Toc495503948)

[7.3. Risk-Reducing Actions 10](#_Toc495503949)

[7.3.1. Design Changes 10](#_Toc495503950)

[7.3.2. Protective Devices 11](#_Toc495503951)

[7.3.3. Warning Devices 11](#_Toc495503952)

[7.3.4. Testing 11](#_Toc495503953)

[7.4. Risk Log 11](#_Toc495503954)

## Definitions

|  |  |  |
| --- | --- | --- |
| No. | Term | Definition |
|  | Hazard | Any real or potential condition that can cause injury, illness, or death to personnel, damage to or loss of a system, equipment or property, or damage to the environment |
|  | Hazard Area | A geographical or geometric surface area that is susceptible to hazard from a planned event or unplanned malfunction |
|  | Life cycle | All phases of the system's life including design, research, development, test and evaluation, production, deployment, operations and support, and disposal |
|  | Mishap | An unplanned event or series of events resulting in death, injury, occupational illness, damage or loss of equipment or property, or damage to the environment |
|  | Mishap risk | An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence |
|  | Mishap probability | The aggregate probability of occurrence of the individual events/hazards that might create a specific mishap (the likelihood that a mishap will occur) |
|  | Mishap probability levels | An arbitrary categorization that provides a qualitative measure of most reasonable likelihood of occurrence of a mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem or component failure or malfunction |
|  | Mishap severity | An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard |
|  | Mishap risk assessment | The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probabilities of occurrence, and prioritizing them for risk mitigation actions |
|  | Residual mishap risk | The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence |
|  | Safety | Freedom from those conditions that can cause death, injury, occupational illness, damage or loss of equipment and property, or damage to the environment |
|  | Safeguard | Hardware component, software routine, operator procedure, or some combination intended to mitigate risk |

## 

## Abbreviation

|  |  |  |
| --- | --- | --- |
| No. | Term | Description |
|  | ABS | Anti-lock Braking System |
|  | FTA | Fault Tree Analysis |
|  | PHA | Preliminary Hazard Analysis |
|  | PHL | Preliminary Hazard List |
|  | SSAP | System Safety Assessment Planning |
|  | SHA | System Hazard Analysis |
|  | ECU | Electronic Control Unit |
|  | CAN | Controlled Area Network |
|  | SSHA | Subsystem Safety Hazard Analysis |

## **Introduction**

## Purpose

The purpose of this document is to submit a functional safety assessment plan for the automotive ABS system and document the means which would be used to reduce the mishap risks to acceptable levels.

The objective of this document SSAP is to identify hazards, severity and probability (mishap risks) associated with each hazard and determines the risk associated with the hazard on personnel, facilities, equipment, environment, the public, as well on the system itself.

## Applicability

This ABS System Safety Assessment Plan (SSAP) reflects the current configuration (main hardware and software elements) of the ABS system. It can be used to overcome the events causing hazards as well as for further refinement processes.

## Assessment Activity Description

The safety process would be conducted according to procedures for functional safety management, which is based on ISO-26262:2 2011.

## **Applicable Documents**

## Automotive Standard

|  |  |
| --- | --- |
| ID | Title |
|  | Parent standard for template documents i.e. IEC - 61508 |
|  | ISO 26262 Automotive standard to follow |

## Additional Documents:

|  |  |
| --- | --- |
| ID | Tittle |
|  | System specifications |
|  | Performance specifications & performance data manual |
|  | System qualification test report |
|  | ISO – 26262:10 – Guidelines and methods for conducting the safety assessment process on automotive systems |

## System safety administrative documents

|  |  |  |  |
| --- | --- | --- | --- |
| No. | ID | Tittle | Description |
|  |  | System Safety Program Plan (SSPP) | Management plan and overview |
|  |  | Preliminary Hazard List (PHL) | Initial potential identified system hazards, based on system knowledge, mission requirements, past experience and lesson learned |
|  |  | System Functional Hazard Assessment (SFHA) | Analysis of hazard conditions and vehicle failure modes which can lead to mishap  Examples may be found in tables ……… |
|  |  | System Hazard Assessment Report (SHAR) | Assessment of the potential severity of each hazard |
|  |  | Software Safety Plan (SPP) | A plan that analyze safety software logic development tools, defines acceptance tests and configuration control |
|  |  | Safety and Maintainability Field data report | Operating experience data including failure reports |

## **ABS System Overview**

The ABS braking system consists of ECU, modulator and sensors. The software system used for ABS is places on ECU. It gets the input from sensor which is connected with the wheel and observing its rotations. ABS software performs some computations and deliver output to the modulators. Afterwards modulator controls the pressure needed to exert on wheel disk using disk pads.

## **Operational Modes**

The list of hazards to identify would be in accordance to the missions specified in the System Specification chapter. These hazards would be first identified, moreover in next sections hazards will be mitigated.

## **System Safety Requirements**

The general requirements concerning the ABS system, quoted from the System Requirements and the System Specification documents, are as follows:

1. System should run diagnostic test for ABS failure on ignition
2. System should notify driver and display signal light for ABS failure
3. System should prevent from sudden wheel lock on applying breaks
4. System should shift to normal breaks if ABS fails
5. System should reduce acceleration gradually upon applying breaks
6. System should disable ABS if speed is below 20 km/h and vice versa

## **Design Considerations for Safety**

## General

Several design considerations would be applied in order to improve the system safety, among others are:

1. Fault tolerance by redundancy of critical functions.
2. Automatic monitoring of system/subsystem health and an alert and warning system designed to enable operator intervention when necessary.
3. Hot backup for the controlling the brakes during run.
4. Double hardware lines (CAN BUS) for safety critical signals.

## Hazard Mitigation Methods

## General

The main hazards are controlled in several ways. Generally they can be divided into several methods:

1. Fault tolerance by redundancies at different levels.
2. Removing single point failure.
3. Safe maintenance procedures.
4. Operational procedures.

## **Safety Analysis Process**

## Safety Analysis Process Overview

The safety analyses would be performed according to the following methods:

1. The Safety Program Plan (SPP) would be prepared during the system design stage.
2. A Preliminary Hazard List (PHL) and a Preliminary Hazard Analysis (PHA) will be submitted in concepts phase.
3. Subsequently, Subsystem Safety Hazard Analysis (SSHA) would be prepared for all the subsystems included in ABS system, which have a safety impact on the system.
4. The safety process would be carried out by specialized Safety Working Groups (SWG), according to the various parts of ISO-26262. Independent Safety Review Board (SRB) meetings would be convened in a timely basis in order to assess the process and approve it.

## Mishap Risk

Decisions regarding hazardous failure conditions has to be based on the assessment of risk involved. To aid in the achievement of objectives of system safety, failure conditions needed to be characterized as mishap severity categories, mishap probability and mishap control levels.

## Mishap Severity

The following severity classes for personal injury needed to be used in the assessment and evaluation of the system’s risks before and after the implemented measures.

|  |  |
| --- | --- |
| Class | Description |
| S0 | No Injuries |
| S1 | Light to moderate injuries |
| S2 | Severe to life-threatening (survival probable) injuries |
| S3 | Life-threatening (survival uncertain) to fatal injuries |

## Failure Conditions Probability

The probability that a hazardous failure condition will be appearing during the planned life expectancy of the system can be described in potential occurrences in system operational hours.The following probability classes for hazard occurrence would be used in the assessment and evaluation of the system’s risks.

|  |  |
| --- | --- |
| Class | Description |
| E0 | Incredibly unlikely |
| E1 | Very low probability (injury could happen only in rare operating conditions) |
| E2 | Low probability |
| E3 | Medium probability |
| E4 | High probability (injury could happen under most operating conditions) |

## Failure Conditions Controllability

The controllability classes for personal control would be used in the assessment system regarding risks occurrence.

|  |  |
| --- | --- |
| Class | Description |
| C0 | Controllable in general |
| C1 | Simply controllable |
| C2 | Normally controllable (most drivers could act to prevent injury) |
| C3 | Difficult to control or uncontrollable |

## Mishap Risk Assessment

Risk is the expression of the possibility of a mishap in terms of hazard severity, hazard probability and the controllability, which may result in mishap.

The following table presents a matrix for hazard risk assessment, which would be used to provide priority factors for assigning corrective actions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity Classes | Exposure  Classes | Controllability Classes | | |
| C1 | C2 | C3 |
| S1 | E1 | QM | QM | QM |
| E2 | QM | QM | QM |
| E3 | QM | QM | **ASIL A** |
| E4 | QM | ASIL A | **ASIL B** |
| S2 | E1 | QM | QM | QM |
| E2 | QM | QM | **ASIL A** |
| E3 | QM | ASIL A | **ASIL B** |
| E4 | ASIL A | ASIL B | **ASIL C** |
| S3 | E1 | QM | QM | **ASIL A** |
| E2 | QM | ASIL A | **ASIL B** |
| E3 | ASIL A | ASIL B | **ASIL C** |
| E4 | ASIL B | ASIL C | **ASIL D** |

## Categories for Risk Level

After risk assessment of performed hazard analysis, according to the standard ISO-26262 the ASIL levels need to be assigned to each of the hazard. The following tables presents the ASIL classes.

|  |  |
| --- | --- |
| ASIL Level | Hazard |
| ASIL A | Minor Accident |
| ASIL B | N/A |
| ASIL C | Vehicle Turn-over |
| ASIL D | Major Accident |

## Risk-Reducing Actions

Actions considered able to reduce/eliminate the risks would be specified and need to be listed properly. Actions could be divided in different action classes. Below is a breakdown of actions in 4 different classes.

## Design Changes

These actions involve some form of redesign. This implies that the risk is managed by removing, adding, replacing or changing something in the system’s physical characteristics.

## Protective Devices

Protective devices mean that the risk is managed through the introduction of e.g. fixed or automatic safety devices, stop modes, protection zones or protective equipment.

## Warning Devices

The risk is managed by warning devices, such as sound or light signals etc. that cannot be misinterpreted.

## Testing

These actions imply that the risk should be verified with some form of trial or testing before final approval is issued.

## Risk Log

In the risk management process the identified risks would be explicitly named and described. The following point needed to be considered for the risk log:

* All identified risks are numbered and named with appropriate names.
* Initial risk assessment and risk evaluation and probabilities must be reported.
* All risk would be reduced using defined actions.