



Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

To be refer as

Appendix X

System Safety Plan

Version 1 — October 10, 2017



Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

This page is intentionally left blank.

Version 1 — October 10, 2017

X-2



System Safety Engineering ......................................................................................... 6

3.

3.1

3.2

4.

4.1

4.2

Scope .................................................................................................................................. 5

System Safety Objective .................................................................................................... 5

References .......................................................................................................................... 5

Definitions and Acronyms ................................................................................................. 5

System Safety Organization............................................................................................... 5

Anti-lock braking system—Safety plan

System Safety Process ....................................................................................................... 6

System Safety Milestones .................................................................................................. 6

Safety Task Schedule ......................................................................................................... 7

Safety Approach and Standards ......................................................................................... 7

Hazard Identification ......................................................................................................... 7

System Safety Administration ................................................................................................. 5

2.2.1

System Safety Overview .......................................................................................................... 6

General Requirements and Criteria .......................................................................................... 7

Version 1 — October 10, 2017

X-3

2.2

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

The anti-clock braking system (ABS) is an automobile product of AAAFAS. This safety-critical

system allows the wheels on the automobile to maintain tractive contact with road surface while

barking, thus preventing the automobile from skidding.

Document Control Panel

Document Details:

Name: Safety Plan.docx

Citation: Appendix X

Author: Muhammad Abbas, Senior System Safety Engineer, AAAFAS

Reviewer: Fitash-Ul-Haq, Team Lead ABS, AAAFAS

Table of Contents

Anti-lock braking system—Safety plan .......................................................................................... 3

Document Control Panel ................................................................................................................. 3

Document Details: ...................................................................................................................... 3

Table of Contents ............................................................................................................................ 3

List of Acronyms ............................................................................................................................ 4

Definitions....................................................................................................................................... 4

1.

Overview .................................................................................................................................. 5

1.1

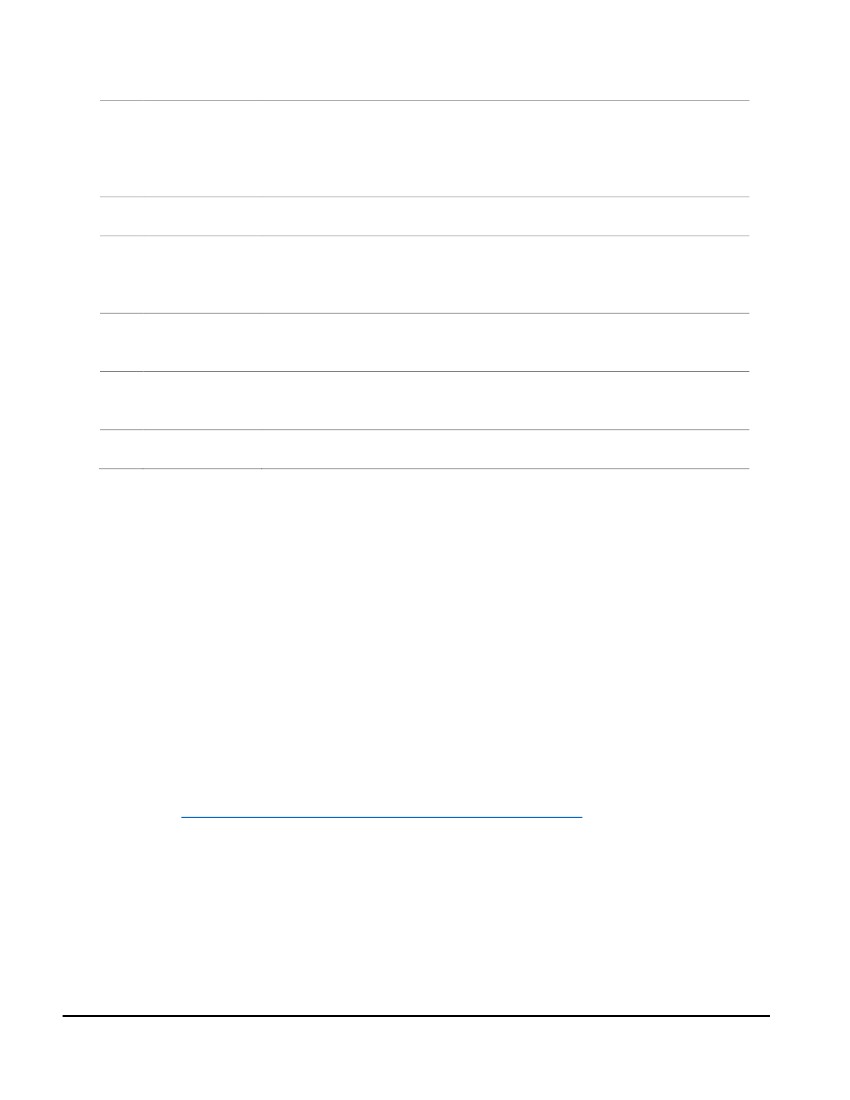
1.2

1.3

1.4

2.

2.3



2.

Safety Training......................................................................................................................... 8

Mishap Investigation and Reporting ........................................................................................ 8

System Safety Interfaces ........................................................................................................ 9

Acronyms and Notes .............................................................................................................. 9

List of Acronyms





ABS – Anti-lock Braking System

AAAFAS – Abbas Ali Ahsan Fitash Automotive Systems

Definitions

No.

1.

Term

Hazard

Definition

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

A geographical or geometric surface area that is susceptible to hazard

from a planned event or unplanned malfunction

All phases of the system's life including design, research,

development, test and evaluation, production, deployment, operations

and support, and disposal

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

An expression of the impact and possibility of a mishap in terms of

potential mishap severity and probability of occurrence

The aggregate probability of occurrence of the individual

events/hazards that might create a specific mishap (the likelihood that

a mishap will occur)

4.3

3.

Hazard Area

Life cycle

4.

Mishap

5.

6.

Mishap risk

Mishap

probability

Version 1 — October 10, 2017

X-4

Safety Data ............................................................................................................................... 8

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

4.4

4.5

4.6

5.

5.1

5.2

5.3

6.

7.

8.

9.

10.

11.

Severity, Probability, Controllability and Risk Assessment .............................................. 7

Hazard Closure Process ..................................................................................................... 7

Engineering and Operational Changes............................................................................... 7

System Safety Precedence ................................................................................................. 7

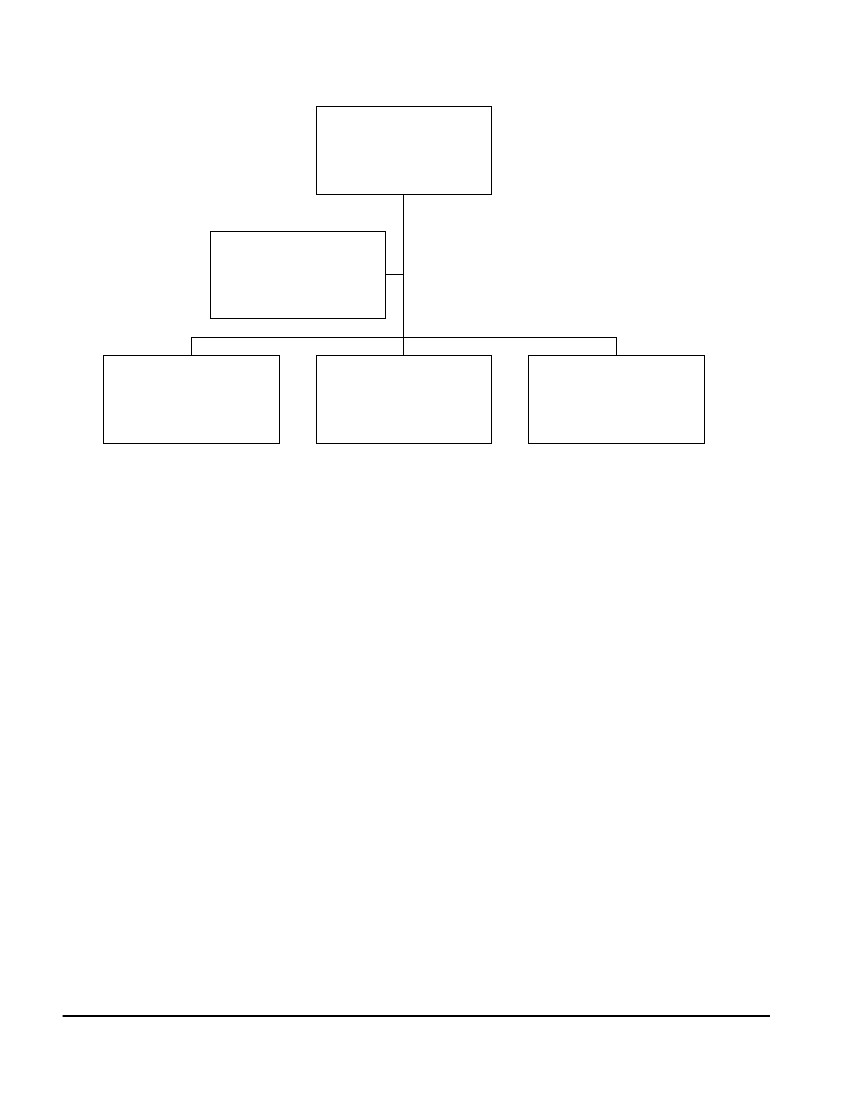
Analysis Techniques .......................................................................................................... 7

Safety Assessment Report.................................................................................................. 7

Subcontractor Safety Program Integration......................................................................... 8

Hazard Analysis ....................................................................................................................... 7

Safety Verification / Testing .................................................................................................... 8



7.

X-5

Version 1 — October 10, 2017

The following heretical tree diagram shows our structure of safety team.

2.2 System Safety Organization

2. System Safety Administration

See the Section Definitions.

1.4 Definitions and Acronyms

ISO 26262: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en

1.3 References

The prime objective of the overall system is to provide a safest possible system to our client with

conformance to the standard ISO 26262.

1.2 System Safety Objective

System safety is implemented to perform a systematic safety analysis on the anti-lock braking

system product of our company. This document plan states and plans all the required safety

measures for closure and elimination of hazards or/and to minimize the probability of failure to

an acceptable level.

1.1 Scope

This section provides a brief, but not complete overview about our safety plan for ABS product

of the company AAAFAS.

1. Overview

Safeguard

12.

11.

Safety

Residual

mishap risk

10.

Mishap

severity

Mishap risk

assessment

9.

8.

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

An assessment of the consequences of the most reasonable credible

mishap that could be caused by a specific hazard

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

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

Freedom from those conditions that can cause death, injury,

occupational illness, damage or loss of equipment and property, or

damage to the environment

Hardware component, software routine, operator procedure, or some

combination intended to mitigate risk

Mishap

probability

levels

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)



Project

Manager

X-6

Version 1 — October 10, 2017

Safety review after formulating requirements



This section describes the critical checkpoints for review of the system safety program.

3.1 System Safety Milestones

3. System Safety Overview

The safety process is presented throughout the development process. The safety engineer must

give input in design keeping in mind the safety requirements. Safety assessment should be

performed by the safety engineer. Identification, management and elimination of hazard should

also be done throughout the project life cycle.

2.3 System Safety Process

Implementation and maintenance of safety program

Identifying safety requirements for implementation in design

Preparing safety checklists and reviewing for safety

Participating in design and code reviews

Utilizing interfaces to comply with applicable safety requirements

Coordinating safety artifacts













2.2.1 System Safety Engineering

The system safety engineer is responsible for development, implementation and maintenance of

the safety program. Establish how authority is given to engineers and act accordingly on safety

issues. The responsibilities assigned to the safety engineer are:

Senior System

Engineer

Figure 1 Safety Team Structure

Safety Analyst

Senior Safety

Engineer

Team Lead

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)











X-7

Version 1 — October 10, 2017

The safety assessment report should be presented after review of the Safety Assessment plan.

5.2 Safety Assessment Report

See the Functional Safety Assessment Plan.docx

5.1 Analysis Techniques

See the Functional Safety Assessment Plan.docx

5. Hazard Analysis

Design with minimum hazards

Re-Design to eliminate hazard

Providing warning devices

Providing pre-use safety training

Incorporate the use of other protective equipment (Like Air-Bag etc.)











To satisfy the safety requirements and to resolve the hazard the following precedence is to be

followed:

4.6 System Safety Precedence

On update for accommodation of any safety requirement must be circulated using a

configuration management tool, to all the stack holders.

4.5 Engineering and Operational Changes

See the Functional Safety Assessment Plan.docx.

4.4 Hazard Closure Process

See the Functional Safety Assessment Plan.docx.

4.3 Severity, Probability, Controllability and Risk Assessment

See the Functional Safety Assessment Plan.docx.

4.2 Hazard Identification

Safety criteria in our case is imposed and managed by external regulatory body of ISO 26262.

The system should must meet at least all the safety objective in the standard ISO 26262 listed in

Sheet 2 (02 Mgmt of Funl. Safety) of the file “SAFE\_D2.1b.xls”.

4.1 Safety Approach and Standards

4. General Requirements and Criteria

Please see the project giant chart in the document “Overall Project Plan”.

3.2 Safety Task Schedule

Preliminary and Critical design review

Review after installation and checkout

Review after integration and testing

Review after operation

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)



5.3 Subcontractor Safety Program Integration

X-8

Version 1 — October 10, 2017

Mishap Investigation and reporting is discussed in detail in our Functional Safety Assessment

Plan.

9. Mishap Investigation and Reporting

It is recommended for end users of our ABS product to avail safety training named “Defensive

Driving” from STC, Lahore.

All the team was trained by STC, Lahore, Pakistan. The team was trained to design safety-

critical systems in automotive industry. Our software and systems engineers were also trained for

safe development and implementation of critical systems.

8. Safety Training

The verification should actually be tested with input from actual operator interface (Braking

paddle).

The software safety requirements are verifiable and testable. The critical functions for hazardous

behavior are required to be tested to satisfy MCDC code coverage criteria. The simulation must

conform to the safety requirements. The system must be test for safety in test environment. The

test environment should be close enough with aim to simulate all the possible hazardous

scenarios. There should be fail-safe modes in the safety requirements and must be tested.

7. Safety Verification / Testing

Prevention for Hazards: Redundant elements, warning messages and proactive actions (Air-

Bag) are taken in hazard analysis phase.

Fire or Explosion Data: The accident caused by failure of the ABS can cause fire or explosion

in case of fuel leak and ignition only.

Physical Data: N/A

Hazardous Products: Pump, Sensor, Modulator and ECU.

Products: The actuators, sensors and ECU all are imported from Texas Inc., Texas, USA.

6. Safety Data

See the Functional Safety Assessment Plan.docx

Hazard Tracking System

5.4

Some of the sensors/actuators to be used in the system to be develop are supplied by Texas Inc.

Texas Inc. have already done safety assessment of their supplied sensors and actuators with

compliance to ISO 26262.

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

Deliverable 1-10

Abbas Ali Ahsan Fitash Automotive Systems (AAAFAS)

10. System Safety Interfaces

An automotive-grade ARM based microcontroller is used to compare speed sensor data, control

brake cylinder pressure and control the return pump for each wheel brake cylinder. The ECU is

also responsible for diagnostics, warning notification and communication with other on board

control units. Newer automotive ECUs from Texas can provide evidence of their suitability for

use in systems where IEC61508 and ISO26262 safety standards compliance are required. This

include discrete sensor data bus, brake fluid pipes interfaces, connected to CAN with CAN type

of “High Speed CAN Signaling. ISO 11898-2”.

11. Acronyms and Notes

STC – Safety Training Center, Lahore, Pakistan, http://www.stc.org.pk/

CAN – Controlled Area Network

ISO – International Organization for Standardization

Version 1 — October 10, 2017

X-9