Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/17/2019	1.0	Bob Li	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

The Safety Plan is a key document in ISO 26262 development project. It specifies how functional safety will be ensured throughout the entire development project and in production. The Safety Plan must identify the various roles and responsibilities as they apply to the development process. The Safety plan lists the various techniques and measures that will be implemented as part of the development project to ensure that the targeted ASIL is achieved. This Safety Plan will focus on the Lane Assistance system and define below contents:

- Item Definition
- Goals and Measures
- Safety Culture
- Safety Lifecycle
- Roles
- DIA
- Confirmation Measures

Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

Product Development at the Hardware Level
Production and Operation

Deliverables of the Project

The deliverables of the project are:

Safety Plan
Hazard Analysis and Risk Assessment
Functional Safety Concept

Technical Safety Concept
Software Safety Requirements and Architecture

Item Definition

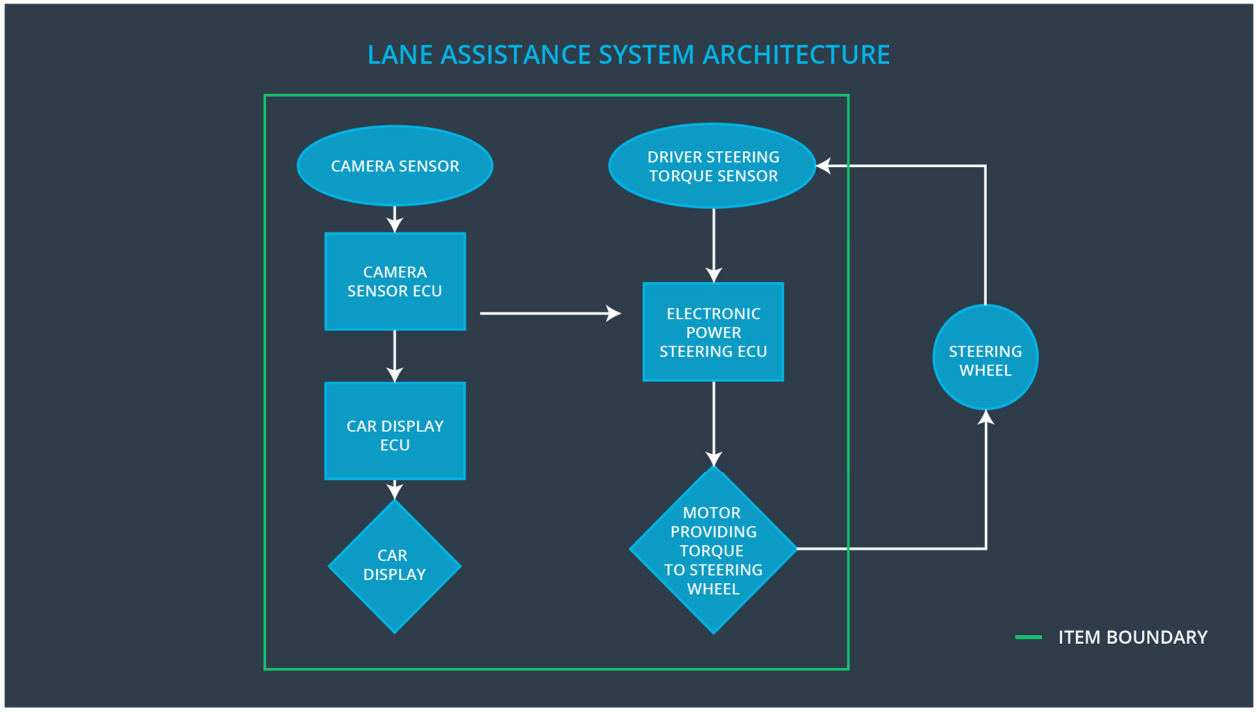
The Lane Assistance System is used to provide assistance to driver and help the driver keep driving in the lance center and alert driver when the vehicle is out of the lane.
The Lane Assistance System has two main functions:

- Lane Departure Warning – Functionality that vibrates the steering wheel when the driver drifts away from center by mistake
- Lane Keeping Assistance – Functionality that turns the steering wheel back towards the center of the lane if the driver starts to drift away from center

The Lane Assistance System contains below three subsystems:

- Camera Subsystem – Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake;
- Electronic Power Steering System – Actuator to provide steering torque to keep the vehicle in lane; Actuator to provide vibration torque to warn driver;
- Car Display System – Display the information to the customer

The steering wheel has interface with Electronic Power Steering System but not below to the Lane Assistance system.



Goals and Measures

Goals

The project goals are:

- Achieve functional safety compliance for Lane Assistance System;
- Provide HARA analysis and derive safety goal;
- Derive FSR and Finish the FSC;
- Derive TSR and Finish the TSC;
- Define HIS;
- Derive HSR and SSR

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety Auditor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

The function safety requires the organization to create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety. The organization will fail the functionality if the safety culture is bad. A good safety culture shall have below characteristics:

- The process assures that accountability for decisions related to functional safety is traceable;
- Safety is the highest priority;
- The reward system supports and motivates the effective achievement of functional safety;
- The reward system penalizes those who take shortcuts that jeopardize safety or quality;
- The process provides adequate checks and balances;
- Proactive attitude towards safety;
- The required resources are allocated;
- Continuous improvement is integral to all processes;
- A defined, traceable and controlled process is followed at all levels

Safety Lifecycle Tailoring

For the Lane Assistance project, below phases are in the scope of the safety lifecycle:

- Concept phase;
- Product Development at the System Level;
- Product Development at the Software Leve;

The below phases are out of the scope:

- Product Development at the Hardware Level;
- Production and Operation

Roles

Role	Org
Functional Safety Manager- Item Level	OEM
Functional Safety Engineer- Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager- Component Level	Tier-1
Functional Safety Engineer- Component Level	Tier-1
Functional Safety Auditor	OEM or external

Functional Safety Assessor	OEM or external

Development Interface Agreement

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.
The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

Activities and processes performed by OEM:

- Appointment of safety manager;
- Do item definition;
- Do HARA and derive safety goal;
- Lead DIA definition;
- Do safety audit for tier-1 supplier;

Activities and processes performed by tier-1 supplier:

- Appointment of safety manager;
- Realize the subsystem by the safety goal from OEM;
- Work with OEM for DIA;
- Do all the design work with safety compliance;
- Deliver safety case to OEM;
- Support the safety audit;

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

Confirmation review:
Ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

Functional safety audit:
Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Functional safety assessment:

Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.