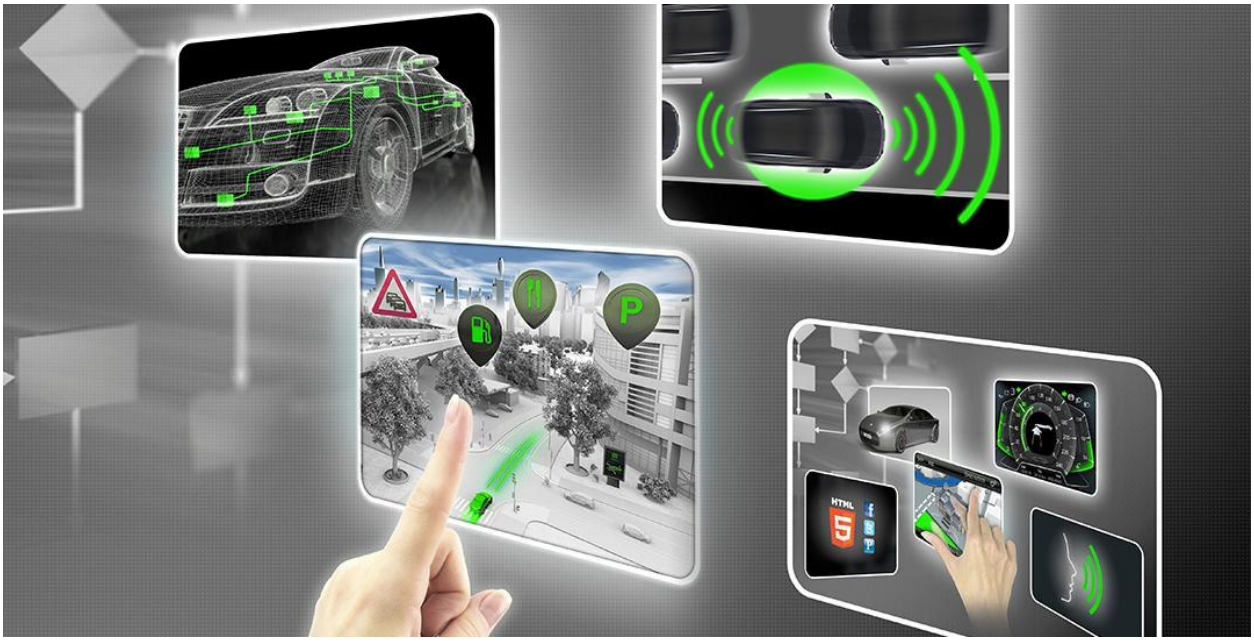
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0, Released 2018-07-01

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
06/30/18	1.0	Anand Mandapati	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

This Safety Plan provides a framework for the assurance of Functional Safety throughout the Lane Assistance System project through concept, development, production, and operation, according to ISO 26262 principles.

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

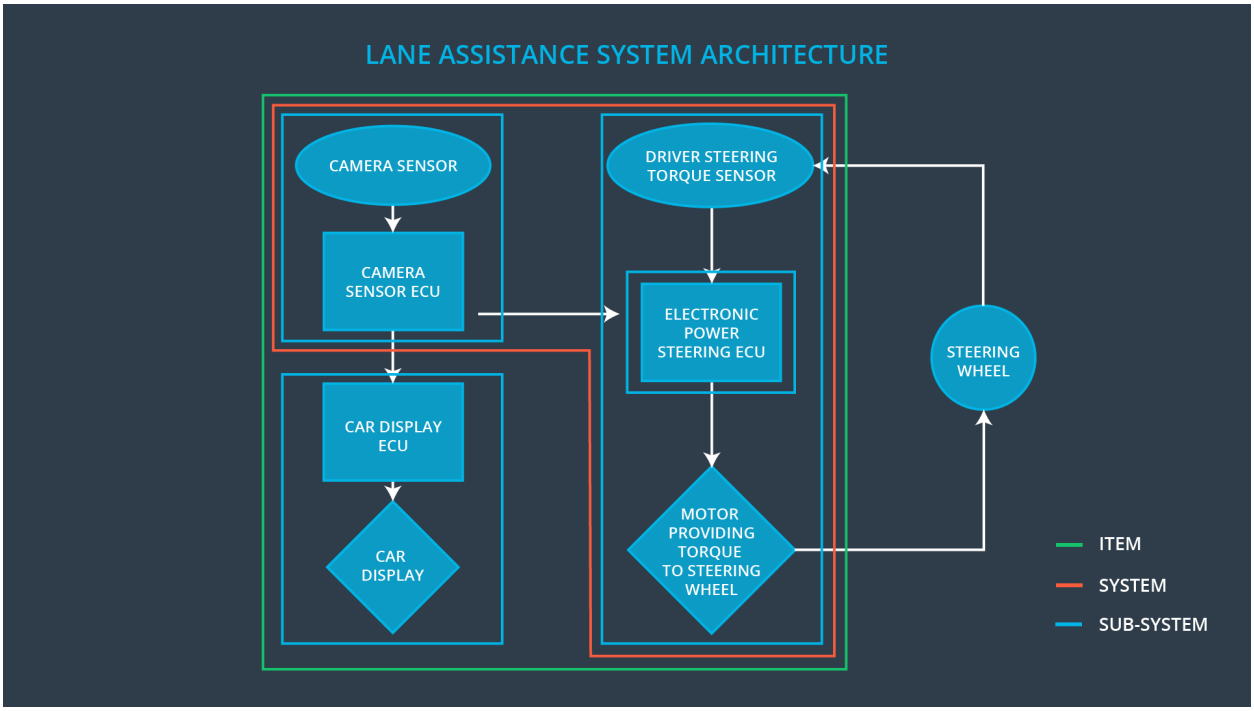
The deliverables of the project are:

Safety Plan
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Software Safety Requirements and Architecture

Item Definition

The item defined here is a simplified version of a Lane Assistance System, which is a type of Advanced Driver Assistance System (ADAS). The Lane Assistance System helps the vehicle's driver keep the vehicle centered in the ego lane by both warning about lane departures and augmenting driver control to remain within the lane. It consists of two main functions - Lane Departure Warning (LDW) and Lane Keeping Assistance (LKA).

The System consists of four Sub-Systems - the Camera Sensor, the Car Display, the Electronic Power Steering, and the Electronic Power Steering ECU. The architecture is described in the figure and text below.



- **Lane Departure Warning (LDW):** This function of the System detects lane lines using the Camera Sub-System, applies an oscillating torque to the steering wheel for haptic feedback when the vehicle departs the ego lane using the Electronic Power Steering Sub-System, and presents a warning light on the Car Display Sub-System.
- **Lane Keeping Assistance (LKA):** If the driver doesn't respond to the LDW, this function of the System adds steering torque to move the vehicle back to the center of the ego lane using the Electronic Power Steering Sub-System, and additionally provides a warning light on the Car Display Sub-System that it is doing this.

Goals and Measures

Goals

The goal of this Safety Plan is to analyze the functional safety case for the Lane Assistance System using the ISO 26262 principles. We identify scenarios of risk within or caused by the electrical and electronic components of the System, quantify the risk of those scenarios, and attempt to eliminate or reduce those risks to an acceptable level.

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

Our organization has the following characteristics of a good safety culture:

- **High priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be clearly defined
- **Resources:** projects have necessary resources including people with appropriate skills
- **Diversity:** intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

For the Lane Assistance System project, the following safety lifecycle phases are in scope:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

The following phases are out of 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

The Development Interface Agreement (DIA) defines the roles and responsibilities between companies involved in developing a product. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262. All involved parties need to agree on the contents of the DIA before the project begins.

Here are the responsibilities of each party to the DIA.

Organization	Responsibilities
OEM	• Manage the overall functional safety project • Plan, coordinate, develop the Lane Assistance System on item level • Provide information support to Tier 1 organization • Audit the functional safety of the System • Assess the functional safety of the System
Tier-1	• Plan, coordinate, and document the development phase of the safety lifecycle • Maintain the Safety Plan • Monitor progress against the safety plan • Perform pre-audits before the safety auditor • Develop, integrate, and test the required hardware and software changes to the System

Confirmation Measures

Confirmation measures serve two purposes:

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

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

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.