Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0. Released 2017-12-22

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/22/2017	1.0	Daniel Prado	Initial version.

Table of Contents

Introduction

Purpose of the Safety Plan

The present Functional Safety Plan provides a framework according to ISO 26262 for the Functional Safety assurance throughout the Lane Assistance System development project and in production. As a reminder, the ISO 26262 only covers functional safety of electronic and electrical systems.

Additionally, this document describes roles and responsibilities taking part in functional safety processes, scope and deliverables of the project from a functional safety perspective. The Safety Plan also lists the techniques, goals and measures that will be implemented.

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

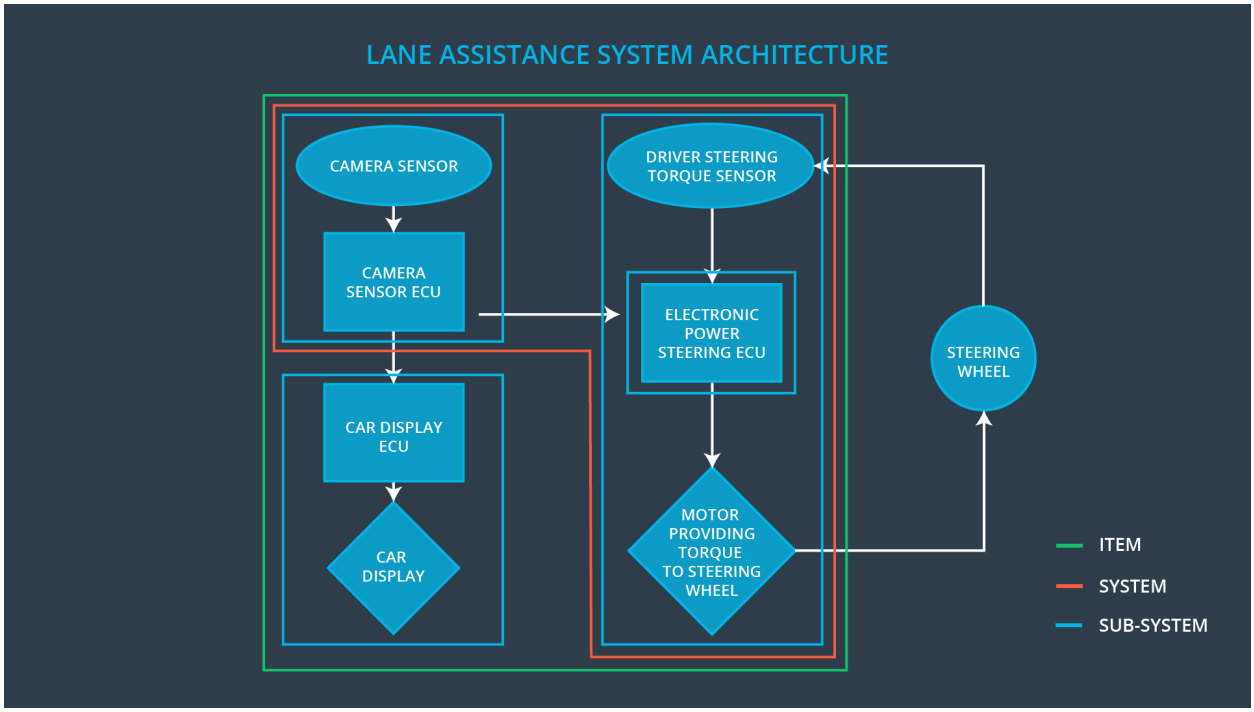
The deliverables of the project are:

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

Item Definition

The item defined is a simplified version of a Lane Assistance System, which is a type of ADAS (Advanced Driver Assistance System). The Lane Assistance System assists the driver of the vehicle to keep the vehicle centered in the current road lane. The criticality of the system derives from the fact that It can take over control from the driver in its purpose of keeping the vehicle in the lane.

The item high level architecture is displayed below showing the item boundaries as well as the boundaries of the subsystems it is composed of:



The Lane Assistance System has the following functionalities:

- **Lane Departure Warning (LDW)**:
  Description: The lane departure warning function applies an oscillating steering torque to provide the driver a haptic feedback.

- **Lane Keeping Assistance (LKA):**
  Description: The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane

The Lane Assistance System is decomposed into the following subsystems:

Camera Subsystem
The camera subsystem is responsible for detecting the lane and determining when the vehicle leaves the lane, sending a signal to the electronic power steering system asking to turn and vibrate the steering wheel. It also requests that a warning light turn on in the car display dashboard when the system is active.

Sub-System Car Display
The car display visualizes the warning signals to the driver related to the LDW and/or LKA functions of the Lane Assistance System system.

Sub-System Electronic Power Steering
The electronic power steering sub-system measures the driver's actual steering torque and process the lane-leaving information from the camera sub-system. The electronic power steering sub-system generates an oscillating steering torque to provide the driver a haptic feedback. It also adds extra steering torque to help the driver move backwards to the centre of the lane.

The steering wheel, throttle, and other vehicle propulsion systems are outside of the boundaries for this item.

Goals and Measures

Goals

The major goal of this project is to create a safety case for the Lane Assistance System that reduces risks to acceptable levels and eliminating unreasonable risks. Following the ISO 26262 provides a methodical, state-of-the-art framework for ensuring a safe electrical/electronic system.
In more detail, this major goal for the Lane Assistance Functional Safety Plan can be decomposed in the following goals:

- Identify situations of risk for the electrical and electronic parts of a tracking system, which could potentially result in physical damage to vehicle occupants.
- Analyse the risk level of those situations.
- Use system engineering methods to eliminate unreasonable risks and reduce 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

Social and organizational factors have an important influence too in the development and assurance of functional safety. Our organization has the 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

The following phases of V model included in the project scope are:

- Concept phase.
- Product development at system level.
- Product development at software level.

For this particular work it is out of the scope:

- Product development at 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 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.
The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities attribution among our Company (as a Tier-1 provider) and the OEM (Original Equipment Manufacturer) are detailed in the following table:

Organization	Responsibilities
OEM	• Manage the whole functional safety project • Plan, coordinate, develop the Lane Assistance System on item level • Provide information support to Tier 1 organization
Tier-1 (Our company)	• Plan, coordinate, develop the Lane Assistance System on subsystem level • Provide all contractual deliverables to OEM organization • Fix software safety issues on subsystem level

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.

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.