Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10/8/2018	1.0	John O'Shea	Initial Draft

Table of Contents

Document history

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

In general the purpose of a safety plan is to provide an overall framework for functional safety, and to provide roles and responsibilities for functional safety for each Item. In this case the identified item is a Lane Assistance system.

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:

1. Safety Plan
2. Hazard Analysis and Risk Assessment
3. Functional Safety Concept
4. Technical Safety Concept
5. Software Safety Requirements and Architecture

Item Definition

Discuss these key points about the system:
This project is focussed on a Lane Assistance System, which is a typically a key feature of an Advanced Driver Assistance System (ADAS).

What is the item in question, and what does the item do?
The item in question is a Lane Assistance system.

What are its two main functions? How do they work?
The Lane Assistance system will have two functions as follows:

1. Lane Departure Warning: This feature shall apply an oscillating steering torque to provide the driver a haptic feedback when the driver moves towards a lane line and indicator is not turned on.
2. Lane Keeping Asistance: This feature when activated shall apply the required steering wheel torque to turn the wheels to stay in the center of the ego lane.

Which subsystems are responsible for each function?
The sub-systems responsibile for each function are:

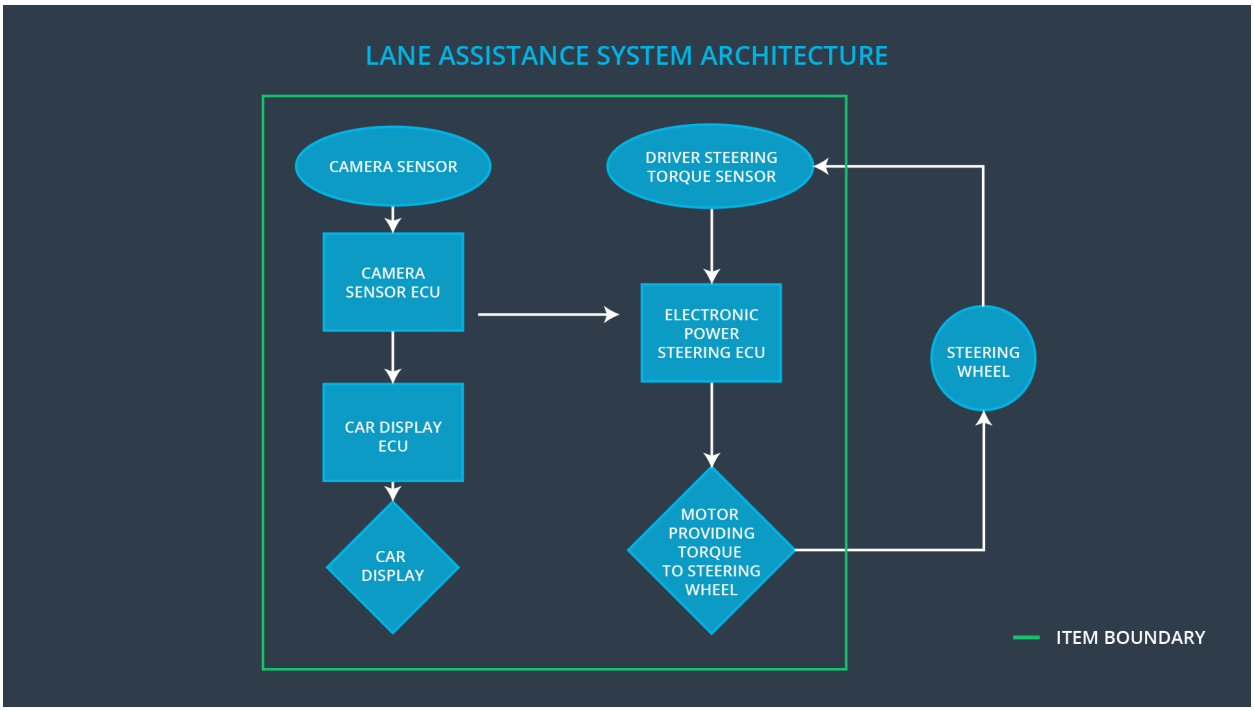
Camera Subsystem: The camera subsystem contains a camera sensor and a camera electronic control unit (ECU), and its role is to read the lane line position and send data about its relative posistion back to the ECU. The ECU will then make the determination if a lane line is crossed or about to be crossed and alerts the lane assistance subystem to take action.

Power Steering Subsystem: The power steering subsystem contains a power steering torque sensor, an electronic power steering ECU, and a power steering motor to turn the wheel.

Car Display Susbsystem: The car display subsystem contains a display ECU, and the display itself to alert the driver

What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?

The item boundaries of the lane assistance system are shown below with the green lines showing the item boundary.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Goals and Measures

Goals

Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]

The major goals of this project are:

1. Identify the hazards associated with the Lane Assistance system that would cause potential harm to all passengers and vehicles.
2. Minimize risks for each identified hazard
3. Identify the Roles and Responsibilities for each member of the functional safety team such that each member has clear and unambiguous roles.

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 Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture.

It is important to impose a good safety culture in order to make functional safety a success. Here are some 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

Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project.

The following phases are in scope for the Lane Assistance Project:

- Concept stage
- System/software development stages

The following phaeses are out of scope for Lane Assistance Project:

- Hardware development
- 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

1. **What is the purpose of a 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. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM?**

   The responsibilies of OEM vs TIER1 supplier is as follows:

   OEM:

   - Responsible for providing a working Lane Assistance system that meets the predefined functional safety specification agreed between the OEM and TIER-1 supplier.

   TIER-1

   - Integrates the Lane Assistance feature supplied by the OEM.
   - Responsible for ensuring all safety items meet the predefined functional safety specification agreed between the OEM and TIER-1 supplier.
   - Responsible for checking the feature against ISO26262 standards after integration.
   - Responsible for confirming that the new feature does not interfere with the existing components in the system.

Confirmation Measures

1. **What is the main purpose of confirmation measures?**
   The main purpose of confirmation measures are twofold:
   - that a functional safety project conforms to ISO 26262, and
   - that the safety measure put in place really do make the vehicle safer.

2. **What is a confirmation review?**
   The confirmation review is peformed by independent party with no project bias. The review will check that the project adheres to ISO 262262 standards.

3. **What is a functional safety audit?**
   A functional safety audit is need to ensure that :
   - Interim and final implementation meets all safety standards and requirements
   - Adheres to ISO262262 standards.

4. **What is a functional safety assessment?**
   A functional safety assessment is needed to ensure that the implementation increases functional safety over previous or existing implementation.