Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
15/05/2018	1.0	Ashith Raghunath	Compiled Safety Plan

Table of Contents

Introduction

Purpose of the Safety Plan

A safety plan is a document that specifies clearly the roles and responsibilities of individuals, and the methods and processes and best practices to be followed to ensure functional safety. To achieve this the document details steps such as clearly defining the system under consideration, the project timeline, the goals and measures of the project, various support processes and finally the confirmation measures adopted to prove that the functional safety has been achieved. This document defines the overall safety plan for the 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:

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

Item Definition

Here we consider a simplified version of the Lane Assistance System. The major functionalities of this item include:

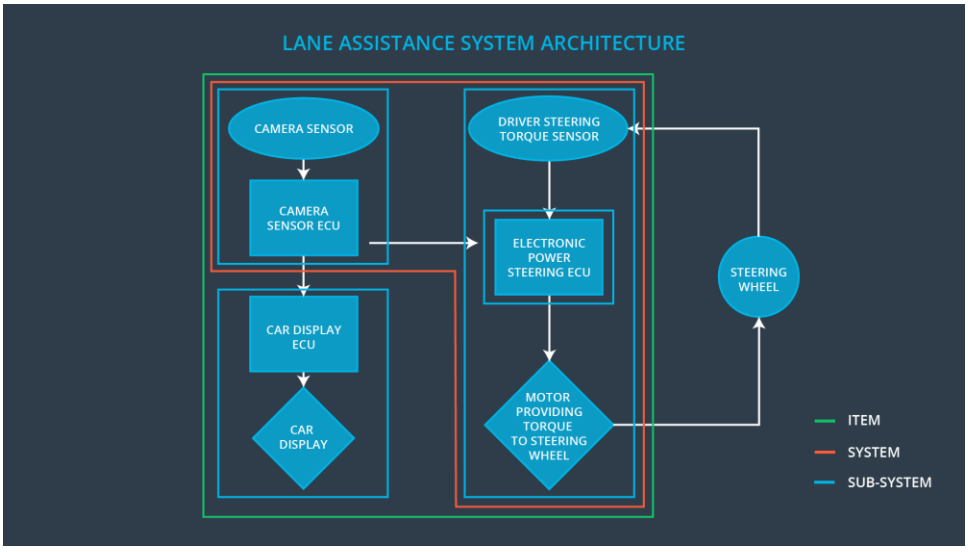
- **Lane departure Warning:** warns the driver by vibrating the steering wheel if the driver departs the lane without turning on the turn signals.
- **Lane keeping Assistance:** Keeps the vehicle centered on the current lane.

Formally the lane departure warning function can be described as “the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback” and the lane keeping assistance function can be described as” the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane”.

These functionalities are implemented using the following subsystems:

1. **The Camera Subsystem:**
   - **1.1. Camera Sensor:** A camera mounted on the car to capture the road ahead.
   - **1.2. Camera Sensor ECU:** contains the AI and logic to detect if the car is departing from a lane and provide feedback.
2. **The Car Display Subsystem:**
   - **2.1. Car Display ECU:** Takes input from the camera system and controls the display
   - **2.2. Car Display:** It displays a warning signal for lane departure or steering correction etc.
3. **The Electronic Power Steering Subsystem:**
   - **3.1. Drive Steering Torque Sensor:** This sensor is used to measure the torque already being applied to the steering wheel by the driver.
   - **3.2. Electronic Power Steering ECU:** takes input from the camera ECU and torque sensor and determines the amount of additional torque required to move the car to the center.
   - **3.3. Motor Providing Torque to Steering Wheel:** Applies the torque received from the ECU to the steering wheel.

The diagram below shows the various subsystems and its boundaries.



When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel. The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

Goals and Measures

Goals

The major goal of this project is to analyze the lane assistance functions with ISO 26262 and make sure that the Lane assistance system and its component subsystems work safely and reliably. To achieve this, we perform Hazard and Risk Analysis and come up with engineering requirements and safety goals that minimize the risk to acceptable levels.

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

Here are the characteristics followed by our company to ensure a good safety culture:

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

Safety Lifecycle Tailoring

For the lane assistance project since it is a new implementation and not a modification, the following safety lifecycle phases are in scope:

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

Since the hardware components development and production are not part of this project 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 DIA defines the roles and responsibilities between the OEM and the Tier-1 organization involved in developing the Lane Assistance System. Both 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 both parties are developing safe vehicles in compliance with ISO 26262.
The major sections of a DIA are:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Roles of the OEM:

- Item Level Safety plan and requirements engineering
- Overall Project management, Resource allocation and Product Development
- Appointment of Safety manager, Auditor and Assessor
- Ensure that the design and production implementation conform to the safety plan and ISO 26262.

- Judge as to whether functional safety is being achieved via a functional safety assessment

Roles of Tier-1(only for the components that need to be modified to confirm with safety standards):

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailors the safety lifecycle for the modified components
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

Confirmation Measures

Confirmation measures serve two main purposes:

1. Make sure that a functional safety project conforms to ISO 26262, and
2. 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 has to review the work to make sure ISO 26262 is being followed properly.
Functional safety audit is done to make sure that the actual implementation of the project conforms to the safety plan.
Functional safety assessment is done to confirm that plans, designs and developed products actually achieve functional safety.

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.