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	Akshatha Holla	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

A Safety plan outlines the steps taken to achieve functional safety. It includes defining the system under consideration, the goal of the project, the steps taken to ensure safety. It also defines the different roles of individuals and the project schedule plan. Further to this it also ensures confirmation measures such as reports that are prepared to confirm that safety has been achieved.

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

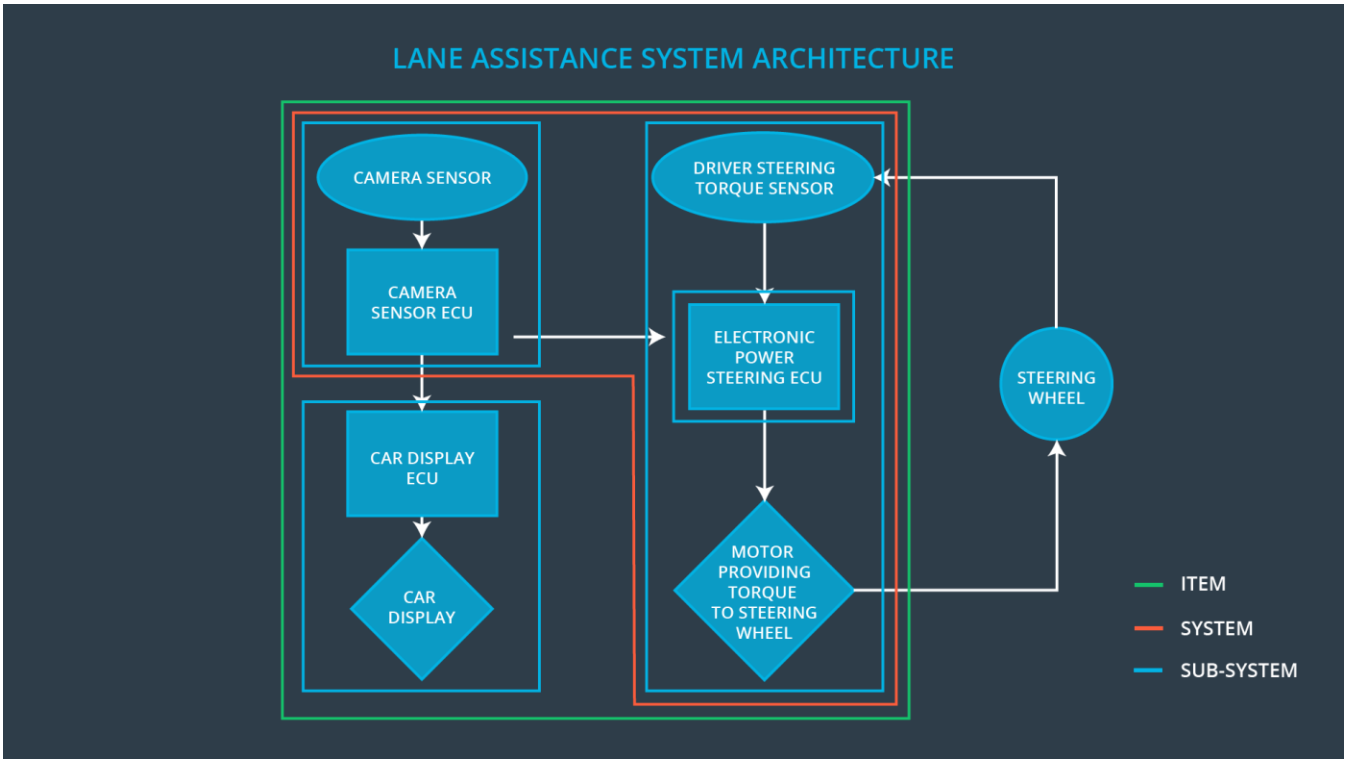
Item Definition

The item under consideration here is a simple Lane assistance system. The two major functionalities of the lane assistance system are:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning system identifies lanes using the camera sensors and vibrates the steering wheel to warn the driver if the change in lane was unintentional (ie. Happens suddenly without any signals).

The Lane keeping assistance functionality assists the driver by turning the steering wheel to turn towards the center of the lane to ensure that the vehicle stays in the ego lane.



The visualization of the various systems, subsystems and their boundaries can be seen in the image shown above.

The system consists of 3 subsystems:

- The Camera subsystem:
    1. The Camera sensor- Detects lane departures
    2. The camera ECU- has the hardware and software required for deep learning or for computer vision techniques like the Hough transform.
- The Car display subsystem:
    1. The Car display ECU- Contains software that controls the car display used to relay information to the driver.
    2. The Car display – Displays warnings when there is unplanned or sudden lane change and other such information.
- The Electronic power steering subsystem:
    1. Driver steering torque system
    2. Electronic power steering ECU- Supplies signals to the motor to add torque to the steering wheel to ensure turns towards the center of the lane.
    3. Motor- provides calculated torque to the steering wheel.

Goals and Measures

Goals

The goal of this project is to check whether the lane assistance system under consideration adheres to the ISO 26262 standard. Here we perform situational analysis and hazard identification to identify and classify all possible risks at system and subsystem level and come up with safety goals based on the hazard analysis and risk assessment. This is further translated to engineering requirements which are applied to reduce the risks at all levels of the system.

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	Safety Manager	3 months prior to main assessment

external functional safety assessor		
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

These are few of the characteristics of a good safety culture for a company:

- 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 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

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 which in this case would be the OEM which provides the lane assistance system and our company (Tier 1) which would analyze the system from functional safety viewpoint. 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 of the OEM would be:

- Overall project management
- Acquiring and allocation of resources needed for the functional safety activities
- Appoints safety manager, auditor and assessor and system level safety engineer
- Does product development, safety management for the entire lane assistance system
- Ensures that the design and production implementation conform to the safety plan and ISO 26262.
- Independent judgement as to whether functional safety is being achieved via a functional safety assessment

The Responsibilities of our (Tier 1) company would be

- Planning, coordinating and documenting of the development phase of the safety lifecycle for the particular component which is modified.
- Tailoring the safety lifecycle according to the changes in the component
- Maintaining the safety plan
- Product development and subsystem change implementation
- Monitoring progress against the safety plan
- Integration
- Testing at the hardware, software and system levels
- Performing pre-audits before the safety auditor

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.