Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

TemplateVersion 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-12-21	1.0	Nick Fiege	Let’s get going

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan will provide the framework for the lane assistent item and it defines the roles and responsibilities of the team working on this item.

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:

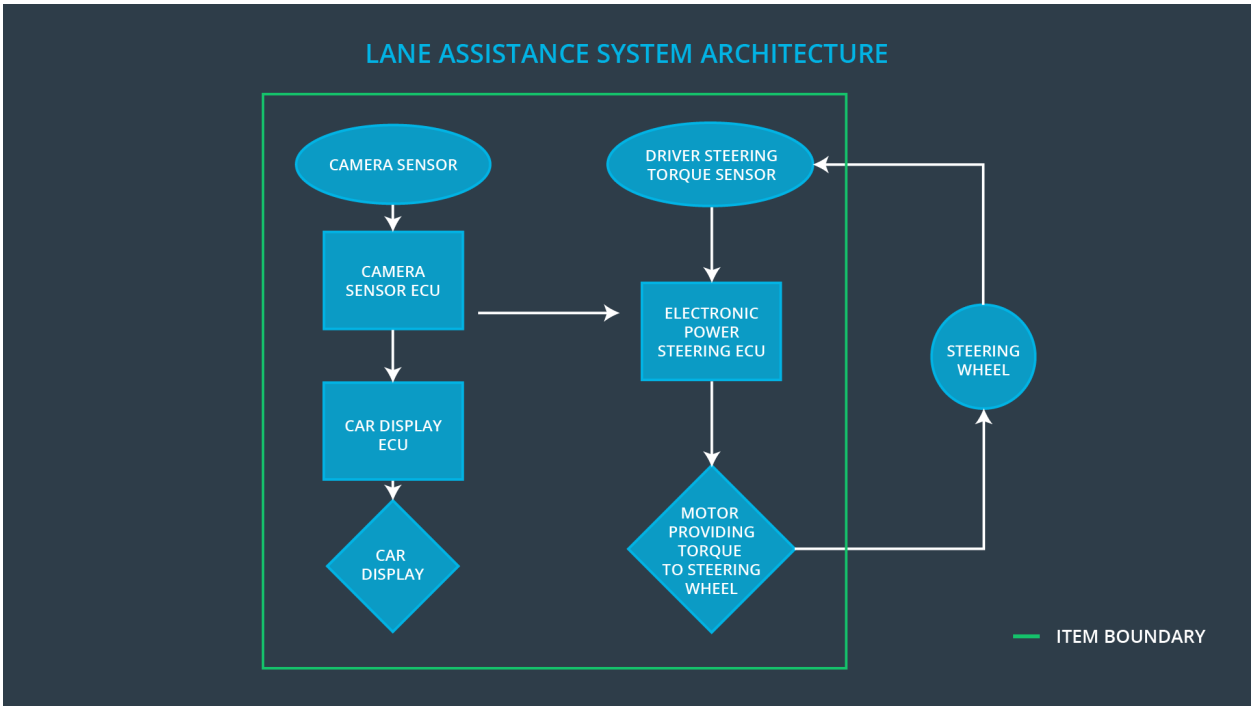
- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

Item Definition

The item under analysis is a simple lane assistance system. This system helps the driver to keep the current lane while driving on a road with standard lane markings.
The two components of the lane assistance item are:

- **Lane departure warning function**
  - When the driver maneuvers out of the current lane, the system moves the steering wheel back and forth to create a vibration to alert the driver.
- **Lane keeping assistance function**
  - When the driver maneuvers to far away from the center of the lane, the system will steer the wheel in a way, that will maneuver the car back to the center of the current lane.

The system is deactivated by using the turn signal. By doing so, the driver indicates that the current lane-change is voluntary. In order to completely turn off the system, the driver can deactivate it with a button on the dashboard.



This system consists of 3 sub-systems:

- **Camera subsystem**
  - Input sensor, which detects lane boundarys and vehicle odometry.
- **Electronic Power Steering subsystem**

    - Actuator, which
        - Generates the steering wheel vibration for the warning functionality
        - Generate the steering wheel torque for the lane keeping functionality
- **Car display subsystem**
    - Warning light, to indicate that the assistance system is active and functional.

This system is not intended to run autonomously. The driver is expected to have both hands on the steering wheel at all times. The lane keeping assistant will therefore detect the torque already exerted by the driver and will only supply the extra torque required to stay inside the lane boundaries.

Goals and Measures

Goals

This analysis will describe the safety and reliability of the automotive systems required for the lane assistance item, therefore the following steps will be executed and documented:

- Identifying potential problems, which could injure people or damage peoples health. These are called hazards.
- Evaluate the risks of the hazards.
- Use systems engineering to lower the risks 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

- **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 are independent from the teams who audit the work
- **Well defined processes**: 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**: communication channels encourage disclosure of problems

The organization has a quality management system in place that complies with quality management standard ISO 9001.

Safety Lifecycle Tailoring

The project describes the development of a new product, so the following steps have to be researched and executed to ensure functional safety:

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

This project does not include hardware or the production phases, therefore the following phases are left out:

- 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. 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:

- 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

Everybody on a team would ultimately be responsible for following safety processes no matter their role in the company. Creating and sustaining a safety culture would also be everybody's responsibility; however, if you were a safety manager, then you would be especially interested in ensuring a safety oriented workplace.

Project Manager

- Overall project management
- Acquires and allocates resources needed for the functional safety activities
- Appoints safety manager or might act as safety manager

Safety Manager

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

Safety Engineer

- Product development
- Integration
- Testing at the hardware, software and system levels

Safety Auditor

- Ensures that the design and production implementation conform to the safety plan and ISO 26262.
- Must be independent from the team developing the project

Safety Assessor

- Independent judgement as to whether functional safety is being achieved via a functional safety assessment
- Must be independent from the team developing the project

Test Manager

- Plans testing activities
- Coordinates testing to show that the vehicle system works correctly

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.