Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018.06.06	1.0	Frank . W	First version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of safety plan is to provide an overall framework for functional safety and to assign roles and responsibilities for functional safety of 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

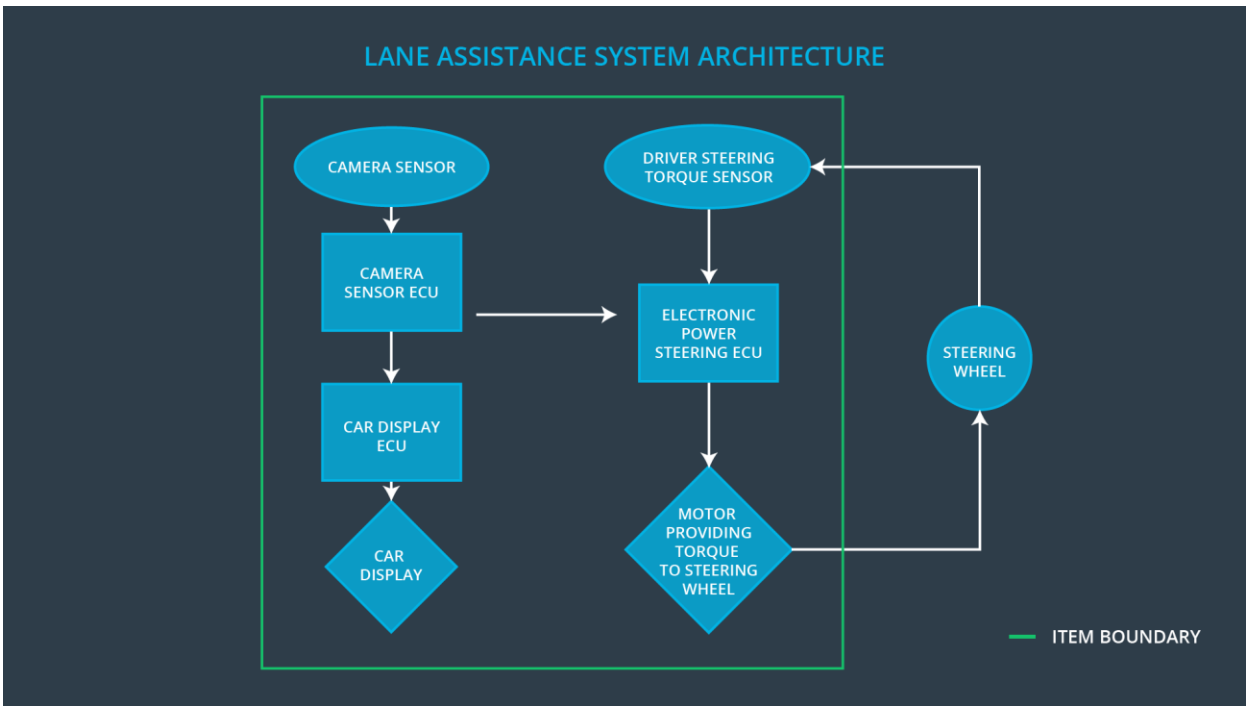
The deliverables of the project are:

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

Item Definition

The lane assistance item is used to help drivers to keep vehicles in a certain lane. The system uses a camera to identify the lane boundaries. When the system detects a small distance between vehicles and lane lines unintentionally, it will alert the driver and try to keep vehicles in current lane.

The Lane Assistance System will have two functions:
(1) Lane departure warning
When camera detects a small distance between vehicles and lane lines, this function shall apply an oscillating steering torque to provide the driver a haptic feedback.
(2) Lane keeping assistance
When camera detects a small distance between vehicles and lane lines, this function shall apply the steering torque when active in order to stay in ego lane.



We can see from the above picture that the item boundary was drawn to include three sub-systems:
(1) Camera system;
(2) Electronic Power Steering system;
(3) Car Display system.

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.

Goals and Measures

Goals

The goal of the project is that according to ISO26262 standard, finding the possible risk of the lane assistance item, and assessing the ASIL level of the risk, then taking the system engineering measures to reduce the risk to the 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

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

According to requirement of the project, the ISO 26262 standard process has been tailored.
The following phases are in scope:
(1) Concept phase;
(2) Product Development at the System Level;
(3) Product Development at the Software Level.
The following phases are out of scope:
(1) Product Development at the Hardware Level;
(2) 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.

In this project, the responsibilities of the OEM are listed as the following:
(1) appointing a safety manager;
(2) supplying the functional requirements to Tier-1;
(3) supplying the hazards and risks analysis to Tier-1;
(4) tailoring of the safety lifecycle with Tier-1;
(5) arranging safety audits;
(6) arranging final safety assessment.
The responsibilities for the Tier-1 are listed as the following:
(1) appointing a safety manager;
(2) tailoring of the safety lifecycle with OEM;
(3) analyzing and implementing the functional requirements;
(4) analyzing and implementing the functional safety requirements;
(5) supplying the final product to OEM on schedule.

Confirmation Measures

Confirmation measures serve two purposes:
(1) ensure that a functional safety project conforms to ISO 26262;
(2) ensure that project really does make the vehicle safer.

Confirmation Measures Definitions
(1) 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.
(2) 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.
(3) 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.