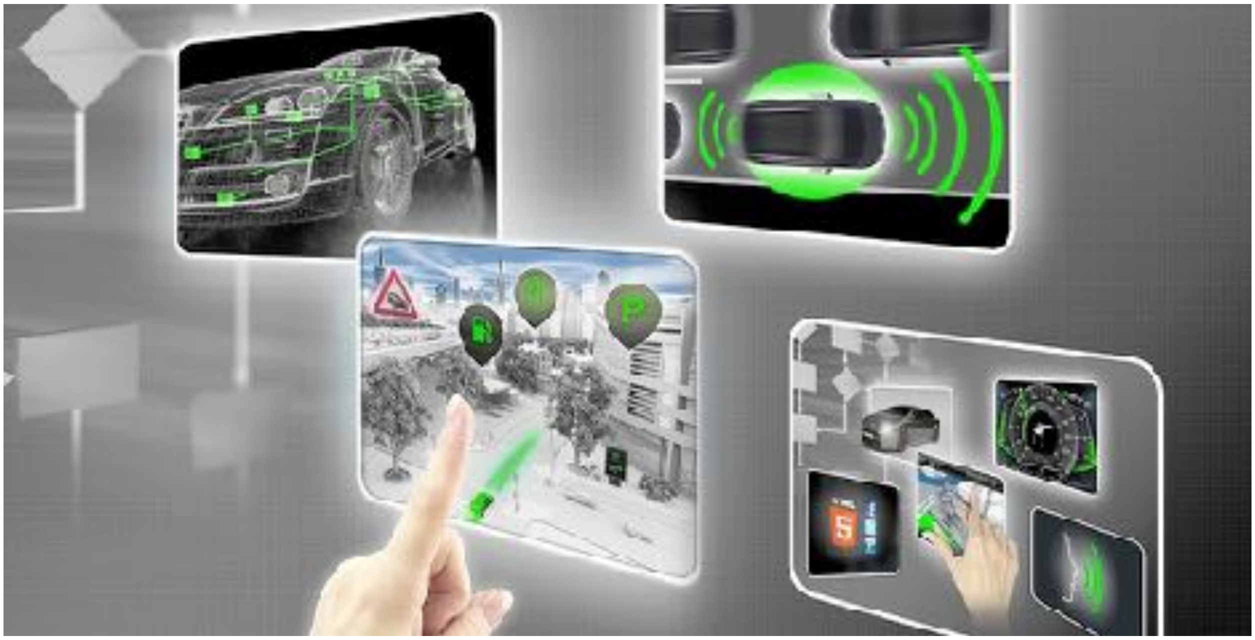
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
Feb 19-21, 2017	1.0	Pages	Filled out the template while watching class

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

A safety plan provides a documentation of an organization's process for ensuring it is has a safety culture in place and all proper protocols are followed. This is especially useful for when an independent audit is being performed or an accident has happened in the field (leading to a lawsuit) and is in fact required by ISO 26262. This safety plan serves as proof that safety is followed at the organization and documents the decisions and processes that were followed. In addition, this provides an easy starting point when making modifications to a system, such as upgrading to a newer version of a part. Finally, the safety plan helps to design the document by forcing one to think through the required design in advance and identify any gaps.

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

What is the item in question, and what does the item do?

> **The item this safety plan covers is the Lane Assistance Item. It is a "system" because it has a control, an actuator and sensors, but we will refer to it as "item" to avoid confusion when talking about 'sub-systems'.**

What are its two main functions? How do they work?

The item has two main functions, which are to:

1. **Alert the driver when the car is drifting from it's 'ego' lane (i.e., the lane that car that the system is installed on is in). This is done by showing a symbol on the dashboard and vibrating the steering wheel.**
2. **If the car continues to drive without driver action, corrective action is applied to the steering wheel to keep the car in the center of its ego lane. If the driver actually desires to turn lanes they should signal (like all drivers should) or they may turn off the item from a button provided not he dashboard.**

Which subsystems are responsible for each function?

1. **For function 1 (lane departure warning), the camera subsystem has a sensor and ECU that is responsible for detecting a lane departure. The warning has two subsystems, where are the car display (dashboard light indicator, and an ECU to control it) and the Electronic Power Steering ECU, which will vibrate the wheel.**
2. **For function 2 (lane keeping), the camera subsystem will provide guidance as to which direction to turn the car toward to keep in the center of the lane. And the electronic power steering subsystem will be responsible for applying the correct torque (going against a driver's torque using a sensor to measure it) to keep the car in the lane.**

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

> **The item encompasses the subsystems as mentioned before, which include the camera subsystem, the electronic power steering ECU and motor wheel torque and torque sensor components and the car display eco (at least the portion that displays the lane-warning sign). The steering wheel itself is considered external to the item as is the rest of the car.**

Goals and Measures

Goals

The main purpose of this project is to get a taste of what it is like to be a functional safety manager and some of the definitions and processes involved with ISO 26262. By working on these projects, we'll become familiar with the 'left-hand side' of the 'V' that is the general outline of the ISO 26262 process, primarily working on designing. Even though most of this course focused on software development, an engineer working on self-driving cars will probably be a part of this process and so should be aware of this to be able to get up to speed faster.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members, but especially the Safety Manager	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

A Safety Culture has a lot of characteristics, which are meant to emphasize that this is not just about ‘checking off some boxes’ to fulfill ISO-26262, but in my opinion, seem hard to instill in a culture. But that is exactly why a Safety Culture involves providing incentives, rewards for good behavior and penalizes bad behavior that jeopardizes safety. For leadership to have good communication, that is vital in order to make it clear to everyone that safety is the highest priority, whereas providing the resources, well defined processes and accountability help to ensure that safety is accounted for. Finally, diversity of thought is critical and has a role with the safety assessor, who must explicitly be separate from the team implementing something.

Safety Lifecycle Tailoring

This Safety Plan takes into account the Concept phase, the Product Development at the System Level and Product Development at the Software Level. What is out of scope are the Product Development at the Hardware Level and the Production and Operation phase.

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. **A development interface agreement is essentially a contract, in the actual legal term, between two parties that defines, as any good legal contract must, the roles and responsibilities of the parties involved in the contract. In this case, the contract is between an OEM and a Tier-1 parts supplier and clearly defines what each must do and the evidence to be documented for completion. The contract must also explicitly follow the process of ISO-26262 to help ensure a safe vehicle is provided to the general consuming public.**

2. **What will be the responsibilities of your company versus the responsibilities of the OEM?**
    B. **To start off, the Tier-1 company I am working for in this theoretical situation needs to appoint a safety manager and tailor the safety lifecycle jointly with the OEM. Given we're working on the component level, there is at least a safety manger and safety engineer. The safety manager has many responsibilities, as outlined in the "measures" sections, such as performing pre-audits of safety plan checks, tailoring the safety lifecycle and monitoring the progress of the project against the safety plan. The safety engineer does the main product development, integration and testing at the hardware and software system levels.**

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures? There are two main purposes of this and they must be explicitly outlined in any good Safety Plan following ISO-26262 standards. One reason is to ensure the project really does make the vehicle safer, and the other reason has already been mentioned: it must be required as part of ISO-26262.**

2. **What is a confirmation review? This is a review done by an independent safety assessor to make sure that ISO-26262 is being followed.**

3. **What is a functional safety audit? This is making sure that the project is conforming to the Safety Plan.**

4. **What is a functional safety assessment? This is a formal assessment of the plans, designs and end products that has the overall question: is this making things safer?**

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.