Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
03/10/18	1.0	Franz Pucher	First attempt

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]

Before analyzing a system under ISO 26262, a company needs to create a safety plan. A safety plan provides an overall framework for a functional safety project. This is a task often performed by a functional safety manager. In the plan, the manager defines roles and responsibilities to avoid missing important design steps. Therefore, the safety plan outlines the required steps to achieve functional safety.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions:

REQUIRED

Discuss these key points about the system:

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

This documents a safety case for the lane assistance item.
When the driver drifts towards the edge of the lane, two things will happen:

- the lane departure warning function will vibrate the steering wheel
- the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

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

The Lane Assistance System will have two functions:

1. **The lane departure warning** function shall apply an oscillating steering torque to provide the driver a haptic feedback." In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration.
2. **The lane keeping assistance** functionality will automatically assist the driver; the steering wheel turns towards the center of the lane. More formally "the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

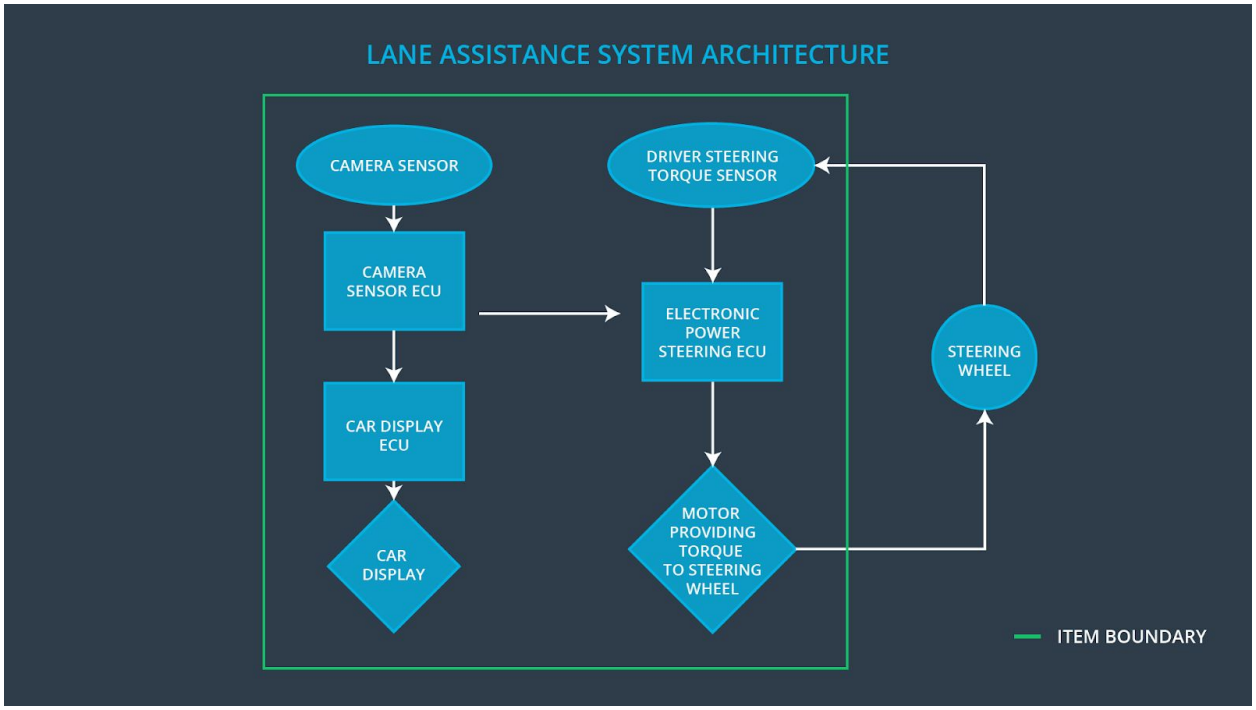
Which subsystems are responsible for each function?

The Lane Assistance item consist of the following subsystems with their responsible functions, also shown in the figure below (source Udacity):

1. **Camera Subsystem:** responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Consists of the camera sensor itself and its ECU.
2. **Electronic Power Steering Subsystem:** responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane

assistance system torque request. It relies on a driver steering torque sensor and the motor providing torque to the steering wheel.

3. **Steering Wheel Motor:** Provides a torque to the steering wheel in order to warn the driver by vibrating slightly. Additionally a corrective course to the center of the lane can be achieved through this motor.
4. **Car Display:** Consists of a display and its ECU. This subsystem signals an active lane assistance item and in case of warnings. When the driver is leaving the lane without using the indicator a warning is displayed.
5. **Lane Departure Warning:** Functionality that vibrates the steering wheel, through the motor providing the torque to the steering wheel, when the driver drifts away from center by mistake.
6. **Lane Keeping Assistance:** Functionality that turns the steering wheel back towards the center of the lane if the driver starts to drift away from center. This function is also accomplished by the steering wheel motor subsystem, which providing the torque to the steering wheel.



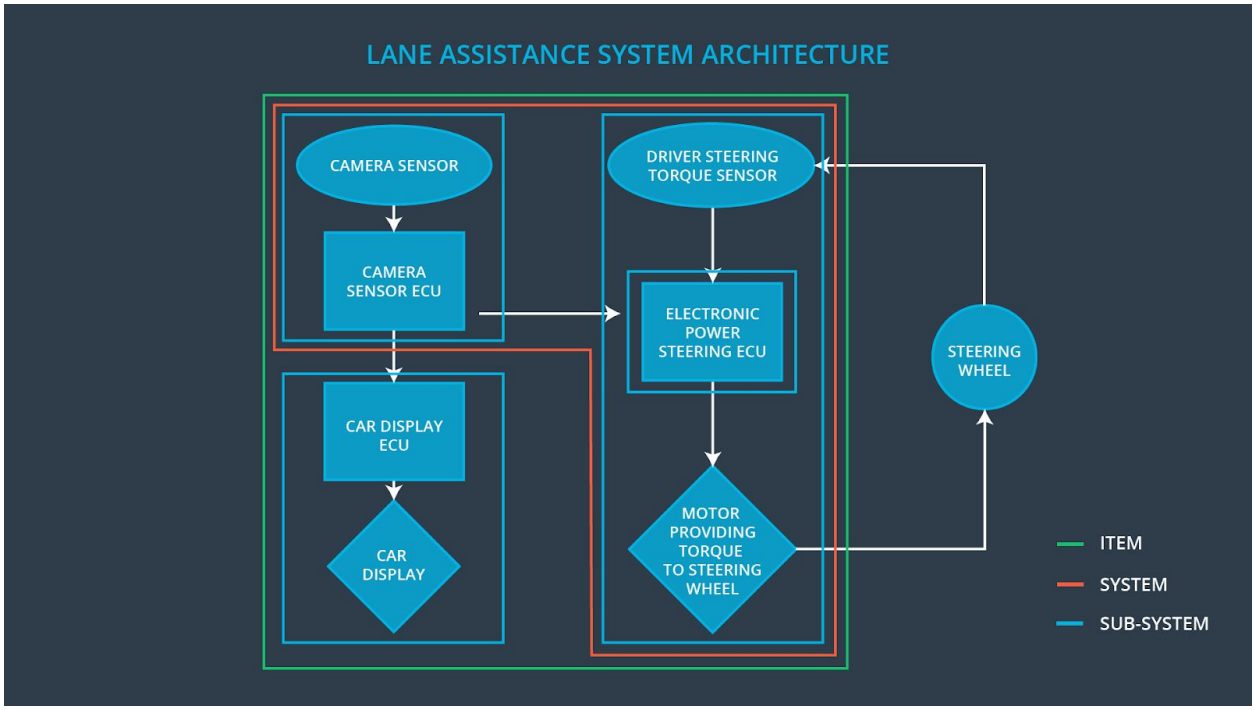
When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.

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.

What if the driver wants to leave the lane? 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.

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



The boundary of the lane assistance item are shown by the green frame in the figure above (source Udacity).

Inside:
Camera, Camera Sensor ECU, Car Display ECU, Car Display, Driver Steering Torque Sensor, Electronic Power Steering ECU, Motor Providing Torque To Steering Wheel, Indicator,

Outside:
Steering Wheel, Motor ECU, …

OPTIONAL
Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**

The item operates best under good weather conditions due to the camera detecting the lane lines. However, it is not limited to those environmental conditions but affected by snow, fog. Low staying sun can lead to bright camera images which can lead to problems as well as too dark conditions.

- **Legal requirements in your country for lane assistance technology**

Currently the driver needs to always supervise a lane assistance item. Often the driver is requrie to prove activeness by having its hands on the steering wheel after the item provides a corresponding signals.

- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

]

Goals and Measures

Goals

[Instructions:
Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]

The goal of functional safety is to reduce risks to acceptable levels. Where the acceptance level is defined by society.

Measures

[Instructions:
Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.

The options are:
All Team Members
Safety Manager
Project Manager
Safety Auditor
Safety Assessor
]

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 Assessor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

[Instructions:
Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture
]

Good Safety Culture

Here are some characteristics of a good 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

Quality Management

ISO 26262 does not cover quality management directly; however, quality management is a required part of safety culture.

Organizations need to have a quality management system in place that complies with quality management standards such as ISO/TS 16949 (replaced in 2016 by IATF 16949 or ISO 9001.

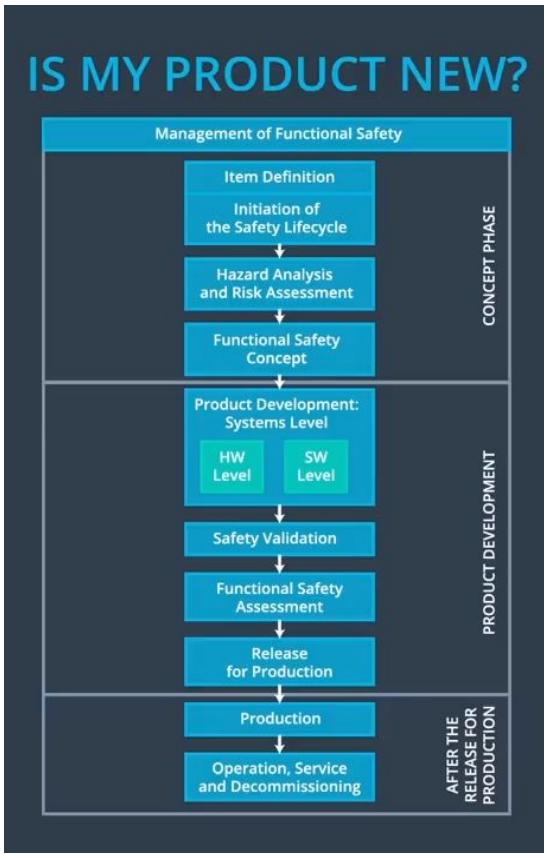
Safety Lifecycle Tailoring

[Instructions:
Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document
]

For the lane assistance project, the following safety lifecycle phases are in scope (see also the figure below - source Udacity):

1. Concept phase:
    a. Item Definition

    b. Initiation of the Safety Lifecycle
    c. Hazard Analysis and Risk Assessment
    d. Functional Safety Concept
2. Product Development at the System Level
   Product Development at the Software Level



The following phases are out of scope:

1. Product Development at the Hardware Level
2. Production and Operation, Service and Decommissioning

Roles

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.
]

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

[Instructions:
Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Please answer the following questions:

1. **What is the purpose of a 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, delineates the design and production responsibilities between the OEM and the Tier 1 supplier, or the Tier 1 supplier and the Tier 2 supplier.

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. If a vehicle has a safety issue after being sold to consumers, a Development Interface Agreement provides clarity about which company is best positioned to fix the system.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

The automotive supply chain is generally divided into three players: OEMs, Tier 1 suppliers, and Tier 2 suppliers. OEM stands for, Original Equipment Manufacturer which sell cars to consumers, but OEMs do not necessarily develop all of their vehicle systems in-house. OEMs outsource some development to what are called Tier 1 suppliers. The OEM and Tier 1 supplier, then take on a customer supplier relationship. The OEM might provide requirements for what a vehicle system needs to do and then, the Tier 1 supplier develops and produces the system for the OEM. Or, the OEM might provide a preliminary product design and then, the Tier 1 will finish the details. Tier 1 companies, oftentimes outsource their own work to Tier 2 companies. In this project, the OEM is supplying a functioning lane assistance system and a Tier 1 company that is specialized on functional safety analyzes and modifies the various sub-systems to meet the standards of ISO 26262. The safety assessment could then be done by a Tier 2 company.
]

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of 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. For example, the department or company who develops a Hazard Analysis and Risk Assessment (HARA) needs to be completely separate from the department or company who makes sure the HARA was carried out according to ISO 26262. That's because HARA is the critical first step in identifying high risk situations.

2. **What is a 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.

3. **What is a 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.

4. **What is a 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.