Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version 1.0]

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
2019-02-24	1.0	Harrison Hou	Initial version
2019-03-02	1.1	Harrison Hou	Update the document according to the guidance video in the project: - Update the purpose of the safety plan - Item Definition

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]

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]
A safety plan provides an overall framework for a functional safety project.
The purpose of the safety plan is to:

- Define how to promote the good safety culture to achieve functional safety within the project;
- Tailor the safety lifecycle based on whether the product is new or a modification;
- Define the major roles and responsibilities in functional safety;
- Define the Development Interface Agreement between OEM and Tier1 supplier or Tier1 supplier and Tier2 supplier to avoid dispute and clear liability;
- Define what specific confirmation measures will be used.

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?

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

Which subsystems are responsible for each function?

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

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**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

]
For the functional safety, we are going to look at a Lane Assistance System. It is an Advanced Driver Assistance System (ADAS) function. Like all the other ADAS systems, it will have two main functions:

- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

And the item contains three subsystems:

- Camera system
- Electronic Power Steering system
- Car Display system

The two functions mean that when the driver drifts towards the edge of the lane, two things will happen:

1. The lane departure warning function will vibrate the steering wheel;

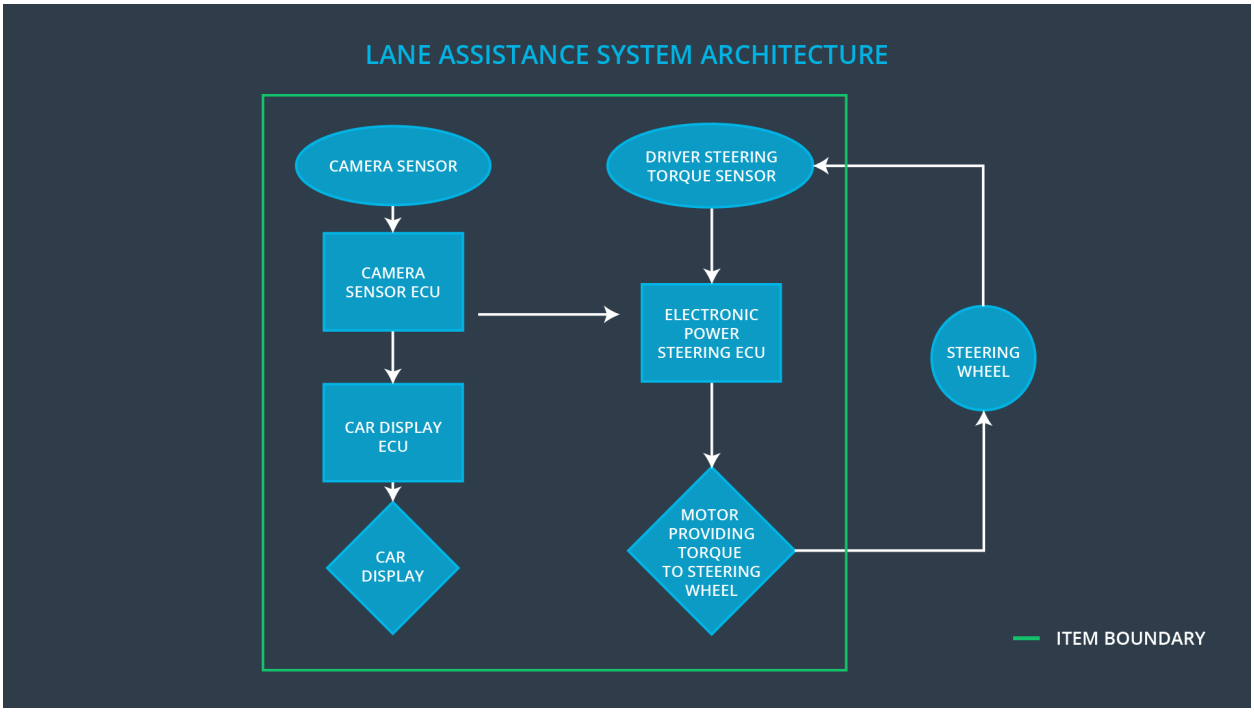
2. The lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

To state the lane departure warning engineering requirement more formally: "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.

To state the lane assistance functionality engineering requirement 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.

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.
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.

To know the boundaries of the item, please check the Lane Assistance System Architecture below:



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 major goal of this project is to reduce the risk of one or more hazardous events of Lane Assistance System to a tolerable level, Automotive Safety Integrity Level.

By analyzing the lane assistance functions with ISO 26262, we can
1. Conduct a situational analysis
2. Identify malfunctions
3. Combine situations and malfunctions and assess risk
4. Determine ASILs
5. Derive safety goals
6. Get functional safety concept
7. Get technical safety concept
8. Get hardware and software safety requirements

Finally, we can implement all the safety related requirements to reduce the system function risk to a tolerable level.

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 Manager	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
]

Because technology malfunctions are not the only source of vehicle accidents. Social and organizational factors are also main sources. People are the ones to make decisions. So the company should define develop clear policies and strategies to support functional safety activities. We need a good safety culture to achieve and functional safety goal.

Here are some characteristics of the 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

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:

Concept phase
- Item Definition
- Initiation of the Safety Lifecycle
- Hazard Analysis and Risk Assessment
- Functional Safety Concept

Product Development at the System Level
Product Development at the Software Level
Safety Validation
Functional Safety Assessment
Release for Production

The following phases are out of scope:

Product Development at the Hardware Level
Production
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?**

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 purpose of a DIA is to avoid disputes, define liability and makes clear who should fix safety issues.

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.

Here are major sections of a DIA:

- 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

The OEM will provide the requirements of what the lane assistance system needs to do from the car view of point and then we will analyze all the system requirements from the system view of point and then develop and produce the system for OEM. OEM needs to provide the preliminary product design and then we finish all the details to finish the development.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

]
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 Measures Definition
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 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.