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
3/10/2018	0.5	Tan Wang	First Draft
3/19/2018	1.0	Tan Wang	Added boundary diagram

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?]

The purpose of the safety plan is to thoroughly assess the potential hazards and risks of lane assistance system, and determines the best measures and practices to reduce the risk to acceptable levels.

In addition, ISO 26262 requires independent audits. This plan provides detailed safety analyses and proposed practices for the lane assistance system, which would provide enough information to auditors for safety assessment.

This document also provides important information about safety standards and practices for modifications of the system or integrations of the system to future car models.

This document also serves as a sound proof about how the system was designed and tested for future government inquiries or lawsuits.

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 is a functional safety plan for a lane assistance system. Lane assistance system reminds and helps drivers to maintain their cars in lane when it determines the car is out of the lane by mistake.

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

The two functions are lane departure warning and lane keep assistance.

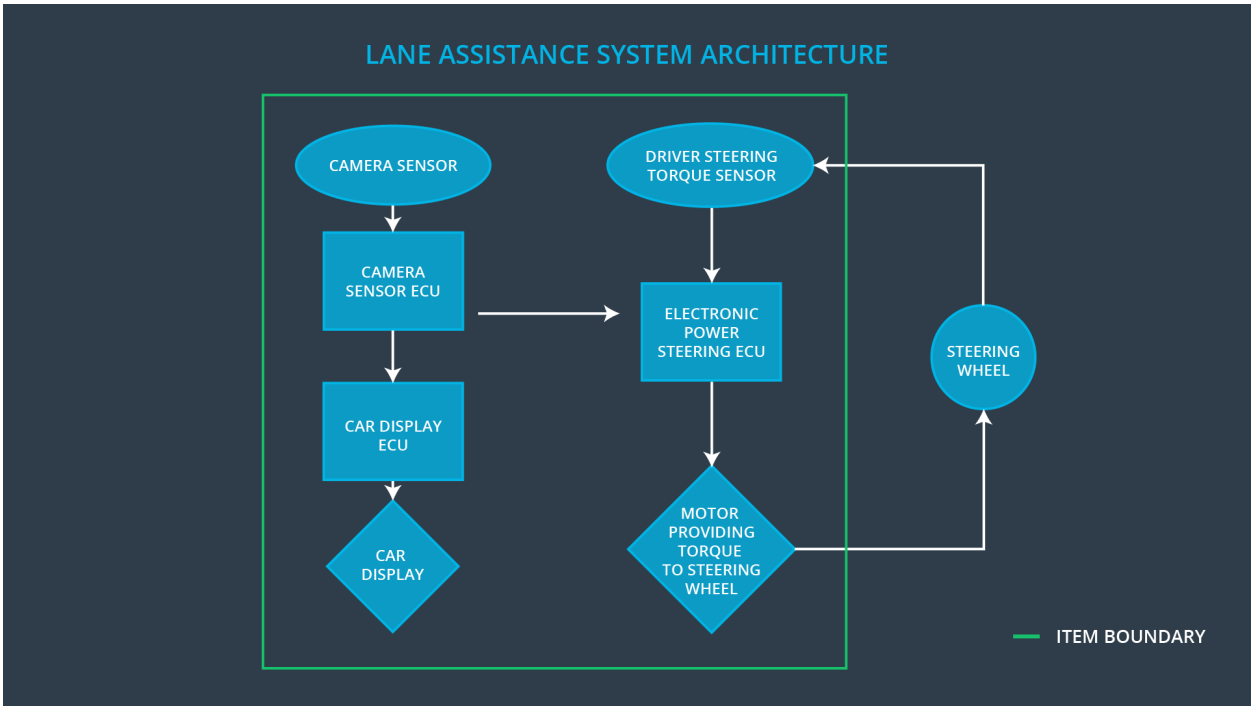
- **Lane departure warning: When the lane assistance system detects the car drifts towards the edge of the lane, the lane assistance system will vibrate the steering wheel**
- **Lane keep assistance: It will also move the steering wheel to the correct direction so that the car could be back to the center of the lane**

Which subsystems are responsible for each function?

There are three subsystems:

- **Camera Sensor: Responsible for detecting lane lines and determining when the car leaves the lane by mistake**
- **Car Display: Responsible to display warning messages to drivers when the camera sensor detects the car leaves the lane by mistake**
- **Electronic Power Steering Subsystem: Responsible to determine the current torque applied by the driver when the car leaves the lane by mistake and vibrate or control the steering wheel by applying appropriate torque.**

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

]

Operational and Environmental Constraints:

- **The camera sensor would have decreased performance when the camera view is obscured. E.g. the car is driving in direct sunlight, inclement weather (heavy rain, snow, fog). The road lacks clear lane markers. Driving in mountainous roads where the road curvature is high.**

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?]
Ensures the safety of the process of the project to develop lane assistance system confirms to ISO 26262, so that we could have a well designed process that facilitates deficiency discovery before production.

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
]

Value Safety as the most important thing: If people value Safety above other competitive constraints like cost or productivity, they will be less likely making unsafe shortcuts or saving crucial material or time cost during production or testing

Make processes more Accountable: If the process is traceable to the exact person or group, they will be more careful when making important decisions

Providing Rewards to people that obeys safety guidelines: This will provide incentives for people that are following safety guidelines and regulations, so people will be more likely to maintain safety culture

Penalize people that undermine safety practices: This will disincentivize people from taking shortcuts that jeopardize safety or quality, so people will be less likely to weaken safety culture

Ensure people who design and develop the work separate from people who test and audit the work: This will make the audits and tests less biased, so more errors and deficiencies can be detected before the product is in market

Make sure the processes are well defined: This would make employees from different departments understand the process of other departments more clearly, which is beneficial in maintain safety culture.

Ample material resources and human resources: This would make sure that safety guidelines and requirements can be properly followed with enough resources and all the required skills.
Making sure the ideas from people in different positions are considered when making crucial decisions: This would ensure the intellectual diversity in decision making and process design, so that the decision and process will be more comprehensive with consideration to different situations.

Encouraging communication: This would ensure people could share their thoughts more freely, so that potential safety problems could be discovered early.

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
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

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?**
   It defines the roles and responsibilities between companies involved in the agreement. It also specifies what kind of product or evidence each party will provide in order to prove the work has done properly.

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.**

   My Company:
   - **Provides information/parameters for most common use cases pertain to the device that the OEM provides**
   - **Provides minimum requirements (including the rights to analyze and modify sub-systems)**
   - **Ensures a reliable communication channel**

   OEM:
   - **Provides the products that satisfy the use case**

- **Provides documentation and training about how to use or integrate the products in a proper way that ensures safety**
- **Provides ways to analyze and modify the sub-systems**
- **Ensures a reliable communication channel**

]

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   Makes sure the project conforms to a given standard (ISO 26262), and ensures the project actually increase safety level.
2. **What is a confirmation review?**
   Ensures the project complies with a given standard (in this case, ISO 26262).
3. **What is a functional safety audit?**
   Checks if the actual implementation of the project conforms to the safety plan.
4. **What is a functional safety assessment?**
   Checks if the plans, designs and developed products actually improves safety.

]

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.