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
14 Jan 2018	1.0	Vilas Chitrakaran	Initial draft

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]

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
  - Confirmation review
  - Functional safety audit
  - Functional safety assessment

Introduction

Purpose of the Safety Plan

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

This document describes the overall framework within which functional safety is achieved for the Lane Assistance Item. Safety management roles and responsibilities are defined, along with associated confirmation measures taken to ensure that a functionally safe product is delivered by the project team.

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: 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]**

The lane assistance item shall alert the driver to impending and inadvertent departure of the vehicle from ego lane and shall assist the driver to steer and keep the vehicle within ego lane. Therefore, the two functions of the Item are

1. Lane departure warning
2. Lane keeping assistance

Specifically, the item shall deliver the following behaviour when the driver drifts towards the edge of the lane,

1. The **lane departure warning** function shall apply an oscillating steering torque to provide the driver a haptic feedback
2. The l**ane keeping assistance** function, when active, shall apply a steering torque in order to steer the vehicle towards the center of the ego lane.

The following subsystems are part of the item:

1. Camera system
2. Car display system
3. Electronic power steering system

The lane departure warning function relies on camera system and the car display system, whereas all three systems listed above are responsible for lane keeping assistance function.

Figure 1 shows the high level system architecture and clarifies the item boundary. The camera system ECU detects lane departure and notifies the power steering ECU, which generates corrective control action through a steering actuator. Simultaneously, the driver receives a lane departure warning from the display system and via vibrations from the steering wheel.

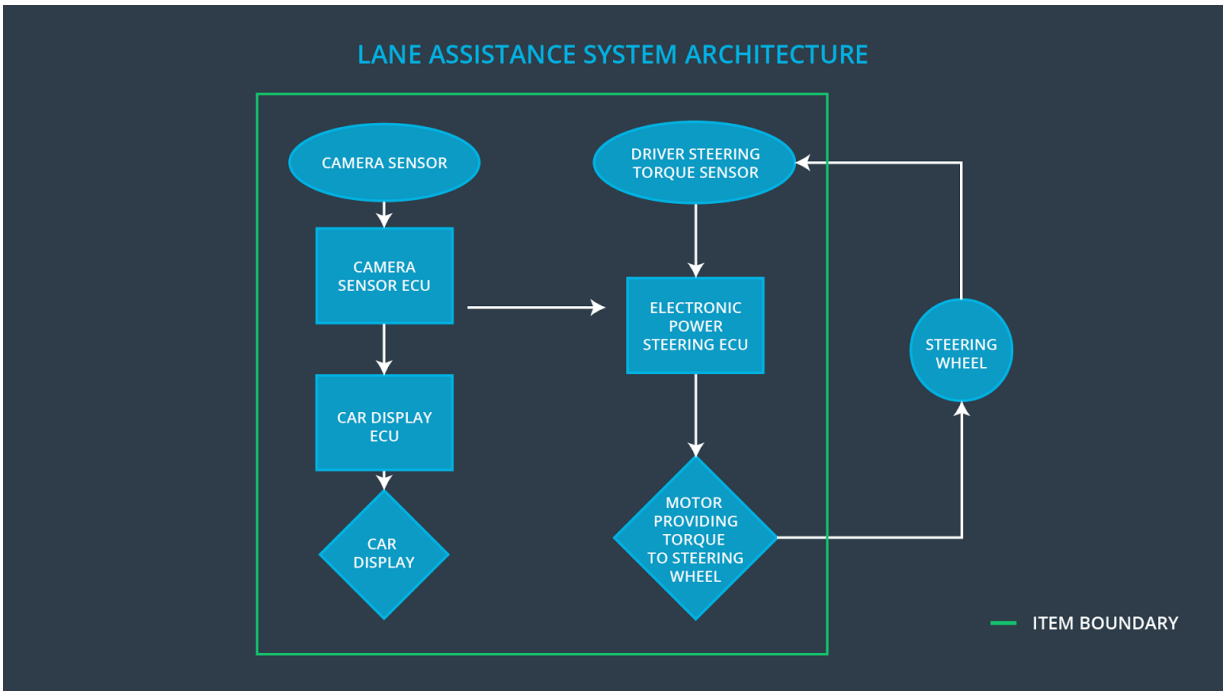

Figure 1

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 fundamental goal of this project is to reduce risk of failure or harm associated with the electronic systems in the lane assistance item by applying principles from the ISO26262 framework to the development lifecycle of the item. Specifically, this includes

- Identification of potential hazards and malfunctions that could cause bodily harm
- Evaluating risks associated with potential hazards and malfunctions
- Engineering mitigation to reduce risks to acceptable levels.

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	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

[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]

The organisation promotes safety culture in the following ways:

- Safety is assigned the **highest priority** amongst competing constraints, including costs and productivity.
- Roles and responsibilities are clearly defined to ensure **accountability**; design decisions are traceable back to individuals within the project team.
- Achieving functional safety related milestones are a key target for the project team. Amongst various **incentives**, the organisation runs a performance related bonus scheme for its employees that is aligned with achieving functional safety targets.
- All Project Managers receive **training** to detect and stop activities that may encourage team members to overlook functional safety or quality.
- The organisation strives to maintain a sufficiently large pool of engineers who are skilled in functional safety. Such engineers work across projects as safety auditors, and to maintain **independence**, they do not contribute to design activities in those projects.
- Product development follows a **well defined process** to ensure timely delivery without compromising quality.
- Project managers are encouraged to establish **teams that are balanced and diverse** in terms of skills and experience.
- To encourage **teamwork and communication**, project teams are not hierarchical and all team members have an equal say in matters of safety.

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:

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

[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.]**

In this project, the design and development responsibilities of this organisation are delineated as follows.

1. Component level Hazard Analysis and Risk Assessment.

2. Definition of a Functional Safety Concept that identifies and allocates additional functional safety requirements on components.
3. Definition of a Technical Safety Concept that identifies and allocates additional technical requirements on components, based on Functional Safety analysis
4. Propose changes to component level software architecture and coordinate their implementation with the OEM in order to reduce risks identified in HARA to acceptable levels.

The Functional Safety Manager shall plan and document the above activities. Additionally, the Functional Safety Manager shall act as the primary point of contact between the organisation and the OEM to communicate and coordinate activities to resolve issues that require collaboration.

The Functional Safety Engineer is responsible for the implementation, integration and testing of any modifications applied at the component level.

The OEM shall assign resources for verification and re-certification at Item level once component level development and testing activities are complete. Functional safety assessment at the Item level shall be performed at the OEM.

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?]**

This section describes confirmation measures that ensure

- The design and development process conforms to ISO 26262, and
- The project really does make the vehicle safer.

Confirmation review

An external independent organisation shall be assigned to review development activities for compliance with ISO 26262.

Functional safety audit

Internal safety audits shall be performed every 2 months by a designated Functional Safety specialist who is not part of the development team. The auditor shall check to ensure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment

Once development activities are complete, the Functional Safety Manager shall perform a pre-audit of functional safety pre-assessment prior to audit by a Functional Safety Assessor from an external independent organisation. Functional safety assessment shall confirm that the plan, design and development actually achieves functional safety through a combination of laboratory tests and engineering reviews.

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.