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
31/07/2018	1.0	Banning Lyth	First edit

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 safety plan documents and outlines steps to be taken to achieve a goal. These steps can be followed in case of an audit to determine whether the safety team responded adequately to the needs of the project while adhering to ISO 26262.

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**

]

The item in this document is the Level 2 Lane Assistance. This is a system of the vehicle that will help the driver maintain course and stay within their driving lane. As the vehicle propels down the roadway the driver may not pay attention to their lane lines, and the vehicle may begin to move out of the lane. If the driver has not signaled a lane change, the Lane Departure warning will alert the driver through sounds, lights, and/or haptic feedback. Lane Keeping

Assistance works to scan the lane to determine the lane edges and will apply torque to help the driver return to the center of the lane if no corrective action is made. A camera mounted near the center of the windshield along with a motor within the steering column assist this system. The camera works with an ECU to scan lane lines and track changes along the course of the road. The motor turns the steering wheel back to center by applying only enough to torque to turn the wheels.

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 goals of this project include identifying the hazards in the lane assistance system that could cause injuries to humans or damages to vehicles and property, evaluating the level of risk in hazardous situations in order to attempt to lower the risk, and using systems engineering to lower risk in effect preventing or mitigating accidents.

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 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 Manger	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
]

Safety culture characteristics include:

- **High Priority –** safety has the highest priority even against constraints like cost and productivity
- **Accountability –** design decisions can be traced back to the people and teams responsible
- **Rewards –** motivation and support for achievements in functional safety
- **Penalties –** penalizing shortcuts and bad decisions that jeopardize safety
- **Independence –** auditors and engineers are separate entities and will have no bias toward either teams' goals
- **Well Refined Process –** design and management are clear in definition
- **Resources –** projects have the necessary resources including skilled intellectuals
- **Diversity –** intellectual diversity is promoted and sought after

- **Communication –** disclosure of issues or problems is promoted

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
]

The concept, and system/software development stages are within the scope of this project. Hardware development and production are outside of this projects scope.

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 following outlines the roles and responsibilities associated with this project in accordance with ISO 26262:

Functional Safety Manager – ITEM - Entire Lane Assist System:

The FSM for the item will coordinate and document the development phase of the safety lifecycle. They are also responsible for tailoring the safety lifecycle and maintaining the safety plan. They will perform pre-audits prior to the safety auditor, and monitor progress against the safety plan.

Functional Safety Engineer – ITEM - Entire Lane Assist System:

The FSE for the item is responsible for product development, integration, and testing at the hardware, software and system levels.

Project Manager – ITEM - Entire Lane Assist System:

The PM manages overall project standards. They acquire and allocate resources for the project and will appoint the Safety Manager or act as one.

Functional Safety Manager – Component:

Same as FSM for the item level, but now only in regard to the component systems of either Lane Departure Warnings, or Lane Keeping Assistance

Functional Safety Engineer – Component:

Same as an FSE at the item level, but also now solely in the component system assigned.

Functional Safety Auditor – Internal or External party:

The FSAuditor is independent from the development team to dissuade and eliminate bias, and is responsible for ensuring the product design and implementation conform to the safety plan and in turn ISO 26262.

Functional Safety Assessor – Internal or External party:

FSAssessor must be independent from development, and determines whether functional safety is being achieved through a safety assessment.

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 are in place to ensure the project conforms to ISO 26262 and that the project has in fact made the vehicle safer. This will be quantified through review, audit and assessment.
The confirmation review is performed by an independent party and determines the project adherence to ISO 26262. This occurs throughout design and development of the project.
Functional safety audits are in place to determine the teams' adherence to the safety plan, these can be periodic and will help safety managers make decisions about project progress.
Confirming that the project achieves functional safety satisfies the needs of the functional safety assessment. The assessment tests that the project has implemented a vehicle that is safer than the previous model or system.

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.