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
2018-12-31	1	Simon Beyer	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?]

This safety plan provides an overall framework for the Lane Assistance item and assigns roles and responsibilities for functional safety for this item.

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**

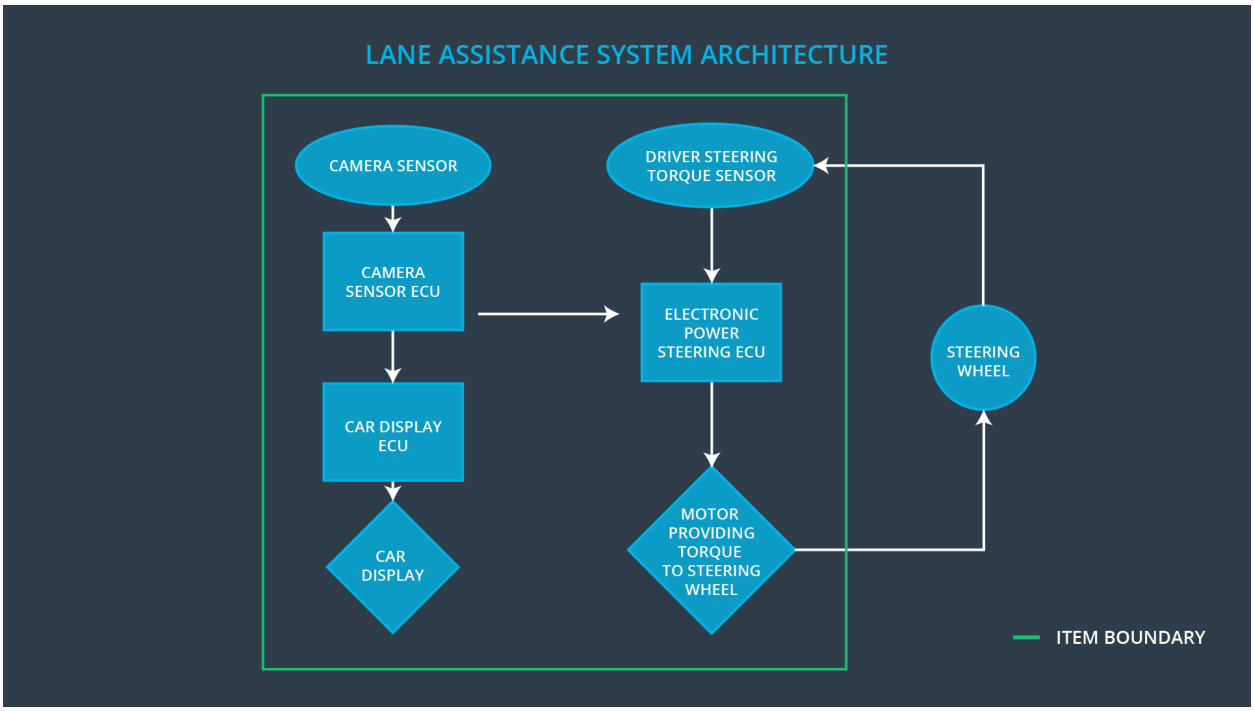
]

The lane assistance item alerts the driver that the vehicle has accidentially departed its lane, and attempts to steer the vehicle back towards the center of the lane.

The Lane Assistance System will have two functions:
1. **Lane departure warning**: The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. **Lane keeping assistance**: The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The Lane Assistance Item includes three sub-systems:
- Camera system
- Electronic Power Steering system
- Car Display system

The following image shows the boundary of the Lane Assistance System.



The Camer system, the Car Display system and the Electronic Power Steering system are inside the boundary of the Lane Assistance system. The Steering Wheel system is not part of the Lane Assistance System.

Operational and Environmental Constraints:

- Headlights must be functional in the night
- Windshield wiper must be functional during rain
- Now snow and fog

Legal requirements for Lane Assistance technology:

- In November 2013, the European Union introduced a regulation, that all new trucks and buses must be fitted with lane departure warning systems. (
- NHTSA recommends lane departure warning systems (

National and International Standards related to Lane Assistance System:

- Informal document GRRF-74-40 (
- ISO 11270:2014; Intelligent transport systems – Lane keeping assistance systems (LKAS) – Performance requirements and test procedures (
- ECE/324: Uniform provisions concerning the approval of motor vehicles with regard to Lane Departure Warning Systems (LDSW) (
- NCAP on Lane Departure Warning ()

Records of previously known safety-related incidents or behavioral shortfalls:

- Lane keeping system accident (
- Electronic Driving Systems Don’t Always Work, Tests Show (
- Quirks and glitches in driver aid systems needed for autonomy – Issues with lane departure warning and keeping: Lane keeping systems feels like “ping-pong” between the lanes (https://www.forbes.com/sites/jensen/2016/12/20/quirks-and-glitches-in-driver-aid-systems-needed-for-autonomy-there-is-room-to-improve-trust/#67ff100b4d73

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?]

By analyzing the Lane Assistant System with ISO 26262 we want to reduce the risk as a result of malfunctioning behavior of the E/E system

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	Project 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
]

Here are some characteristics of our company’s 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 achievments 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 enncourage disclosure of problems.

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 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?**

The development interface agreement (DIA) defines the roles and responsibilities between companies involved in developing a product. The purpose of the DIA is:

- Clarifiy the responsibilities of the different parties involved in a functional safety project
- Describe the work products that each company will provide
- Help avoid disputes between companies
- Clarifies who will be responsible for any safety issues in post-production

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.**

]

Responsibilities of our company (Tier-1): Component Level

- Functional Safety Manger – Component Level

    - Planning, coordinating and documenting of the development phase of the safety lifecycle
    - Tailors the safety lifecycle
    - Maintains the safety plan
    - Monitors progress against the safety plan
    - Performs pre-audits before the safety auditor
- Functional Safety Engineer – Component Level
    - Product development
    - Integration
    - Testing at the hardware, software and systems levels

Responsibilities of OEM: Item Level

- Functional Safety Manager – Item Level
    - Planning, coordinating and documenting of the development phase of the safety lifecycle
    - Tailors the safety lifecycle
    - Maintains the safety plan
    - Monitors progress against the safety plan
    - Performs pre-audits before the safety auditor
- Functional Safety Engineer – Item Level
    - Product development
    - Integration
    - Testing at the hardware, software and systems levels
- Project Manager – Item Level

    - Overall project management
    - Acquires and allocates resources needed for the functional safety activities
    - Appoints safety manager or might act as safety manager
- Functional Safety Auditor
    - Ensures that the design and production implementation conform to the safety plan and ISO 26262
    - Must be independent from the team developing the project
- Functional Safety Assessor
    - Independent judgement as to whether functional safety is being achieved via a functional safety assesment
    - Must be independent from the team developing the project

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?**

]

1. The confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262
- that the project really does make the vehicle safer

2. *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. *Functional safety audit*
Checking to make sure that the actual implementation of the project conforms to the safety plan.

4. *Functional safety assessment*
Confirming that plans, designs and developed products actually achieve functional 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.