Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
25th May, 2018	1.0	Anant Yash Pande	Initial document

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan should provide an overview of the functional safety plan and help us plan a secure system. In order to realize the functional safety of a vehicle, we must clearly state what we must do. We define roles and outline how we can achieve them. The vehicle system to be analyzed is also described in this document. In addition, the document should talk about the safety culture including beliefs, perceptions and values and how the plan actually leads to a secure system.

Scope of the Project

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

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

This document focuses on a Lane Assistance System that can monitor the position of a vehicle on the road. It checks if a lane change is intentional and issues a warning and / or control signals to correct if it isn't. The system implemented in our case follows a sensory warning system, which gives it the name Haptic Lane Feedback System. The following points describe the main functions of the Lane Assist system:

- Lane Departure Warning: A warning is issued when the lane change is unintentional or defined by the system. It checks systems such as turn indicators or sensors, on whose behavior warnings are issued, in the form of steering oscillations or an acoustic signal as a warning.
- Lane Keeping Assist: The vehicle provides assistance when an inadvertent lane change warning is received to stay on the current lane. This is done by gently steering to the center of the lane.

Components of the Lane Departure Warning System:

- Sensors: A variety of sensors can be used to check if a lane change is unintentional. Cameras are the most commonly used sensor, followed by lasers or infrared or even as simple as turn signals
- Warning System: Provides a driver alarm system to prevent inadvertent lane changes. Normally, an audible signal such as a beep or a steering vibration is generated. Our system generates a steering vibration to warn the driver

Components of the Lane Keeping Assistance System:

- Power Steering / Steering Assist: When the lane departure warning system issues a warning, the steering system is activated to generate a reverse torque that slowly corrects the deviation.

Components of the Control System:

- Electronic control unit (ECU): Coordinates between the sensors and the Steering Assist System, deciding which signal to issue a warning for.

Lastly, we will talk about the system boundaries in which we describe how the Lane Assistance System fits in with other vehicle functionalities and systems:

- Camera: The system connects to a camera as a sensor to detect when the vehicle is leaving its lane.
- Lane Change Indicator Lights: When the camera detects a lane change, it sends a command to the ECU, which then checks to see if the lane change indicators are being used.

- ECU: Compares sensor data and issues a warning if the lane change appears inadvertent. Otherwise, the system remains dormant.
- Steering Assist: When a lane change warning is issued, the system activates an opposite torque to gently guide the vehicle back to the center of the lane.

The steering assistant and the ECU can be considered as components in the Lane Assist system itself. The camera and lane change indicators work as components outside the system and pass their input to the Lane Assist system.

Goals and Measures

Goals

ISO 26262 is the standard for defining functional safety standards. We have set ourselves the goal of defining a standard for the security policies that are defined for Lane Assist Functions that are analyzed by ISO 26262 processes. This will help us better plan our development as we:

- We understand the work and are able to identify all possible dangers.
- Analyze the potential dangers and calculate the risk they generate.
- Use this analysis as a basis for introducing reviews in our system in the design and implementation of the system so we can address vulnerabilities.

The ultimate goal is therefore to develop a system that is functionally safe and contains checks or warnings for hazards that are considered risky. The ISO standard offers us a means to establish the same in a defined structure.

Measures

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	All Team Members	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 Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

The safety of a system is ensured not only by reviewing the technical aspects, but also by maintaining a consistent organizational culture of safety. Safety is not a limitation but a necessity in all planning processes. Safety culture is discussed in the following points:

- Security is the top priority: No other perspective such as cost or profit or deadline can take precedence over security. This means that security is the only solution when faced with a decision.
- Safety is a well-defined process: The ISO 26262 standard is maintained in maintaining the functional safety of the system according to structured processes and documentation.
- Traceability: All steps as Part of the functional safety procedure must be well documented so that each step can be reviewed and traced back to its creator. Not only does this provide a strong, structured foundation for our purposes, it also strengthens accountability in the system. Communication: Ideas are encouraged and everyone is invited to participate in the planning and planning of the safety plan.
- Independence: The audit team is an independent team that draws up the safety plan.

A constant review process is required to ensure that all aspects of safety achieve the desired level of excellence, which is achieved through appropriate quality management measures.

Safety Lifecycle Tailoring

The following phases of the Safety Life Cycle fall within the scope of the document:

- Concept Phase: It is important to plan functional safety already in the concept phase. This allows the integration of safety into the design itself to ensure a robust system plan that can anticipate most possible risks.
- Product development at the system level: Through this phase, we have a clear direction for the development of our system. We know how to proceed and what the system consists of. Planning safety becomes more direct and essential, as we now have a system that we can focus on in terms of system structure and function.
- Product development at the software level: With system development, the software requires how each functionality works within the EU to be achieved and monitored System. When planning safety for internal work, care must be taken to consider software malfunctions. Some phases are also outside the scope of this security plan.
- Hardware-level product development: While we plan how the system works and where software works, it does not matter how the hardware is allocated, as long as it achieves the desired functionality.
- Production and Operation: The functional safety plan takes into account possible risks due to the electrical and electronic components of the system. We will ensure that all functionalities work as they should.

Roles

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

The Development Interface Agreement (DIA) describes the roles of stakeholders involved in a product development plan. The DIA assigns responsibilities for the safety and fixes the liability. It defines who the producer is and who should consume the product, along with the requirements and expectations. The product and the information to be exchanged between the parties involved, with the assignment of roles to be led in product development, are also

mentioned here. The interaction between the parties involved and how resources can be shared, including designs and information, are discussed in this document. The clarification of the agreement allows for a clear distinction between roles and responsibilities, so that in the event of failure, no disputes arise. It also clarifies who is responsible for correcting a failure. The following points explain how the various bodies involved in the manufacture of the vehicle contribute:

- OEM: Purchases a Lane Assist System that matches the steering mechanism. The OEM participates in the design aspects of the system as a whole to make demands and to check its coordination with other components. It must check the functional safety aspects of the Lane Assist System with the rest of the vehicle.
- Tier 1: Produces the required Lane Keeping System. It is responsible for the proper functioning of the system and how each subsystem works. It also takes into account the functional safety aspects of the overall system and subsystems.
- Tier 2: Produces individual parts used to build the components of the subsystems and systems of the Lane Assistance System

Confirmation Measures

The confirmation actions are as follows:

- Functional safety complies with ISO 26262.
- The project creates a more secure system.

Based on a verification check, functional safety checks and a functional safety assessment, it performs the following:

- Confirmation check: Must be performed. Ensure that the project complies with the functional safety standard ISO 26262. An independent person/team must perform the verification to verify compliance.
- Functional safety check: A comparison must be made to compare the actual execution of the project with the safety plan created in this way. The test must be performed by a person who is independent of the team that creates the safety plan.
- Functional safety evaluation: The final step is to verify that the safety plan and functional safety project actually does provide security for the system.

All confirmatory actions must be performed by independent teams / individuals, independent of the team involved in the planning, documentation or implementation of the safety project. On the basis of the document under review, varying degrees of independence are considered appropriate.
This concludes the initial phase of the safety plan of the Functional Safety project.