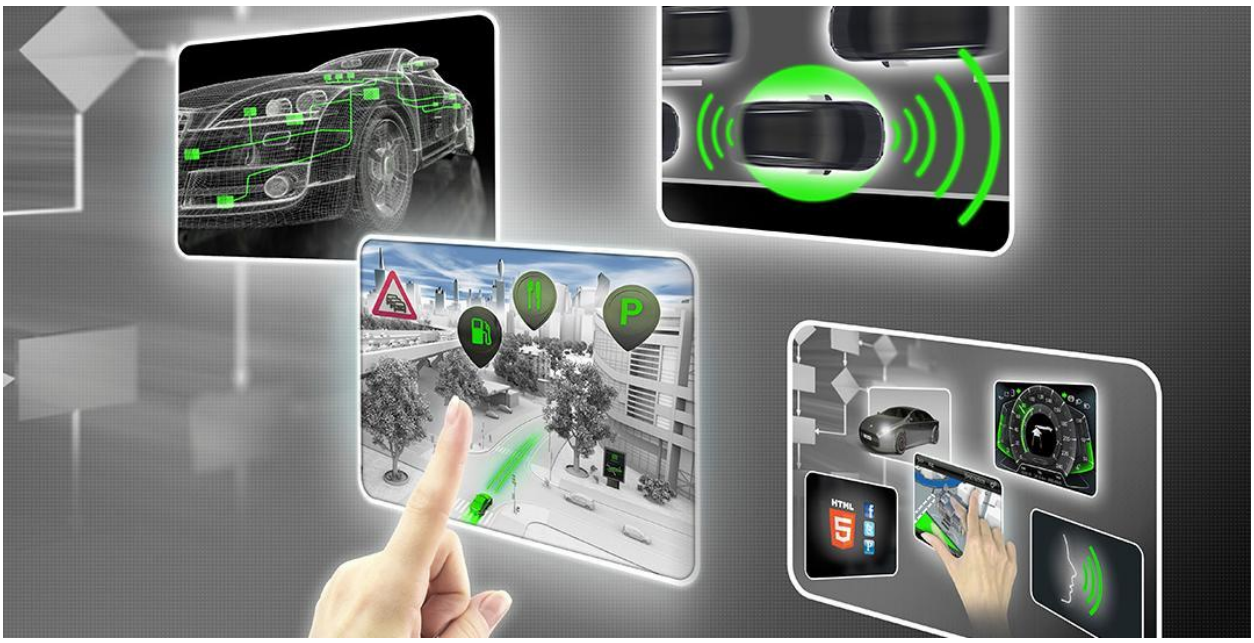
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
12/30/2017	1.0	Me	Initial submission

Table of Contents

Introduction

Purpose of the Safety Plan

This document defines the roles and the steps taken to achieve functional safety of the Lane Assistance item.

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

The item under discussion is the Lane Assistance feature, which helps the driver stay within their selected lane.

The two main functions of Lane Assistance are:

1.) Lane Departure Warning – the vehicle indicates to the driver by vibrating the steering wheel when the vehicle is drifting away from the center of the lane and the driver has not indicated that they are intending to change lanes.

2.) Lane Keeping Assistance – in the event that the car drifts from center without indication from the driver of the intent to change lanes, the vehicle automatically steers back to the center of the lane.

The following vehicle subsystems implement the Lane Assistance function:

1.) Camera Subsystem – identifies the position of the vehicle with respect to the center of the lane. Initiates request to Electronic Power Subsystem in the event of unplanned lane departure. Subsystem comprises the Camera Sensor and Camera Sensor ECU.
2.) Display Subsystem – provides visual notification to the driver about the current status of the Lane Assistance feature. Comprises the Car Display and Car Display ECU.
3.) Electronic Power Steering Subsystem – steers vehicle by desired amount by providing torque to steering wheel. Comprises the Driver Torque Sensor, Electronic Power Steering ECU, and Steering Wheel Torque Motor.

The remaining subsystems, including the Steering Wheel, are outside the boundary of the Lane Assistance item.

Goals and Measures

Goals

The goals of the project are:

1.) identify hazards in the Lane Assistance item that could cause physical injury
2.) evaluate the risk of the identified hazards to identify the scope and priority of risk reduction efforts
3.) apply systems engineering processes to lower the identified risks to acceptable levels.

Measures

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

Our company's safety culture is characterized by the following:

- 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 achievement of functional safety
- Penalties: the organization penalizes shortcuts that jeopardize safety or quality
- Independence: teams who design and develop a product are independent from the teams who audit the work
- Well defined processes: company design and management processes are 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 encourage disclosure of problems

Safety Lifecycle Tailoring

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

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) defines the roles, responsibilities, and deliverables between companies that are working together to develop a system.

For the Lane Assistance Item, the OEM provides item-level functional safety management and engineering while our company, a Tier-1 company, provides subsystem-level safety management and engineering. Depending on the situation, the OEM will provide requirements or a basic product design to our Tier-1 company.

Confirmation Measures

Confirmation measures confirm that the Lane Assistance project conforms to the ISO 26262 standard and that it identifies and minimizes safety risks.

A Confirmation Review ensures that the project complies with ISO 26262.

A Functional Safety Audit ensures that project conformed to the safety plan as it was executed.

A Functional Safety Assessment ensures that the plans, designs, and developed products 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.