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
26.03.2018	0.1	Stefan Cyliax	Initial version for functional safety project
01.04.2018	1.0	Stefan Cyliax	First RC

Table of Contents

Contents

Introduction

Purpose of the Safety Plan

This safety plan gives an overview of how we are going to derive a safe system. What are the main risks of the system and how they are going to be mitigated?

A few of the major elements include:

- What system is under consideration
- The goal of the project
- What steps will be taken to ensure safety
- The roles and personnel involved in the project
- The project timeline

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

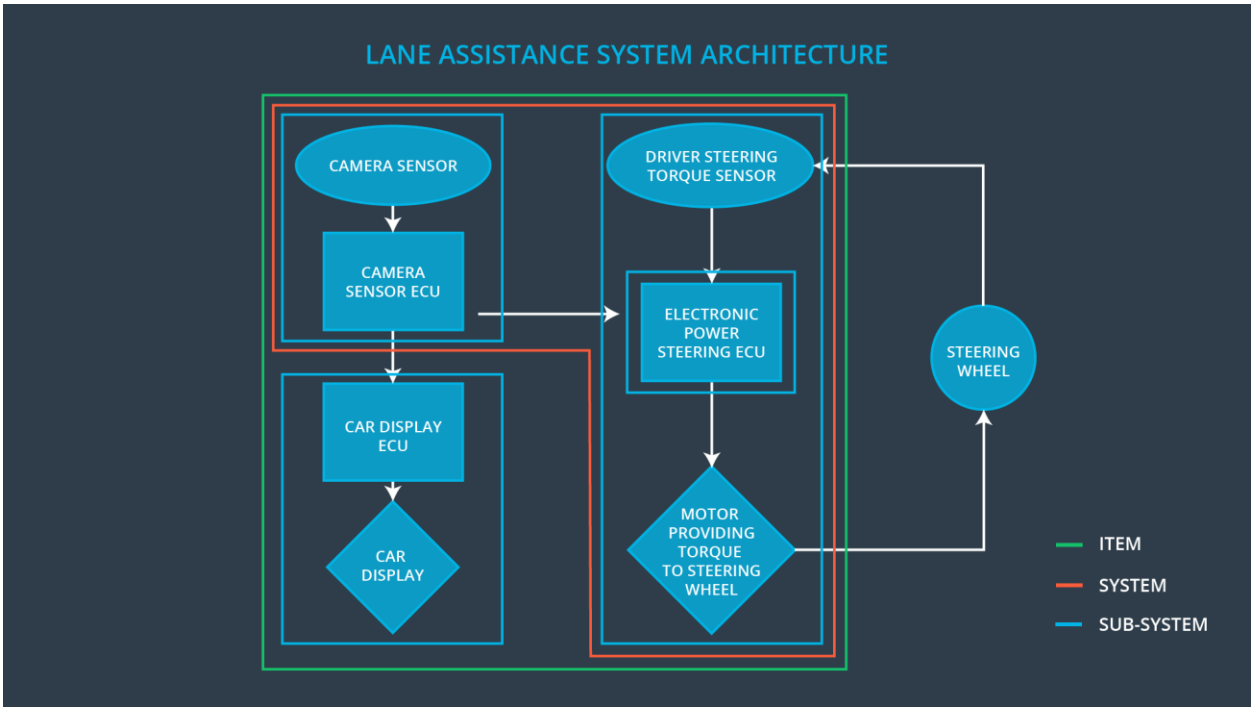
Item Definition

This Safety Plan regards a Lane Assistance system including the customer display and interface. It has two main functions: Line Departure Warning (LDW) and Lane Keeping Assistance. (LKA). The LDW detects lane lines using a camera sub-system and warns the driver about unintentional departures by vibrating the steering wheel. LKA builds on this and adds steering torque to help the driver move back towards the center of the lane.

1. Lane Departure Warning:
   The lane departure warning function will vibrate the steering wheel
2. Lane Keeping Assistance:
   The lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

The system consists of four sub-systems

1. Camera system
2. Electronic Power Steering system
3. Car Display system
4. Electronic power steering ECU



Goals and Measures

Goals

The goal is to analyze the Lane Assistance system using ISO 26262. We analyze which malfunctions can occur and which possible hazards and harm they cause. For each scenario a risk is calculated. Next we analyze the system architecture layer by layer to identify measures to mitigate the risk.

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	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

There are several characteristics of a good safety culture in a company:

- 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 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 encourage disclosure of problems
- Testing and auditing independent
- Hazard analysis with diverse team

Safety Lifecycle Tailoring

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:

- 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

What is the purpose of a development interface agreement?
It defines the roles and responsibilities between companies involved in developing the product. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

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.
Tier1: Responsibilities of the Safety Manager

- 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
- Safety Engineer
- Product development
- Integration
- Testing at the hardware, software and system levels

OEM: Responsibilities of the Project Manager

- Overall project management
- Acquires and allocates resources needed for the functional safety activities
- Appoints safety manager or might act as safety manager

Confirmation Measures

What is the main purpose of confirmation measures?

that a functional safety project conforms to ISO 26262, and
that the project really does make the vehicle safer.

What is a 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.

What is a functional safety audit?

Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

What is a functional safety assessment?

Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

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.