Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-09-22	1.0	Rob Poyck	First iteration

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan will provide the framework for the lane assistent item and it defines the roles and repsonsibilities of the team working on this 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

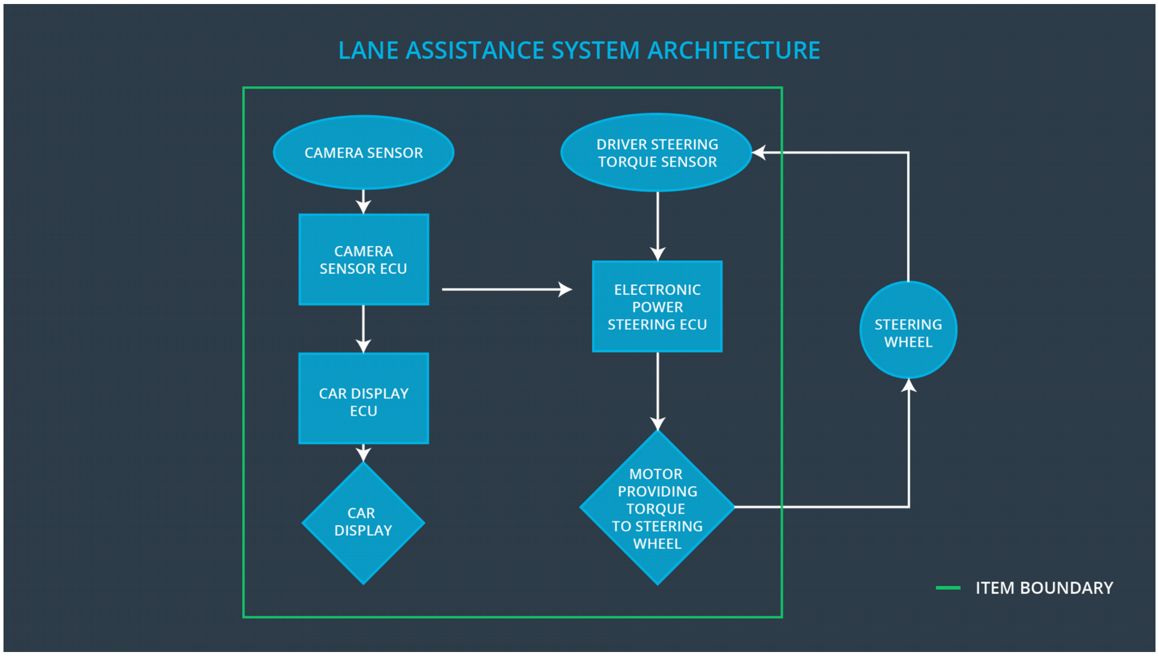
The item under analysis in this plan is a simple version of a lane assistance system. The lane assistance item helps the driver to keep the current lane while driving on a normally marked road.

The two components of the lane assistance item are:

- **Lane departure warning function**
  - When the driver veers from the current lane, this system moves the steering wheel back and forth to create a vibration to alert the driver.
- **Lane keeping assistance function**
  - Will turn the steering wheel back to the centre of the current lane when the vehicle veers to far away from it.

The system is deactivated by using the turn signal, in doing so the driver indicates that the current lane-change is voluntary. In order to completely turn off the system the driver can deactivate it with a button on the dashboard.

The most important high level sub-systems of the lane assistant can be seen in this architecture diagram:


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

There are three sub-systems in this system:

- **Camera subsystem**
  - Which detects if the vehicle is leaving the current lane, which will act as an input for the lane departure warning and lane keeping functionalities.
- **Electronic Power Steering subsystem**
  - Which drives the actuator to both:
    - Generate the steering wheel vibration for the warning functionality
    - Generate the steering wheel torque for the lane keeping functionality
- **Car display subsystem**
  - To show a warning light to indicate that the assistance system is active.

An important detail is that the system is not intended to run autonomously. The driver is expected to have both hans on the steering wheel at all times.
The lane keeping assistant will therefore detect the torque already exerted by the driver and will only supply the extra torque required to stay inside the lane boundaries.

Goals and Measures

Goals

The documentation in this project gives an overview of how the team is going to achieve a safe system. It grants the possibility to externally audit the functional safety design process. An audit may be followed by a safety assessment, used to determine if the decisions made and steps taken achieve appropriate safety. It helps in proving that best practices have been followed if there has been a safety issue in the field.

Documentation also provides a reference when modifying a system.

This project will therefore analyse the safety and reliability of the e/e systems required for the lane assistant item.
In this context the following steps will be executed and documented:

- Identifying potential problems, which could injure people or damage peoples health. These are called hazards.
- Evaluate the risks of the hazards.
- Use systems engineering to lower the risks to acceptable levels.

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

The characteristics of the safety culture include:

- **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

The organization has a quality management system in place that complies with quality management standard ISO 9001.

Safety Lifecycle Tailoring

Since the project involves a new product, all the phases mentioned in the scope of the project section will have to be in the scope of this research, namely:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

This project does not include hardware or the production phases to keep it within the boundaries of the possibilities within this course. Therefore the following phases are left out:

- 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 DIA delineates the design responsibilities between the OEM and tier 1 supplier or the tier 1 and tier 2 supplier. A DIA is included for the following reasons:

- Avoid disputes during the planning and development of a product
- Liability definition
- Clarity who should fix the safety issue
    - If there is a safety issue after coming to the market there is a clear distinction of the responsibilities for fixing.

The high level sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

The work division amoung team members of the two major parties is:

- OEM – Will supply the fully functional lane assistance system
    - Functional Safety Manager- Item Level – Planning, coordination and documenting of the development phase of the safety lifecycle, maintain and track progress of the safety plan. Will perform pre-audits before handing the result over to the safety auditor.
    - Functional Safety Engineer- Item Level – Develop, integrate and test the system in both software and hardware.
    - Project Manager - Item Level – Overall project management. Acquiring and allocating resources needed for the functional safety activities, including appointing the functional safety manager.
    - Functional Safety Auditor - Outside of the project team – Ensures that the design and production implementation conform to the safety plan and ISO 26262.
    - Functional Safety Assessor – Outside of the project team – Independently judge wether the functional safety is actually being achieved

- Tier 1 – Analyse and modify the various sub-systems from a functional safety viewpoint
    - Functional Safety Manager- Component Level - Planning, coordination and documenting of the development phase of the safety lifecycle, maintain and track progress of the safety plan. Will perform pre-audits before handing the result over to the safety auditor.
    - Functional Safety Engineer- Component Level - Develop, integrate and test the components of both software and hardware.

Confirmation Measures

The main purpose of confirmation measures is to make sure:

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

This is achived by checking three things:

- If processes comply with the functional safety standard
- Project execution is following the safety plan
- Design really does improve safety

The confirmation measures consist of three steps/actions:

- Confirmation review
  - Ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person reviews the work to make sure ISO 26262 is being followed.
- Functional safety audit
  - Checking to make sure that the actual implementation of the project conforms to the safety plan.
- Functional safety assessment
  - Confirming that plans, designs and developed products actually achieve functional safety.

Nota bene

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.