Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
18.03.2018	1.0	P. Schalast	Initial Safety Plan
31.03.2018	2.0	P. Schalast	Review for project commit

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan gives an overview of how to achieve a safe system. 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

The system in focus of these documents is the Lane Assistance System as part of the ADAS (Advanced Driver Assistance System). ADAS systems have two functions:

- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

Some examples of ADAS systems that can already be found in passenger vehicles today:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Lane Departure Warning
- Lane Keeping Assistance
- Tire Pressure Monitoring
- Pedestrian Protection

The system in focus of this project and documentation is the Lane Assistent System. It will have two functions:

1. Lane departure warning
2. Lane keeping assistance

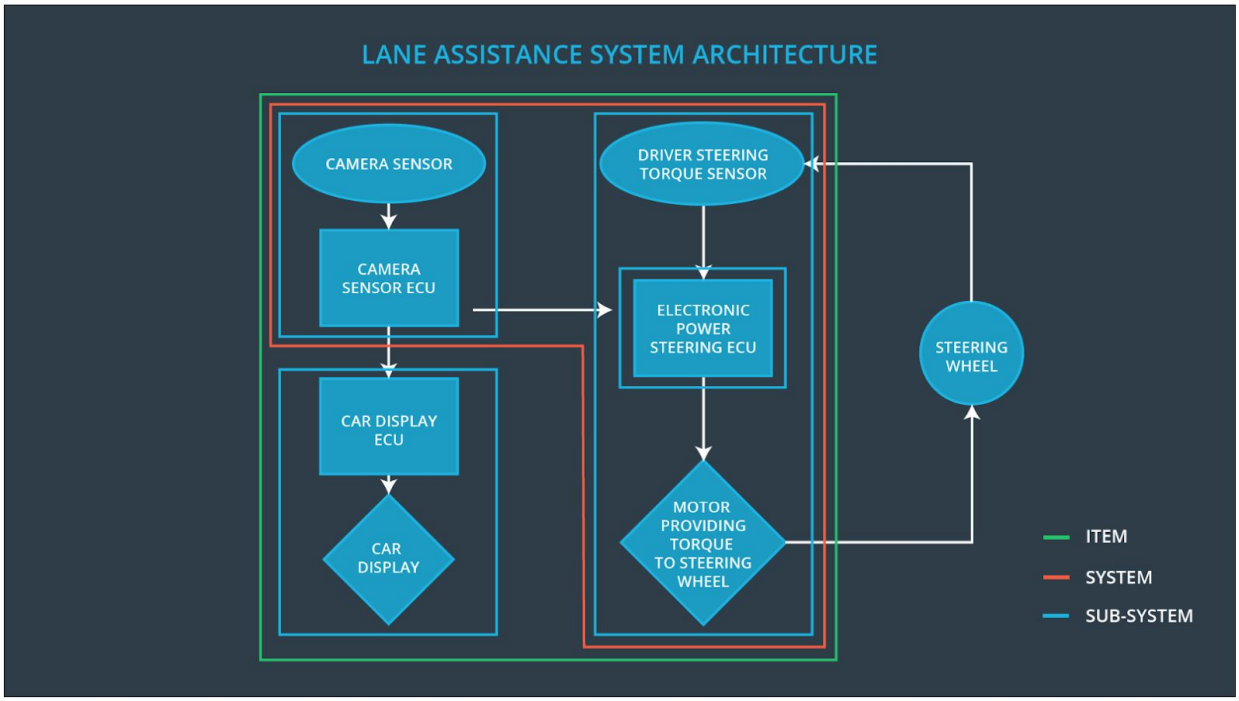
When the driver drifts towards the edge of the lane, two things will happen:

- the lane departure warning function will vibrate the steering wheel
- the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

In the following diagram the item boundaries for the following three subsystems with its elements are shown:

- Camera system
- Electronic Power Steering system
- Car Display system

Both camera system and electronic power steering system are included in the system. The car display system as HMI is outside the system.


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

Goals and Measures

Goals

The goals of the project are:

- Identify risk and hazardous situations in the Lane Assistance system components malfunction causing injuries to a person
- Evaluate the risks of the hazardous situations
- Lower the risks of the malfunctions to a reasonable levels acceptable by current sociatity.

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

These are the characteristics of our 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 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

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

1. What is the purpose of a development interface agreement?
   A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.
   The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.
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.

Tier1:

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:

Project Manager

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

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

Confirmation Measures

1. What is the main purpose of confirmation measures?
   Confirmation measures serve two purposes:
   - that a functional safety project conforms to ISO 26262, and
   - that the project really does make the vehicle safer.
2. 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.
3. 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.
4. What is a functional safety assessment?
   Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.