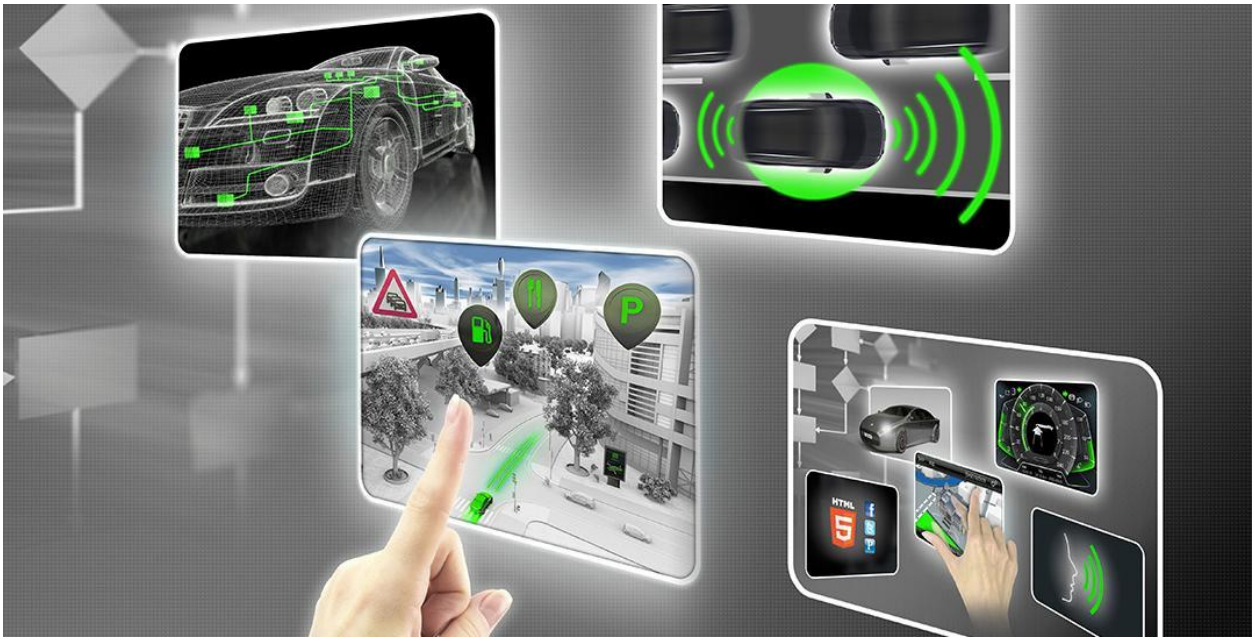
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
10/21/2018	1.0	Chunfeng Yang	Initial version.
10/21/2018	2.0	Chunfeng Yang	Minor change of responsibility for "Create and sustain a safety culture" to “Safety Manager”.

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for 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 considered in this plan is a simplified version of a Lane Assistance System.

The Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System have two main functions:

1. Lane departure warning
2. Lane keeping assistance

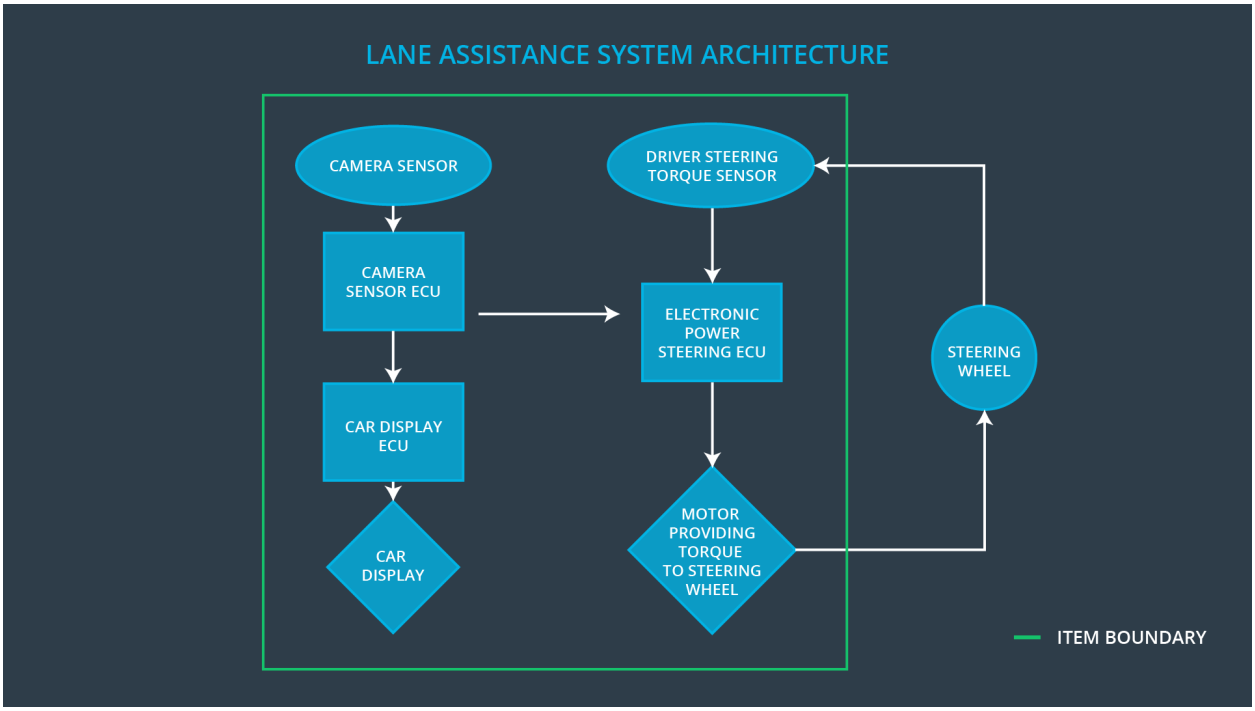
When the driver drift out toward the edge of the lane, the steering wheel vibrates to warn the driver. Safety requirement: *The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.*

When the driver drift out toward the edge of the lane, the lane keeping assistance functionality will move the steering wheel so that the wheels turn toward the center of the lane. Safety requirement: *The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane (this is the lane where the car is)*.

The item functionalities are implemented by the camera subsystem, the electronic power steering subsystem, and the car display subsystems:

- **Camera subsystem**: This subsystem is composed by two components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This subsystem is composed by three components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering ECU.
  - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem**: This subsystem is composed by two components:
  - Car Display ECU
  - Car Display

The following diagram shows the interaction between different subsystems.



When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel. The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard. The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

The Line Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

Goals and Measures

Goals

This project's major goals are:

- Identify risk and hazardous situations in the Line Assistance system components (*lane departure warning* and *lane keeping assistance*) malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Lower the risk of the malfunctions to a reasonable level.

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

Here are some characteristics of a good 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

The purpose of the development interface agreement (DIA) is to delineate the roles and responsibilities between OEM and tier-1 involved in developing this product. Both parties 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.

The OEM provides a functioning lane assistance system. Tier-1 is going to analyze and modify various sub-systems according to functional safety requirements.

The following steps are part of a separate DIA documentation which will be attached to this safety plan:

- 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

Confirmation Measures

The purpose of the confirmation measures is:

- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project really does make the vehicle safer.

The Confirmation review ensure the projects comply 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.

A Functional safety audit make sure the actual implementation of the project conforms to the safety plan.

A Functional safety assessment confirms that the plan, design and developed product actually 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.