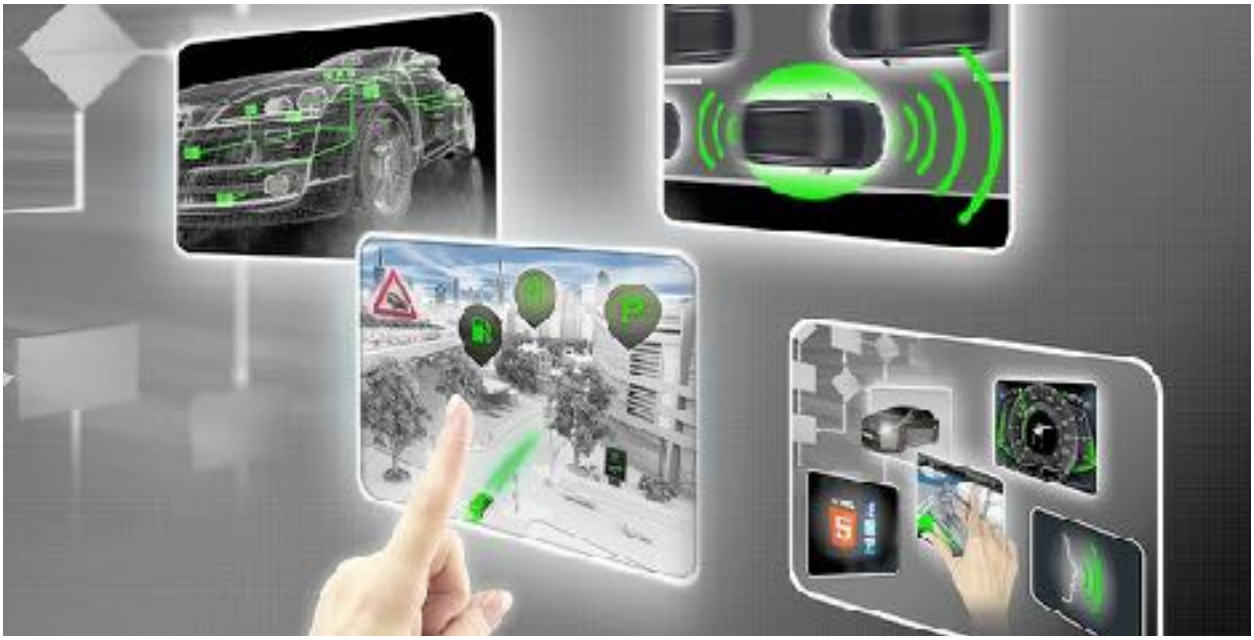
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/24/2018	1.0	Huaping Gu	First submission
2/25/2018	2.0	Huaping Gu	Update “Goals and Measures” section
3/3/2018	3.0	Huaping Gu	Use more material from the lesson and enrich the document

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 team, and to assign roles and related 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 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 will have two functions:

1. Lane departure warning

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

2. Lane keeping assistance

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

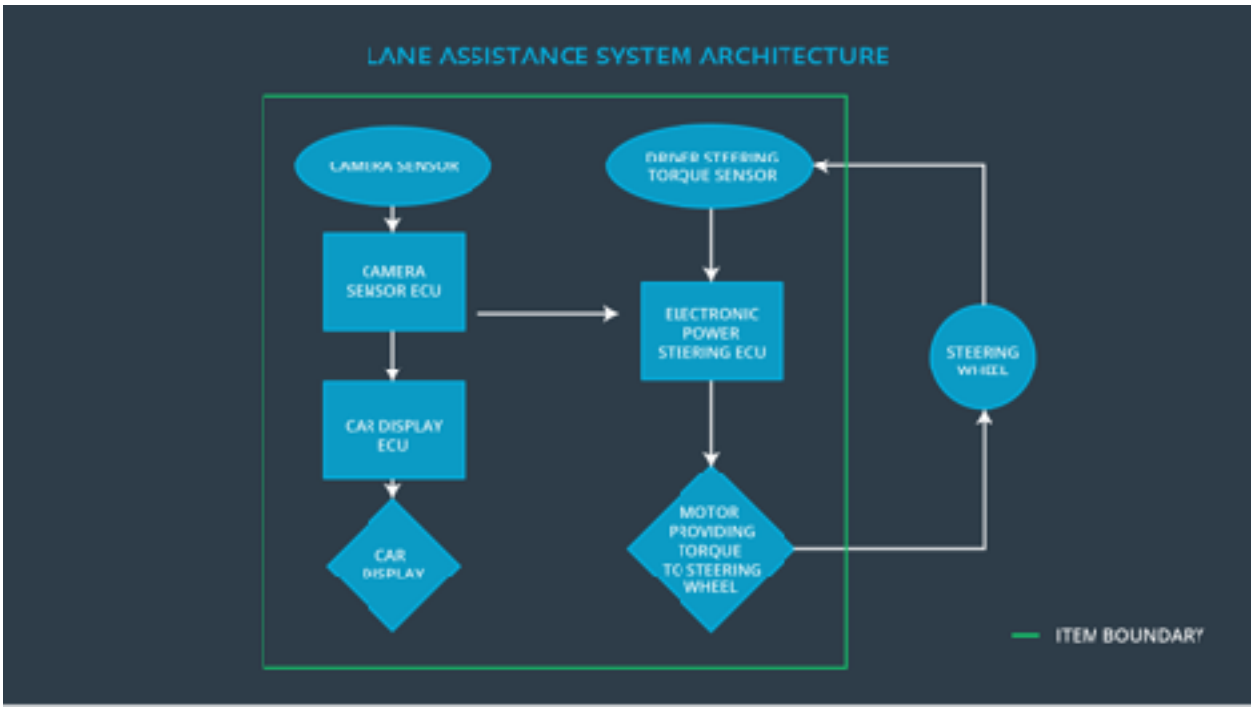
In this Lane Assistance system, the camera subsystem, the electronic power steering subsystem, and the car display system are all responsible for each of the functions.

Bellow diagram shows the boundaries of the item and subsystems inside and outside of the item. you can see that the item boundary was drawn to include three sub-systems:

- Camera system
  Responsible for detecting lane lines and determining then the vehicle leaves the lane by mistake. This subsystem includes camera sensor and camera sensor ECU

- Electronic Power Steering system
  Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lance assistance system torque request. This includes driver steering torque sensor, electronic power steering ECU and Motor providing torque to steering wheel.

- Car Display system
  Display the warning message and other related info in the car display screen. It includes car display ECU and display.



Goals and Measures

Goals

The goals of this document are to

1. **Identify hazards** in a passenger vehicle's electronic or electric system that could cause physical injury or damage to a person's health
2. **Evaluate the risk** of the hazardous situation so that we know how much we need to lower the risk
3. **prevent accidents** from occurring by lowering risk to reasonable levels Via systems engineering

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

We will promote and build a good safety culture in our daily tasks with very clear definitions of bellow characteristics:

- **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

Note: Culture usually as part of a live eco-system which has its own life, is always evolving alone with acceptable levels of current society.

Safety Lifecycle Tailoring

Based on our current resources delivery requirements (please check "Scope of the Project"), in this Lane Assistance document, we try to include following safety lifecycle phases:

Concept Phase
Product Development at System level
Product Development at Software level

But will exclude following phases in this document:

Product Development at 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

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.
The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

OEM responsibility:
OEM will provide requirements for what a vehicle system needs to do with preliminary product design and then outsourced to tier1 suppliers. Our functional safety manager and engineer will work on both software and hardware design on both item and component levels for Lane Assistance. More details will be discussed in the design documents. Name of the managers will be assigned there.

We will also ensure all the suppliers complies with the ISO 26262 and will provide independent functional safety audit and assessment.

Tier1 Responsibilities:
Tier1 supplier develops and produces the system for the OEM. Tier1 companies, oftentimes outsource their work to Tier 2 companies.

We will have 3 Tier1 suppliers on each of bellow:
- Camera system
- Electronic Power Steering system
- Car Display system

Each of the suppliers need to follow out design guidelines, provides related systems implementation, needed training and documents. We allow tier 1 to outsource some work to Tier 2 supplier.

Tier2 Responsibilities:
Tier2 usually does not contact with OEM directly, they talk to Tier1 suppliers. Tier1 should provides clear guidances and DIA to Tier2, including which company is best positioned to fix the system issue. Responsibilities between Tier1 and Tier2 are managed by Tier1 side, all the related disputes and liabilities need to be covered by Tier1.

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.

The people who carry out confirmation measures need to be independent from the people who actually developed the project. Bellow are three main confirmation measures we will carry out:

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.

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.

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

Note:
The person who developed a document, plan, design or product should not be the same person who carries out a confirmation measure; confirmation measures require independence.
ISO 26262 requires different levels of independence depending on what part of the functional safety lifecycle is under review.