Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version:1.0

Document history

Date	Version	Editor	Description
05/23/18	1.0	Ganesh Prabakaran	Initial version

Table of Contents

Contents

Introduction

Purpose of the Safety Plan

The purpose of safety plan is to define an overall framework for the functional safety of Lane Assistance project, and to assign roles and responsibilities for executing the functional safety for this item. This will help in defining and manage the execution planned to identify high risk situations that could cause harm and then find ways to lower the risk to reasonable, acceptable levels. This will provide an evidence that the project has built a safer product.

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

Lane Assistance System:
The purpose of the lane assistance system is to assist the driver in order to ensure the vehicle is driven in the center of the lane.

The lane assistance system has two main 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 shall apply an oscillating steering torque to vibrate the steering wheel in order to provide the driver a haptic feedback.
- The lane keeping assistance function shall apply the steering torque to move the steering wheel so that the wheels turns toward the center of the lane.

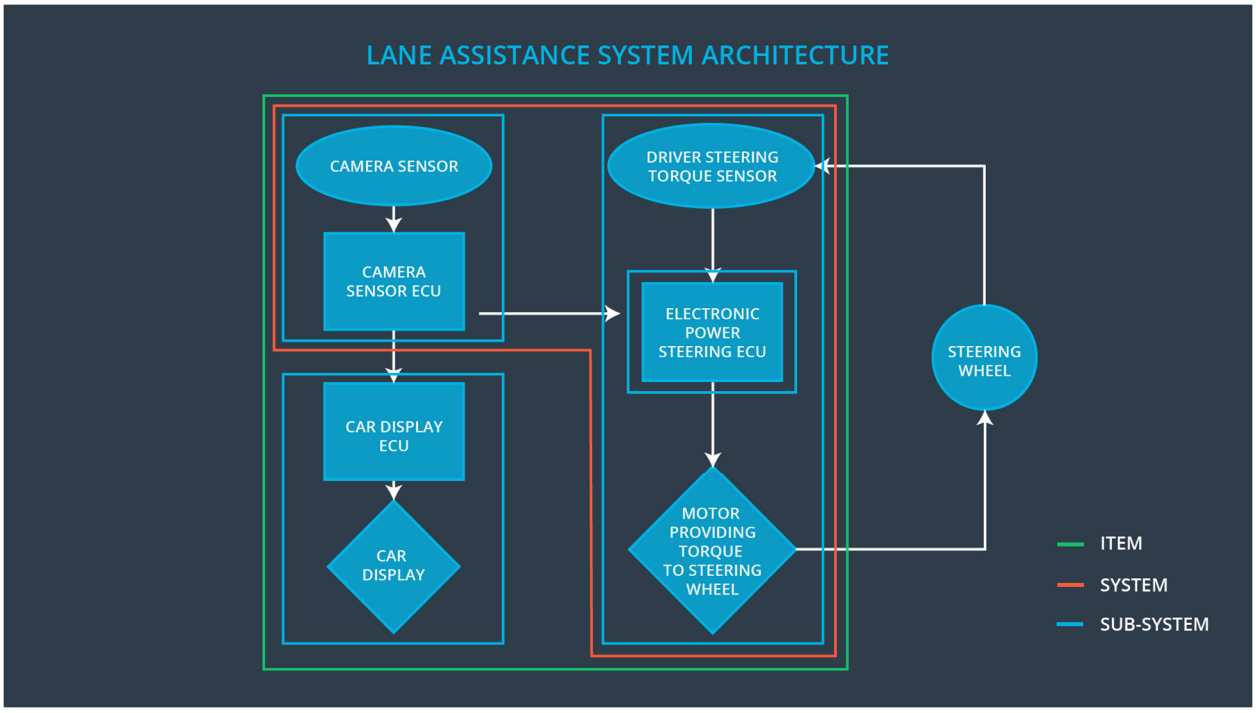

Fig 1 Lane Assistance System Architecture
[Image source: https://udacity.com]

There are three subsystems involved in the lane assistance system architecture.

1. Camera
2. Display ECU
3. Electronic Power Steering ECU

Each of the subsystems are responsible for both of the functions.

Camera sub system is responsible for detecting and measuring the deviation of the vehicle from the center of the lane for the lane keeping assistance function.

Display ECU sub system contribute to lane keeping assistance function and is responsible for providing indication that the lane keeping assistance function is ON or OFF and also

provide a warning if the vehicle deviates from the center of the lane. Also, Display ECU sub system is outside the lane assistance system.

Electronic Power Steering ECU is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request and aid the lane keeping assistance function.

The functionality of the lane assistance system is subject to some operational and environmental limitations like the availability of lane markings, and ability of the camera to detect the lane markings and paintings.

Standard ISO 26262 provides a framework for reducing risks that could harm people's health and only covers electronic and electrical malfunctions in passenger vehicle systems.

Standard ISO 11270:2014 contains the basic control strategy, minimum functionality requirements, basic driver interface elements, minimum requirements for diagnostics and reaction to failure, and performance test procedures for Lane Keeping Assistance Systems (LKAS). LKAS is intended to operate on highways and equivalent roads.

Goals and Measures

Goals

The main goal of this project is to ensure functional safety of Lane assistance system by identifying hazards in Electrical/Electronic components of Lane Assistance system that could cause physical injury or damage to a person’s heath, evaluate the risk of the hazardous situation and via systems engineering prevent accidents by lowering the risk to reasonable 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	Safety	Constantly

planned safety activities	Manager	
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 the company's 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

A typical safety lifecycle contains three phases – Concept Phase, Development Phase and Post Production release. For this project, the scope of safety lifecycle is limited to Concept Phase and Development Phase pertaining to system design and software product development.

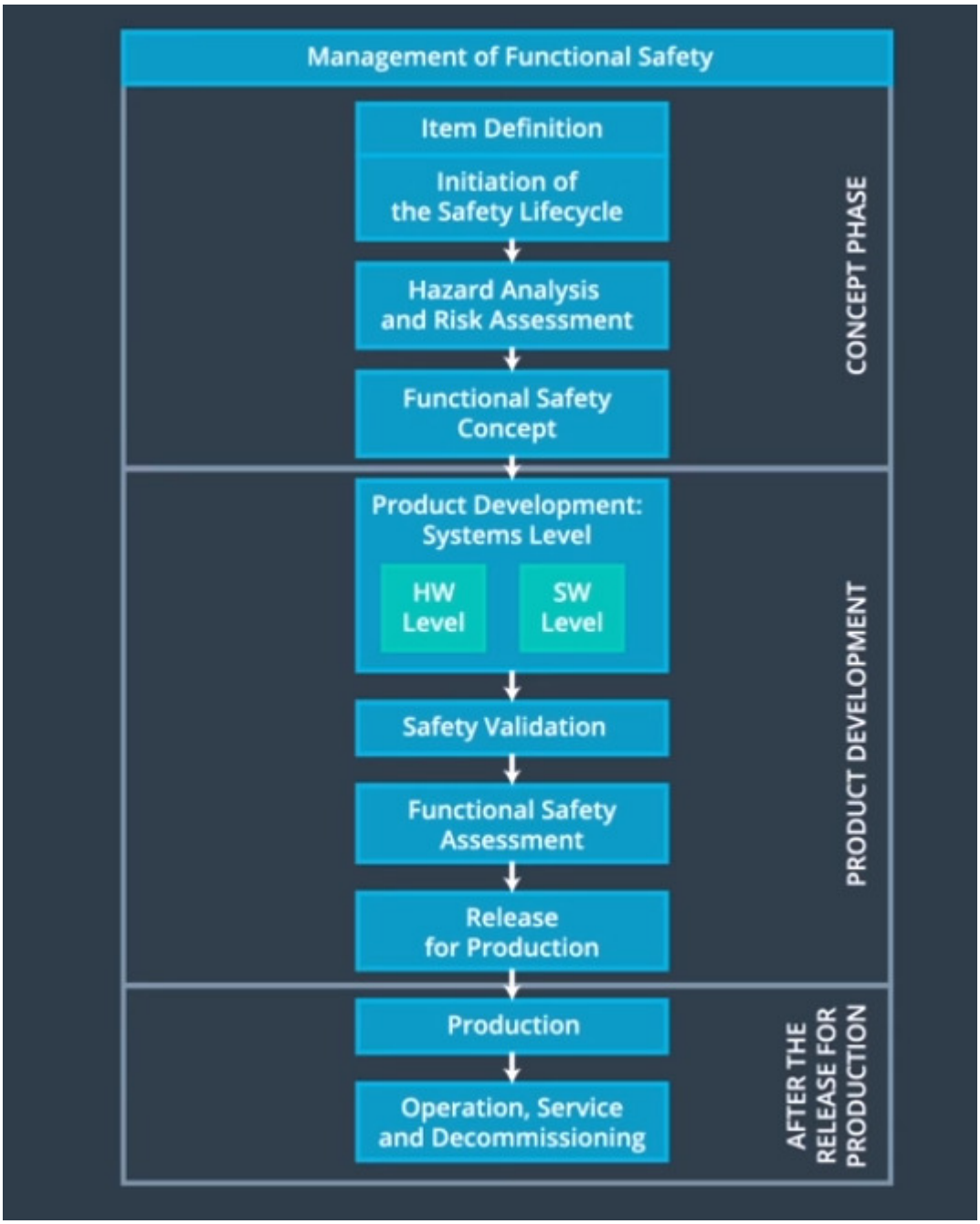

Fig 2 Safety Lifecycle
[Image source: https://udacity.com]

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 a development interface agreement is to ensure all parties involved in developing safe vehicles are in compliance with ISO 26262. It avoids disputes and define the liability in the way to clearly know who should fix safety issues.

OEM will provide the requirements on the functioning of lane assistance system to Tier I supplier. The Tier I supplier should define the safety plan, identify hazards and evaluate risk associated with the sub systems and modify sub-system design with respect to the functional requirements and reduction of the level of risk.

Confirmation Measures

The main purpose of confirmation measure is to ensure

- the functional safety project confirms to ISO 26262
- the project really does makes the vehicle safer

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. People who performs the confirmation review need to be independent people who actually developed the project.

Functional safety audit is a check performed by safety auditor to make sure that the actual implementation of the project confirms to the safety plan.

The functional safety assessment is performed by the safety assessor who confirms that plans, designs and developed products actually achieve functional safety.