Safety Plan Lane Assistance

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

Document history

Date	Version	Editor	Description
5/23/2018	V1	Shamsher Singh Thind	Version-1

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan is created to manage and guide the execution of safety related activities Identify the high risk situation and lower risk to reasonable levels. And to prove the solution with actually lower the risk

Using the following three step approach:
- Identifying hazards
- Measuring risk
- Using System Engineering to lower risk

As functional safety manager, we also need safety engineer to anticipate what will go wrong with a vehicle when the vehicle is still in the design phase.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

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 drivers that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back towards the center of the lane.

Lane assistance system has to functions.
- Lane departure warning
- Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback
Lane keeping assistance function shall apply the steering torque when in order to stay in current lane.

Item boundary includes three sub-systems which are all responsible for each function:
- Camera system
- Electronic Power Steering system
- Car Display system
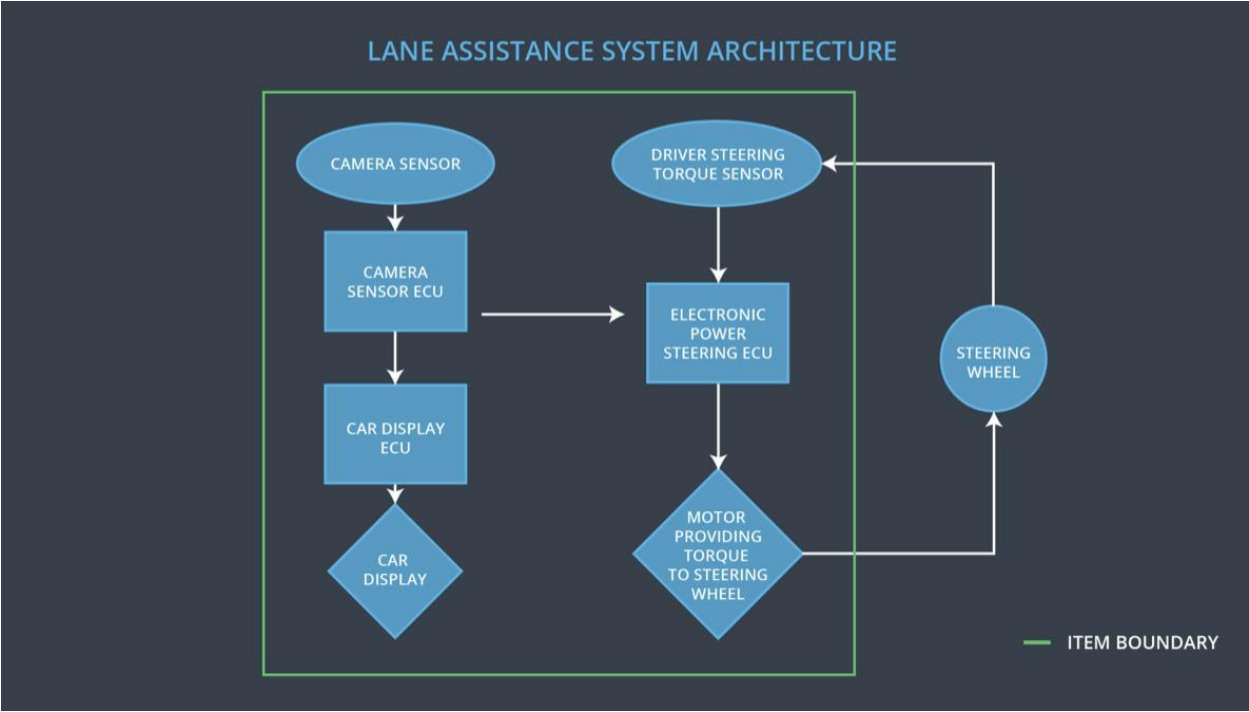
Goals and Measures

Goals

The main goal of this project is to ensure the functional safety of the item during usage, by Identifying the high risk situation and lower risk to reasonable levels, as per ISO 26262

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

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 is the highest priority, all the design decisions are independent made by different team. And then tested & validated independent of the team designing it. And any person or group that help identify the risk shall be rewards by the organization

Safety Lifecycle Tailoring

The following phases of the safety lifecycle are in scope:

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

The following phase 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

Purpose of a development interface agreement:

- A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product.
- **Avoid disputes**: 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.
- **Liability** and makes clear who should fix safety issue

As functional safety manager and functional safety engineer from tier-1 organization, we would need the following:
- 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

Confirmation measures serve two purposes:
- That a functional safety project conforms to ISO 26262 and
- That the project really does make the vehicle safer.

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.

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.