Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
08/08/2017	1.0	Thomas Ho	Initial version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this document is to specify how functional safety will be achieved for the lane assistance system throughout the entire development project and in production. The safety plan lists the various techniques and measures that will be implemented as part of the development project to ensure that the targeted ASIL is achieved.

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

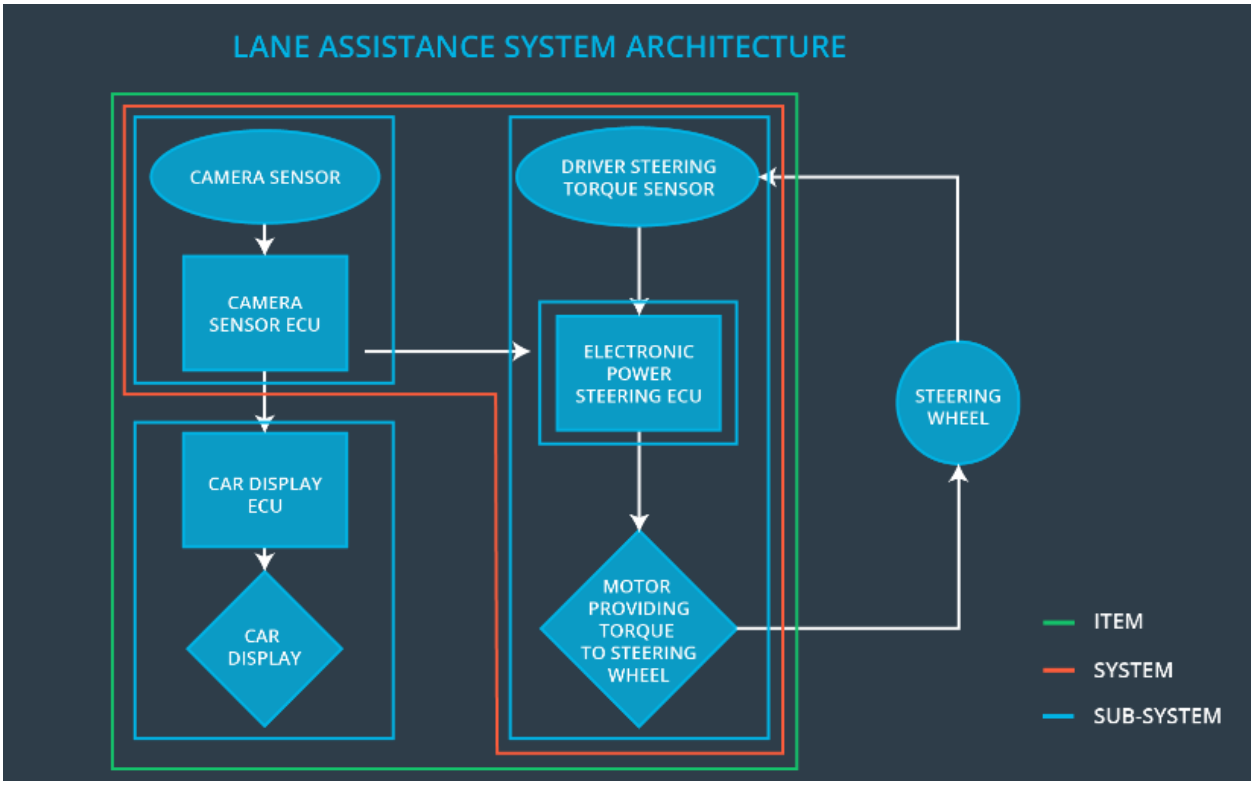
Item Definition

The Lane Assistance System is vehicle safety feature designed to alert the driver when the vehicle moving from its lane unintentionally, and assist the driver to navigate the car to stay on the current lane.

The lane assistance system has two main functions:

1. **Lane Departure Warning** alerts the driver when the vehicle starts to deviate from its lane and apply an oscillating steering torque to provide the driver a haptic feedback.
2. **Lane Keeping Assistance** helps the car to stay near the center of lane by applying an amount of torque in a limit time.

Following figure shows the lane assistance system architecture



The lane assistance system consists of three subsystems:

1. Camera subsystem
2. Electronic Power Steering subsystem (EPS)
3. Car Display subsystem

The camera monitors the road and recognizes the lane structure. Once it detects the vehicle is drifting out of the current lane, it sends a signal to car display ECU to turn on a warning light, at the same time, it also send a signal to electronic power steering subsystem to asking it to vibrate the steering wheel.

If the driver wants the change the lane, 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.

Goals and Measures

Goals

The goals of this functional safety project are:

1. Identify the hazardous situation from electronic malfunctions that could cause injury to human or damage human health.
2. Assess the risk level of hazards
3. Lower the high risk level of hazardous situation to an acceptable risk level via system 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	Project 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

Safety is critical to the success of a vehicle product and the organization:

- **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 make 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 process.
- **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 development interface agreement (DIA) defines the roles and responsibilities between companies involved in the product development. All involved parties need to agree on the contents of the DIA before 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.

The responsibilities and personals of the companies involved in the project include:

- An **OEM program manager** who will communicate with OEM partners on product schedule, resource allocation and component selections. Functional safety plan shall be provided to OEM partner at the beginning and ensure the confirmation of requirements by working with third party auditor and safety assessor.
- **OEM Safety manager** who will develop safety plan and work with OEM safety manager during the whole safety lifecycle.

Tier one OEM is responsible for supplying a functioning lane assistance system. The persons interfaces with the company include:

- A **project manager** who will manage the resource to develop the lane assistance system based on the requirement provided by the vendor. The manager also communicates with vendor program manager on product requirement and development schedule.
- **Safety manager** who will work with vendor's safety manager to ensure the product confirms the safety requirement.

Confirmation Measures

The confirmation measures serve two purposes:

- The lane assistance system safety project conforms to ISO26262, and
- The project does make the vehicle safer.

The **confirmation review** ensures that the product compiles with ISO26262. As the product is developed, a third party safety auditor will review the work to ensure its compliance with standard. The **functional safety audit** will ensure the actual implementation of the project conforms to safety plan. The **functional safety assessment** will ensure that plans, designs and product development 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.