Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 4.0
Released on 2017-10-31

Document history

Date	Version	Editor	Description
10-23-2017	1.0	Brian McHugh	Set up template
10-24-2017	2.0	Brian McHugh	Initial draft
10-27-2017	3.0	Brian McHugh	Complete up to DIA
10-29-2017	4.0	Brian McHugh	Finalize

Table of Contents

Introduction

Purpose of the Safety Plan

Provide an overall framework for the Lane Assistance item, and to assign/define roles and responsibilities with respect to functional safety for this item. This plan lists the techniques that will be utilized and the steps that will be taken to in order to achieve functional safety.

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/feature for this functional safety project is one form of an Advanced Driver Assistance System (ADAS): **Lane Assistance System**. Whilst activated and when no turn signal has been triggered, the system shall take steps to keep the vehicle centered within ego lane.

The Lane Assistance System will have two functions:

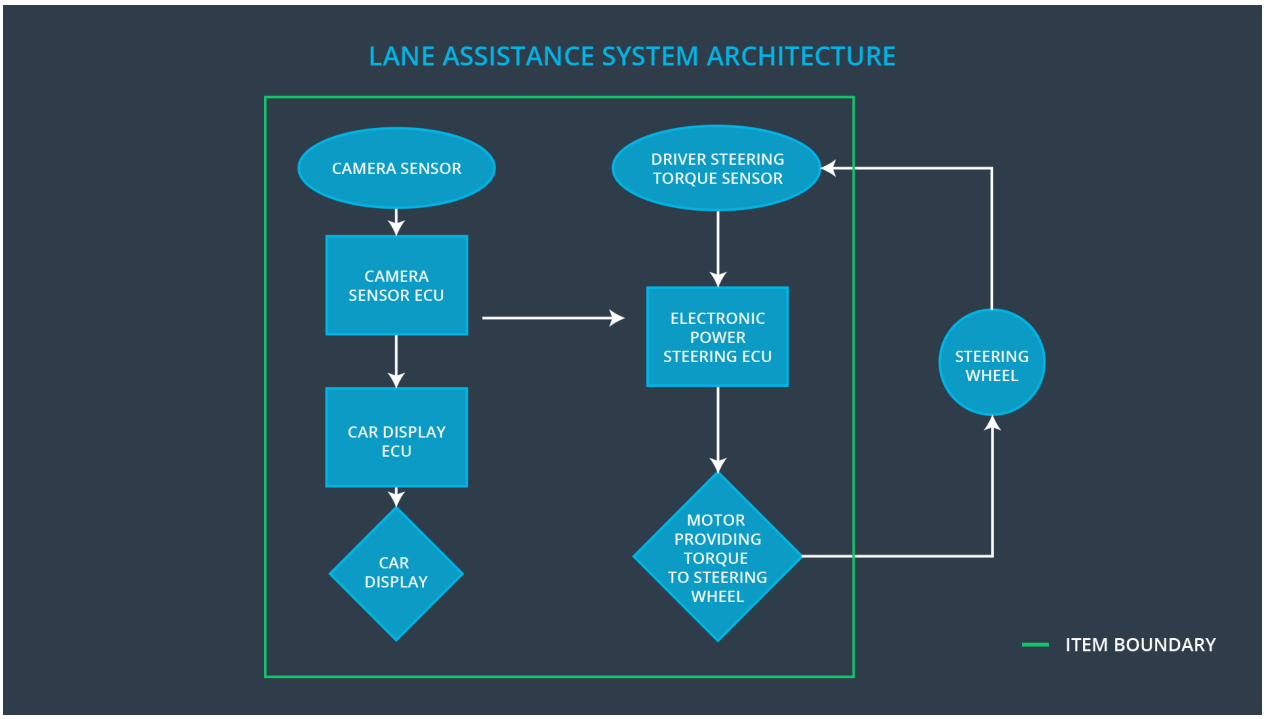
- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

When the driver drifts towards the edge of the lane, two things will happen:

- The **Lane Departure Warning (LDW)** function shall apply an oscillating steering torque to provide the driver with haptic feedback
- The **Lane Keeping Assistance (LKA)** function shall apply the steering torque when active to stay in ego lane

The Lane Assistance System will involve these three subsystems and the system architecture with respect to the item can be seen in the diagram further below:

- Camera Subsystem
- Electronic Power Steering (EPS) Subsystem
- Car Display Subsystem



Operational and Environmental Constraints

The Lane Assistance System relies upon a set of stereo cameras (mounted inside and at the top of the windshield) to identify lane markings on the road. If the cameras' view is obstructed or lane boundaries are not evident, the system will be unavailable for use by the vehicle operator.

Possible hindrances that could prevent the system from being operational:

- Roads that lack lane markers
- Obstructions on the windshield, such as dirt or snow
- A damaged windshield, whereby cracks in the glass alter the view of the cameras
- Lane markers that are covered by things such as snow or standing water
- Weather that prevents the cameras from detecting lane markers (e.g., fog, heavy rain)
- Sunlight or other light source that shines directly into cameras, effectively blinding them
- Vehicle operator following another vehicle so closely that there's no room to detect lane markers

Legal Requirements

In the US, street vehicles must be compliant with the standards set forth by the National Highway Traffic Safety Administration (NHTSA). The vehicle's OEM is responsible for providing proof of compliance for all its vehicles and the systems contained within them.

Standards

The Lane Assistance System shall be designed, developed and implemented utilizing the framework of Standard 26262 from the International Organization for Standardization (ISO).

Goals and Measures

Goals

The goals for this functional safety project are as follows:

- Identify possible hazards resulting from electronic malfunctions that could cause injury to humans or damage human health
- Assess the risk level of hazards
- Bring high risk hazards down to acceptable risk levels using 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	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

Fostering good safety culture within the company is viewed as vitally important to company success:

- **Accountability** - steps are taken to ensure that records are maintained regarding the people/teams responsible for design decisions
- **Benefits** - the company motivates and rewards the achievement of functional safety
- **Communication** - fluid lines of communication encourage disclosure of problems
- **Consequences** - shortcuts that jeopardize quality or safety will be met with consequences for those responsible
- **Diversity** - input from all team members is encouraged, appreciated and integrated into processes
- **Expectations** - design and management processes are clearly defined so all participating team members know exactly what is expected of them
- **Highest Priority** - safety supersedes all competing constraints, such as cost and productivity
- **Independence** - the auditing process is carried out by a team independent of the ones that design and develop a product
- **Resources** - all projects are provided with the necessary resources, which includes appropriately skilled manpower

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
Project Manager - Item Level	OEM
Functional Safety Manager - Item Level	OEM

Functional Safety Engineer - Item Level	OEM
Functional Safety Manager - Component Level	Tier-1 Supplier
Functional Safety Engineer - Component Level	Tier-1 Supplier
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

Development Interface Agreement

A **Development Interface Agreement (DIA)** 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, in an effort to avoid disputes later on. The DIA also specifies what evidence and work products each party will provide to prove that work has been done according to the agreement, in an effort to avoid disputes later on. Clarification on who will be responsible for any safety issues in post-production is also addressed.

Ultimately, the goal of a DIA is to ensure that all parties involved are developing safe vehicles in compliance with ISO 26262.

The OEM shall deliver a functioning Lane Assistance System. The Tier-1 Supplier shall develop and produce the system, whilst providing functional safety support at the component-level, with analysis and modifications to the specified subsystems in accordance with ISO 26262.

OEM responsibilities:

- Assign a **Project Manager** who will oversee the overall project and allocate the necessary resources, including personnel, namely a Safety Manager and Safety Engineer
- The Project Manager will provide requirements for the Lane Assistance System to the supplier
- Provide a **Safety Manager** who will write the safety plan for the Lane Assistance System and monitor the project's progress against that plan
- Allocate a **Safety Engineer** who will be responsible for architectural designs and integration and testing for the Lane Assistance System and who will provide requirements for the Lane Assistance System to the supplier
- Assign a **Safety Auditor** (internal or external) to make sure all processes are implemented in accordance with ISO 26262
- Provide an **independent** Safety Assessor (internal or external) to judge whether or not the project has made the vehicle safer

Tier-1 Supplier responsibilities:

- Provide a **Safety Manager** who will write the safety plan for the Camera, EPS and Car Display subsystems and monitor the progress of that plan
- Provide a **Safety Engineer** who will be responsible for architectural designs and integration and testing for the subsystems associated with the Lane Assistance System

Confirmation Measures

Confirmation Measures serve two purposes and shall be carried out by personnel who are independent from the development team:

- ensure that a functional safety project conforms to ISO 26262
- confirms that a functional safety project does in fact make the vehicle safer

A **Confirmation Review** will be completed to ensure that the project complies with ISO 26262. As the product is designed and developed, an independent person will review the work to make sure ISO 26262 is being followed.

A **Functional Safety Audit** shall be done to make sure the project conforms to the safety plan.

Additionally, a **Functional Safety Assessment** is expected, which will seek to confirm that plans, designs and the end products do in fact achieve functional safety.

Note: 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.