Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-09-10

Document history

Date	Version	Editor	Description
Sept 09 2017	0.1	RE	Draft
Sept 13 2017	1.0	RE	INITIAL RELEASE

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan outlines and documents the process used to achieve functional safety for the implementation of an Advanced Driver Assistance Systems (ADAS). The safety plan provides traceability of the process used to achieve functional safety. It defines roles and responsibilities of the project team members and provides accountability for safety performance. The safety plan defines safety goals for the project and outlines the corresponding confirmation measures. In the case where the project is developed across multiple parties, Development Interface Agreements are issued to define responsibilities and interface specifications across departments or companies. The safety culture of the organization executing the project is also described as evidence of safety oriented process.

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 Advanced Driver Assistance System is an electromechanical system which, for the scope of this project shall provide two functions:

1. Lane departure warning: The system will provide feedback to driver when the system detects that the vehicle is unintentionally departing its current lane.
2. Lane keeping assistance: The system will actuate vehicle controls to assist the driver in positioning the vehicle into the center of the current lane.

The system shall be limited such that it may not be used for autonomous driving functionality, only warnings and assistance will be provided. Limitations on the usability of the system will also be described based on the operating environment and scenarios for the vehicle.

This functionality will be achieved by implementing a camera and camera ECU / processor to perform computer vision of lane markings on the road. The camera control unit will calculate desired torque requirements and issue requests to the electronic power steering ECU. It will also issue lane departure warning requests to the electronic power steering ECU where the steering wheel should be vibrated to warn the driver. The camera control unit will communicate with the car display ECU to indicate its state (ON/OFF/FAULT) on car display.

The electronic power steering system shall receive torque requests from the camera ECU and actuate the power steering motor to achieve the desired response. The power steering motor shall also detect driver steering input and ensure that the ADAS system is only functional when the driver is in control of the vehicle.

The overall hardware system architecture is given in Figure 1. The scope of the system is shown in the orange box and is made up of two sub-systems shown in blue boxes:

1. The camera sensor and camera sensor ECU subsystem: is responsible for detecting lane lines and determining when the vehicle leaves the lane lines. Issues steering and warning request to the electronic steering ECU.
2. The electronic power steering subsystem: is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a llane assistance system torque request. Vibrates the steering wheel to warn the driver of lane departures. This system consists of the electronic steering ECU, the motor actuator for the electric steering system and a torque sensor for driver input.
    a. The electronic steering ECU and on board software are considered to be a subsystem of the electronic power steering subsystem. This shall carry out all software functionality required to safely detect and actuate the steering wheel based on commands from the camera subsystem.

The ADAS interfaces with the vehicle’s display subsystem, including the car display and car display ECU but this sub-system does not fall within the scope of the ADAS.

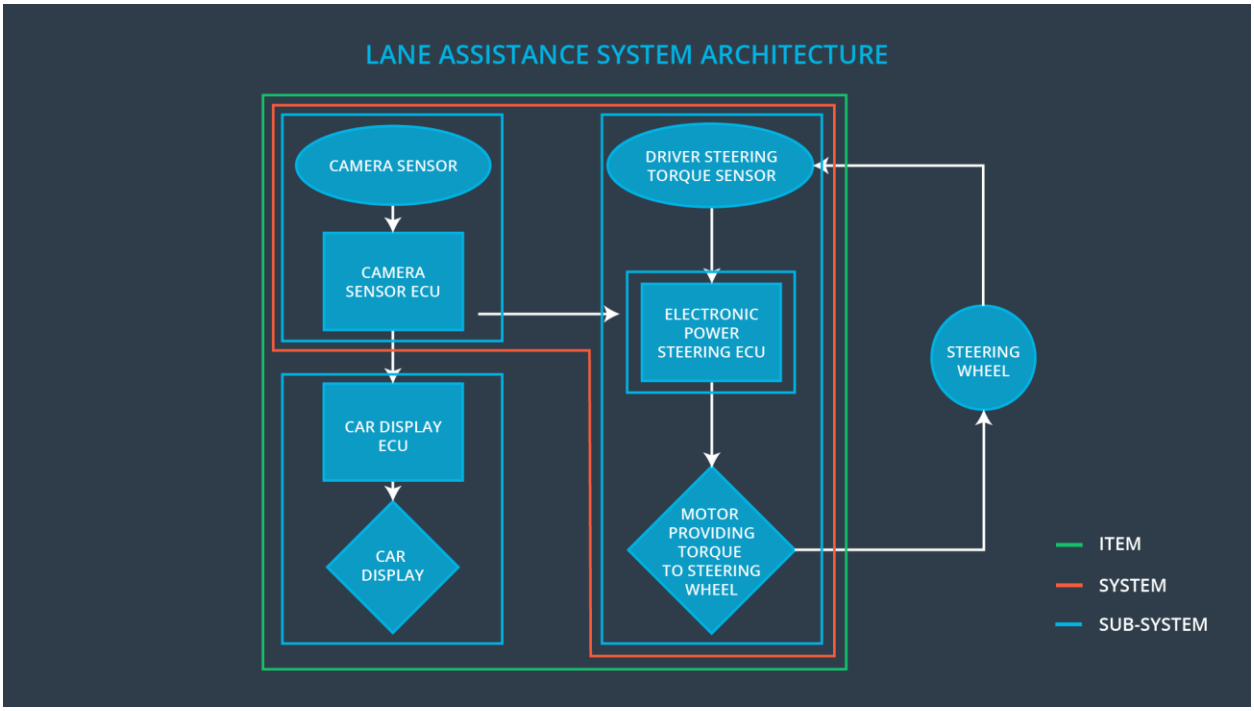

Figure 1: ADAS general hardware architecture

Operating Constraints and Limitations

The ADAS system under consideration shall be designed to operate under most normal driving conditions. It will not function under certain operation and environmental constraints. The system shall shut off and indicate its status on the vehicle display when it is being operated outside physical or software capabilities. In general, line lanes must be detectable by the camera sensor and require proper illumination, line patterns must also correspond with normal road marking patterns. Some examples of situations outside of the ADAS' capabilities are listing in Table 1.

Table 1: ADAS performance violations

Case	Example situation	Cause of performance violation
1	Driving at night without headlights on	Improper illumination
2	Driving on a dirt road	No lane markings for detection
3	Driving with snow on the ground	Lane markings obscured
4	Driving in fog	Lane markings not visible to camera system
5	Driving in a parking lot	Markings inconsistent with traffic lane marking standards
6	Driving in a construction zone	Lane markings may not be present or may be inconsistent

		with standards
7	Driving in heavy rain	Lane markings may not be continuously detectable, rain on windshield obscures camera optics

Legal Requirements in Canada

TBD – not included for this submission

International Standards

TBD – not included for this submission

Previously known safety-related incidents

TBD – not included for this submission

Goals and Measures

Goals

The goal of this project is to achieve functional safety of the ADAS item by analyzing the system functions with ISO 262626. This will allow identification of hazards and quantification of risk. Systems engineering will be used to minimize risk to a level such that it is acceptable to the public and does not further increase the level of risk pertaining the operating the vehicle. Through this process all unreasonable risk situations are mitigated for the ADAS.

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 Manager	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 at Edwards Kill-Bot corp, a subcontractor to ADAS engineering inc, safety of our engineering services is paramount to our workplace and the success of to our company. We are ISO 9001 compliant. Safety is prioritized over both deadlines and profitability. Your project will not ship unless it has passed stringent engineering testing consistent with quality management standards. The following themes make up the safety culture at the Edwards Kill-Bot Corporation:

Empowering employees: Employees are incentivized and promoted based on adhering to company standards to produce documented, tested and verified kill-bot systems. Our platforms are engineering according the latest in international standards. Our management sits on the board of international safety committees which develop standards in killer robot automation and ADAS.

Penalizing employees: Employees found to be in non-compliance with our safety culture do not last long at kill-bot corp. Project managers who compromise safety, testing and documentation to promote project schedule and budget are terminated.

Documented accountability: At each stage of the project responsibility for design decisions, execution and testing is clearly outlined and communicated in our project planning structure. Decisions are traceable and staff are acutely aware of their responsibilities.

Traceable design process: Design and process decisions are recorded at each step of the process. Compliance with applicable standards is reported during the concept and design phase. This is accomplished the creation of Product Requirements Documents (PRD) and subsequent Technical Requirements Documents (TRD).

Independent verification: Independent testing organizations or industry peer companies are contracted to provide independent verification of our non-standard platforms which will work in the field along human-operators. Feedback and guidance is incorporated into future work. All valid concerns from the verifying party will block a project until resolved to our satisfaction.

Engineering workflow and production process: Our project execution and engineering follow a strict reporting structure. Production is carried out with detailed check-lists and system tests which must be complete and signed before release.

Resources and skills: Only sufficiently skilled employees and robots are assigned to engineering projects. Junior engineers only work under the guidance of a supervisor.

Reporting: Our continuous employee training and safety awareness programs ensure workers have the knowledge and confidence to report safety related issues and design flaws.

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

This product shall be integrated into existing vehicle architecture. All relevant interfaces and integration to the vehicle shall be included in the scope. Functional safety shall be considered

for all interactions and 2nd order interactions with other vehicle systems. Examples include: the car display, the car cruise control.

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

1. **What is the purpose of a development interface agreement?**

The DIA defines the roles and responsibilities between companies participating in a product development. It provides accountability between the companies. It also outlines what evidence shall be provided to substantiate work was executed according to the agreement. This may including reporting on testing, independent verification results.
The DIA may include the following sections:

- Appointment of supplier and client safety managers
- Tailoring of the safety lifecycle
- Scope of work and activities to be performed by each party
- Information to be exchanged.
- Processes and tools which support the project to ensure compatibility across organizations.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

]

<This isn't clear, nowhere else in this project can I find the role definition of my company. I'll assume I'm a tier 1 supplier, specifying the systems level architecture to the OEM and carrying out the software work per the scope of the project>

OEM:

- Appoint safety manager
- Supply hardware – responsible for manufacturing prototypes and production
- Define hardware safety lifecycle
- Supply all interface specifications suitable for analyzing hardware, all data sheets, MTFB data, design documents, schematics and drawings
- Supply all specifications required for programming the hardware
- Supply all test data to date

Edwards Kill-Bot Corp:

- Appoint company safety manager
- Supply systems level architecture specifications
    - Define the item, system and subsytems
    - Define component functionality
    - Define interface specifications between components
- Supply safety lifecycle of the system
- Provide a functional safety analysis on the systems level architecture (big V)
- Provide a functional safety analysis on the software level architecture (little V)
- Provide Subsystem verification and design documentation
- Provide Systems level verification and design documentation

Confirmation Measures

1. **What is the main purpose of confirmation measures?**

Confirmation measures ensures that the functional safety project conforms to ISO 26262 and does make the system safer

2. **What is a confirmation review?**

The confirmation review ensures that the project complies with ISO 26262. This is carried out as the product is designed and developed by an independent person.

3. **What is a functional safety audit?**

The functional safety audit confirms the actual implementation of the project conforms to the safety plan

4. **What is a functional safety assessment?**

A safety assessment confirms that the design and product 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.