Elektrobit

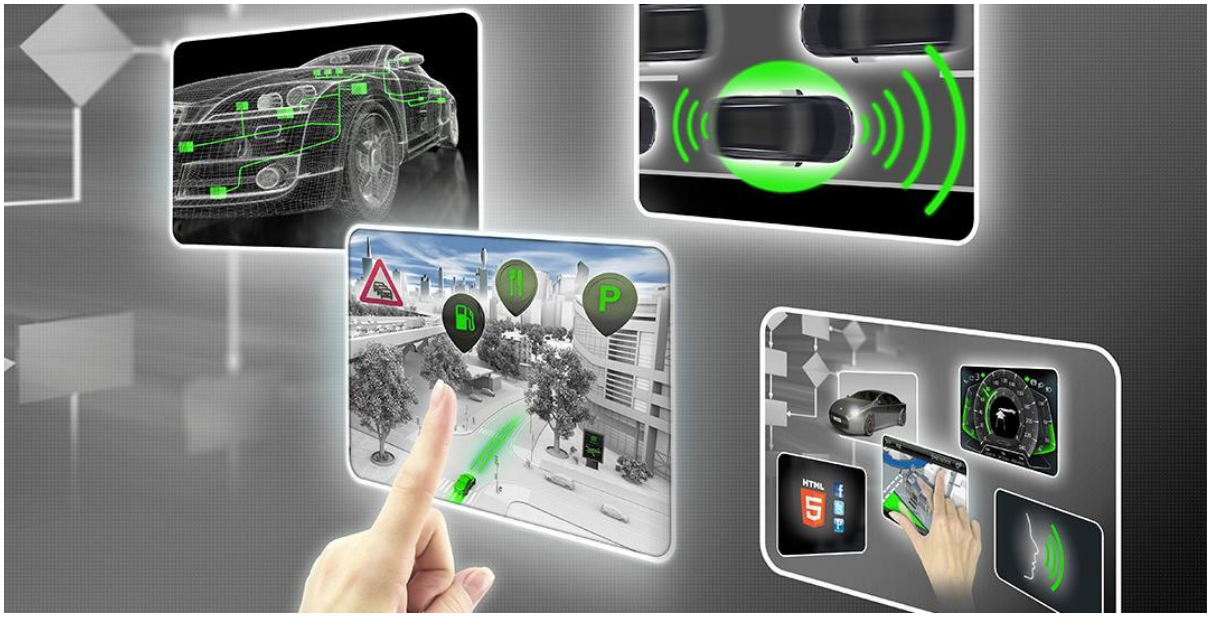
UDACITY

Safety Plan

Lane Assistance

Document Version: 0.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2017-09-13	0.1	Olli Vertanen	Initial version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is describe the item under development, its general functionality and boundaries — also from the environmental and legal point of view.

In addition, the objective of this plan is to define safety management roles and responsibilities, and the liabilities of the organisations that participate development of the item. Also, the safety plan describes how the organisational safety culture contributes to the safety of the item.

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

ISO 26262 defines an item as a system, or array of systems to implement a function at the vehicle level. A system, in turn, consists of elements that can be sensors, actuators, controllers, or another system (sub-system).

The Lane Assistance System (LAS) is one type of Advanced Driver Assistance System (ADAS). The purpose of the item is to help the driver in keeping the vehicle within the ego (current) lane, and by doing so, avoid possible hazards caused by unintentional drift off the lane.

Functional and non-functional requirements

The functional concept

The lane assistance (LA) system has two main functions:

1. Lane departure warning (LDW)
2. Lane keeping assistance (LKA)

The lane departure warning function is responsible of detecting situation, where the vehicle is drifting off the current lane unintentionally. The function will alert the driver when it notices this happening. Alert is given visually and haptically. The visual warning is a warning light on vehicle display, which is switched on. The haptic feedback is given to driver via steering wheel vibration. When driver is intentionally departing the lane, or the function is turned off, there will be no alert.

The lane keeping assistance function will assist the driver to keep the vehicle within the ego lane. This function is only active, when the lane departure warning function has detected lane departure (i.e. alert is done). In this situation, the function will reactively steer the vehicle back towards the centre of the lane. Driver is expected to keep both hand on steering wheel all the time, and the responsibility for the safe operation of the vehicle always remains with the driver.

The function is mainly targeted for highway or equivalent driving.

The system can be in three states:

1. Enabled, Inactive
2. Enabled, Activated (LDW warning given, LKA assisting)
3. Disabled

Operational and Environmental Constraints

The system uses camera that is mounted on the top of the windshield, behind the rear-view mirror. The camera constantly monitors lane markings ahead. The system cannot be operational, if the camera cannot detect lane markings. At least the other of the lane boundaries must be clearly marked.

Lane detection is not possible if

- Camera is obscured (e.g. snow or dirt on windscreen, windscreen broken etc.)
- Both lane markings are missing or vague.
- Both lane markings are temporarily undetectable because of environmental conditions (e.g. snow, water, fog, low light situation, direct sunlight to camera).
- Lane markings are temporarily undetectable because of technical issues (e.g. direct sunlight to camera's lens, vehicle's head lights not working)
- Lane markings are ambiguous e.g. because of road work markings.
- Driver's behaviour like driving too close to vehicle in front, or driving too fast on curves

The system will not be active if

- Ego-lane cannot be detected.

- Turn indicator is active (intentional lane change).
- Vehicle's speed is below 40 km/h.
- Vehicle is heavily accelerating or decelerating.
- The steering angle exceeds threshold value (as when trying to avoid collision).
- Failure in the motor that gives torque to steering wheel.

Also, other ADAS functions may co-operate with the system, and deactivate it:

- Side-collision warning should deactivate LKA in case the warning comes from the side LKA is steering to.
- If lane change assistant is active, the LA system should deactivate

Legal requirements, National and International Standards

In the U.S. market, the vehicle must be compliant with the standards from National Highway Traffic Safety Administration (NHTSA). The vehicle manufacturer is self responsible for providing proof for the compliance.

In the European market, new car model are approved by national government authorities. Approval requires compliance with Committee of the United Nations Economic Commission for Europe (UNECE) WP.29 recommendations (WP.29 is Working Party on the Construction of Vehicles.)

Compliance with ISO 26262 helps achieving these goals. This plan is a part of item compliance with ISO 26262 - Road Vehicles - Functional safety standard. The non-functional requirements of the LA system are regulated by two other international standard:

1. ISO 17361:2007 Intelligent transport systems -- Lane departure warning systems -- Performance requirements and test procedures: Specifies the definition of the system, classification, functions, human-machine interface (HMI) and test methods for lane departure warning systems.

2. ISO 11270:2014 Intelligent transport systems -- Lane keeping assistance systems (LKAS) -- Performance requirements and test procedures: 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)

General quality requirements for the item development are found in ISO/TS 16949 - Automotive Quality Management standard. These apply to safety related as well as to non-safety related features of the item.

For safety case development, the MISRA guidelines (Guidelines for safety analysis of vehicle based programmable systems, ISBN 978-0-9524156-5-7) shall be followed.

Behavioural Assumptions

The item is assumed to

- Indicate the driver the state of the system.
- If active, give warning to the driver when lane departure is detected, and assist the driver back to the centre of the ego lane.
- The system should be able to measure the steering torque the driver is using, in order to avoid over steering.
- The system should detect drive's manoeuvres for avoiding side-collision and not do any counter actions.
- The warnings from the item should not cause harmful driver distraction.

Consequences of Behavioural Shortfalls

The potential benefits of the system are two-fold. First, the system decreases the amount of unintentional drifts of the vehicle off the road, or to the adjacent lane. Second, the system prevents or at least mitigates the effects of intentional lane changes without turn signal.

The failure of the system may lead to:

- Head-on collision with on-coming traffic.
- Side-swipe collision with the traffic going same direction.
- Impact with the vehicle in the rear or in the front going the same direction.
- Driving off the road accident.

An other type of shortcoming is a false alarm from the system. False alarms should not cause any unacceptable harm. Too frequent false alarms may, however, lead to frustration and turning off the system, or the driver just ignore the warnings.

Item Boundary

The item consists of three sub-systems:

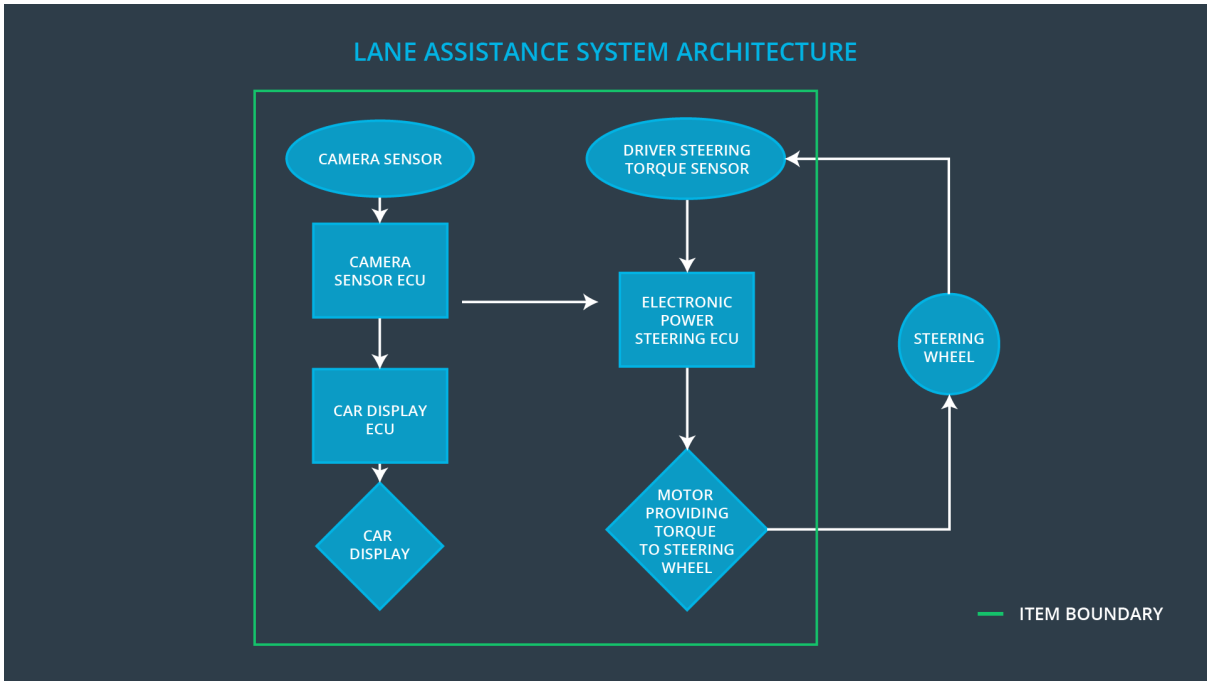
1) Camera sub-system (CSS)
2) Electric power steering sub-system (EPSSS)
3) Car display sub-system (CDSS)

The actual Lane Assistance System consist of sub-systems 1 and 2. Display sub-system is used for informing the driver about the state of the LA system. Display sub-system has many other responsibilities.

The camera sub-system has two components: 1) camera sensor and 2) camera sensor ECU. It is responsible of detecting the lane ahead of the vehicle and the lane departure, and giving the departure alert. Camera sensor is mounted on the top of the windscreen and provides the road view in the front of the car. The camera sensor ECU receives camera images and applies computer vision techniques in order to detect lanes and vehicle's position within the lane. The sub-system will give a visual alert request signal to CDSS, and haptic alert request signal EPSSS. If the lane assistance function is activated, but the CSS cannot detect lane markings, a warning light is activated.

The electronic power steering sub-system has three components: 1) driver steering torque sensor, 2) motor providing torque to steering wheel and 3) electronic power steering ECU. The EPCSS is responsible of giving assisting and alerting steering power to the steering wheel. This is done by motor that applies torque to the steering wheel when alerting or corrective steering is needed. The sensor measures how much torque the driver is currently applying to the steering wheel in order to adapt the given steering torque. In case of lane departure alert the EPSSS applies vibrating torque to the steering wheel. This means turning the wheel back and forth in certain frequency. Also, the lane keeping assistance function can apply steering torque to the steering wheel.

The car display sub-system has two components: 1) Car Display and 2) Car Display ECU. It is responsible of giving the driver visual lane departure alert on car's instrument cluster display. Also, if the item is active, but lane markings could not be detected, a visual warning is given.



There are vehicle elements outside the item boundaries that affect the item.

1. Steering wheel: Turning steering wheel gives input to the steering torque sensor.
2. Turn signal: When turn signal is activated, the LA function is turned off.
3. Dashboard switch: Switch can enable/disable the LA function

Goals and Measures

Goals

This work aims to identify the risks related to the lane assistance system and reduce the risks to a level that is acceptable by current legislation and society standards, and thus prevent traffic accidents.

The goal is achieved by following item's safety lifecycle phases described in 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

Meeting the criteria of the safety standard is not just a technical issue. The organisation must also adopt way of work that emphasises safety of the product. This safety culture shall include for example following principles:

- High priority: safety has the highest priority among competing constraints like cost and productivity. Human life cannot be compromised over cost!

- Proactive attitude towards safety: safety issues are discovered at the earliest stage possible in the product lifecycle.
- Continuous improvement: Dedicate resources for functional safety skill development and promote better safety development processes. Safety practices should be a constantly developing process.
- Authority: people that lead safety relevant activities should be explicitly appointed in all development phases.
- Accountability: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.
- Well defined processes: company design and management processes should be clearly defined.
- Documented work products: development of the safety work should be documented, as well as meetings, found issues etc.
- Independence during audit and reviews: teams who design and develop a product should be independent from the teams who audit the work.
- Independence during safety development: engineers developing safety related code or hardware should be different from the ones developing functional parts of the product.
- Resources: projects have necessary resources including people with appropriate skills.
- Communication: communication channels encourage disclosure of problems instead of hiding them.
- Diversity as advantage: intellectual diversity is sought after, valued and integrated into processes.
- Commitment: promote, with organisational decisions (rewards, penalties) and personnel training, overall commitment of the personnel to the safety culture.

Safety Lifecycle Tailoring

By safety lifecycle we understand all the safety activities during the concept phase, product development and after the release for production.

The purpose of this section is to make the distinction between a new item development and a modification to an existing item. In case of a modification, safety-related activities can be tailored, and impact analysis of modifications must be carried out.

Item definition is a prerequisite to safety lifecycle initiation. The item in question is defined in page 3. This information can be later supplemented by supporting information, like requests for change and implementation plans.

The safety item in question is a new a product, and thus no safety lifecycle tailoring will take place. All sub-phases of the lifecycle, as presented in figure 2 of ISO 26262, part 2 must be covered.

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

Development interface agreement (DIA) is an agreement between customer (OEM) and suppliers in which the responsibilities for activities, evidence or work products to be exchanged by each party, are specified. The objective of the DIA, is that the OEM and the suppliers jointly comply with the requirements specified in ISO 26262.

In this project the OEM is supplying a functioning lane keeping assistance product. The Tier-1 should analyse the product and modify it in order to achieve ISO 26262 compliance.

This DIA applies to lane assistance system (only within the scope defined in the introduction of this document) and involves the OEM, the Tier-1 and an independent external audit/ assessment company.

Responsibilities of the OEM

- Provide the initial design documentation (Systems functional and non-functional requirements, Software and hardware specification,
- Acceptance of the plans and work product from Tier-1 on the basis of the independent assessment.
- Implementation of the safety features

Responsibilities of the Tier-1

- Provide Safety Plan
- Provide Hazard Analysis and Risk Assessment
- Provide Functional Safety Concept
- Provide Technical Safety Concept
- Software Safety Requirements and Architecture
- Pre-assessment of the plans

Responsibilities of the Auditor/Accessor

- Independent assessment of the plans and work products (see confirmation measures)

Confirmation Measures

The purpose of confirmation measures is to give assurance that the project conforms to ISO 26262, and that the safety measures really does make the vehicle safer.

Confirmation measures include confirmation reviews, functional safety audit and functional safety assessment. Confirmation measures shall be independent with regard to the developers and management of work products.

Confirmation review is a confirmation that a work product meets the requirements of ISO 26262. In this project confirmation review must be conducted to following work products:

- Safety plan: evaluation of the compliance of the safety plan with the ISO 26262 safety lifecycle
- Hazard analysis and risk assessment: Evaluation of the completeness of the hazard analysis and risk assessment, and the correctness of the determined ASILs/QMs and the safety goals.

Functional safety audit evaluates the implementation of the processes required for functional safety. This should be done during the execution of these processes and against the definitions of the activities referenced in the safety plan.

The purpose of functional safety assessment is to confirm that plans, designs and developed products actually achieve functional safety. The assessment includes safety audits, evaluation of the work products required by the safety plan (confirmation reviews), and a review of the appropriateness and effectiveness of the implemented safety measures. Functional safety assessment shall be conducted before the item is released to production. The assessment can be repeated and updated.

In this project, all confirmation measures are executed by an external and independent company. Confirmation measures are accepted by the OEM.

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.