Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-05-2018	1.0	Fuqiang Huang	First Attempt for Submission

Table of Contents

Table of Contents

Introduction

Purpose of the Safety Plan

Vehicle are complex systems with both sociological and technical requirements. Designing a safe vehicle requires more than a methodical analysis of hardware and software components. The purpose of the Safety Plan is

- to force the teams and the companies involved to define roles and responsibilities, and
- to outline the steps to take 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 definition describes which vehicle system is under consideration as well as the system boundaries clarifying what is inside versus outside the system.

Item Definition

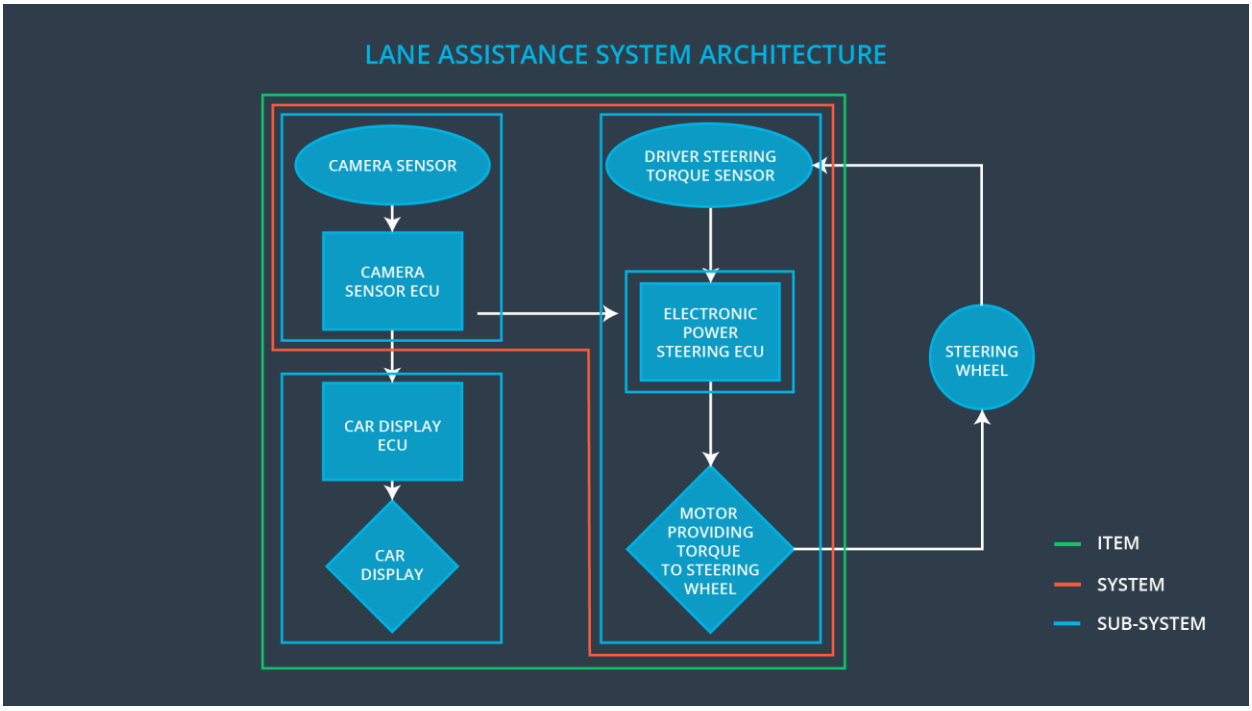
The item in the safety plan is the Lane Assistance System, part of an Advanced Driver Assistance System (ADAS), which shall alert the driver to potentially dangerous situations and take control over the vehicle to prevent accidents from occurring.

Main Functions

The Lane Assistance System has two functions:

- **Lane departure warning**: shall warn the driver by vibrating the steering wheel (i.e., shall apply an oscillating steering torque to provide the driver a haptic feedback) when the driver drifts towards the edge of the lane.
- **Lane keeping assistance**: shall automatically assist the driver by moving the steering wheel so that the wheels turn towards the center of the lane (i.e., shall apply the steering torque when active in order to stay in ego lane which refers to the lane in which the vehicle currently drives) when the driver drifts towards the edge of the lane.

Subsystems



As shown in the architecture of lane assistance system above, the item consists of three subsystems:

- Camera subsystem: detects lane departures, sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel, and requests a warning light in the car display dashboard. It includes two elements:
  - Camera sensor
  - Camera sensor ECU
- Electronic Power Steering subsystem: vibrates the steering wheel to give a warning to the driver, and adds extra steering torque to help the driver move back towards the center of the lane. It includes three elements:
  - Driver Steering Torque Sensor
  - Electronic Power Steering ECU
  - Motor Providing Torque to Steering wheel
- Car Display subsystem: turns on a warning light in the car display dashboard to let the driver know that the lane assistance system is active, and provides a button on the dashboard so that the driver can also turn off the system completely if in need. It includes two elements:
  - Car Display
  - Car Display ECU

Where ECU stands for Electronic Control Unit. An ECU is a small computer that contains the hardware and software for a specific vehicle functionality.

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.
The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

What if the driver wants to leave the lane? If 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.

Boundaries

The item boundary is drawn to include three sub-systems:
- Camera subsystem,
- Electronic Power Steering subsystem, and
- Car Display system

But Steering Wheel subsystem is outside of the item.

Operational and Environmental Constraints

The item relies on visible lane markings. It has limitations and does not work properly
- where lane markings are not visible (e.g., worn out or covered by snow),
- when the road has a small curve radius,
- at low speeds (typically below 65 km/h), or
- in heavy precipitation.

There are also other factors that could cause the system to not function adequately, such as
- lighting,
- temporary lane markings at construction zones, or
- poor contrast between the road surface and lane markings.

Some of the limitations are technical and some are an effect of attempts to avoid frequent warnings in situations where the driver is deemed to be in control of the vehicle.

Source: The safety potential of lane departure warning systems

Legal Requirements

The lane assistance technology is designed to minimize accidents by addressing the main causes of collisions: driver error, distractions and drowsiness.
Under the common law approach, as applied by the states in the US, anything is allowed unless prohibited by law. In 2009 the U.S. National Highway Traffic Safety Administration (NHTSA) began studying whether to mandate lane departure warning systems and frontal collision warning systems on automobiles.

Source: Lane Departure Warning System at Wikipedia

National and International Standards

- The system is not particularly suitable for urban driving or driving on country roads. Use of this system is more sensible on motorways and similar fast roads.
- The driver remains responsible for controlling the vehicle even after LKAS has been activated, as a result of which the system measures the steering torque applied by the driver.
- The system is deactivated if the driver applies the brakes. The LKA system is automatically reactivated at the end of the braking procedure.
- The system is deactivated if the driver announces a lane change by operating the turn indicators.

Source: Lane Keeping Assist Systems at VDA

Records of previously known safety-related incidents or behavioral shortfalls

Based on Swedish data, Sternlund et al. conducted a real-world benefit study of LDW systems. Vehicle Identification Numbers were used to identify the specific equipment level of Volvo passenger cars. The study showed that LDW system-equipped cars experienced a reduced number of crashes. A 53% crash reduction was found for injured passenger car drivers involved in head-on or single-vehicle crashes on roads with speed limits of 70 km/h and above and when the road was not covered in snow or ice. This estimate represents a 30% reduction of all Swedish head-on and single-vehicle crashes involving injured drivers in passenger cars.

Some incidents with these ADAS systems being misused is driver complacency. The systems work so well in most situations that drivers begin to let their attention waver for longer and more extended periods of time. “The first thing that happened when I drove a Tesla on Autopilot was an instant, unsettling feeling of not being comfortable in the car at all, thinking it’s always a moment away from crashing. Slowly, I got used to it and calmed down, just like everyone else I’ve talked to who has used Autopilot.”

For example, in March, 2018, a Tesla Model X owner had the vehicle’s Autopilot system engaged when the all-electric SUV crashed on a California highway, Tesla confirmed on Friday while alleging the driver who died in the crash missed key warnings to take control of the car. The driver, Walter Huang, had received “several visual and one audible hands-on warning” earlier in the drive. Huang’s hands weren’t detected on the wheel six seconds prior to the collision, Tesla said. Huang died in the crash.
“The driver had about five seconds and 150 meters of unobstructed view of the concrete divider with the crushed crash attenuator, but the vehicle logs show that no action was taken,” Tesla wrote in a blog post late Friday.

Source: The safety potential of lane departure warning systems
Why people still crash with driver assistance systems

Goals and Measures

Goals

The project goals are:

- Identify hazards in the Line Assistance System that could cause physical injury or damage to a person's health.
- Evaluate the risk of the hazardous situation so that we know how much we need to lower the risk.
- Via systems engineering, prevent accidents from occurring by lowering risk to reasonable levels acceptable by society as a whole.

Measures

Responsibilities of involved persons are defined as below:

- Safety Manager
  - Planning, coordinating and documenting of the development phase of the safety lifecycle
  - Tailors the safety lifecycle
  - Maintains the safety plan
  - Monitors progress against the safety plan
  - Performs pre-audits before the safety auditor
- Project Manager
  - Overall project management
  - Acquires and allocates resources needed for the functional safety activities
  - Appoints safety manager or might act as safety manager
- Safety Auditor
  - Ensures that the design and production implementation conform to the safety plan and ISO 26262.
  - Must be independent from the team developing the project
- Safety Assessor
  - Independent judgement as to whether functional safety is being achieved via a functional safety assessment
  - Must be independent from the team developing the project

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

Our company understand that functional safety is difficult to achieve without a good safety culture and hence has defined a high quality safety culture to achieve functional safety:

- **High priority**: we recognize safety as the highest priority among competing constraints like cost and productivity
- **Accountability**: we ensure accountable processes such that design decisions are well documented and traceable back to the people and teams who made the decisions
- **Rewards**: we motivate, support and reward the achievement of functional safety
- **Penalties**: we penalize shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product are independent from the teams who audit the work
- **Well defined processes**: we have clearly defined company design and management processes
- **Resources**: we allocate necessary and sufficient resources to projects, including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: we provide effective and efficient communication channels to encourage disclosure of problems
- **Quality Management**: we have a quality management system in place that complies with quality management standards

Safety Lifecycle Tailoring

For this 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 (DIA)

Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Purpose

A DIA (development interface agreement) 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. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.
The purpose of a DIA is:

- To avoid disputes between companies during the planning and development of a product.
- To ensure liability by describing the work products that each company will provide and clarifying the responsibilities of the difference parties involved in a functional safety project.
- To clarify who will be responsible for any safety issues in post-production, or fix safety issues.
- To ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Responsibilities

Responsibilities of the OEM Company are:

- To provide Lane Assistance System which matches the requirements and fulfills adequate functional safety competency,
- To provide all useful development documents related function safety.

Responsibilities of Our Company (the Tier-1 Organization) are:

- To analyze and modify various sub-systems of Lane Assistance System from a functional safety viewpoint.
- To plan, coordinate, document the safety activities,
- To perform functional safety pre-assessment prior to audit by external functional safety assessor

Confirmation Measures

Main purpose

Confirmation measures serve two purposes:

- that a functional safety project conforms to the safety plan and follows the ISO 26262 standard, and
- that the project really does make the vehicle safer.

Confirmation review

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.