Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
4/17/2018	1.0	Noriaki.H	First attempt

Table of Contents

Introduction

Purpose of the Safety Plan

We the purpose pf this safety plan ts to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

- Safety Culture
- Safety Lifecycle
- Safety Management Roles and Responsibilities
- Development Interface Agreements
- Confirmation Measures

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 item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

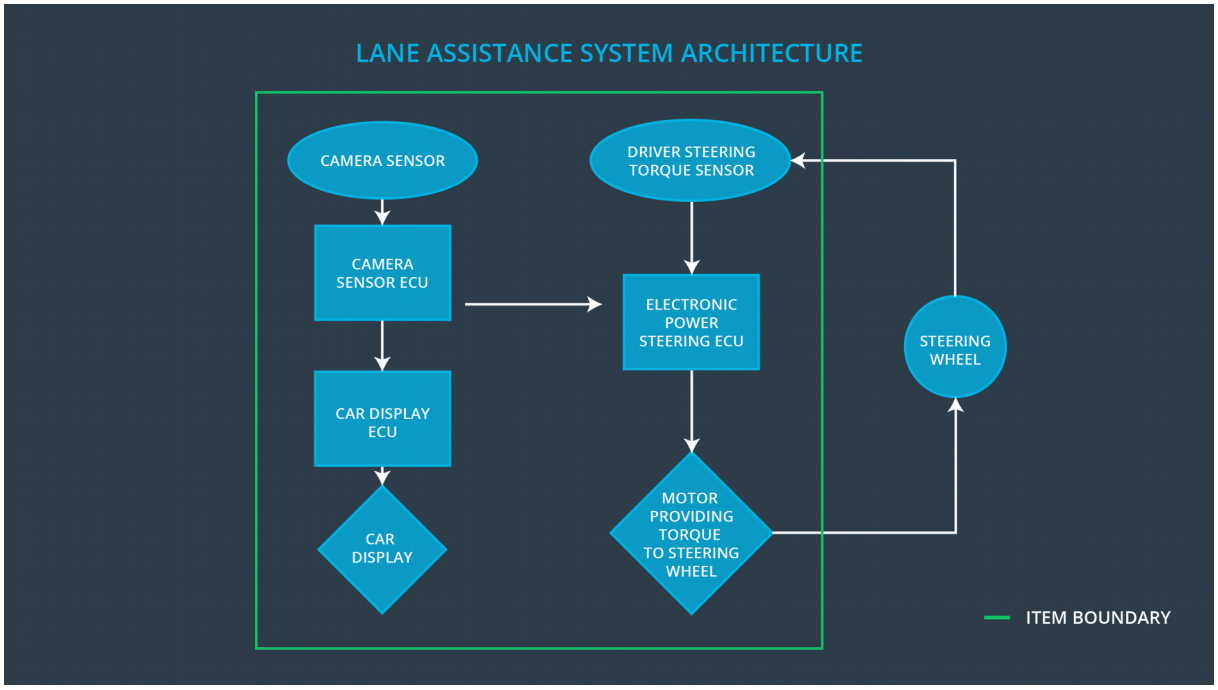
The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

The line depature warning function shall apply an oscillating sttering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering toqrue when acticve in order to stay in ego lane

The camera subsystem, the electronic power steering subsystem, and the car display system are all resposible for each of the functions.



Goals and Measures

Goals

Identify hazards in a passenger vehicle's electronic or electric 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. Systems engineering helps you figure out what your vehicle needs to do and what your vehicle design needs to look like in order to remain safe.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Member	Constantly
Create and sustain a safety culture	All Team Member	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

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 made 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 processes
Communication: communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

concept phase or prodct development phase
example,
・Hazard Analysis and Risk Assesment
・Functional Safety Concept
・Product Development: Systems Level (HW Level)
・Production

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

About 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
・Safety Engineer

About Product development,
・Integration
・Testing at the hardware, software and system levels

Here are major sections of a DIA:
・Appointment of customer and supplier safety managers
・Joint tailoring of the safety lifecycle
・Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
・Information and work products to be exchanged
・Parties or persons responsible for each activity in design and production
・Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Why include the Development interface Agreement in the safety plan ?
1.To avoid disputes during the planning and development of a product.
2.Liability. If a vehicle has a safety issue after being sold to consumers, a Development interface Agreement provides clarity about which company is best positioned to fix the system.

Confirmation Measures

1. Confirmation measures serve two purposes:
   that a functional safety project conforms to ISO 26262, and
   that the project really does make the vehicle safer.
2. 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
3. Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.
4. 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.