- Logout
-

Back to Self-Driving Car Engineer

Functional Safety of a Lane Assistance System

- Review
- History

Meets Specifications

Congratulations on completing this project!

For additional reading, here are a few interesting articles.
https://medium.com/@jamasoftware/balancing-automotive-functional-safety-and-efficient-software-development-56745b4848c8
https://medium.com/futuremobile2025/functional-safety-making-inroads-one-automotive-chip-at-a-time-e4ea76689a58

Functional safety is extremely crucial in autonomous driving, this is a difficult skill set to acquire and you should be proud of gaining deep knowledge on these topics.

Keep up the good work and best wishes for your future projects!

Happy learning!!

Project Documents

The submission should include five documents all in pdf format:
SafetyPlan
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Software Requirements and Architecture

Safety Plan

All required sections of the template should be filled out and contain reasonable answers: purpose of the safety plan, item definition, goals and measures, safety culture, safety lifecycle tailoring, development interface agreement, confirmation measures. We want to make sure that you understand what a safety plan is and how to make a safety plan.

All sections in this document are filled-in appropriately.

Minor Correction
Measures

Responsibility for "Create and sustain a safety culture" is with all team members. However, this is primarily with Safety Manager.

Hazard Analysis and Risk Assessment

The lessons contained a hazard analysis and risk assessment for the lane departure warning and the lane keeping assistance functions. These two analyses should be documented using the Excel template.

Nice work completing the situations, hazard identification, hazardous event classification, ASIL, and safety goals for HA-001 and HA-002.

Besides the two analyses from the lecture, the project should include two extra hazard analyses and risk assessments. These two extra analyses should include a situational analysis, hazard identification, hazardous event classification, ASIL and safety goals. The two hazards should be related to the Lane Assistance Item.

Good attempt at situation analysis for HA-003 and HA-004.

Suggestion
HA-003 & HA-004: Situation Description
It is good to follow the following convention for situation description: [Operational Mode] on [Operational Scenario] during [Environmental Details] with [Situational Details] and [Item Usage] system.

Functional Safety Concept

All required sections from the functional safety concept template are complete.

All sections are neatly documented. Good analysis on the safety goals and requirements are discussed in detail.

Minor Correction
Purpose of the Functional Safety Concept
In Functional Safety Concept, safety goals are refined into safety requirements. These safety requirements are then allocated to the appropriate parts of the item's architecture. The functional safety concept looks at the general functionality of the item and does not go into technical details.

Minor Correction
Warning and Degradation Concept
Malfunction_03 is not included in the table. Referring to "Functional Safety Analysis" above, Malfunctions 01,02 (LDW) become trigger modes for WDC-01 and Malfunctions 03 (LKA) for WDC-02.

Technical Safety Concept

All required sections of the template should be filled out. The five technical safety requirements for the lane departure warning amplitude, as taught in the lessons, are documented correctly.

Most of the sections from the technical safety concept template are well covered.
A few suggestions are provided to further improve the documentation.

Minor Correction
Purpose of the Technical Safety Concept
The technical safety concept is more concrete and gets into the details of the item's technology such as sensors, control units, and actuators. Technical safety requirements are general hardware and software requirements but still without getting into specific details.

Minor Correction
Technical Safety Requirements
Technical Safety Requirements related to Functional Safety Requirement 01-01
"Safe State" for Technical Safety Requirement 01 to 05 should refer to LDW torque amplitude.

Technical safety requirements should also be derived for the lane departure warning frequency malfunction and the lane keeping assistance time malfunction.

Minor Correction
Technical Safety Requirements
Technical Safety Requirements related to Functional Safety Requirement 01-02
"Safe State" for Technical Safety Requirement 01 to 05 should refer to LDW torque frequency.

Software Requirements and System Architecture

All required sections of the software requirement and architecture document are complete (inputs to software requirements.., software requirements, and refined architecture).

The submission only needs to document software safety requirements for the lane departure warning amplitude malfunction, which were given in the lessons.

This document looks good, refined requirements are neatly documented. Great job!

Minor Correction
Purpose
The purpose of this document is to derive Software Safety Requirements from Technical Safety Requirements. Software Safety Requirements are more specific than Technical Safety Requirements so that a software engineer should be able to implement them in code.

Minor Correction
Inputs to the Software Requirements and Architecture Document
Technical safety requirements
Update this section for changes (Safe State) in technical Safety Concept document. Cascade the changes to all sections in the document.

- Student FAQ