ISO 26262 General Instructions

You are going to document a safety case for the lane assistance item. Your project will include:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture Document

We have provided templates for each of these documents. The Hazard Analysis and Risk Assessment is a spreadsheet, but all other documents are word processor files. Because different reviewers might not have access to the software you used, please export all files to a pdf format before submitting.

Each template contains instructions for you to follow. We are also providing extra instructions in this document about how to fill out the spreadsheet for the hazard analysis and risk assessment.

All of the information you will need is in the functional safety lessons. Your job will be to use the information from the classroom to build a safety case. Functional safety is oftentimes learned on the job from somebody with more experience, so we are simulating what you might be expected to do as an entry level functional safety manager.

Most of the functional safety requirements, technical safety requirements and software safety requirements needed for the project have already been provided for you in the lectures. As a hint, look for many of the lane departure warning information in the videos. The lane keeping assistance information was mostly in the text portion of the module. We will ask you to derive a couple of requirements on your own as well.

Some documents will have sections marked as OPTIONAL, which are more challenging. You do not need to complete those sections. But we highly suggest completing them!

We encourage you to go beyond what was in the lecture, but you are not required to do so. For example, what would happen if the vibration torque warning was too weak and the driver did not sense it? You could do a hazard and risk analysis, engineer new requirements, and modify the system architecture accordingly. You will not be penalized for going beyond what the rubric asks for.

As a hint, here is an outline of the functional, technical and safety requirements discussed in the lecture.

Lane Departure Warning

Functional Safety Requirement 01-01	
Technical Safety Requirement 1.1	
Software Safety Requirement 1.1.1	
Software Safety Requirement 1.1.2	
Software Safety Requirement 1.1.3	
Technical Safety Requirement 1.2	
Software Safety Requirement 1.2.1	
Software Safety Requirement 1.2.2	
Software Safety Requirement 1.2.3	
Software Safety Requirement 1.2.4	
Software Safety Requirement 1.2.5	
Technical Safety Requirement 1.3	
Software Safety Requirement 1.3.1	
Software Safety Requirement 1.3.2	
Technical Safety Requirement 1.4	
Technical Safety Requirement 1.5	
Software Safety Requirement 1.5.1	
Software Safety Requirement 1.5.2	
Software Safety Requirement 1.5.3	
Software Safety Requirement 1.5.4	
Software Safety Requirement 1.5.5	

Functional Safety Requirement 01-02	
Technical Safety Requirement 2.1	

Lane Keeping Assistance

Functional Safety Requirement 02-01	
Technical Safety Requirement 3.1	

Hazard Analysis and Risk Assessment Instructions

To complete the hazard analysis and risk assessment, you will need to analyze at least four potential hazardous situations and assess their risk. Then you will derive safety goals for each hazardous situation.

Two of the hazard-situation combinations will be the ones discussed in the classroom. So you will need to go through the lesson lectures and document:

- the lane warning departure hazard and risk analysis
- the lane keeping assistance hazard and risk analysis

Then it will be your turn to analyze at least two more situations or hazards. For example, you could use the same two hazards but change the situations. Or you could come up with your own hazards. Or you could change both the hazards and the situations.

We are providing you with the actual guidewords that Elektrobit uses. So you can use these lists of guidewords to come up with your own hazards and situations.

Your analysis will be done in the provided spreadsheet document "HazardAndRiskAnalysis". In that same document, we are also providing guidewords you can use to help complete the analysis.

Here is a description of all the tabs in the spreadsheet:

Hazard Analysis and Risk Assessment - This will be where you do your analysis of the lane assistance item. This is the only tab you need to edit.

Examples - This is example of hazard analysis and risk assessment for a headlamp system.

Situational Analysis Guidewords - Guidewords for situational analysis.

Hazard Analysis Guidewords - Guidewords for hazard analysis.

Severity, Exposure, Controllability - Guideline for choosing S, E and C levels.

ASIL Table - Table for calculating ASIL from severity, exposure and controllability.

Five Steps to Complete

There are five parts to conducting the hazard and risk analysis for this project:

1. Situational Analysis
2. Hazard Identification
3. Hazardous Event Classification (Exposure, Severity, Controllability)
4. ASIL Determination
5. Safety Goal Identification

In practice, a hazard and risk analysis might be carried out by a team of multiple people. More complex systems or systems requiring high levels of safety will require more input. A hazard and risk analysis can be like a brainstorming session; we have to imagine all different types of scenarios, potential hazards and potential outcomes. Some scenarios might be more obvious than others either because they occur often in people's everyday lives (driving slowly on a paved city road, for example); other situations might occur rarely and be more difficult to identify. Some scenarios could be relevant to a certain vehicle system but not relevant to a different system.

The same could be said for hazard identification; some potential system malfunctions might be obvious based on simple logic or based on an engineer's experience. Other system malfunctions, especially for new systems and technology, might be more difficult to identify.

We want to be as thorough and logical as possible; we want to avoid missing a potential hazard that later becomes an accident. Automotive recalls, for example, could occur because a hazard and risk analysis never identified the issue before the system was designed and put into production.

Example

Let's work through a headlamp system as an example before you start. The low beam headlamps are used to help the driver see at night. What might happen if the electrical system fails and the headlamps turn off?

Situational Analysis

Hazard ID	Situational Analysis						
	Operational Mode	**Operational Scenario**	**Environmental Details**	**Situation Details (optional)**	**Other Details (optional)**	**Item Usage (function)**	**Situation Description**
HA-001	Normal Driving	City Road	Normal Conditions	Low Speed	Night time + Obstacle on the road	Correctly Used	Normal Driving on a City Road in Normal Conditions at Low Speed at Night with an Obstacle on the Road

So we are going to look at the headlamp system with "normal driving on a city road in normal conditions at low speed at night with an obstacle on the road". The operational mode, operational scenario, environmental details, situation details, and item usage values all came from a guidewords list provided by Elektrobit. You can find these guidewords in the "Situational Analysis Guidewords" spreadsheet tab.

Remember from the classroom that a situation will look like:

[**Operational Mode]** on [**Operational Scenario**] during **[Environmental Details]** with **[Situational Details]** and **[Item Usage]** system.

You can use the guidewords to fill in the blanks.

Hazard Identification

Hazard Identification					
Function	**Deviation**	**Deviation Details**	**Hazardous Event (resulting effect)**	**Event Details**	**Hazardous Event Description**
Low beam illuminates the roadway in the dark	Function not activated	Both headlights stop working	Front collision with obstacle	Vehicle crashes into the obstacle with injury to driver	Total loss of low beam

For the hazard identification, we used the "deviation" and "hazardous event" guide words found in the "Hazard Analysis Guidewords" tab. The "function" was something we defined. For the lane assistance example, we looked at two functions:

- Lane keeping assistance function
- Lane departure warning function

The other columns in hazard identification can be filled out based on the deviation and hazardous event.

Hazardous Event Classification

Hazardous Event Classification					
Exposure (of situation)	**Rationale (for exposure)**	**Severity (of potential harm)**	**Rationale (for severity)**	**Controllability (of hazardous event)**	**Rationale (for controllability)**
E4 - High probability	Night driving in the city is a regular activity	S1 - Light and moderate injuries	In city traffiic, speed of vehicle is expected to be low	C0 - Controllable in general	At city speed, most drivers will be able to control the situation by applying brakes and there is additional illumination on city roads

The exposure, severity and controllability can be determined with the help of the "Severity, Exposure, Controllability" spreadsheet tab. You will then fill out your rationale for choosing each level. There is not necessarily a right or wrong answer as long as everything is well justified.

Determination of ASIL and Safety Goals

Determination of ASIL and Safety Goals	
ASIL Determination	**Safety Goal**
QM	Total Loss of Beam Shall Be Prevented

Using the severity, exposure and controllability, you can determine the ASIL. In this case, the ASIL is QM since controllability was C0. Because we are trying to avoid the situation where the driver has no functioning headlamp, the safety goal would be to prevent the total loss of the headlamp beam.