Safety Plan Lane Assistance

Document Version: [0.1]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5/Sep/2017	0.1	Andrew Wilkie	Updating while following T3.M2.E2.L5 videos

Table of Contents

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]
To define the objectives / measurements, scope, roles, process and schedule required to achieve and confirm our functional safety goal of reducing risks to acceptable levels.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

The deliverables of the project are:

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

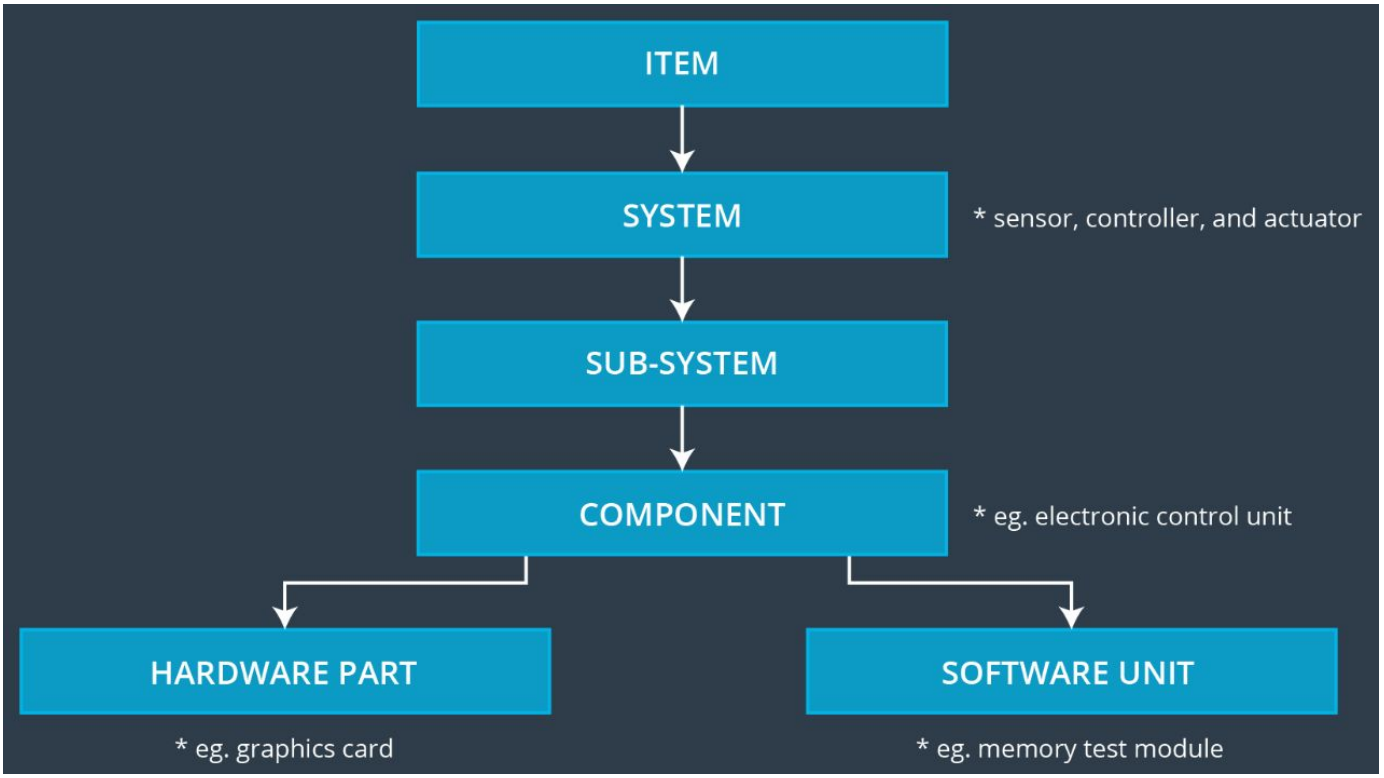
Item Definition

[Instructions:

REQUIRED

Discuss these key points about the system:

Diagram 1 : Item hierarchy



What is the item in question, and what does the item do?

The Advanced Driver Assistance System (ADAS) alerts drivers to potentially dangerous situations and takes control of the vehicle to prevent accidents from occurring.

As a part of the ADAS, the **Lane Assistance** system is the **item** in question, which assists the driver to remain in the current road lane.

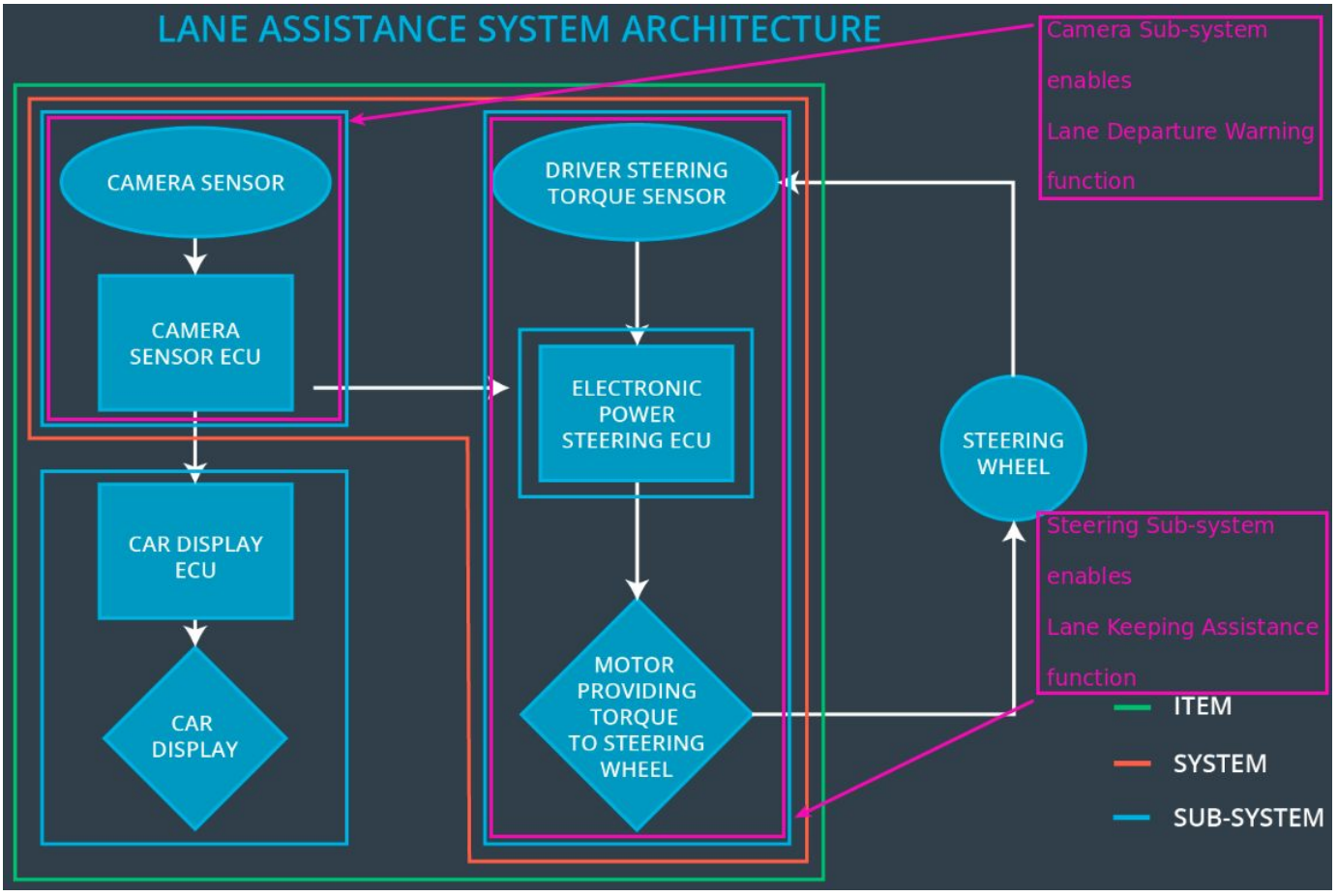
What are its two main functions? How do they work?

Lane Assistance has 2 main functions :

1. Lane Departure Warning ; alerts the driver by vibrating the steering wheel.
2. Lane Keeping Assistance ; moves the steering wheel so the wheels turn towards the centre of the lane.

Which subsystems are responsible for each function?

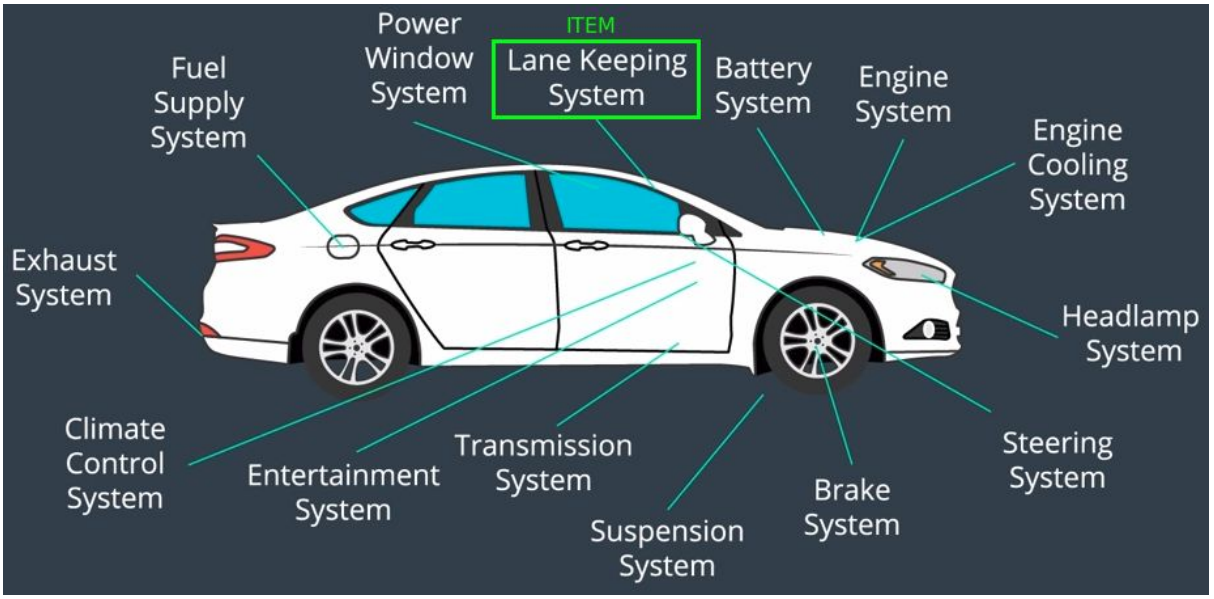
Diagram 2 : Sub-systems enabling functions



From the above diagram, the Camera sub-system is responsible for enabling the Lane Departure Warning function. This sub-system interfaces with the Steering sub-system, which is responsible for enabling the Lane Keeping Assistance function.

What are the boundaries of the item?

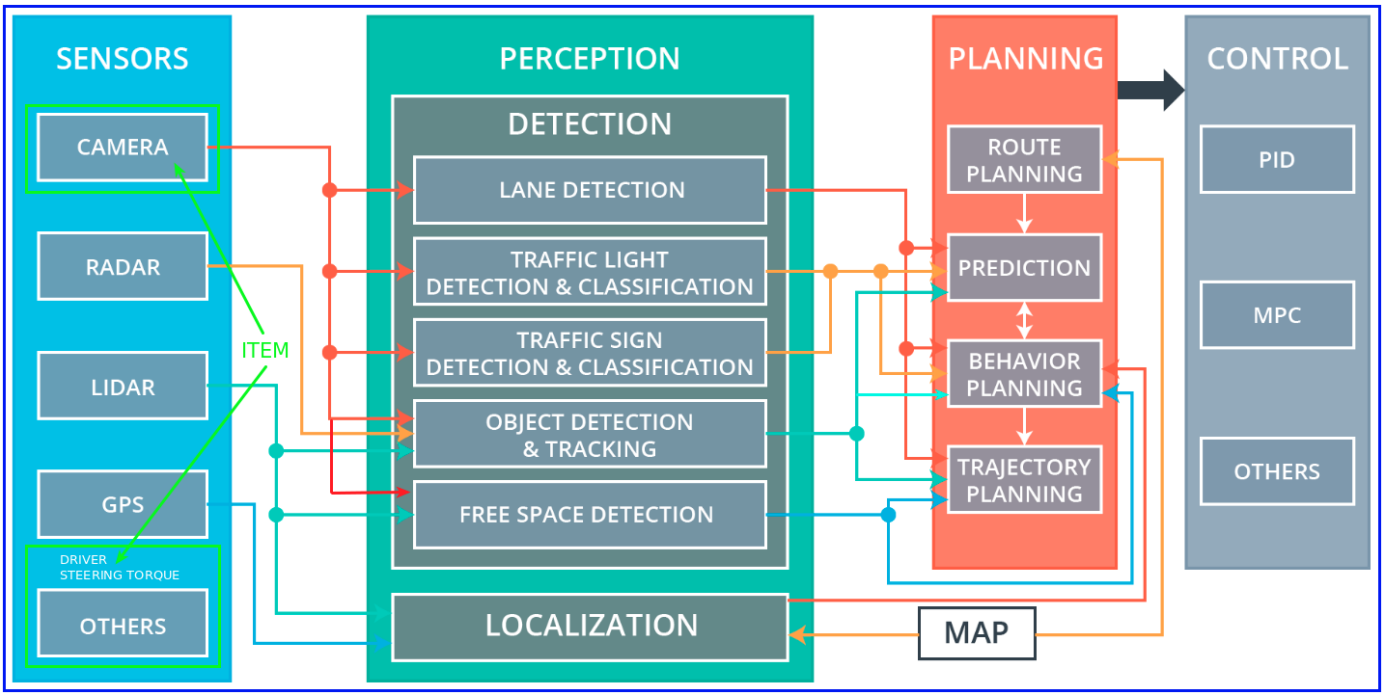
Diagram 3 : Item boundaries



The Lane Assistance item in the above diagram is one of many systems within the Vehicle system.

In addition, Autonomous Vehicles under current development build upon the Lane Assistance item and extend into other advanced systems.

Diagram 4 : Autonomous vehicle architecture

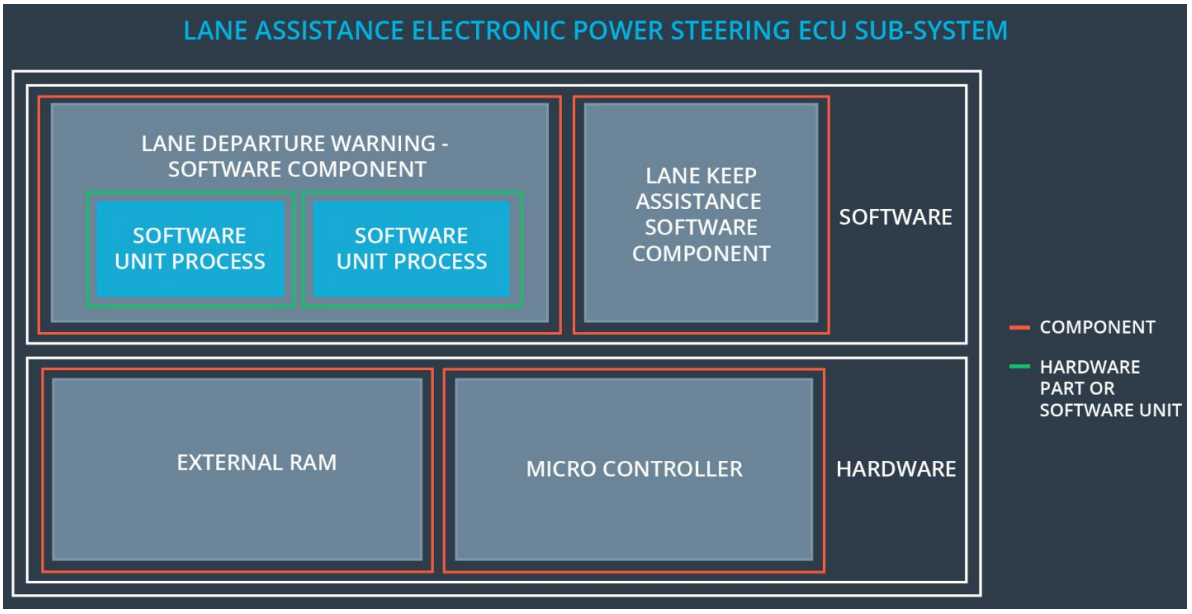


What subsystems are inside the item?

The Lane Assistance item contains the following sub-systems :

1. Camera
2. Steering
    a. Sub-system within Steering ; Electronic Power Steering ECU

Diagram 5 : Electronic Power Steering ECU sub-system



What elements or subsystems are outside of the item?

The Lane Assistance item does not contain the following sub-system :

1. Display
    a. Elements within Display :
        i. Car Display ECU
        ii. Car Display

OPTIONAL

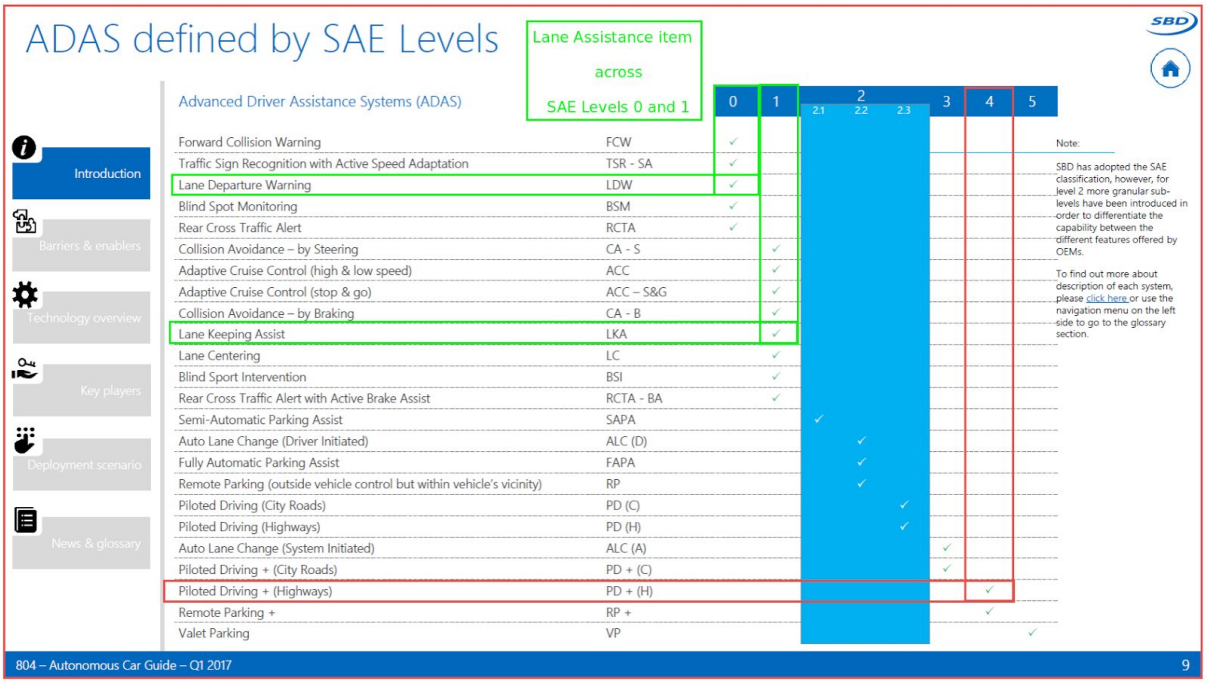
Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

-
- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
-
- **Legal requirements in your country for lane assistance technology**
-
- **National and International Standards Related to the Item**
-
- **Records of previously known safety-related incidents or behavioral shortfalls**

]

As a side note, Lane Assistance item features fall under SAE Levels 0 and 1.

Diagram 6 : SAE Levels 0, 1 for Lane Assistance item



Goals and Measures

Goals

[Instructions:
Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]
The Lane Assistance projects goal is to reduce the risk of vehicle accident to an acceptable level, caused by unintended lane departures.

Measures

[Instructions:
Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.

The options are:
All Team Members
Safety Manager

Project Manager
Safety Auditor
Safety Assessor
]

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 Assessor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

[Instructions:
Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture
]

We constantly strive to maintain a good safety culture by :

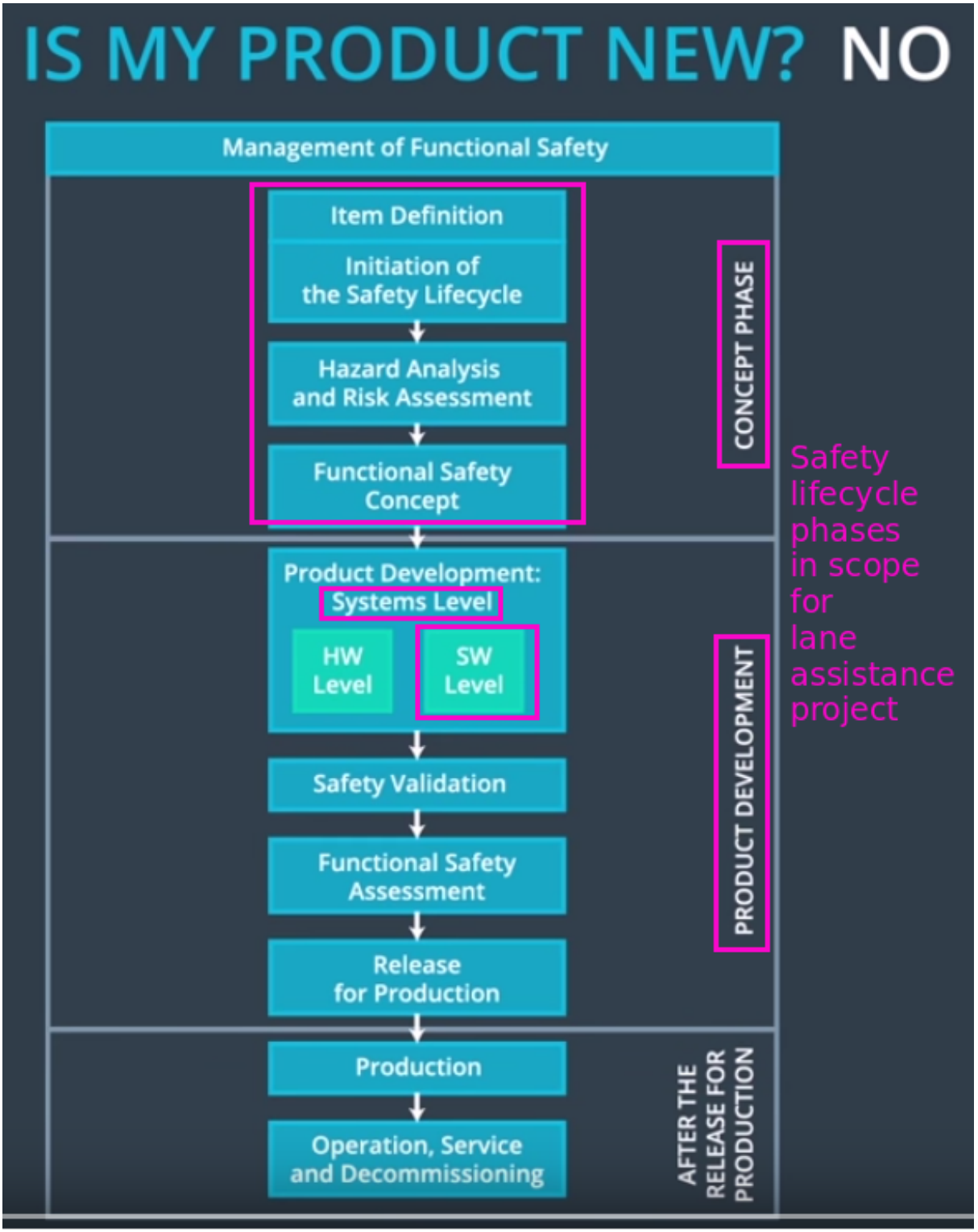
1. Making safety a high priority amongst competing constraints like costs and productivity.
2. Ensure teams and people are accountable for all design decisions.
3. Achievement of functional safety the team is both recognised and rewarded regularly.
4. Taking shortcuts that put safety / quality at risk are penalised.
5. Auditors have a separate reporting structure to the design and development teams to maintain independence.
6. Management and design processes are clearly defined and Quality Management audits are performed regularly.
7. All functional safety projects have the necessary people assigned to them possessing the appropriate skills.
8. We value intellectual diversity, especially during risk ‘brain-storming’ sessions.
9. Problem disclosure is encouraged as part of daily team project meetings and through our open issue task management system.

Safety Lifecycle Tailoring

[Instructions:
Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document
]

All of the Concept Phase is in-scope for the Lane Assistance project and parts of the Product Development Phase. All other activities not boxed in pink below are out-of-scope for this functional safety project.

Diagram 7 : [Project scope safety lifecycle phases / activities]



Roles

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.
]

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

[Instructions:
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.

Please answer the following questions:

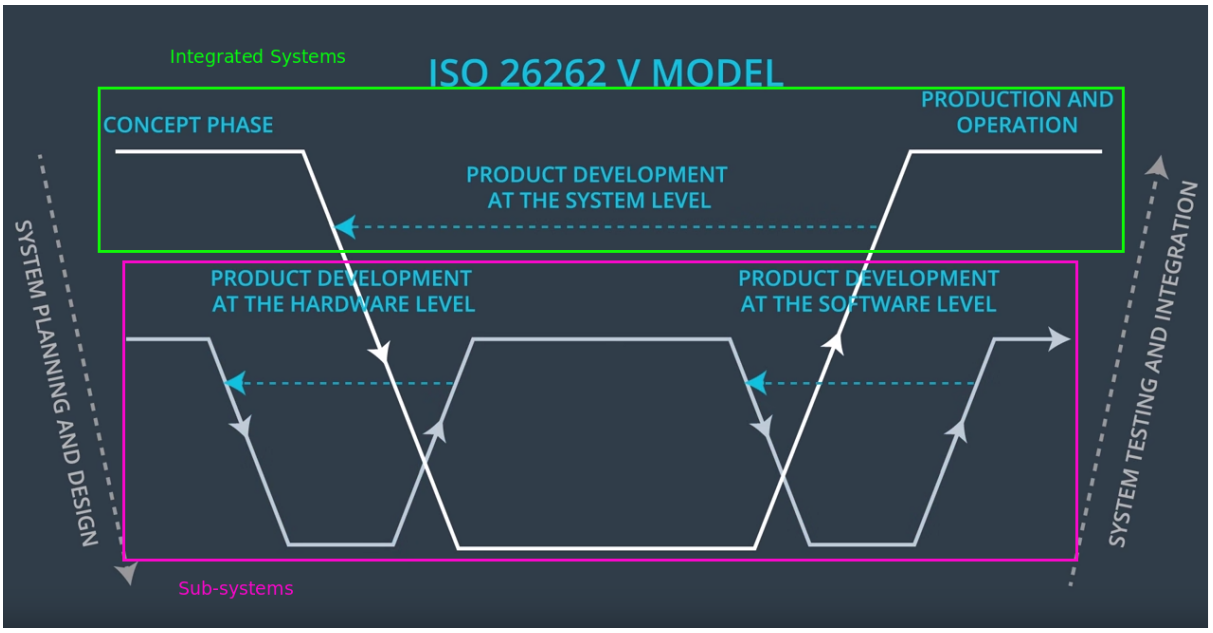
1. **What is the purpose of a development interface agreement?**
   The goal of a Development Interface Agreement (DIA) is to ensure all parties (OEM, Tier 1 and Tier 2 suppliers) are developing safe vehicles in compliance with ISO 26262.
   The main purpose is to :
   a. Clarify the responsibilities of the different parties involved in a functional safety project.
   b. Describe the work products that each company will provide.
   c. Help avoid disputes between companies.
   d. Clarify who will be responsible for any safety issues in post-production.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane**

assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

Role	Org	Responsibilities
Functional Safety Manager- Item Level	OEM	Plans the safety lifecycle with a focus on Integrated Systems level activities - see green box in Diagram 8 below.
Functional Safety Engineer- Item Level	OEM	Integrated Systems level development, integration and testing - see green box in Diagram 8 below.
Project Manager - Item Level	OEM	Acquires / allocates Functional Safety Manager and Engineer(s) which will be the counterparts to the Tier 1 roles.
Functional Safety Manager-Component Level	Tier-1	Plans the safety lifecycle with a focus on Sub-system level integration - see pink box in Diagram 8 below.
Functional Safety Engineer- Component Level	Tier-1	Sub-systems level development, integration and testing - see pink box in Diagram 8 below.
Functional Safety Auditor	OEM or external	Ensures design and production implementation conform to Integrated Systems and Sub-system levels safety plans - see green and pink boxes in Diagram 8 below.
Functional Safety Assessor	OEM or external	Judges whether functional safety has been achieved.

Diagram 8 : [OEM (integration level) VS Tier 1 (sub-systems level) activities]



]

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   To verify that :
   a. Processes comply with the functional safety standard ISO 26262.
   b. Project execution is following the safety plan.
   c. Design really does improve safety.

2. **What is a confirmation review?**
   Ensures that the project complies with ISO 26262 throughout product design and development.

3. **What is a functional safety audit?**
   Ensures that the actual implementation conforms to the safety plan.

4. **What is a functional safety assessment?**
   Verifies that the plans, designs and developed products actually achieve functional safety.

]

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.