SAFETY STANDARDS FOUNDATION

# FUNCTIONAL SAFETY COURSE #2


Renault Group

NXP

SECURE CONNECTIONS FOR A SMARTER WORLD

# Awareness of Functional Safety

- Overview of the ISO26262
- The Concept phase
  - Item definition
  - Hazard Analysis and Risk Assessment (HARA)
  - Functional Safety Concept (FSC)
- System level development
  - Technical Safety Concept
- Design decisions : ASIL decomposition
- Safety Analysis at system level
- Test & Integration

Renault Group

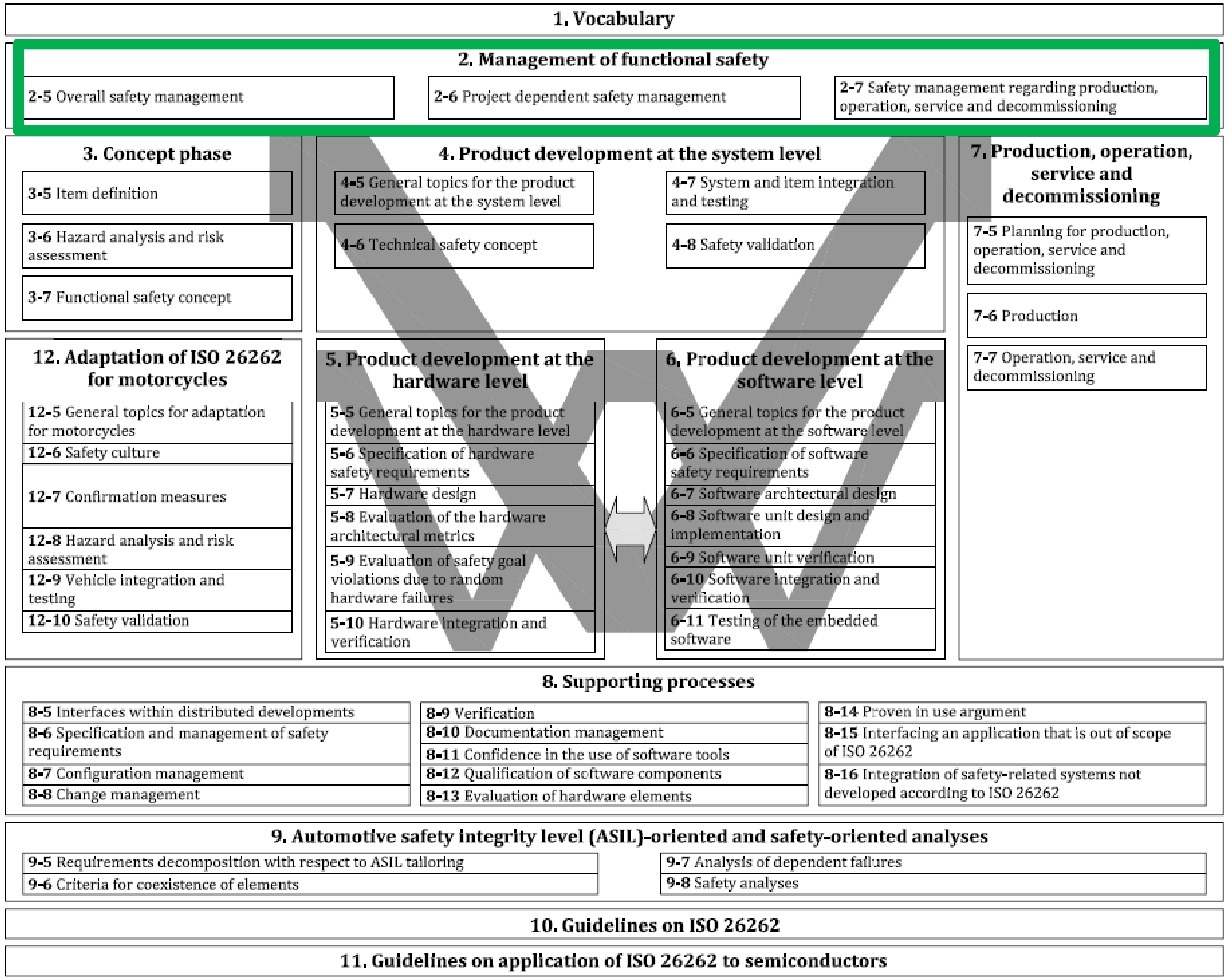
# 01

# OVERVIEW OF THE ISO26262

SECURE CONNECTIONS
FOR A SMARTER WORLD

# Part 2: Safety Management

- Safety Lifecycle
- Safety Culture
- Competence Management
- Quality Management
- Tailoring

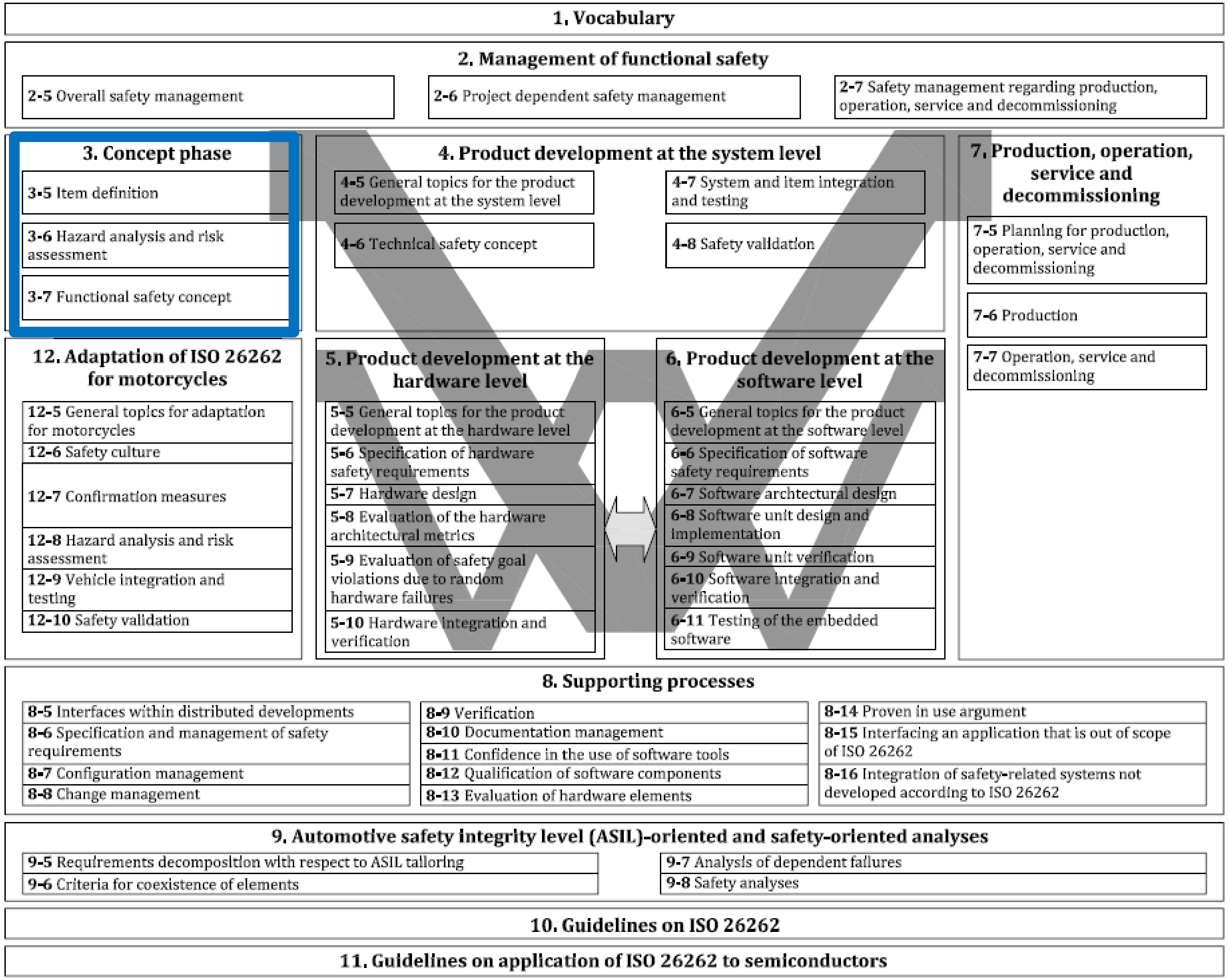



Renault Group

# Part 3: Concept Phase

Car OEM / Tier1

- Item definition
- HARA
- FSC

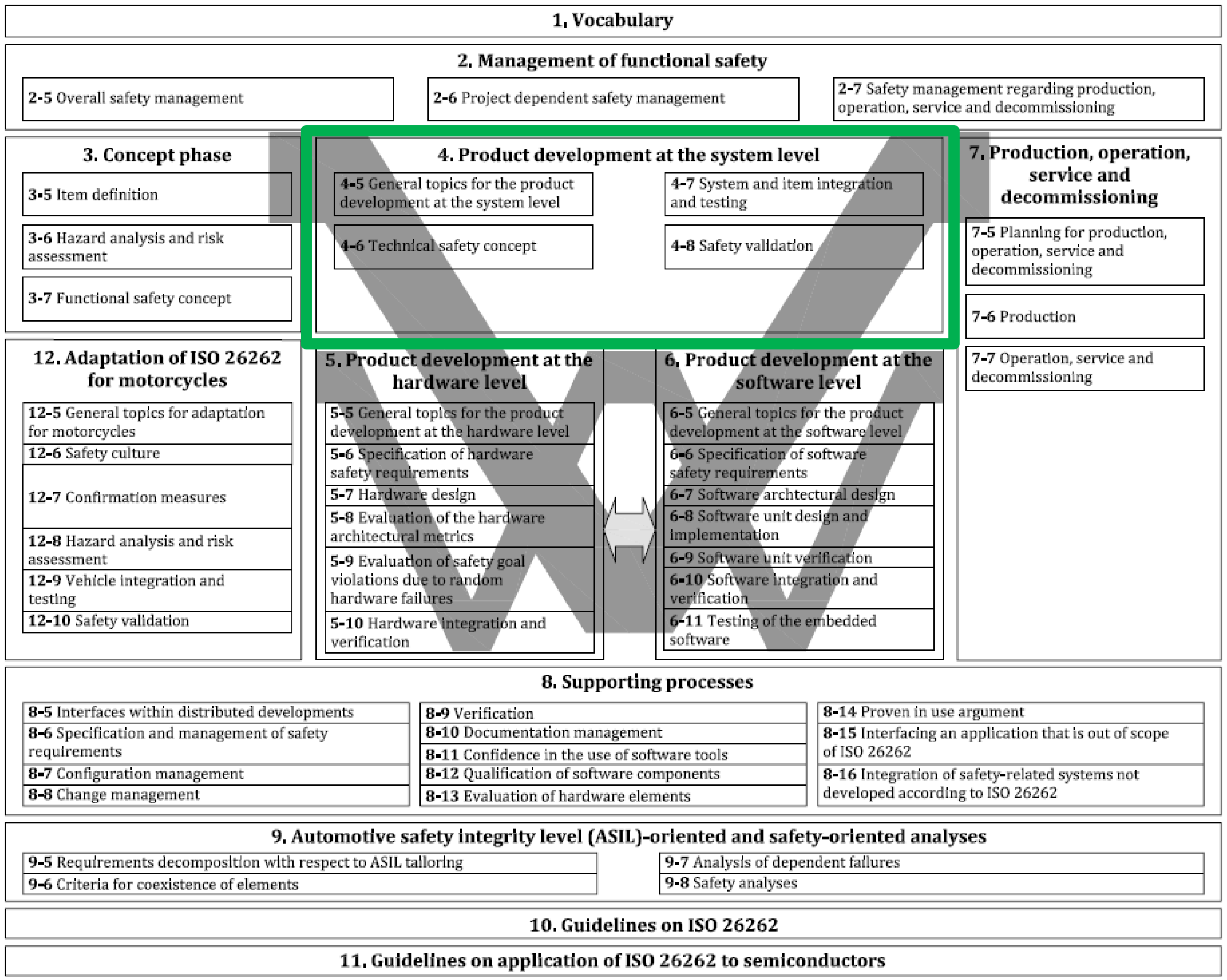



Renault Group

# Part 4: Product Development at the System Level

Car OEM / Tier1

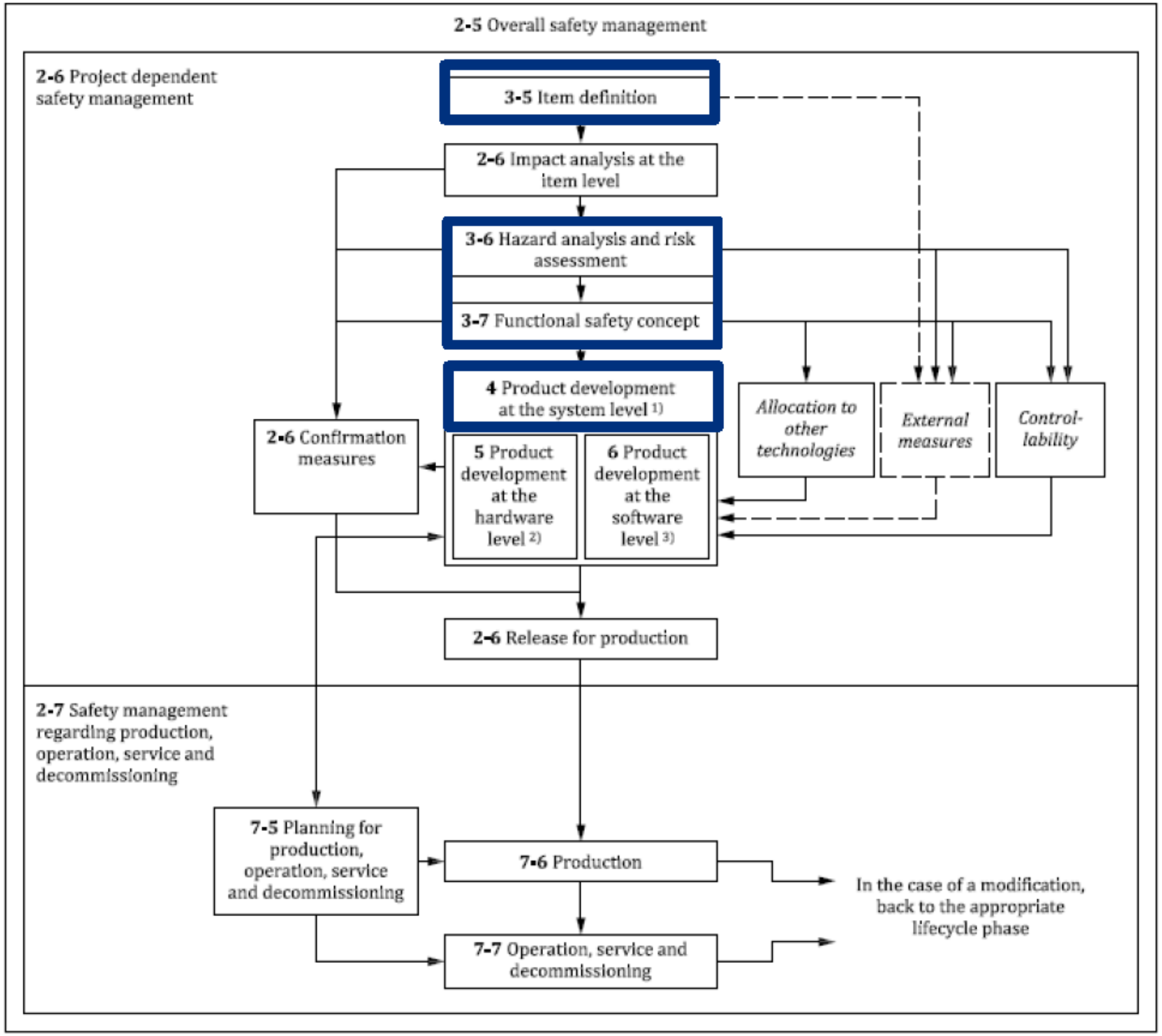
- Technical Safety Requirements
- System Architectural Design
- Technical Safety Concept



# 02

# THE CONCEPT PHASE

# Concept development context



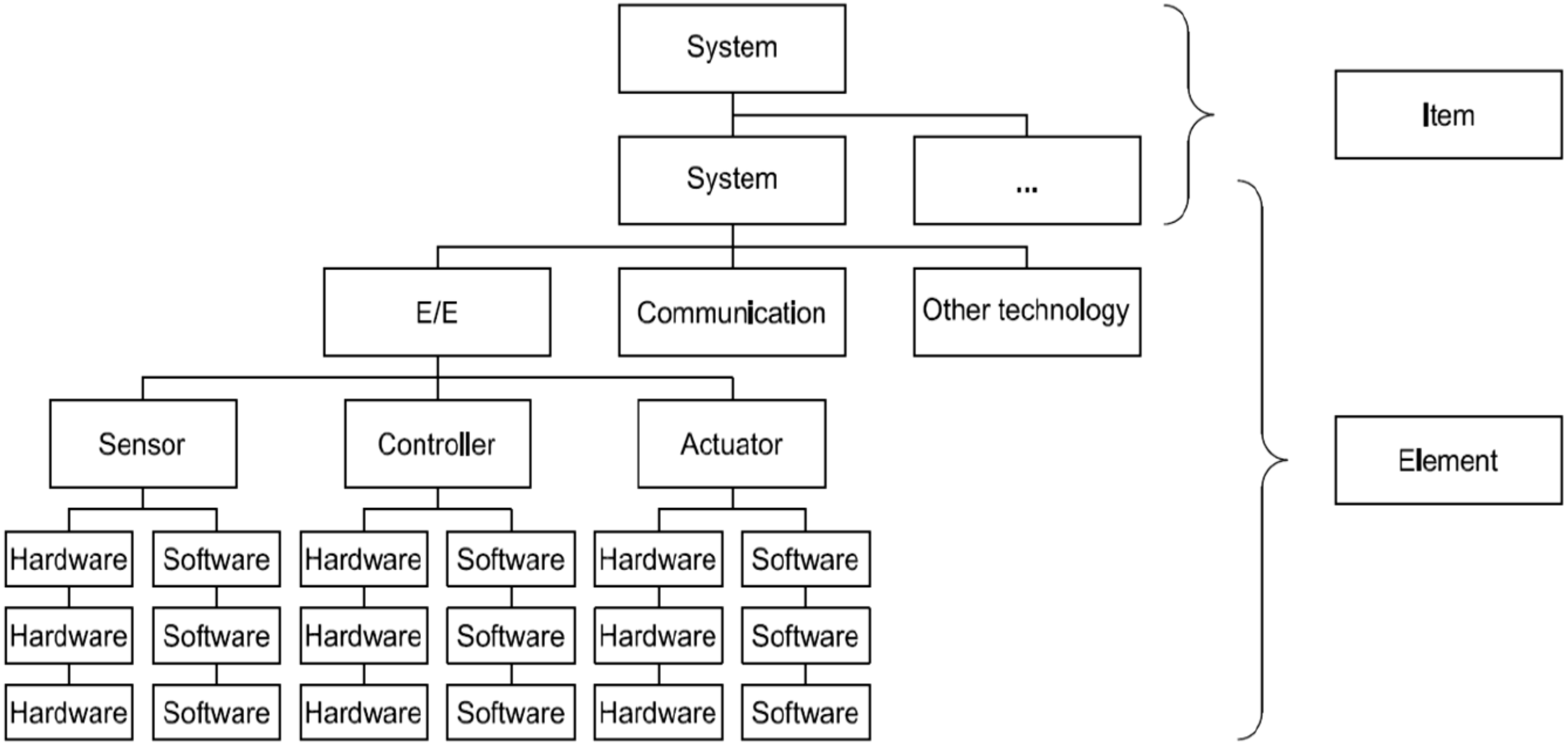

- - - - - - -: outside the item
———————: inside the item

# 02.1

## THE ITEM DEFINITION

SECURE CONNECTIONS
FOR A SMARTER WORLD

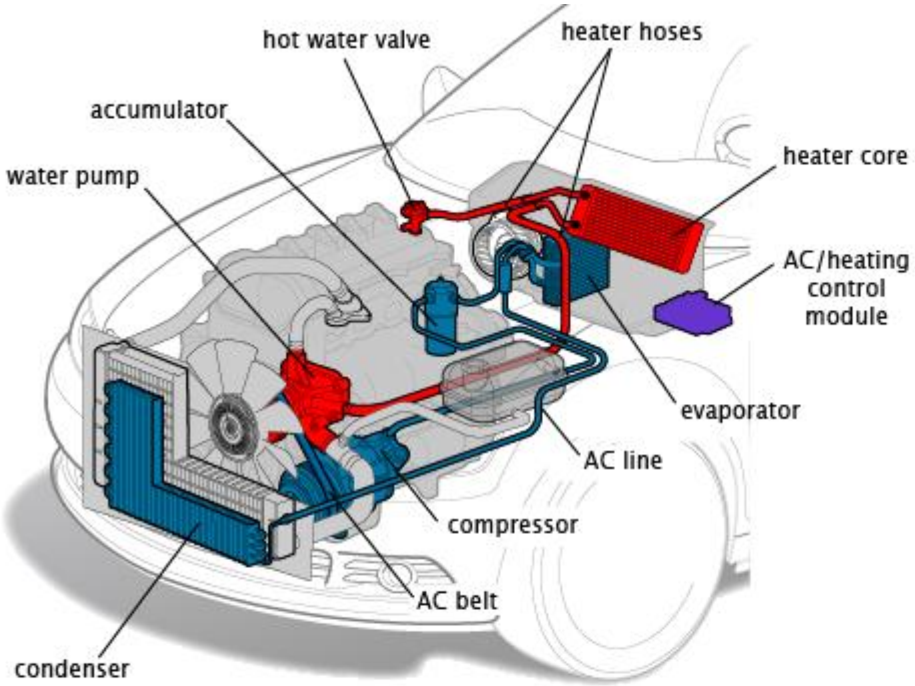
# Item Definition – What is an Item ?



# Item Definition

The first objective is to **define and describe** the item, its dependencies on, and interaction with, the environment and other items.

The second objective is to support an adequate **understanding of the item** so that the activities in subsequent phases can be performed.

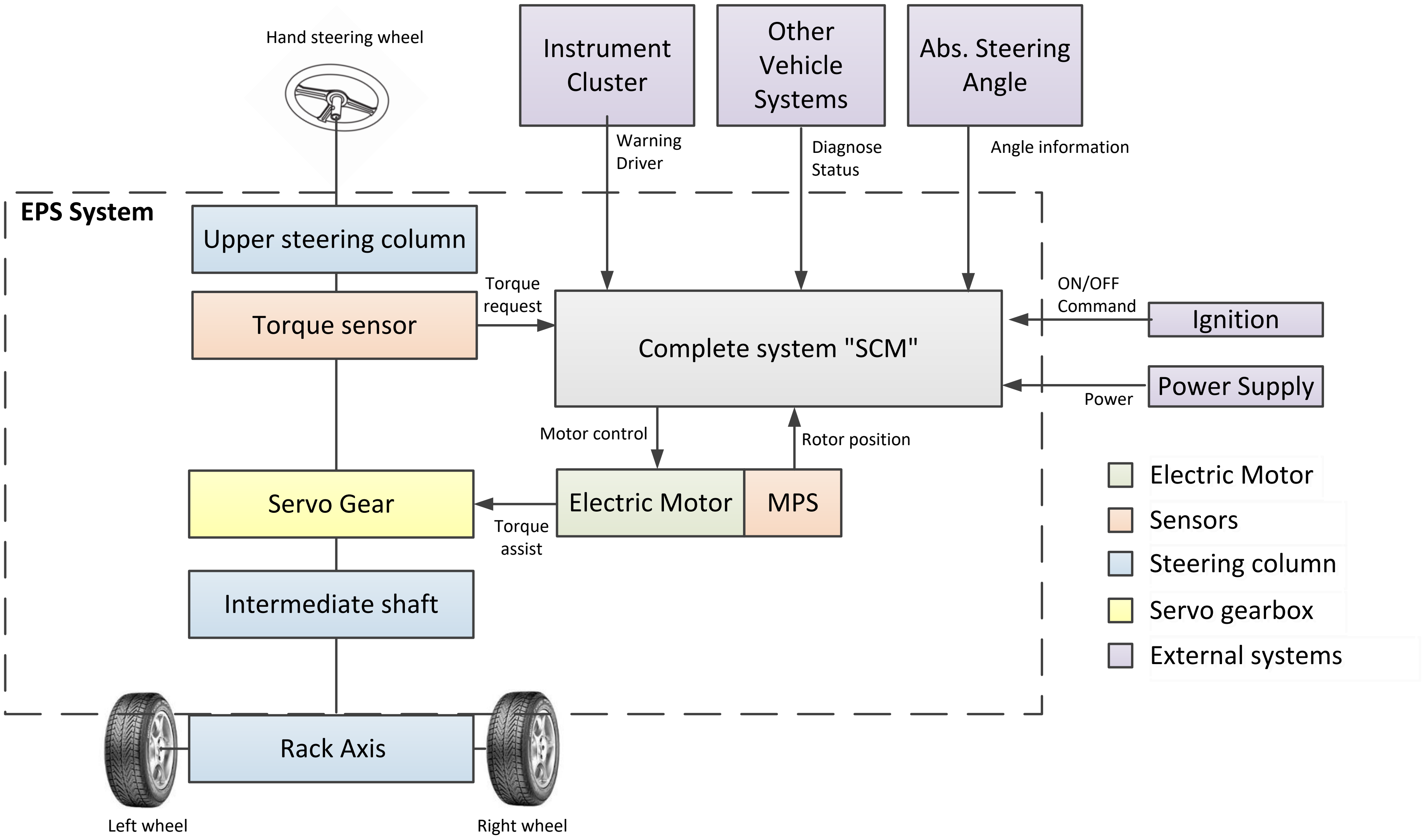



The Item Definition contains all the information defining the product :

- Functional requirements of the Item
- Environmental conditions for the intended use
- Legal requirements
- Known Safety requirements
- Elements of the item
- Requirements/interaction by and upon other items

Renault Group

# Item Definition – Example of the Electrical Power Steering (EPS)




Renault Group

# 02.2

# THE HAZARD ANALYSIS AND RISK ASSESSMENT (HARA)

# Hazard Analysis and Risk Assessment

## Flow

**1 Situation analysis and identification of hazards**

- Systematic specification of the driving situations
- Identification of possible related hazards

**2 Classification of the hazards**

- Derivation of risk parameters (S, E, C)

**3 ASIL determination**

- Derivation of the ASIL using a risk matrix

| | | Controllability C | | |
|---|---|---|---|---|
| Severity S | Exposure E | C1 | C2 | C3 |
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | ASIL A |
| | E4 | QM | ASIL A | ASIL B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | ASIL A |
| | E3 | QM | ASIL A | ASIL B |
| | E4 | ASIL A | ASIL B | ASIL C |
| S3 | E1 | QM | QM | ASIL A |
| | E2 | QM | ASIL A | ASIL B |
| | E3 | ASIL A | ASIL B | ASIL C |
| | E4 | ASIL B | ASIL C | ASIL D |

**4 Definition of the Safety objectives**

- Description of the Safety Goals to be complied with

**5 Review**

- Check for completeness, accuracy and consistency of the classifications

Renault Group



NXP

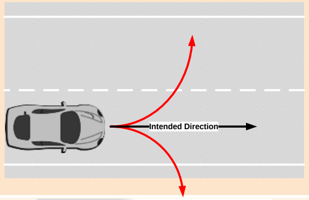
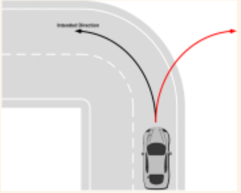
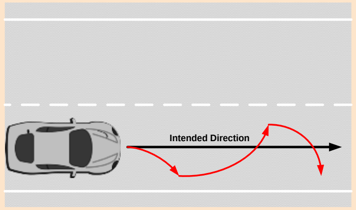
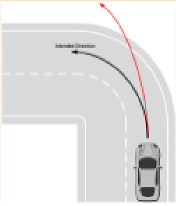
# HARA
## Criteria for analysis

| Failure modes |
|---|
| Loss of function |
| Function delayed |
| Function corrupted |
| Untimely function |
| Etc. |

| Driving conditions | Road conditions | Vehicle conditions | Road layout |
|---|---|---|---|
| Stopping, Parking | Normal road | In repair garage | One-street way |
| Traveling at low speed | Wet road | Trailer attached | Highway |
| Traveling at high speed | Snow and ice on road | Vehicle being refueled | Highway exit ramp |
| Towing | Slippery leaves on road | Vehicle during jump start | Country road |
| Etc. | Etc. | Etc. | Etc. |

# Hazard Analysis and Risk Assessment

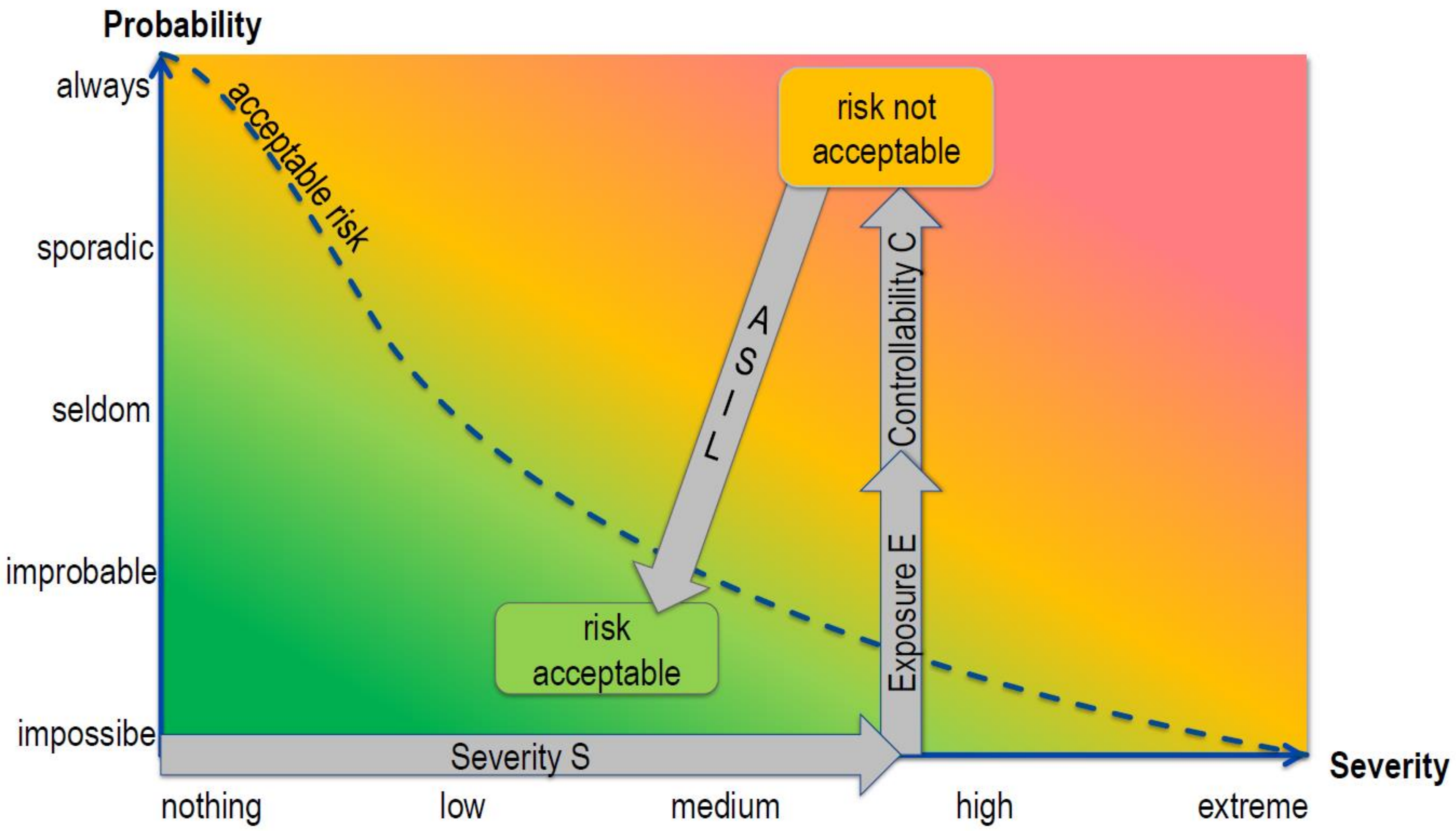
## Example of risk identification - EPS

| HE # | Hazardous Events | ASIL | Effect on vehicle |
|---|---|---|---|
| HE-A1 | Unintended vehicle lateral motion (eg. auto steering) | D |  |
| HE-A2 | Unintended vehicle reverse steering | D |  |
| HE-A3 | Uncontrolled vehicle lateral motion due to steering over assistance and steering assistance oscillations | D |  |
| HE-A7 | Sudden loss of driver steering assistance | B |  |

Safety goals definition
\+
Safe States

# Hazard Analysis and Risk Assessment

## Classification of the risk



# Hazard Analysis and Risk Assessment

## ASIL Determination

S= Severity

E= Exposure

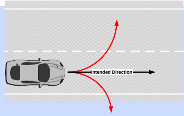
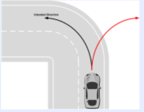
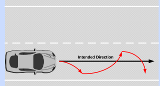
C= Controllability

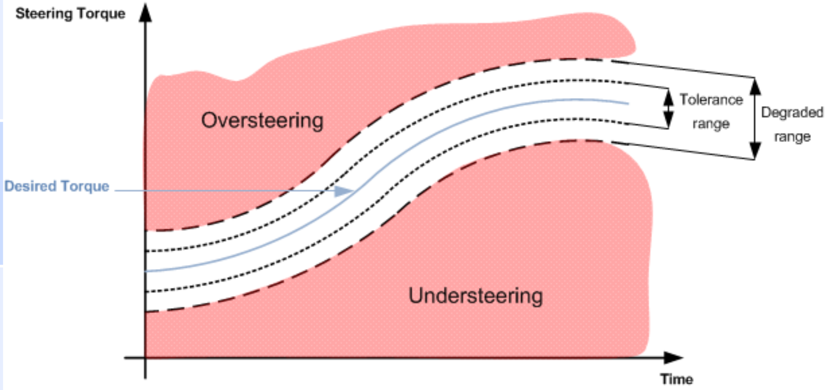
| | | **C1** – SIMPLE | **C2** – NORMAL | **C3** – DIFFICULT |
|---|---|---|---|---|
| S1 LIGHT | E1 (very low) | QM | QM | QM |
| | E2 (low) | QM | QM | QM |
| | E3 (medium) | QM | QM | A |
| | E4 (high) | QM | A | B |
| S2 SEVERE | E1 (very low) | QM | QM | QM |
| | E2 (low) | QM | QM | A |
| | E3 (medium) | QM | A | B |
| | E4 (high) | A | B | C |
| S3 FATAL | E1 (very low) | QM | QM | A |
| | E2 (low) | QM | A | B |
| | E3 (medium) | A | B | C |
| | E4 (high) | B | C | D |

*(QM: “quality managed” → no requirements from standard applied explicitly)*

Renault Group

# Hazard Analysis and Risk Assessment
## Safety Goals – EPS Example

| SG # | Safety Goal | ASIL | Safe State | FTTI |
|---|---|---|---|---|
| SG-A1 | Avoid self steering  | D | Switch-off assistance and warning lamp | 20ms |
| SG-A2 | Avoid reverse steering  | D | Switch-off assistance and warning lamp | 20ms |
| SG-A3 | Avoid over or oscillated steering   | D | Switch-off assistance and warning lamp | 20ms |
| SG-A7 | Avoid sudden loss of steering  | B | Ramp down assistance and warning lamp | 20ms |



# 02.3

# THE FUNCTIONAL SAFETY CONCEPT (FSC)

# Functional Safety Concept
## Elements

Conceptual description of the functional interrelationships required to achieve the Safety Goals

The derivation of the Functional Safety Requirements for each Safety Goal

Functional parameters (*Operating conditions, FTTI, Safe State, Transition to safe state, Functional redundancies*)

Warning and degradation concept

Emergency running operation

Driver actions that contribute to achieving Safety Goals

# Functional Safety Architecture
## Assignments

### Deriving a Safety Architecture

- Block diagram with representation of :
  - Functional redundancies
  - Independence of the individual functional blocks

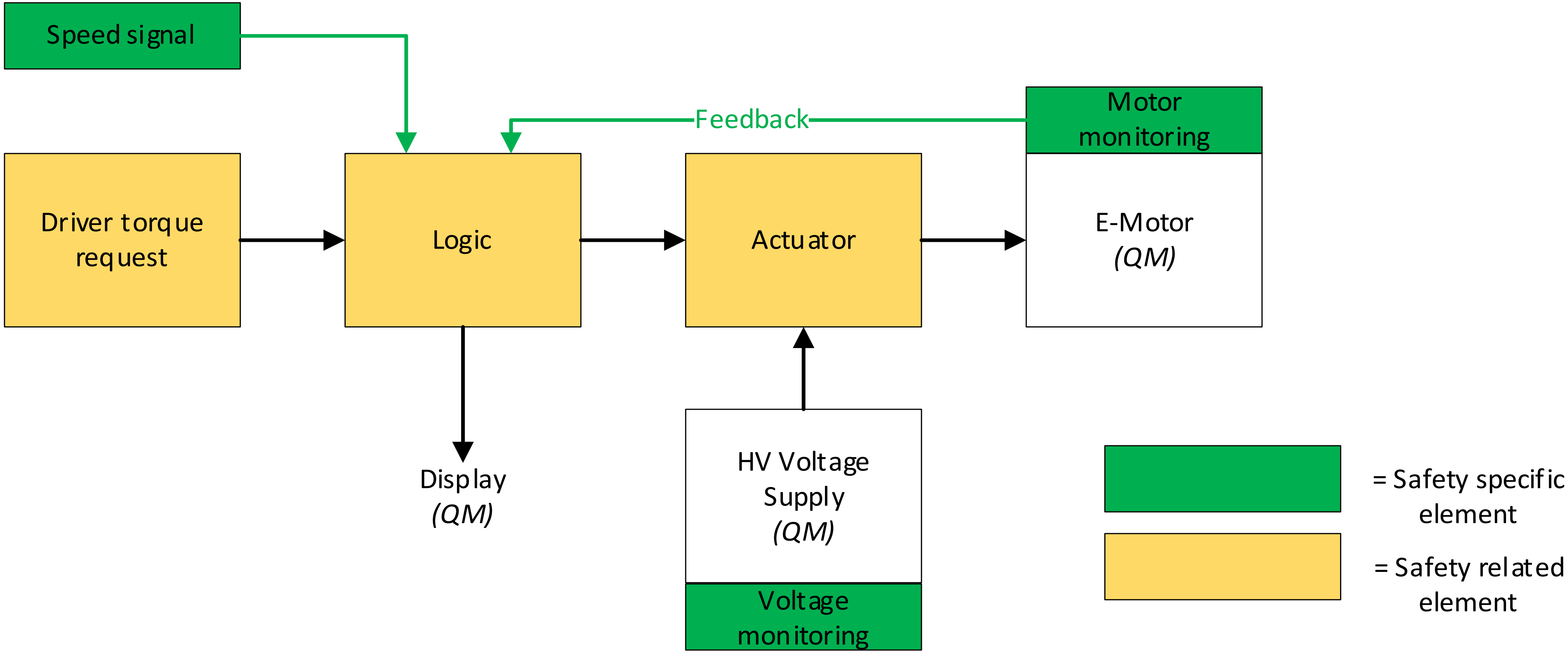
### Assignment of the ASIL requirement to the E/E elements

- Assignment of the ASIL requirement to the individual functional blocks
- Possibility of “ASIL decomposition” *(see later)*

### Representation and description of measures from other technologies or external measures

# Functional Safety Concept

## Example of the EPS



# 03.

## SYSTEM LEVEL DEVELOPMENT

SECURE CONNECTIONS
FOR A SMARTER WORLD

# Technical Safety Concept

The Technical Safety Concept refines the functional safety concept, considering both the functional concept and the preliminary architectural assumptions.

It is a specification of Safety requirements at the system and/or element level. It includes:

**Technical Safety Requirements derived from the Functional Safety Requirements and the preliminary system architecture**

- Safety Mechanisms **to identify and control faults in the system itself**
- Safety Mechanisms **to identify and control faults in other systems**
- Measures to **achieve and maintain the safe state** (transition, fault tolerant time, emergency running interval)
- Measures for implementing the **warning and degradation concepts**

# Technical Safety Concept

## Specification for the item validation

- Separate validation plan relating to the Safety Goal

## Avoidance of latent faults

- Multiple-point fault detection interval (e.G at any start-up or shutdown)

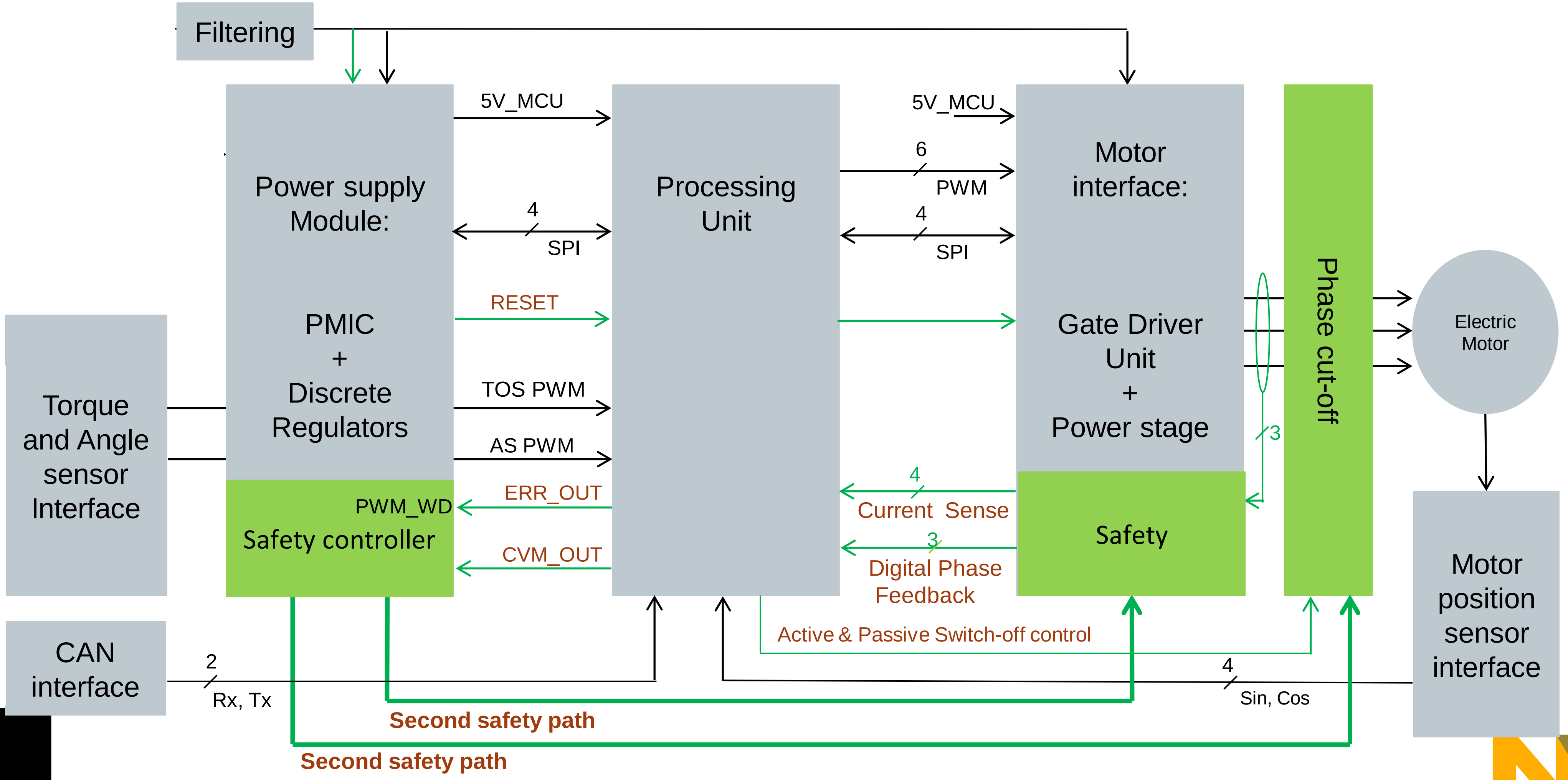
## Fault control mechanisms for latent faults (Safety measures)

- They must satisfy the following requirements:
  - ASIL B for ASIL D safety goals
  - ASIL A for ASIL B and C safety goals
  - QM for ASIL A safety goals

Renault Group

# Technical Safety Concept

## Example of the EPS




Renault Group

# Technical Safety Concept

## Properties of a Safety Mechanism

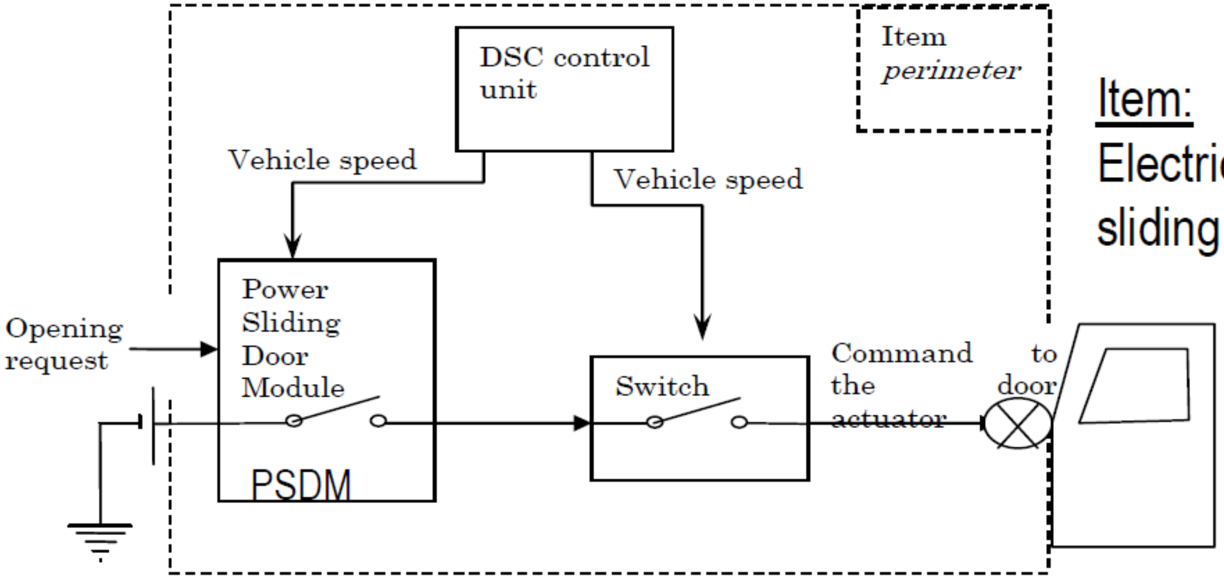
| Diagnostic Method | Communication Control |
|---|---|
| ID Number | SM 18 |
| Description<br>(References ISO/DIS 26262) | The "Inspection using test patterns" (D 2.7.4) Table D8 is chosen. The Aim is to detect static failures (stuck-at failure) and cross-talk.<br>This is a dataflow-independent cyclical test of data paths. It uses a defined test pattern to compare observations with the corresponding expected values.<br>Test coverage is dependent on the degree of independence between the test pattern information, the test pattern reception, and the test pattern evaluation. In a good design, the functional behavior of the system is not unacceptably influenced by the test pattern. **This execution of test pattern has to be reviewed during a Safety Assessment.**<br>Additionally Transmission redundancy (D2.7.5.) and Information redundancy (D2.7.6 is used). |
| Diagnostic coverage | 99% regarding Table D8 for the D 2.7.4.<br>90% for regarding Table D8 for the D 2.7.5<br>90% for regarding Table D8 for the D 2.7.6<br>MAX is 99% for using in the FMEDA |
| Fault Diagnostic | Data set entry in the fault memory |
| Fault reaction and safe state | Start UP: AB01 is put out of action – *VCU opens contacts*<br>During operation: Upper and lower port shut down Communication circuit is switched to high |
| Diagnostic test interval | < 100 ms |
| Fault recognition time | < 300 ms |
| Affected component | Upper and Lower port communication interface |
| Allocation | Specification of the safety requirement (assumption) is SA 215, safety function FB235 to FB325 |
| Responsible for the realization | For the Software: Software department and SW-Designer<br>For the hardware: Hardware developer |

Renault Group

# 04.

# DESIGN DECISIONS : ASIL DECOMPOSITION

# ASIL Decomposition
## Example – Electric sliding door




Item:
Electrically driven sliding door

**Top safety requirement: "Prevent door opening at vehicle speed > 15 km/h → ASIL C"**

SR1: The DSC shall provide accurate speed data from 0 to 15km/h → ASIL C

SR2: The PSDM shall power the switch only when vehicle speed data from DSC indicates speed not greater than 15 km/h → ASIL B(C)

SR3: The switch remains in open position when vehicle speed data from DSC indicates speed not greater than 15 km/h → ASIL A(C)

Renault Group

# ASIL Decomposition

"ASIL Decomposition" covers the decomposition of one Safety requirement into **redundant/complementary** Safety requirement**s** according to ISO26262-9.

The decomposition is only allowed if there is **sufficient independence** between the elements implementing the decomposed requirements.

| ASIL initial | Possibilities for ASIL decomposition with redundant elements | | |
|---|---|---|---|
| ASIL D | ASIL D + QM(D) | ASIL C(D) + ASIL A(D) | ASIL B(D) + ASIL B(D) |
| ASIL C | | ASIL C(C) + QM(C) | ASIL B(C) + ASIL A(C) |
| ASIL B | | ASIL B(B) + QM(B) | ASIL A(B) + ASIL A(B) |
| ASIL A | | | ASIL A(A) + QM(A) |

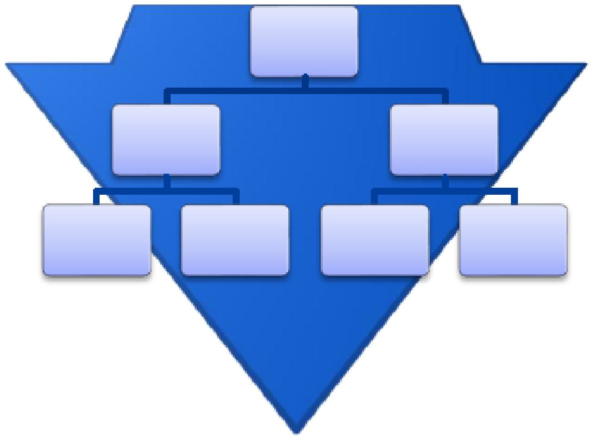
ASIL Decomposition allows to lower the requirements for the systematic capability of the element but does not change the requirements/targets for random HW failures.

# 05.

# SAFETY ANALYSIS AT SYSTEM LEVEL

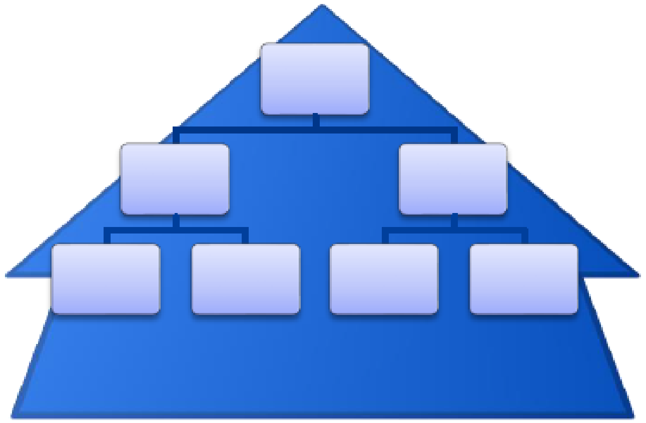
# System level Safety Analysis
## Types of Safety analysis

**Deductive analysis**
(e.g. FTA)



- From the top of the hierarchy to the bottom
- Leaves at one level become the top events in the next level

**Inductive analysis**
(e.g. FMEA)



- From the bottom of the hierarchy to the top
- Effects at one level become the causes at the next level

# System level Safety Analysis

## Types of Safety analysis

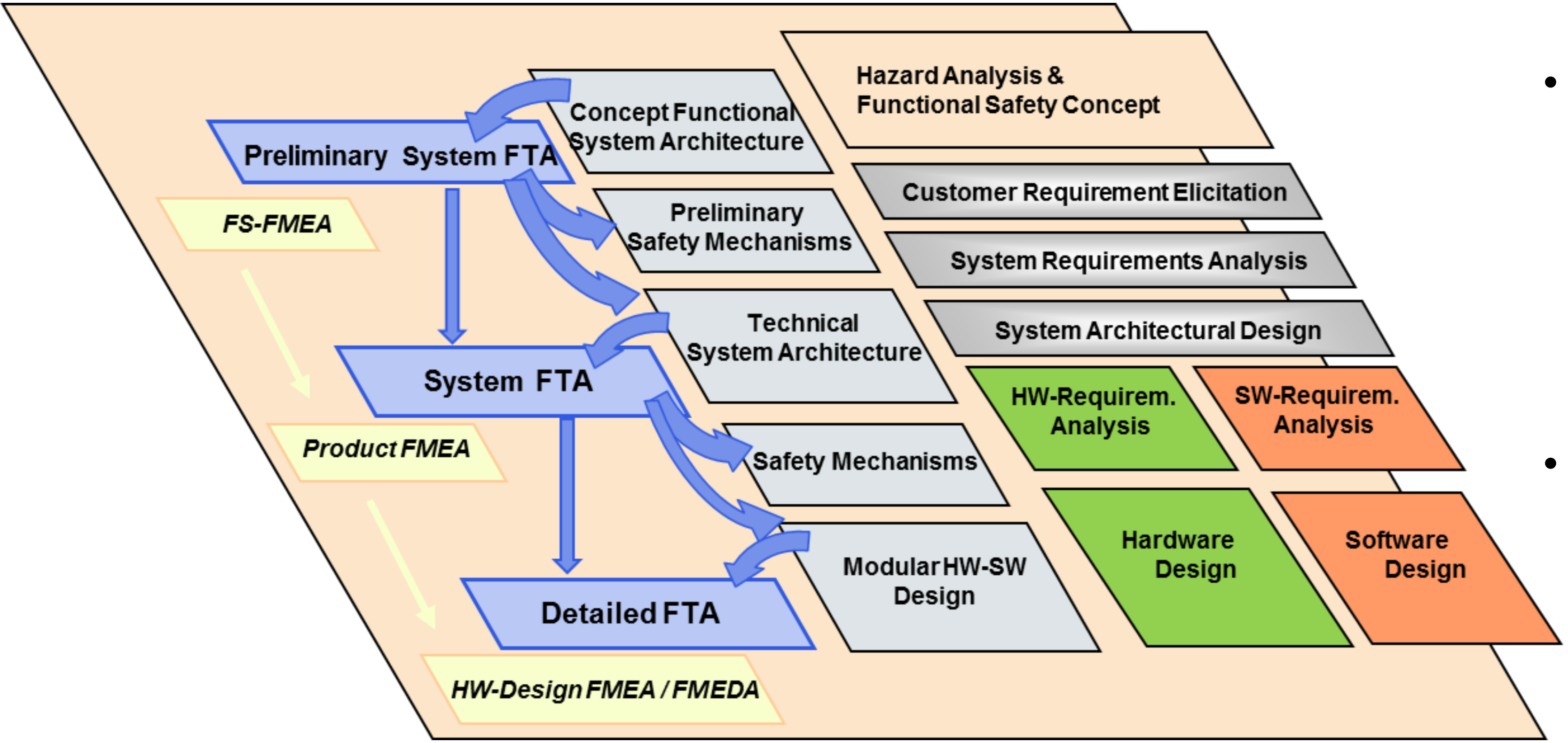
| Inductive analysis | Deductive analysis |
|---|---|
| Bottom-up methods | Top-down methods that |
| Start from defined causes | Start from defined effects |
| Forecast the effects at higher level | Seek the causes at lower level |
| May identify previously unknown hazards | May identify previously unknown causes |

**Notes:**

- Deductive analysis are able to **cope with complexity and redundancy**, which are **typical for systems and functions with ASIL C or ASIL D**
- Inductive and deductive approach are complementary, each having individual „blind spots". **Applying them both for ASIL C and ASIL D** (as required by ISO 26262), the **certainty of sufficient analysis coverage** is increased

Renault Group

# System level Safety Analysis
## Flow

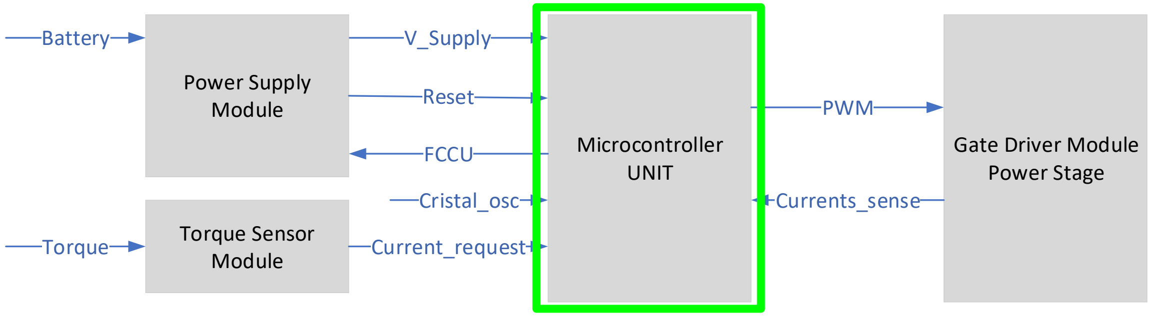


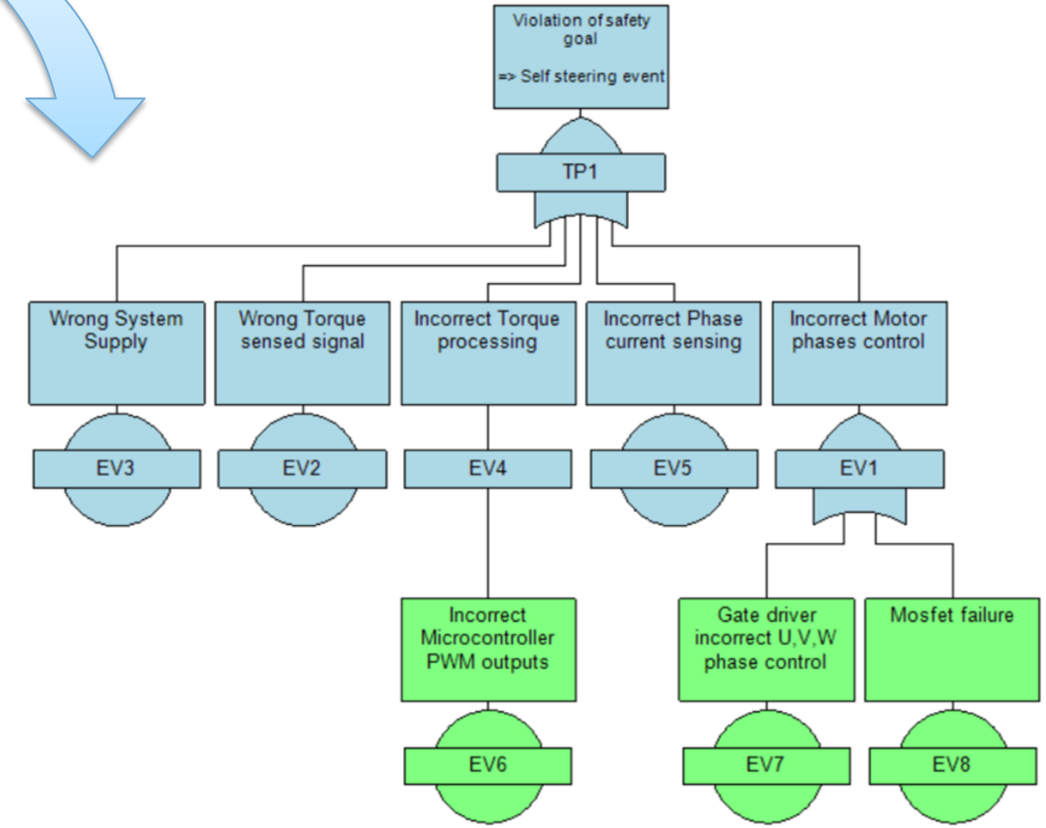

- Iterative FTA and FMEA in 3-steps:
  1) FSC
  2) TSC
  3) HW design- implement failures at parts level (R, C, Mosfets, ICs,..)
- Qualitative and Quantitative analysis are required by the ISO.

Renault Group

# System level Safety Analysis

## Fault Tree Analysis (FTA) Example

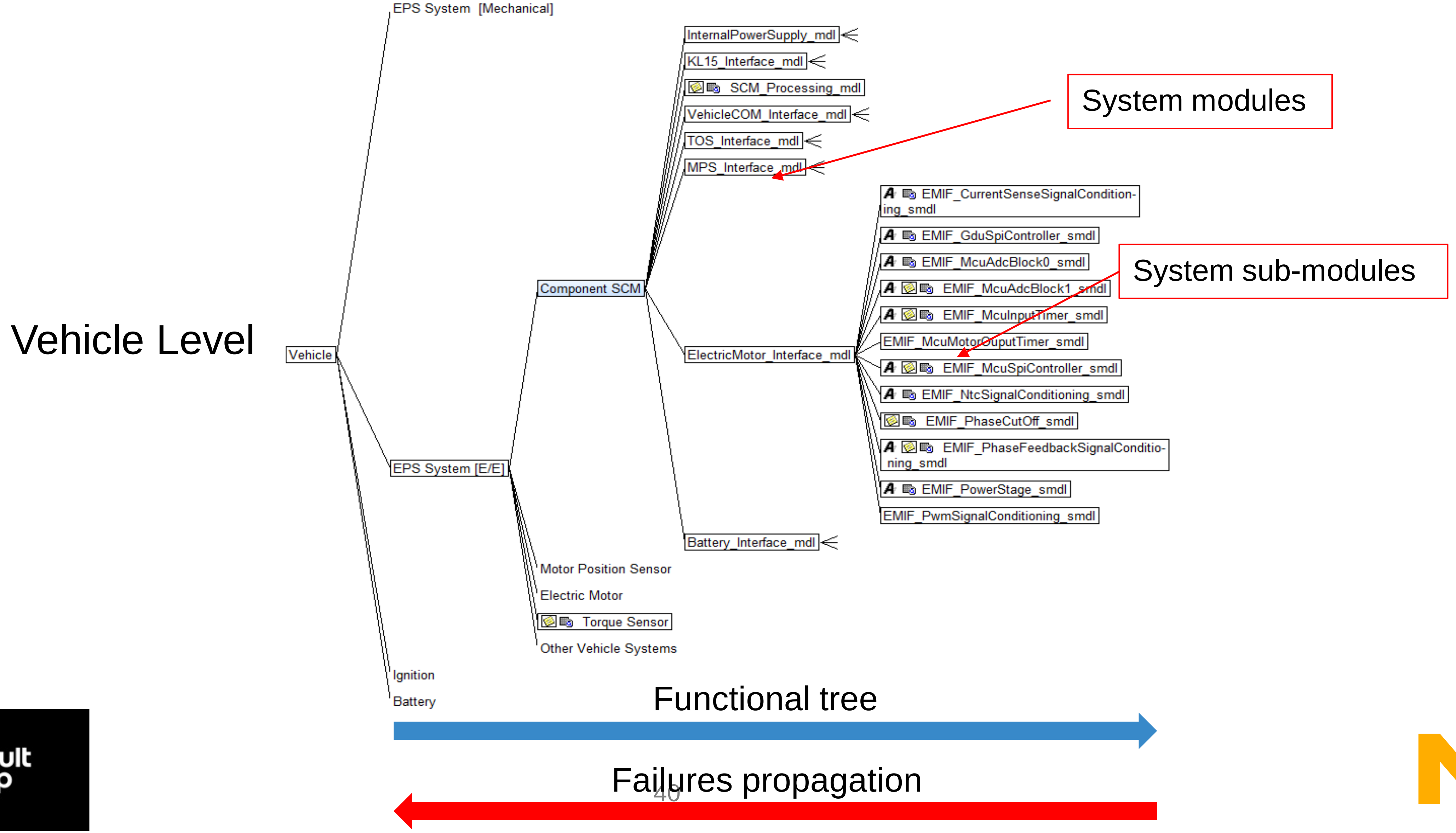



Renault Group

# System level Safety Analysis

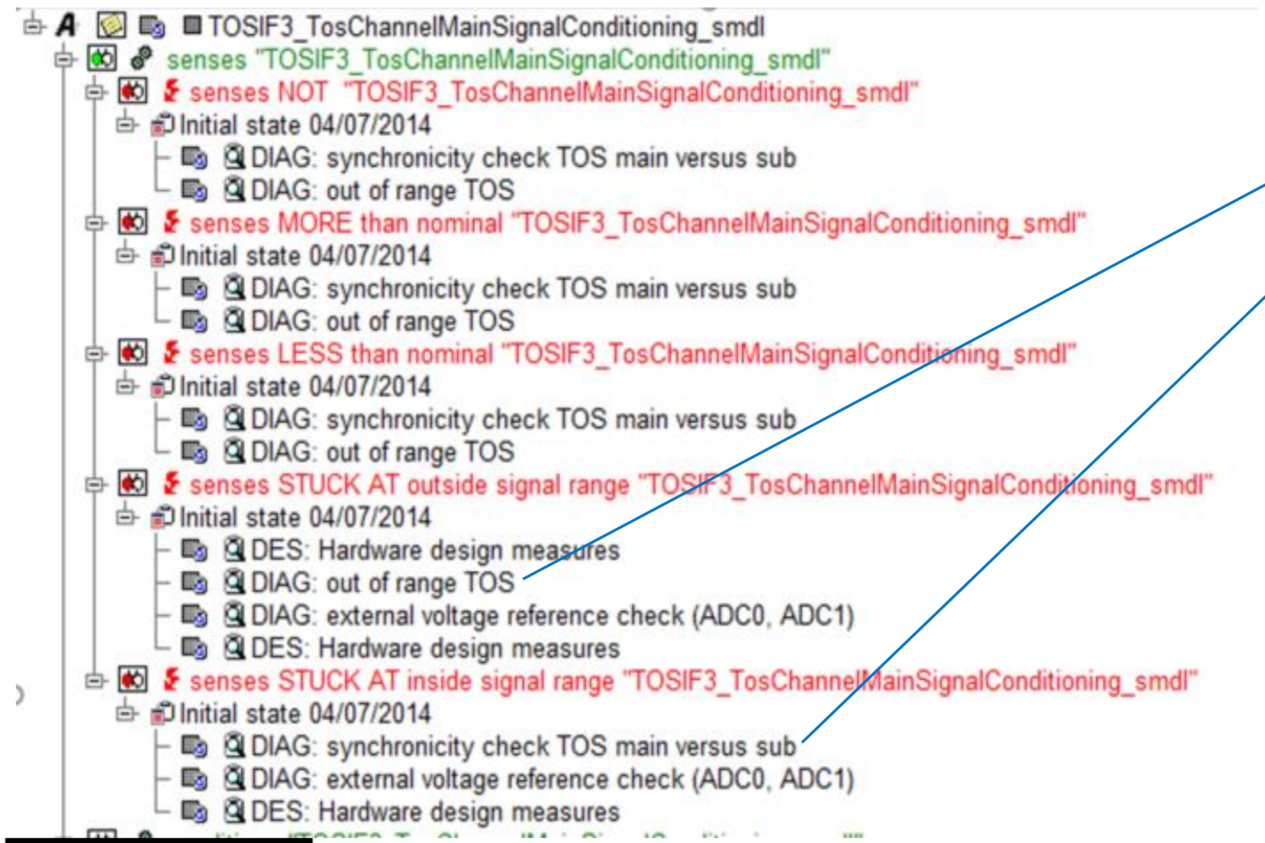
## Failure Modes and Effects Analysis (FMEA) Example




Renault Group

# System level Safety Analysis

## Failure Modes and Effects Analysis (FMEA) Example




- **Diagnostic or SM** is defined for each function failures at system sub-function level.

«TSC requirements specification» can be updated to implement as requirements the new defined SMs .

# System Safety Analysis Summary

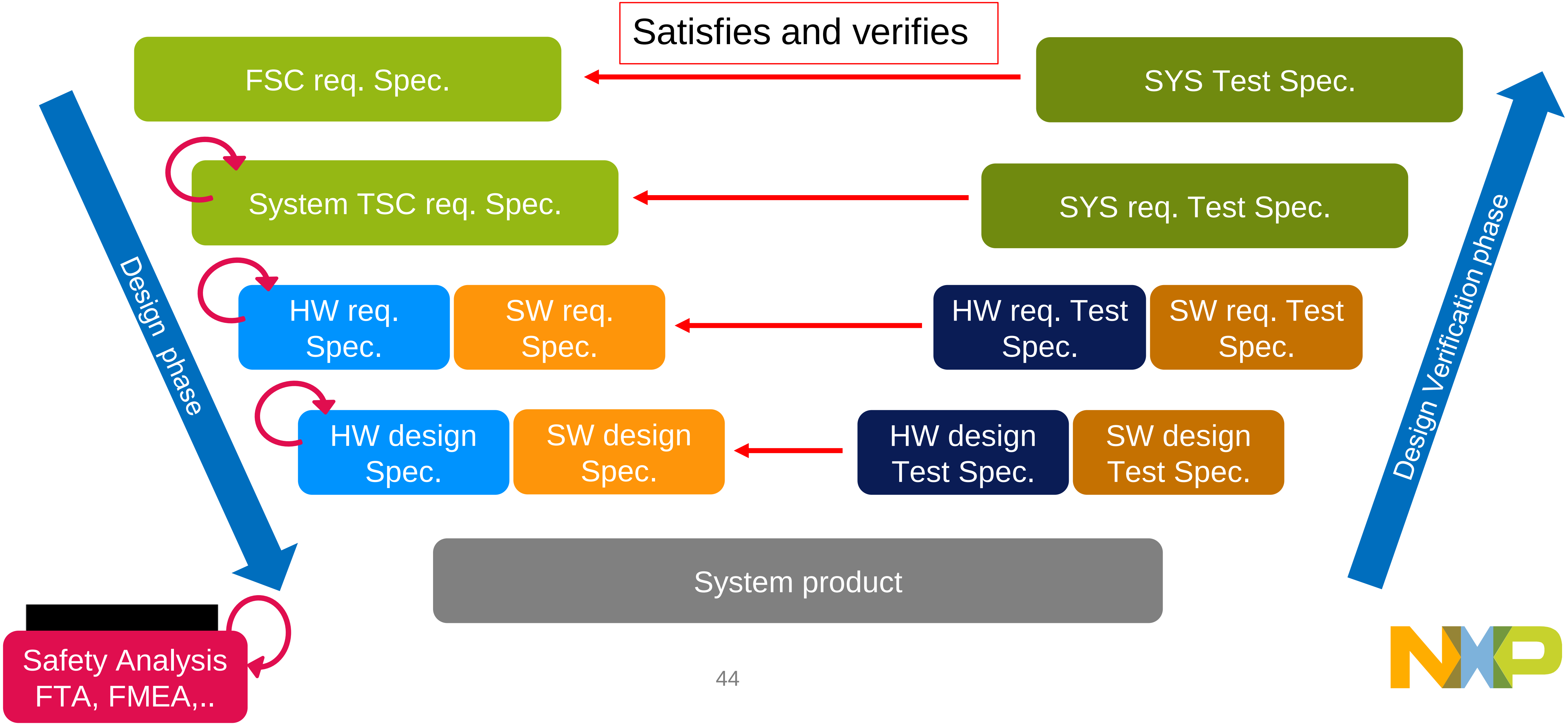
| FMEA | FTA |
|---|---|
| Inductive method (Bottom up) | Deductive method (Top down) |
| Influence / effect analysis of failures | Analysis of root causes |
| Error propagation | Error / failure chain,<br>also used for identifying dependent failures |
| Failure analysis<br>with keywords, catalog of causes, and lesson learnt | Logical root cause analysis<br>Architecture analysis |
| Risk assessment for systematic faults (S, O, D ratings)<br>Safety FMEA for verification of the SYS, HW, SW concept | For hardware random faults and software failures<br>Safety FTA for verification of the SYS, HW, SW concept<br>Preliminary/RFQ phases to allocate safety requirements and ASIL decomposition. |

Renault Group

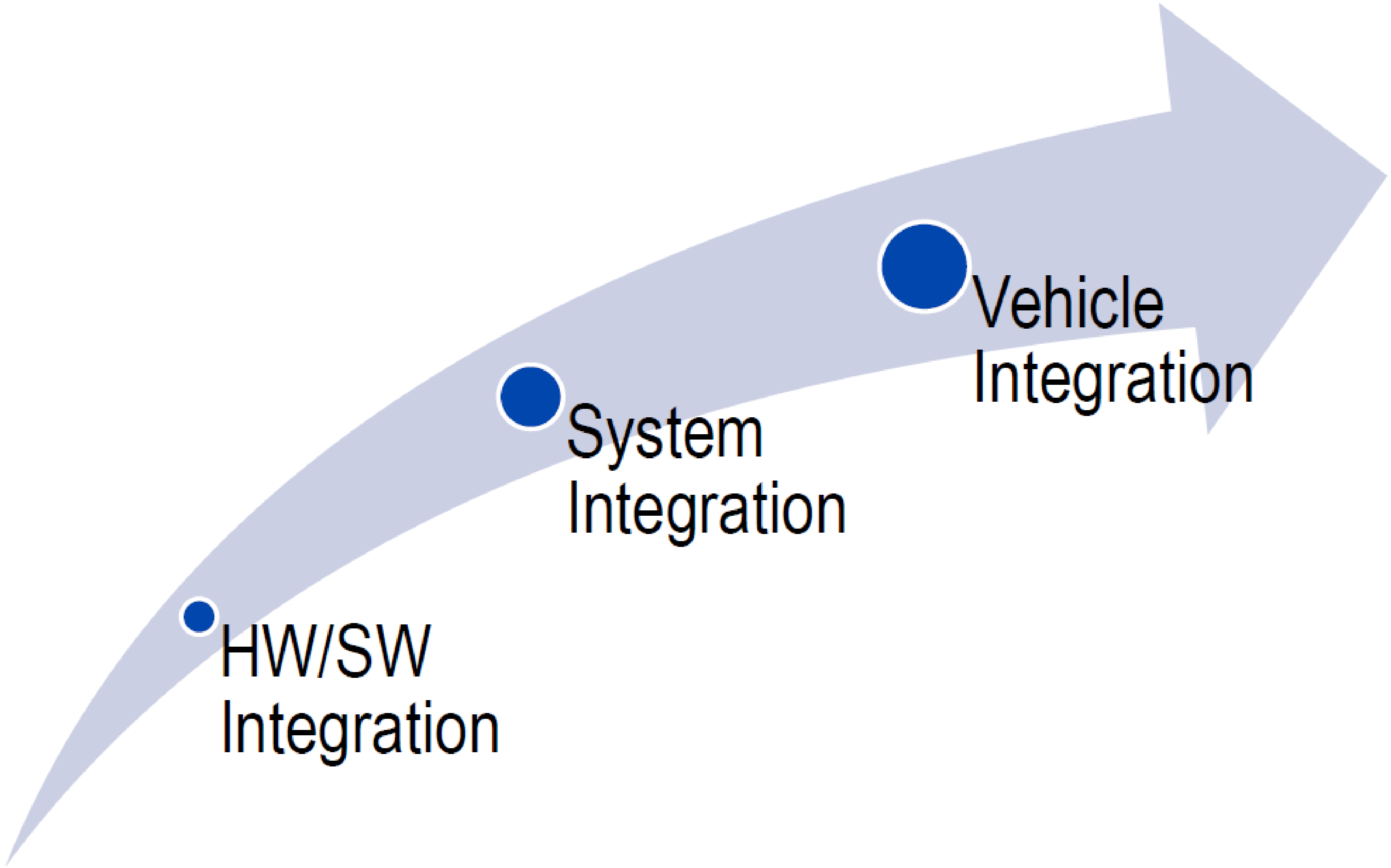
# 06.

# TEST & INTEGRATION

# V-model of System development



# Test & Integration



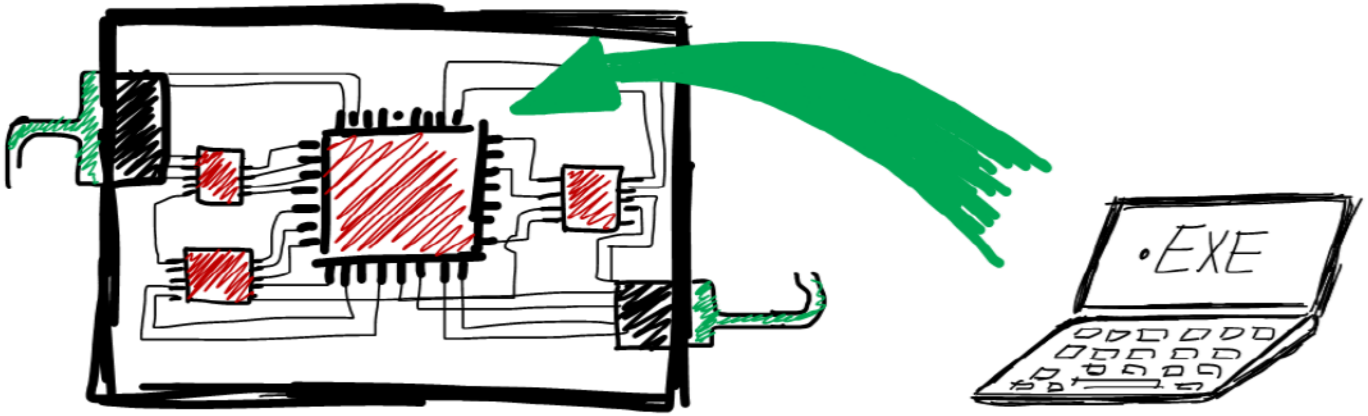
# Test & Integration

## HW/SW Integration :

- Put the SW on the HW ➔ similar to testing of SW safety requirements

- Ensure the correct functional performance, accuracy and timing of the safety mechanisms at the hardware-software level

  - *HIL testing, simulated environment, real environment, etc.* ***=> With Fault injection***




**Goal**: Verify the Hardware Software Interface (HSI), confirm safety measures and DC

**Result**: ECU (possibly including actuators and/or sensors)

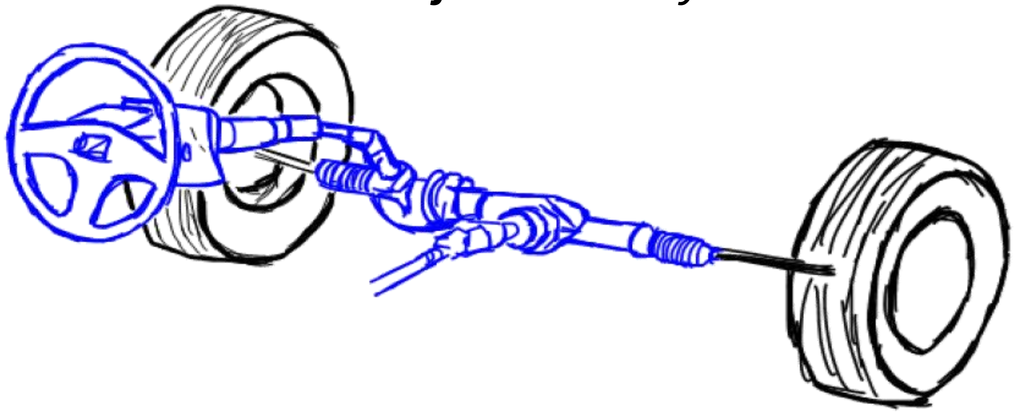
# Test & Integration

## System Integration :

- Put together the subsystems of the ECU (e.g. sensors, logic solvers, actuators), Integrate ECU with elements of other technologies (mechanics etc.)

- Ensure the correct functional performance, accuracy, coverage of failure modes at the system level, and timing of the safety mechanisms at the system level

  - *HIL Tests, Lab Car tests* ***=> With Fault injection*** *at system level*



**Goal**: Verify that the effects of the safety measures including other involved technologies work

Renault Group

**Result**: Complete item



NXP

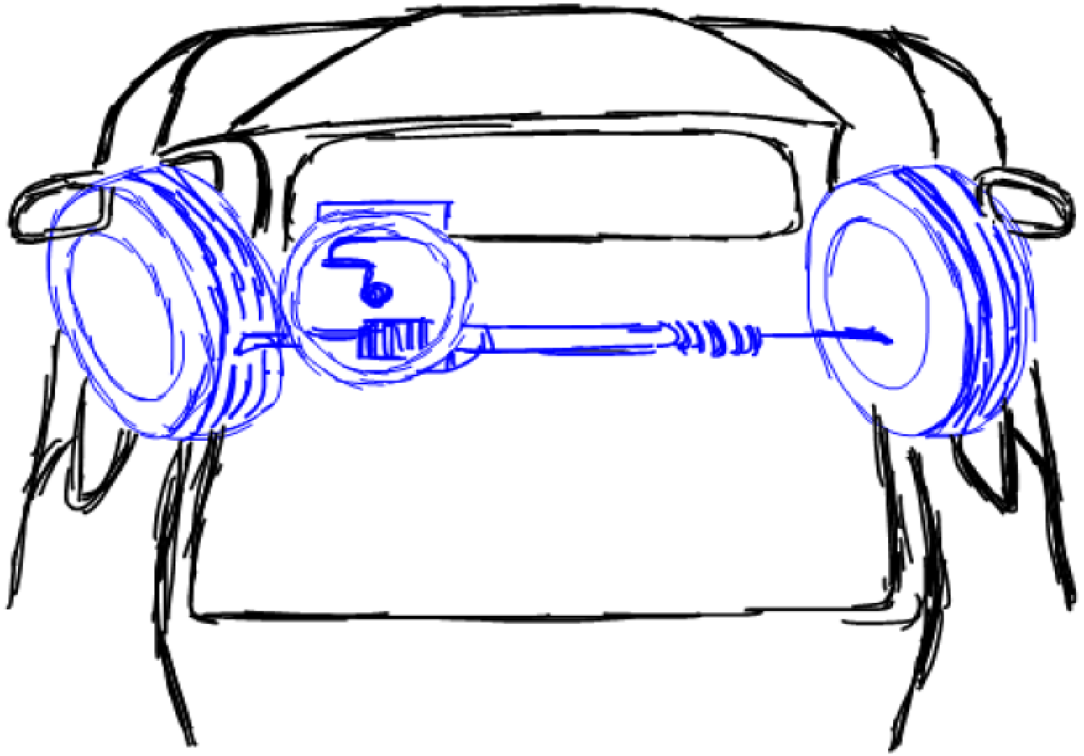
# Test & Integration

## Vehicle Integration :

- Put together the item with depending other items and/or elements

- Ensure the correct functional performance, accuracy and timing of the safety mechanisms at the vehicle level

    - *HIL tests, Lab Car tests, vehicle tests* **=>** ***With Fault injection*** *at vehicle level*



**Goal**: Confirm that the item interacts with other systems correctly (incl. tolerance of failures in other elements)

Renault Group

**Result**: Vehicle

# 07.

# COURSE TAKEAWAYS

SECURE CONNECTIONS
FOR A SMARTER WORLD

# Course takeaways

Explored Functional Safety/ISO 26262 applied to an EPS System

| | |
|---|---|
| Item Definition | Torque assistance steering |
| HARA => Safety Goals | Avoid over/understeering |
| Functional Safety Concept | Monitoring of the three Motor phases |
| Technical Safety Concept | Current sense feedback |
| System Safety Analysis | Analyze possible failure of current sense feedback |
| Test & Integration | SW/HW integration, System integration, Vehicle integration |

Renault Group

SECURE CONNECTIONS
FOR A SMARTER WORLD