Development of ASIL D double rear electric drivetrain
Functional safety’s impacts on development process and product

12/10/22

Andrea Palazzetti

Marelli Electric Powertrain’s products

e-Powertrain Drive System

Inverter

e-Motor

e-Axle*

Power Electronics

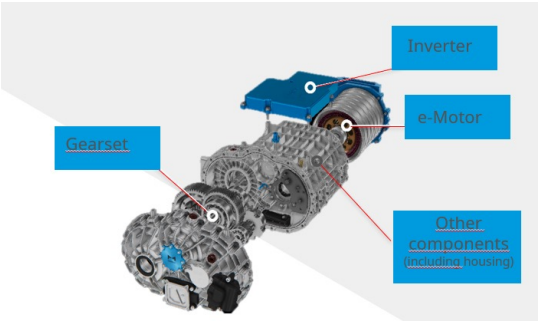
DC-DC Converter*

On Board Charger*

Power Distribution Unit*

Battery System

Battery Management System (BMS)



ISO 26262:2018 General

➔**ISO 26262** is the adaptation and the replacement of IEC 61508 to address the sector specific needs of electrical and/or electronic (E/E) systems **within road vehicles**

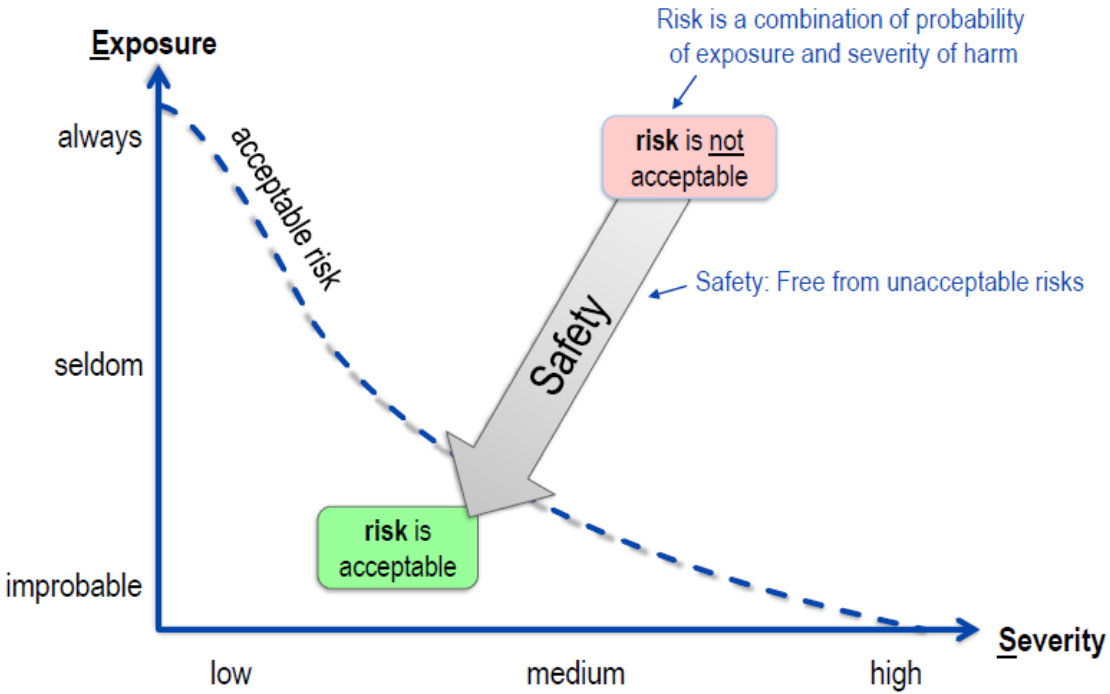
This adaptation applies to all activities during the safety lifecycle of safety-related systems with electrical, electronic (E/E) and software components.

ISO 26262 addresses possible hazards caused by malfunctioning behavior of safety related E/E systems, including interaction of these systems

ISO 26262 does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of safety related E/E systems

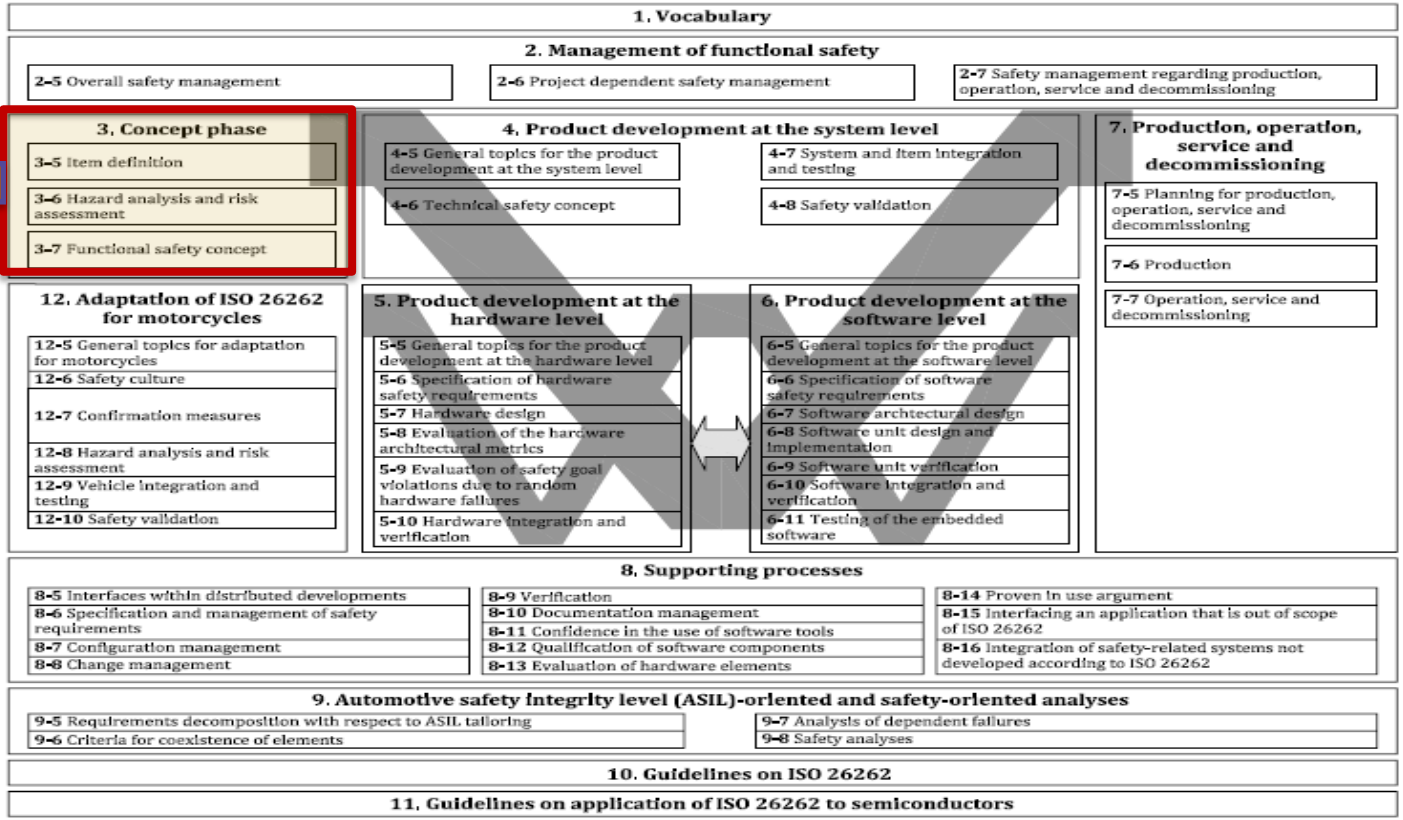
Objective

Objective: Reduce **risk** to a socially **acceptable** level



Development cycle overview

Performed by OEM



Hazard analysis and risk assessment (HARA)

Assessment of potential malfunctions in different scenarios and determination of **"safety goals with the associated integrity requirement (ASIL)"**.

ASIL: Automotive Safety Integrity Level

Each hazardous event is assessed considering its Severity, Controllability and Exposure:

- ASIL is identified according to a specific table
- Starting from the hazardous events, SAFETY GOALS are defined, and they inherit the corresponding ASIL

Hazard analysis and risk assessment (HARA)

Severity S	Exposure E	Controllability C		
		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[a]
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

ASIL's impacts on development

ASIL has a huge impact on the development, management and company organization as well.

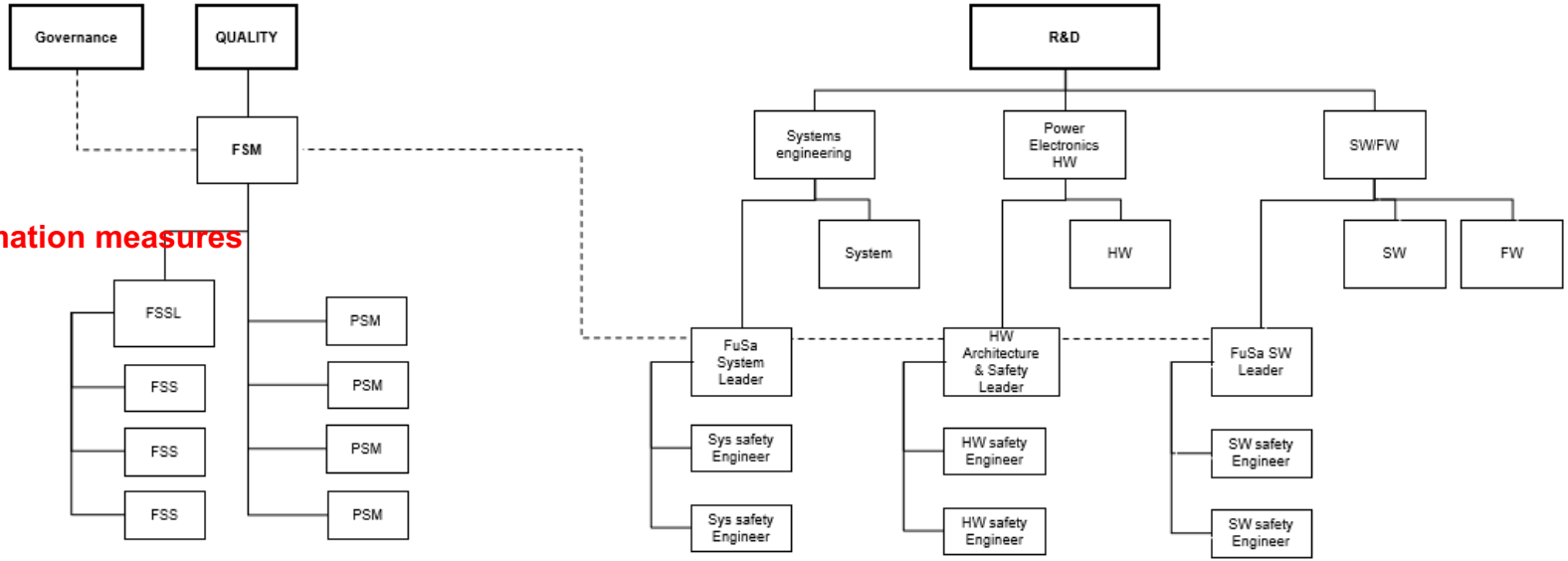
The higher the ASIL is, the more stringent and severe the required methods to be applied are

- Inductive and deductive analysis shall be performed (FMEA. FTA) as well as quantitative analysis (FMEDA)
- High required diagnostic coverage for single point fault (e.g. > 99% for ASIL D)
- Low value of FIT (10 FIT for ASIL D of the whole system)
- High value of software coverage and more severe methods to be applied (e.g. 100% MCDC coverage for unit testing ASIL D)

Functional Safety – Marelli Electric Powertrain Safety organization

The higher the ASIL is, the more the level of independence needed for the confirmation measures and assessment is

Assessment

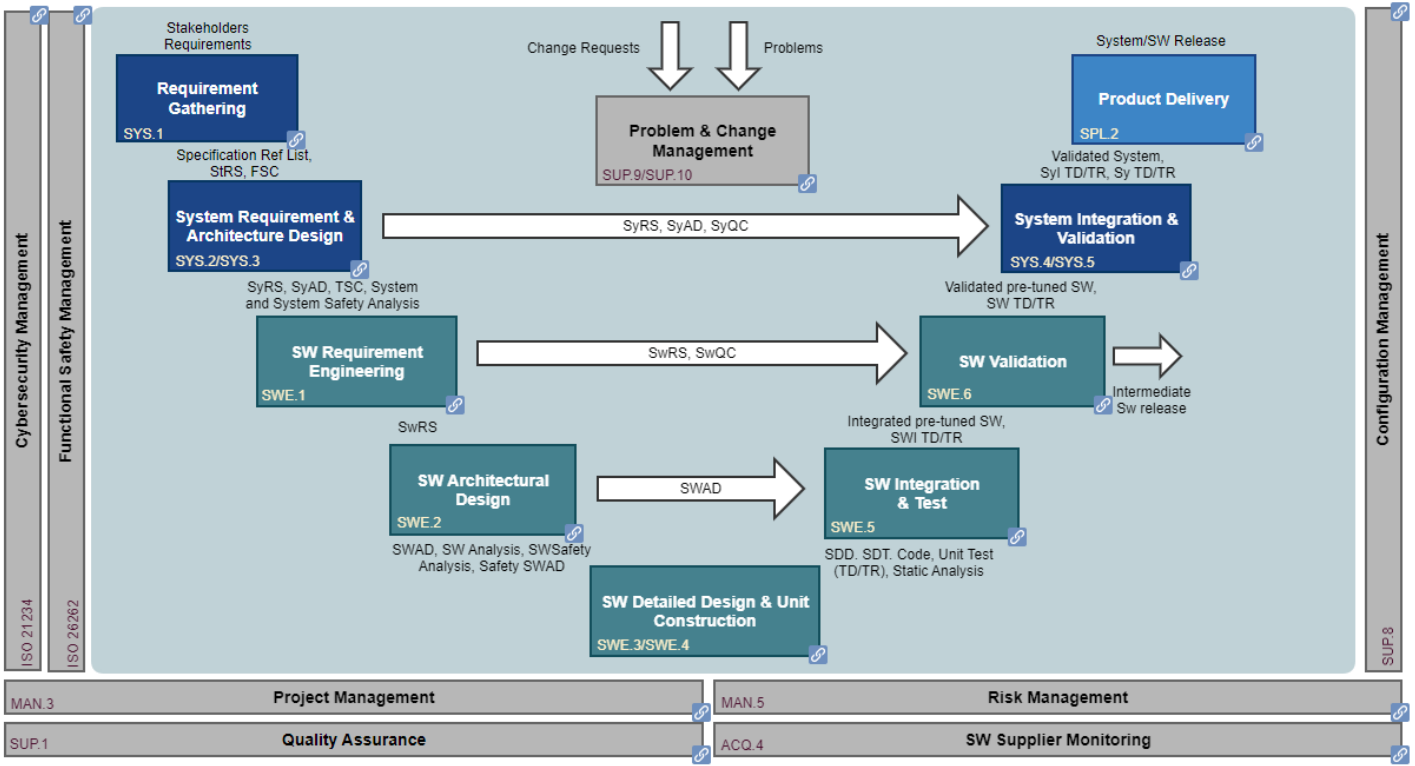


Confirmation measures

Fusa's workproducts development

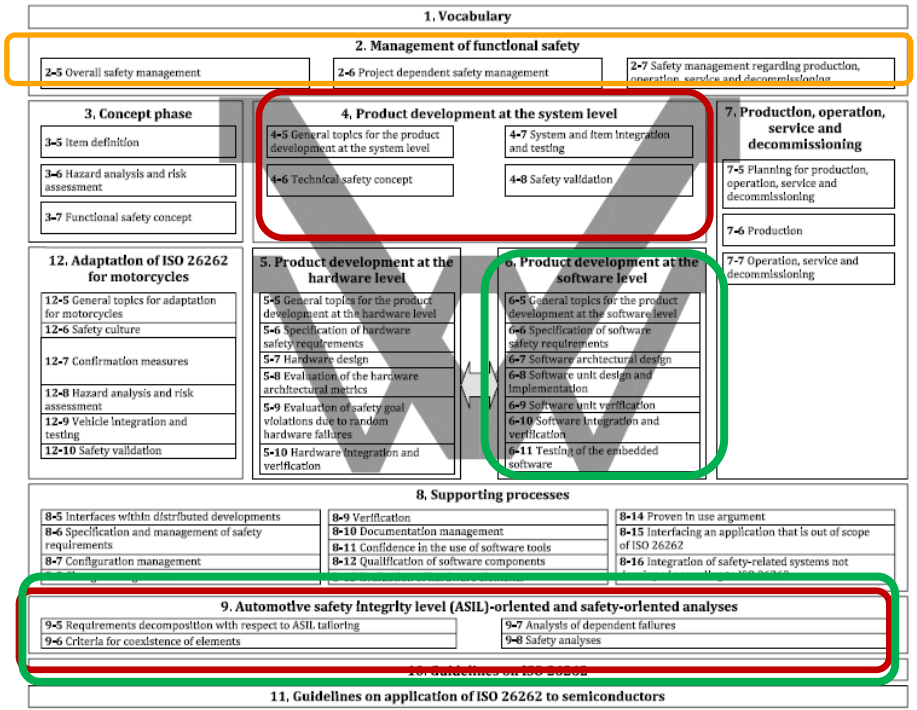
Marelli's development process

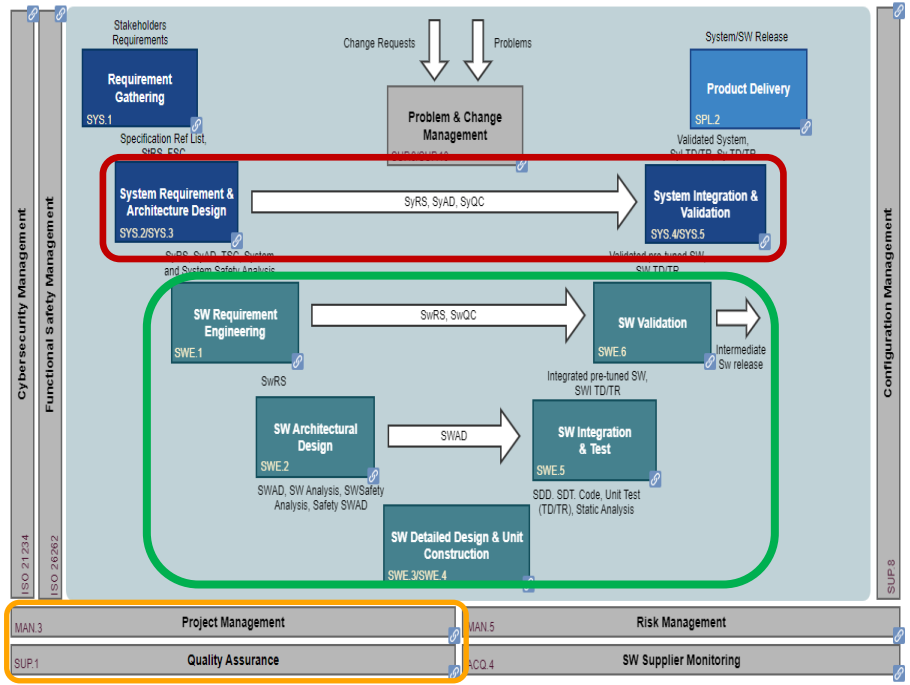
It is based on A-SPICE (3.1) reference model for system and software development, integrated with requirements derived from ISO26262 when needed



Marelli's development process VS ISO26262: example SW/Sys development

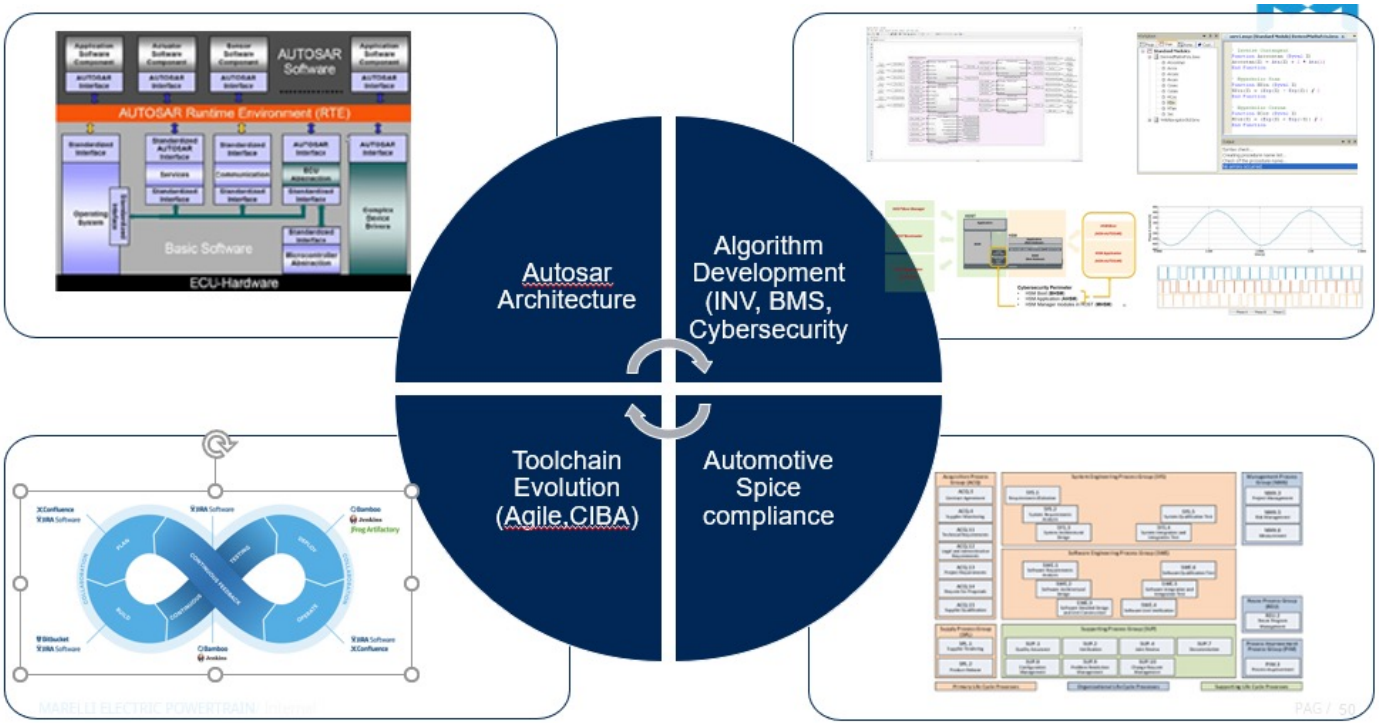
The goal is to have one development process suitable for both safety and not safety development





Overview on SW development and management

SW development is based on Autosar architecture, Model Based Design, A-Spice



Example of work products development at system level

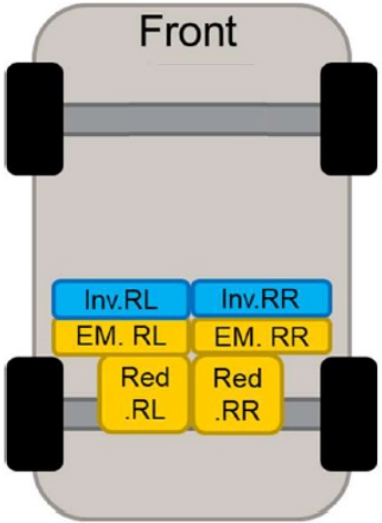
The following work products foreseen by ISO26262 are “mapped” on Sys1- Sys2 - Sys3 A-SPICE’s processes:

- Impact Analysis
- System Requirements and Architecture Plan => one single document for both ASIL and not ASIL development which considers the methods specified by the safety plan
- System Integration and testing plan => the same as the previous one: one single document for both ASIL and not ASIL
- Technical safety requirements (including reviews and confirmation reviews)
- Hardware software interface (at system level)
- Safety analyses according to safety plan (depending on ASIL):
  - System FMEA, System FTA, System DFA including reviews and confirmation reviews
- System architectural design (including reviews and confirmation reviews) for both safety and not safety requirements

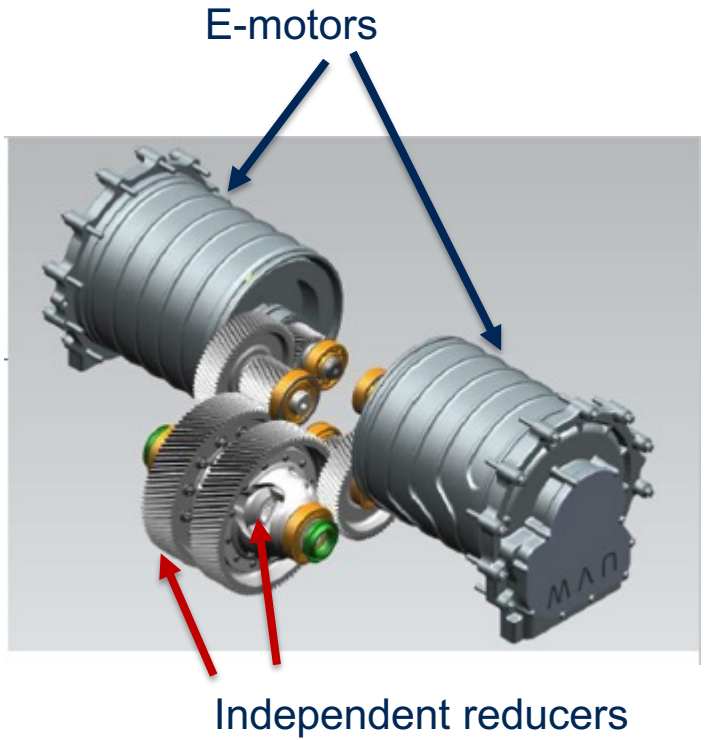
Case study: Rear double electric powertrain

The system consists of a complete electric powertrain for independent delivery of torque to each rear wheel for a sporty electric car and it is composed by:

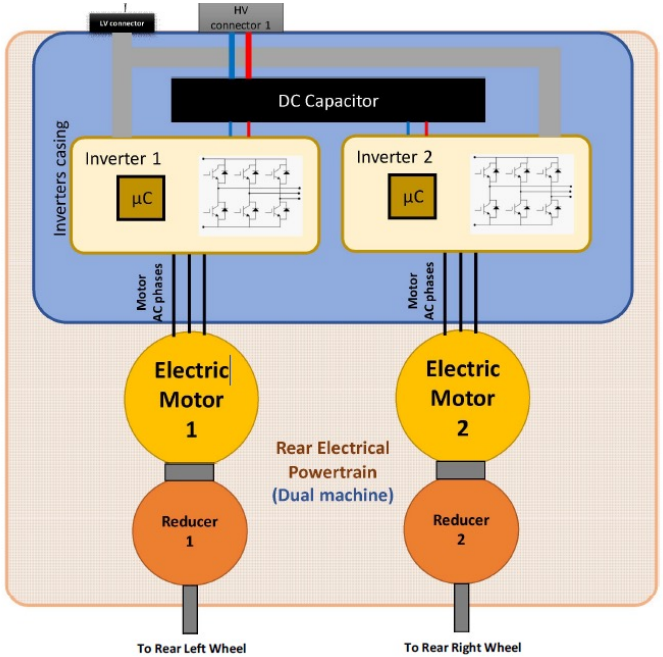
- ❑ 2 x Inverters hardware
- ❑ 2 x Inverters software
- ❑ 2 x electric machines
- ❑ sensors involved in the control logic or the monitoring of the powertrain
- ❑ Two mechanical reducers



Case study: Rear double electric powertrain



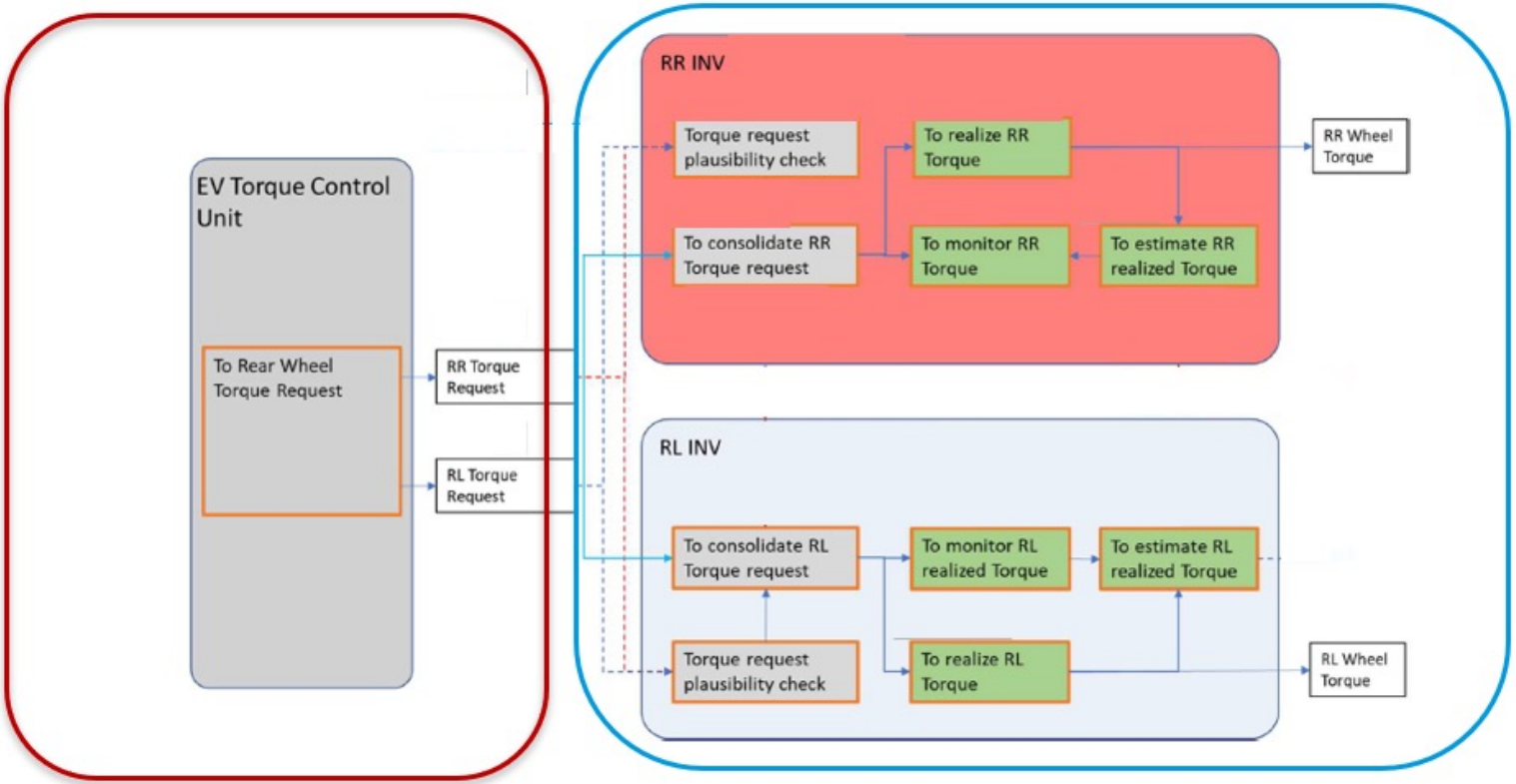
System overview



Main system's function: Torque actuation

OEM's responsibility: reference torque calculation

Marelli's responsibility: torque actuation and monitoring



Safety Goals

- No overheating => **ASIL D**
- No risk of electric shock => **ASIL D**
- No unwanted over traction torque => **ASIL D**
- No unwanted over generative torque => **ASIL D**

Safe state

- Actual torque at wheels shall be close to zero in all operational conditions
- ECU shall stop transmitting messages over can in all operational conditions
- Safe state shall be active till key off.

Safe state's impacts

The definition and achievement of safe state has a huge impact on system and HW development

- Zero torque is achieved by means of phases circuit opening (6 switch open) or phases short circuit (3 phase short) depending on electric motor speed. It means that the system shall be able to activate the proper action even in case the control logic is not working at all. => additional mechanism implemented in HW
- The can communication shall be always stopped, even in case the control logic is not properly working, which means that an additional mechanism implemented in HW is needed.

Safety concept

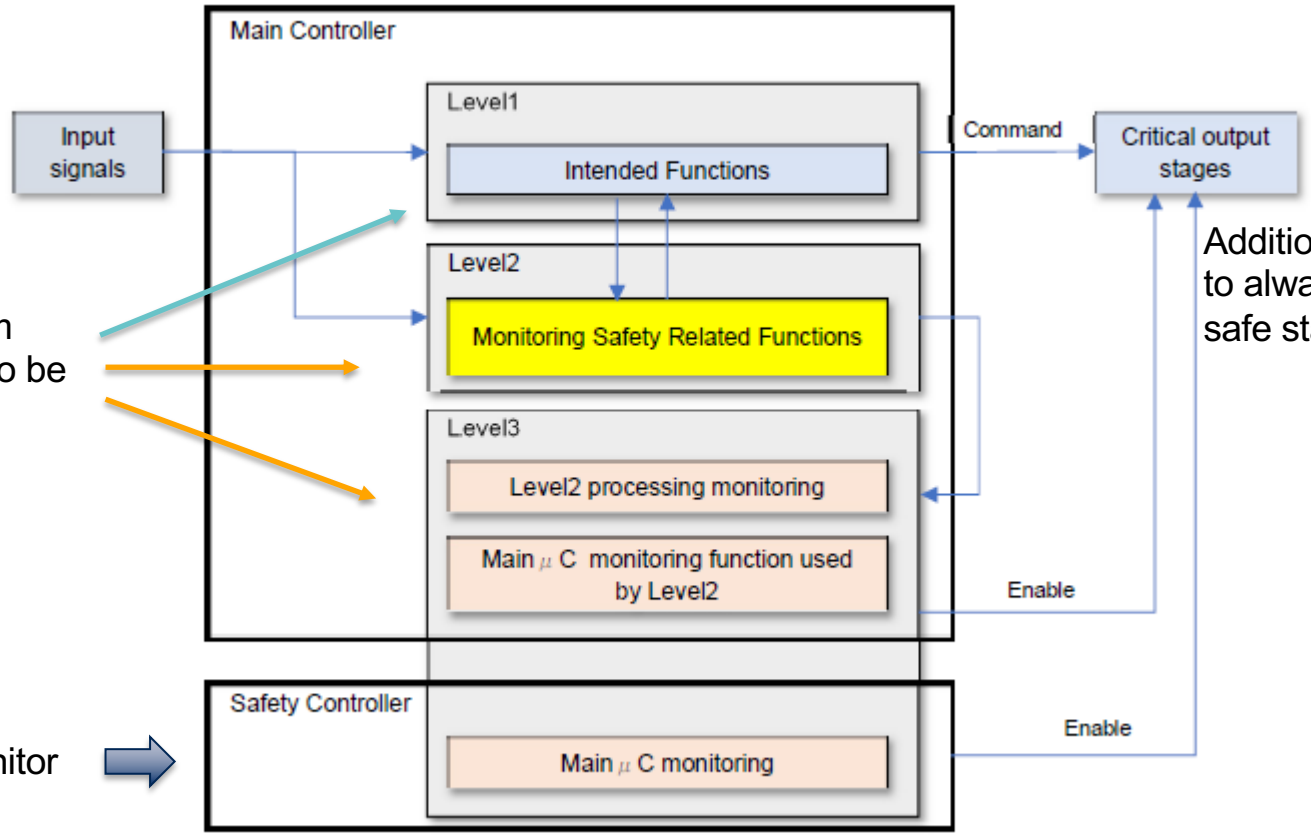
Based on E-Gas safety concept: three levels

- ❑ Level 1: it implements the «intended functions» compliant to ASIL QM
- ❑ Level 2: it performs an independent sw monitoring of level 1 compliant to ASIL D
- ❑ Level 3: it performs an independent monitoring of the uP HW integrity compliant to ASIL D

Constraints

- ❑ Freedom from interference shall be achieved between level 1 and 2/3 which means additional safety analyses to be performed and appropriate uP HW features (e.g. MPU)
- ❑ Independent HW able to perform the monitoring on main uP HW integrity (level 3)
- ❑ Independent HW able to always achieve the safe state when needed

Safety concept

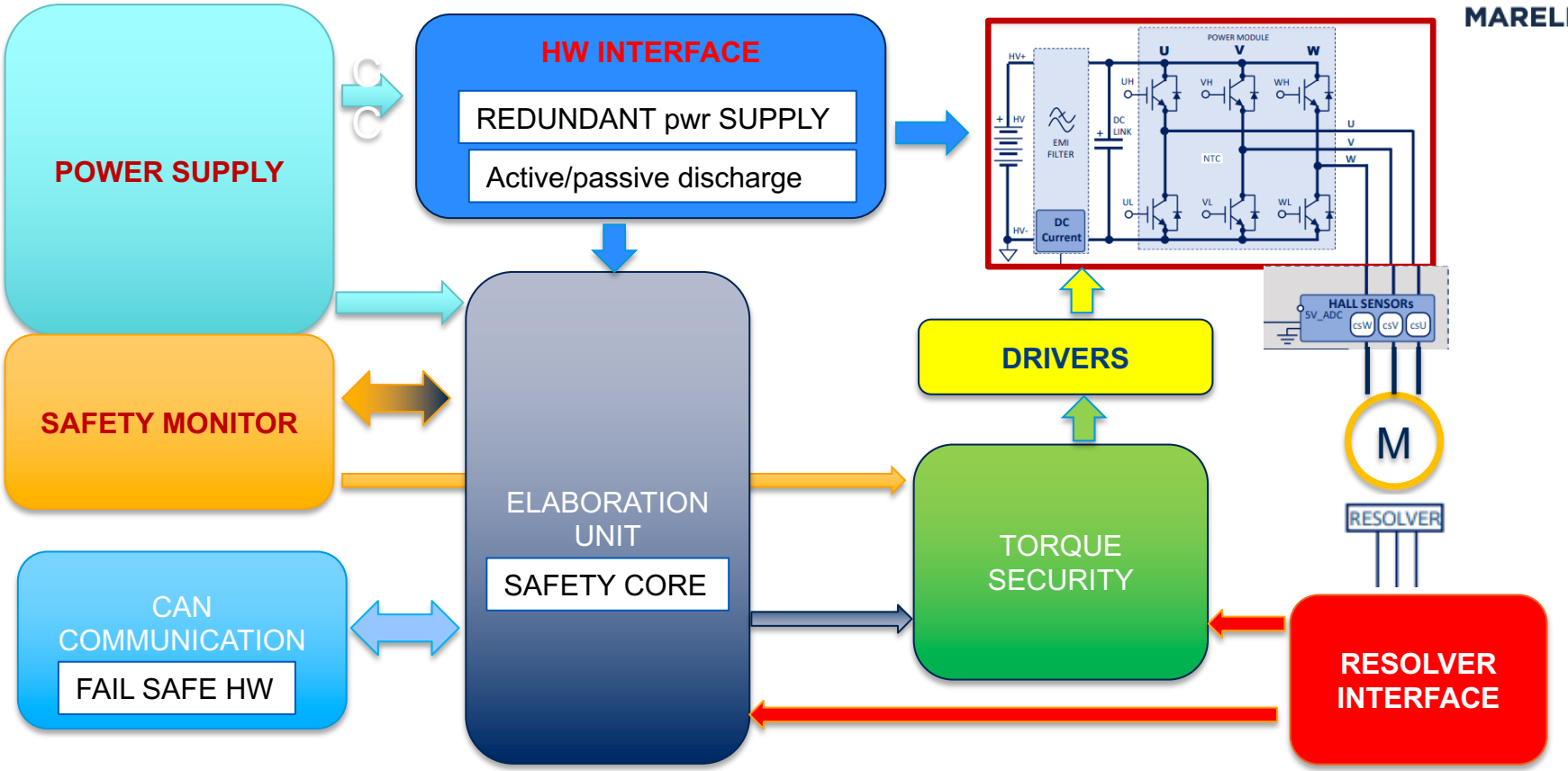


Freedom from interference to be achieved

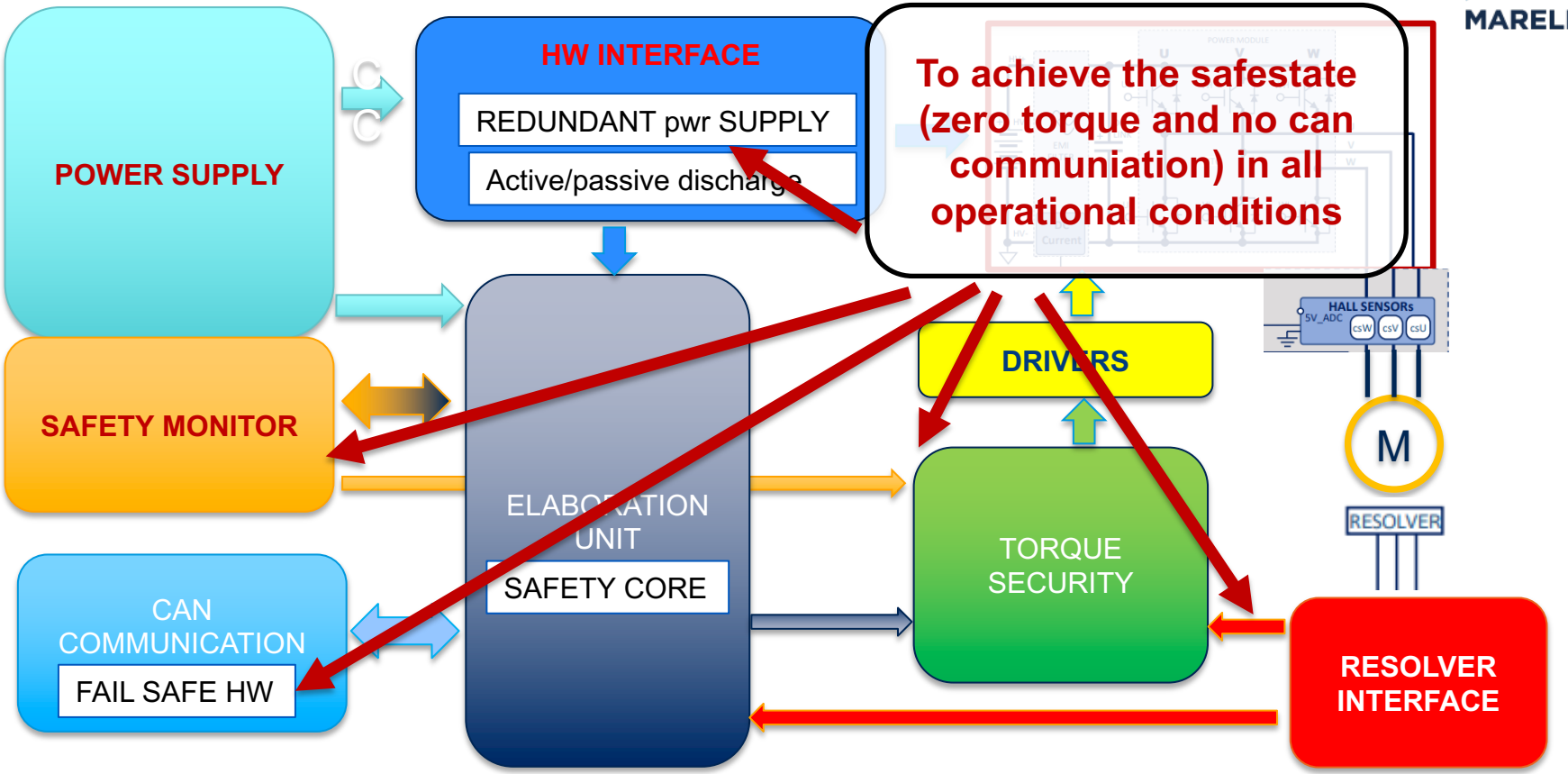
Safety monitor

Additional safety HW to always achieve the safe state

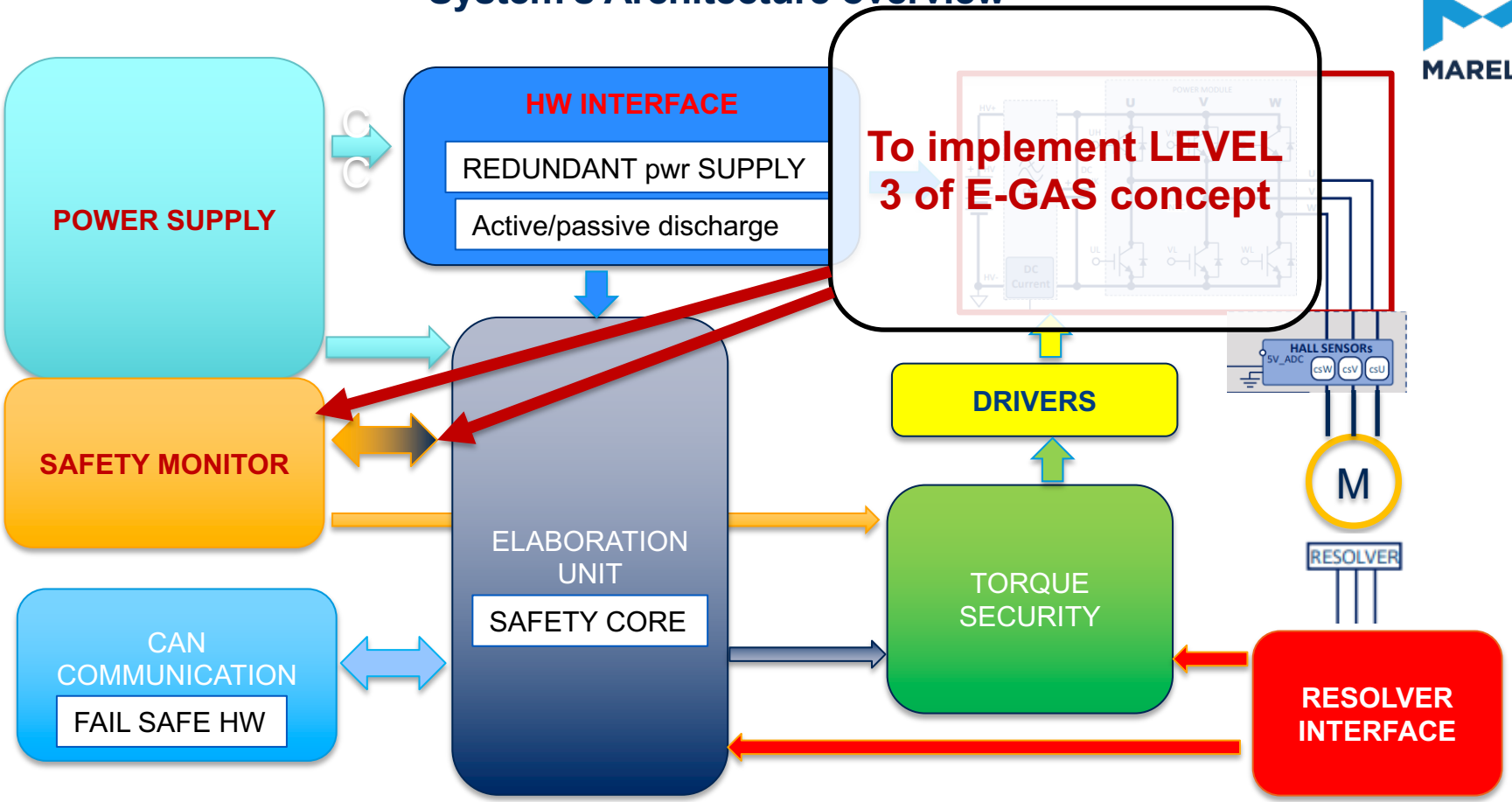
System's Architecture overview



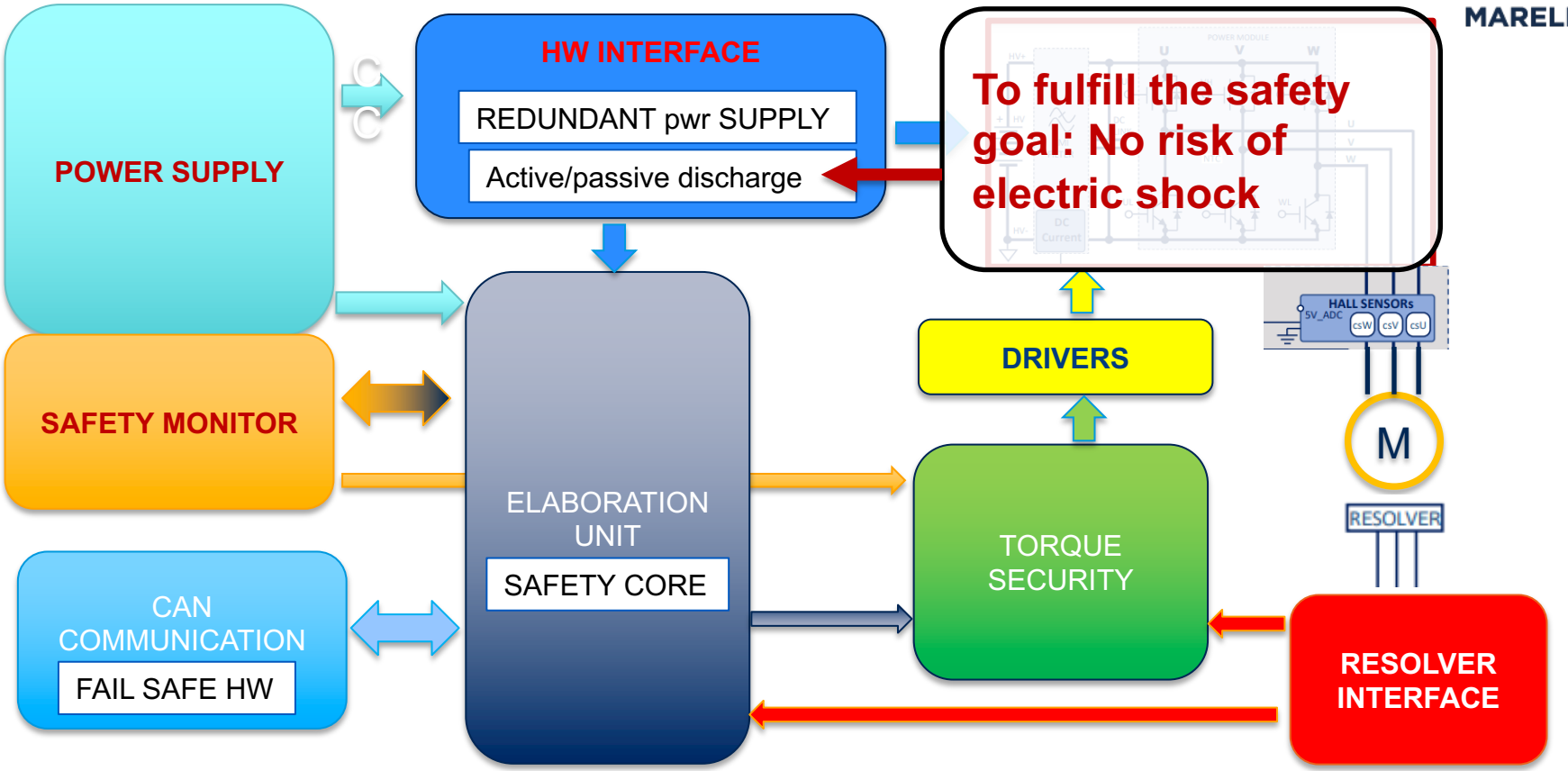
System's Architecture overview



System's Architecture overview



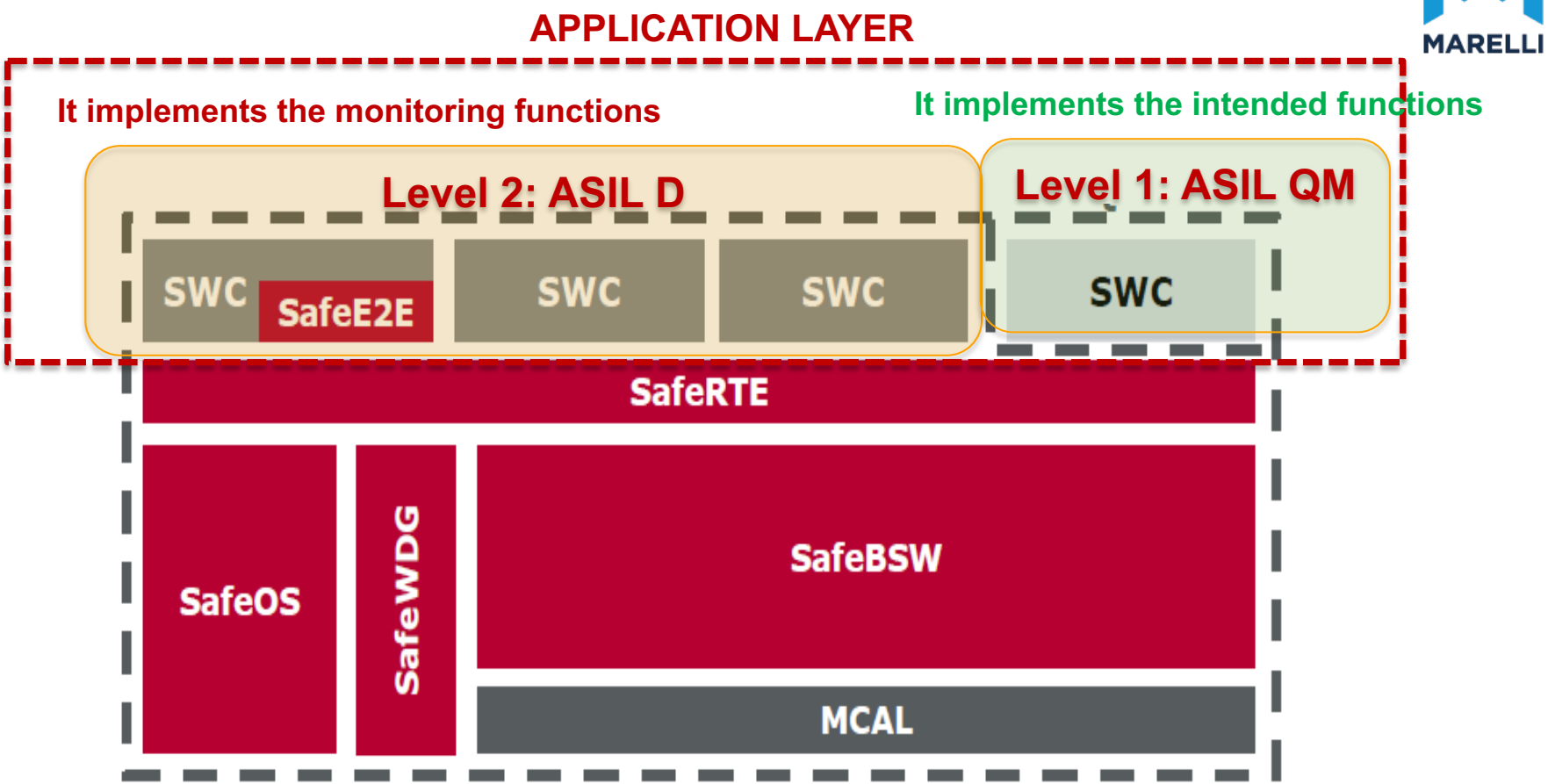
System's Architecture overview



SW's Architecture overview

- AUTOSAR 4.3 SW architecture
- ASIL D qualified O.S (Scalability Class 4)
- E2E protection to achieve Freedom From Interference
- Safety relevant SW Components (both Application SW and Basic SW) are allocated on uP' safety core (with Lockstep)

SW's Architecture overview

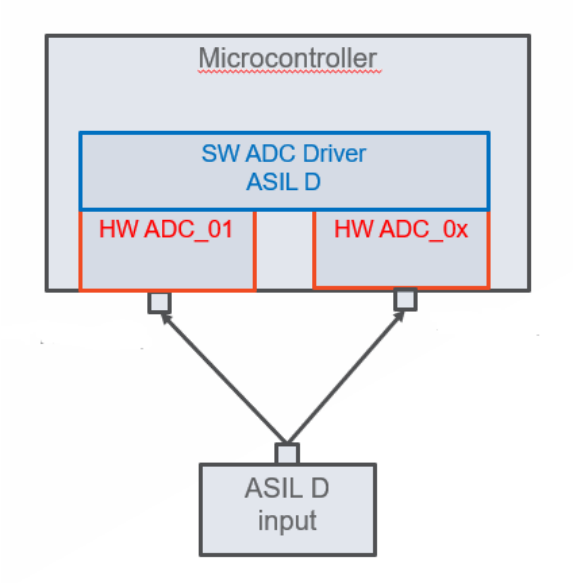


HIDDEN TRAPS : SAFETY MANUALS

- The safety manuals are related those components which implement internal safety mechanisms or logic.
- They specify additional requirements to be fulfilled in order achieve the needed ASIL which can have a huge impact on System and HW preliminary architecture
- Since the safety manuals are not immediately available and their analysis takes time, this topic represents a potential risk of reworking, or delay, to be properly managed
- For that reason safety manuals should be available and analysed during the earliest stages of the project.

Example safety requirements coming from safety manuals

- In order to achieve ASIL D for analogue signals acquisition, Hw redundancy shall be implemented:



Required HW redundancy can become a severe issue for the project's time scheduling if not managed as soon as possible.

CONCLUSION

The capability of developing safety relevant complex systems (ASIL C or D), in the required time, and in accordance with ISO 26262:2018, is a discriminating factor in order to acquire new customers and new projects.