Industrial battery safety

Safe design through layers

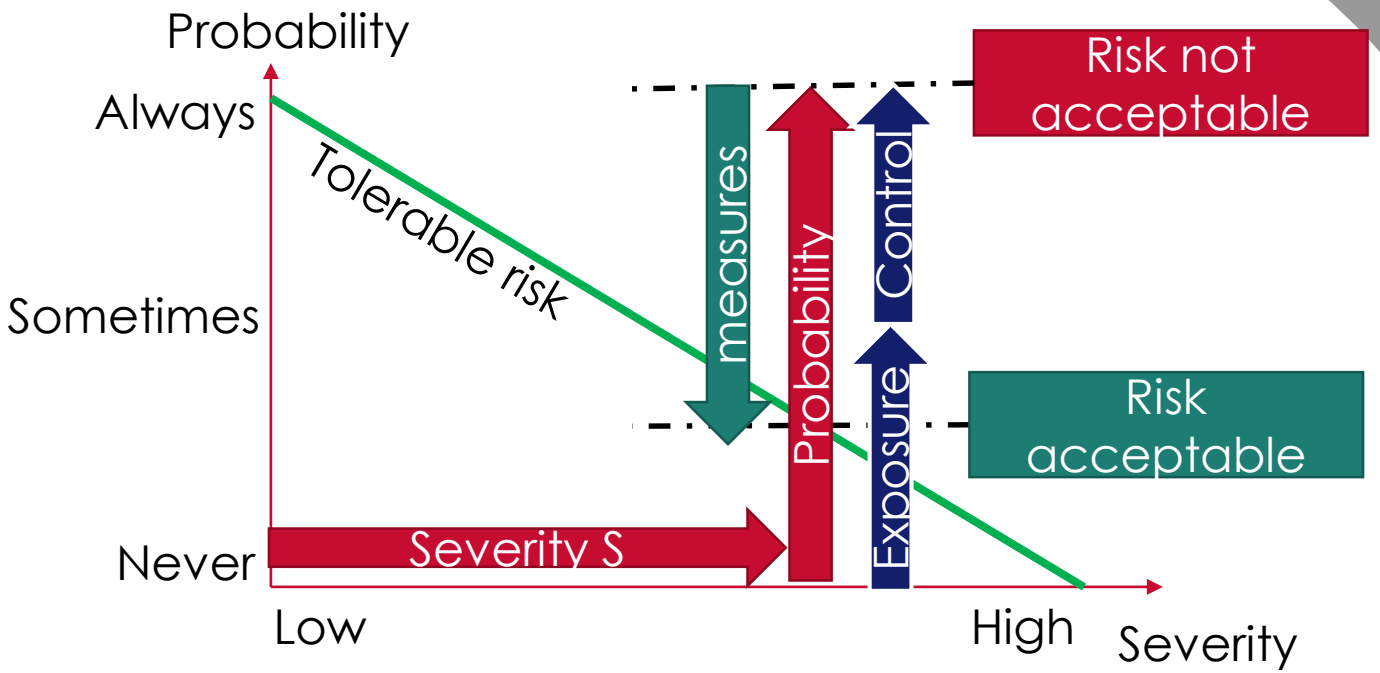
Manuel Rabl

Senior Director Project Management

What is safety?

Safety	Freedom of unacceptable **risk**
Risk	Combination of probability of occurrence and severity of **harm**
Harm	Injury or death of people /catastrophic consequences for the environment

Examples of risks:
- Unintended acceleration
- Unintended breaking
- Loss of braking capabilities
- High voltage
- Penetration
- Fire
- Explosion

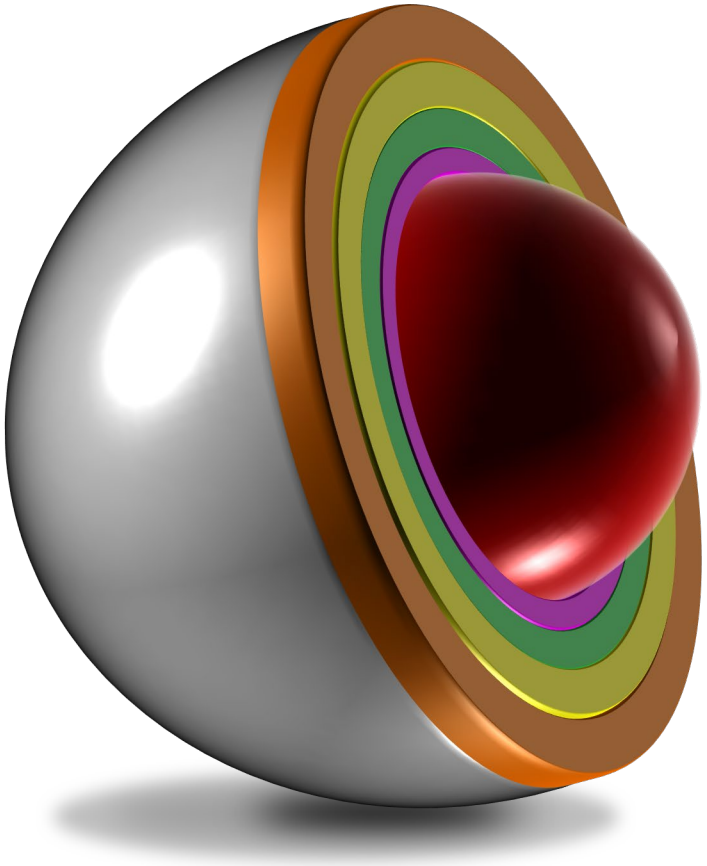


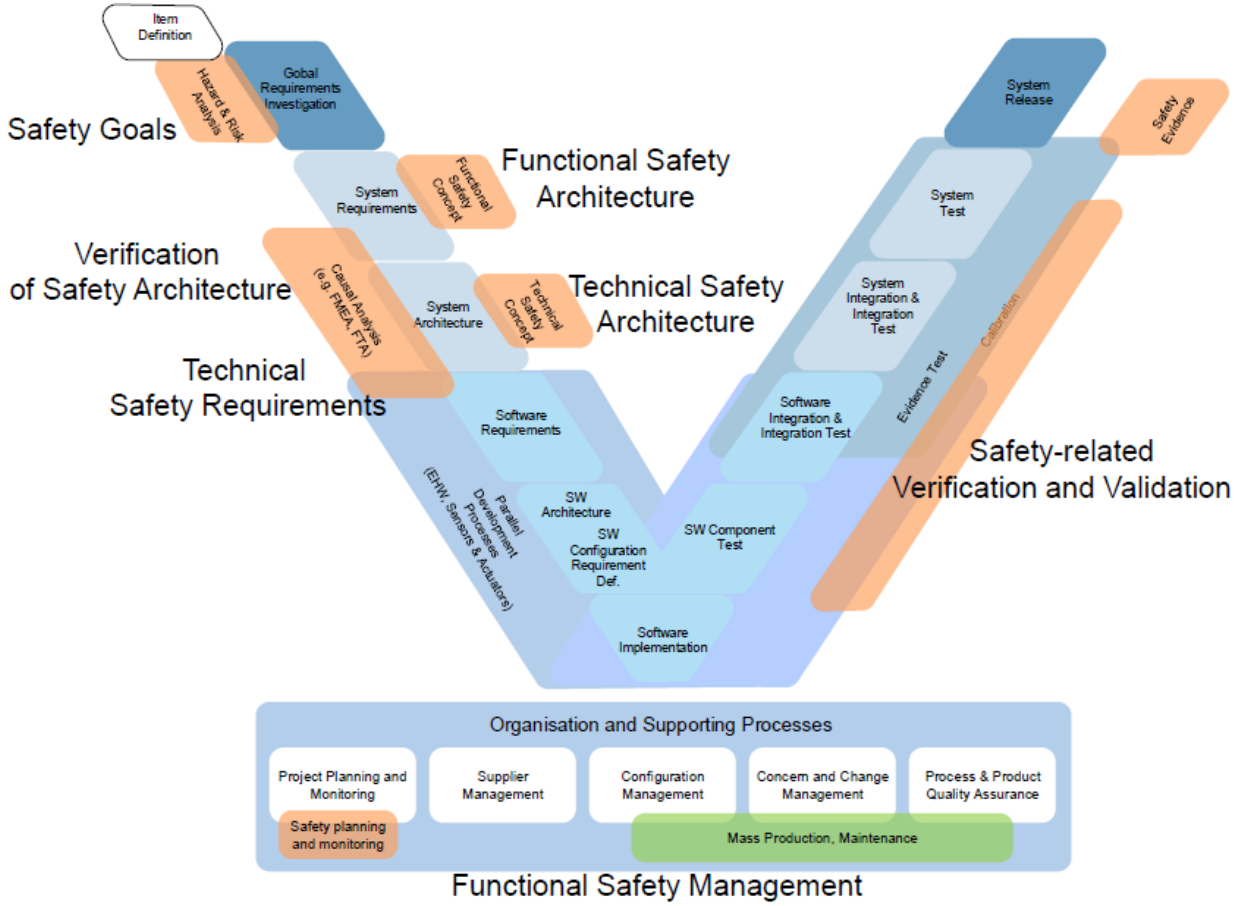
Overall goal to be achieved during development/ production/ maintenance/ operation:

→ Risk reduction to an acceptable level

How to achieve safety?

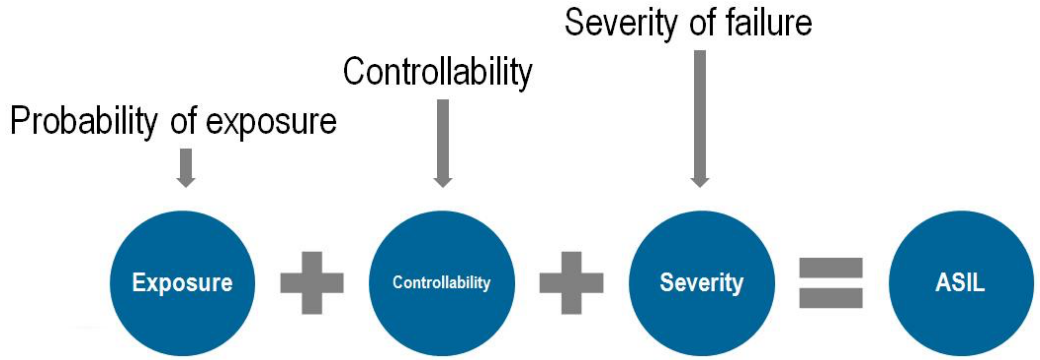
Safe design through layers

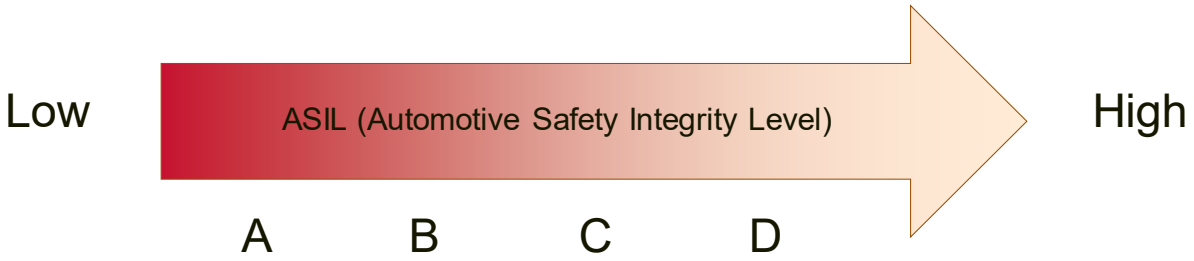


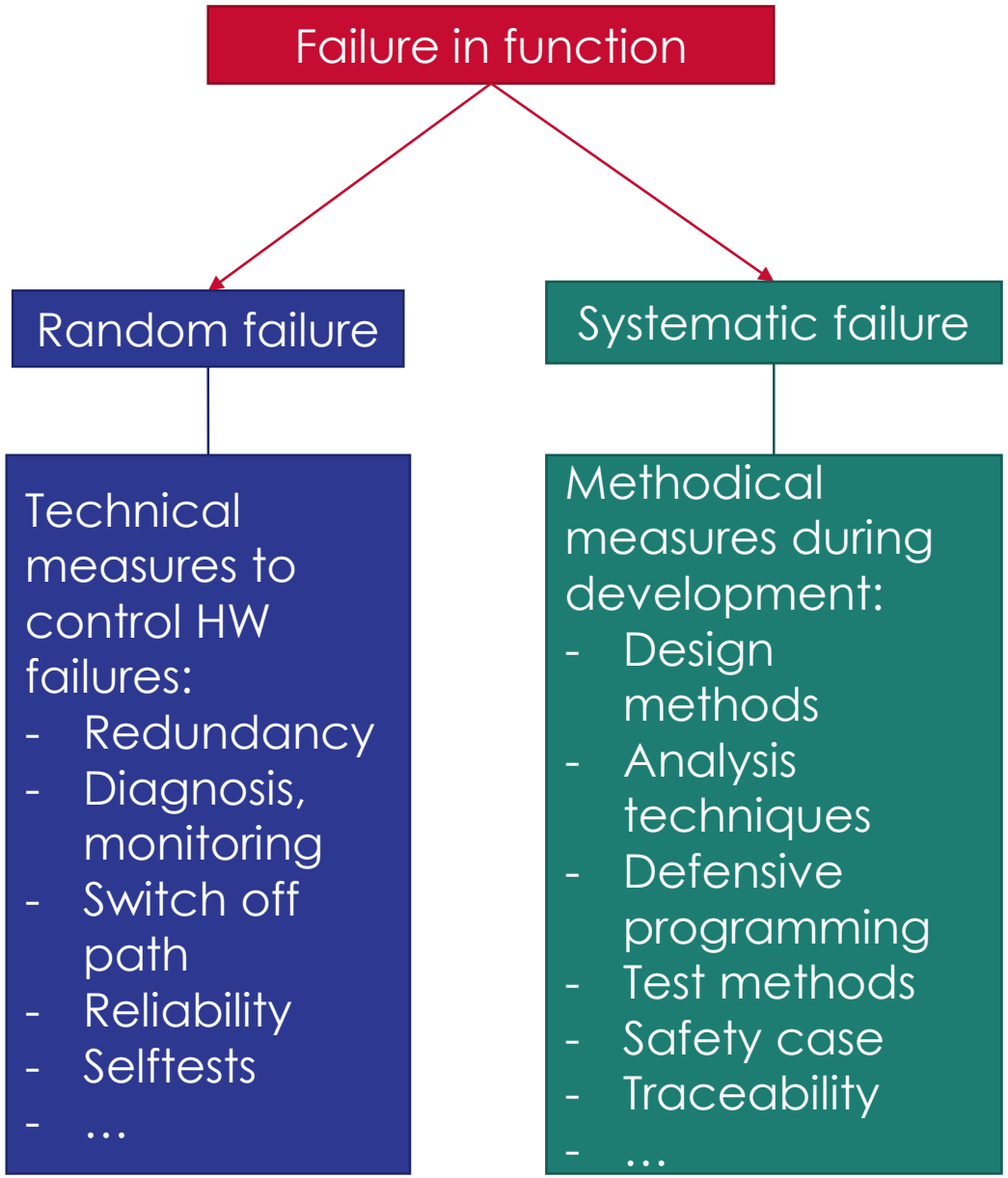


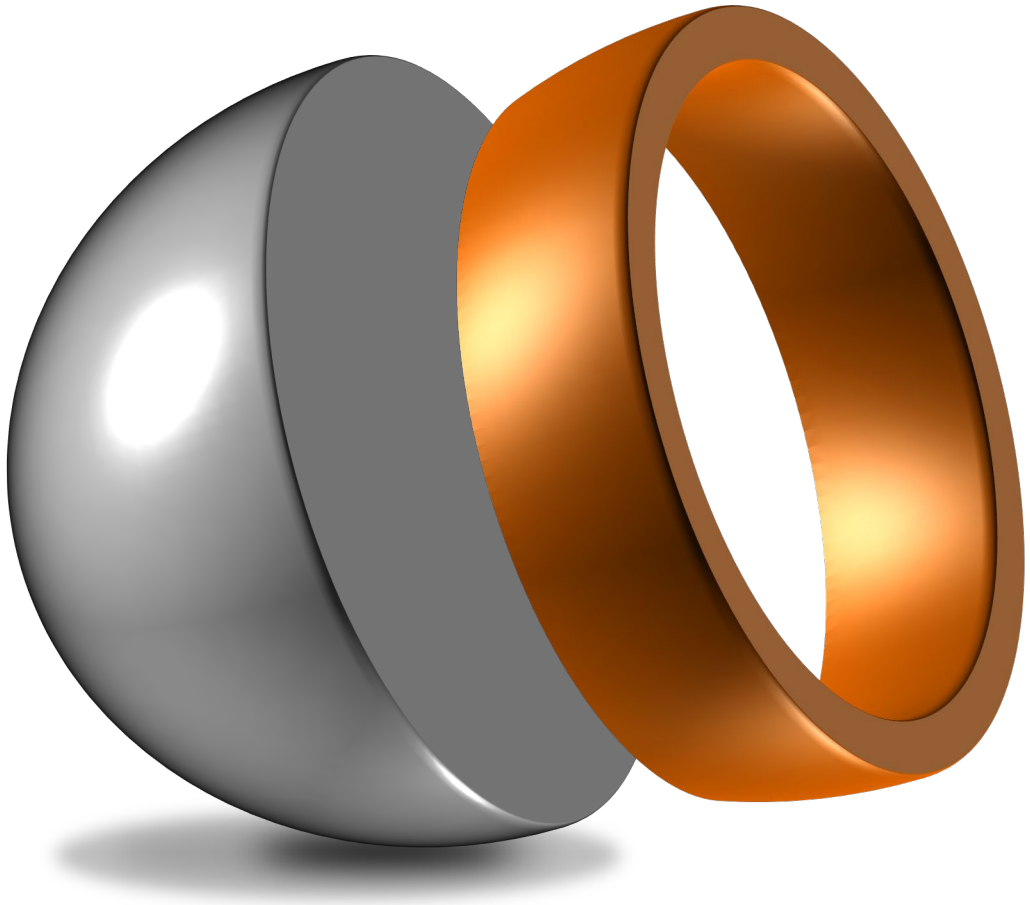
Development according to ISO26262

Why ISO26262?





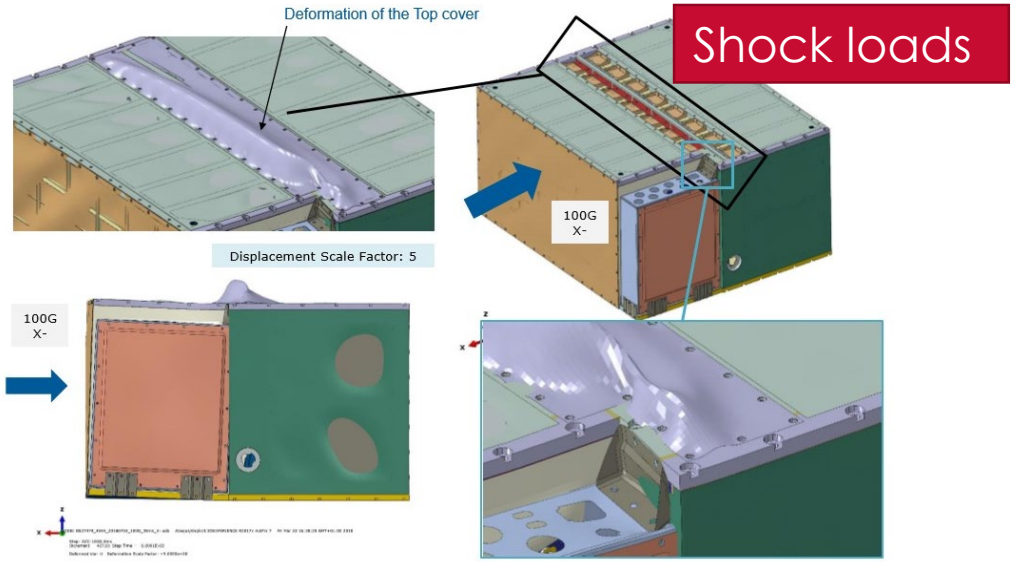




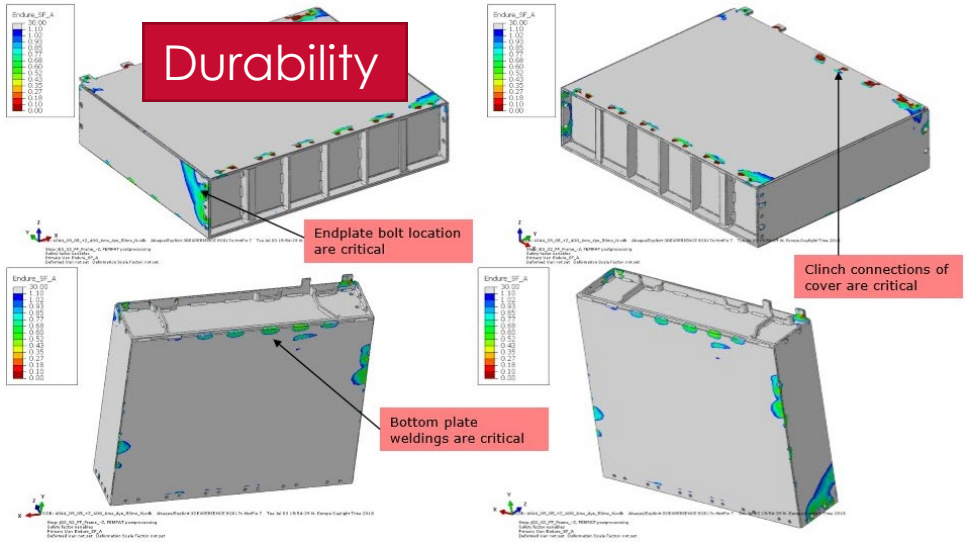
Mechanical Safety System

Mechanical integrity

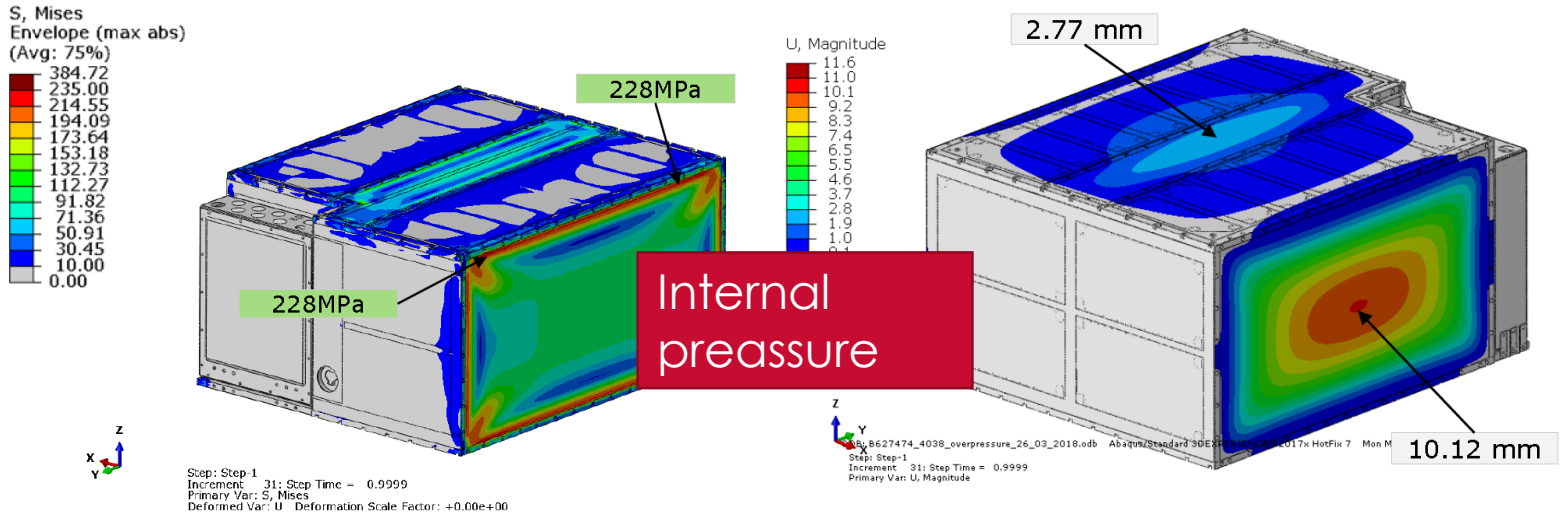
Frontloading by mechnical simulation



Shock loads



Durability

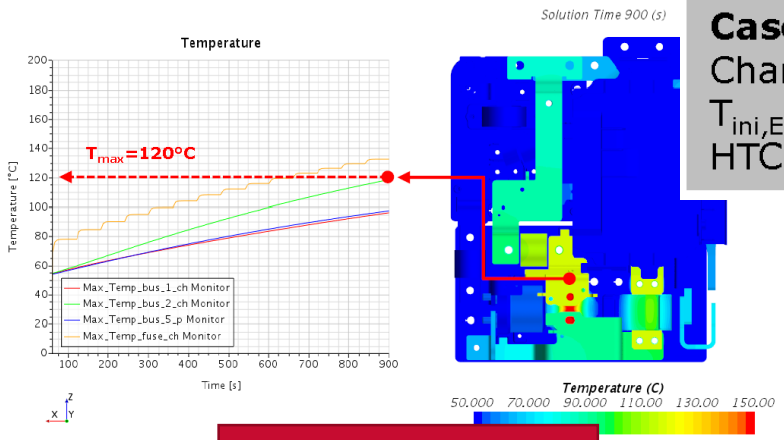


Internal preassure

Thermal behavior

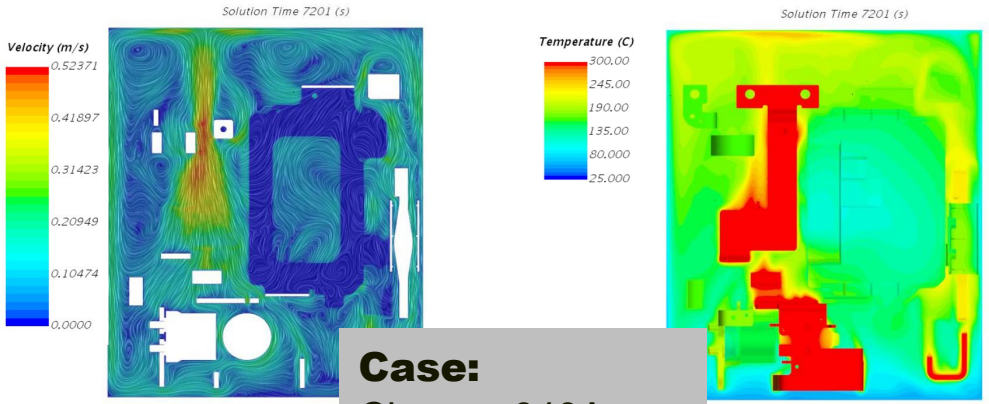
Frontloading by thermal simulation

B-Sample



Case:
Charge: 480A, 900 s
$T_{ini,EE}$: 50°C, $T_{ini,Air}$: 40°C
HTC=5 W/m²-K, no air

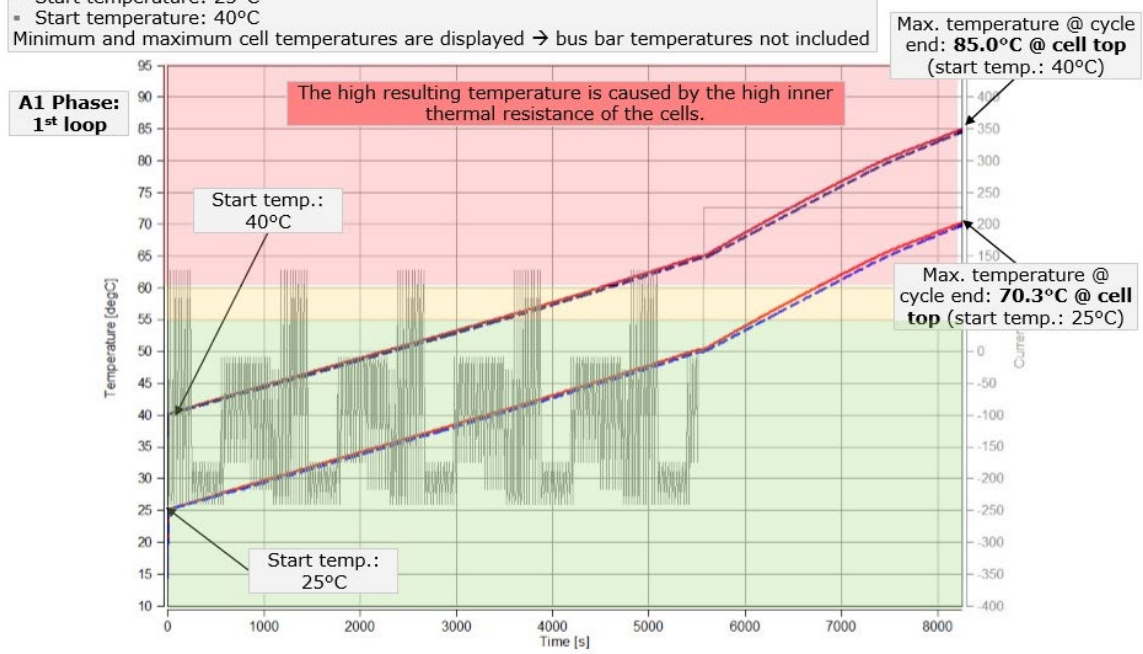
Current paths



Case:
Charge: 640A

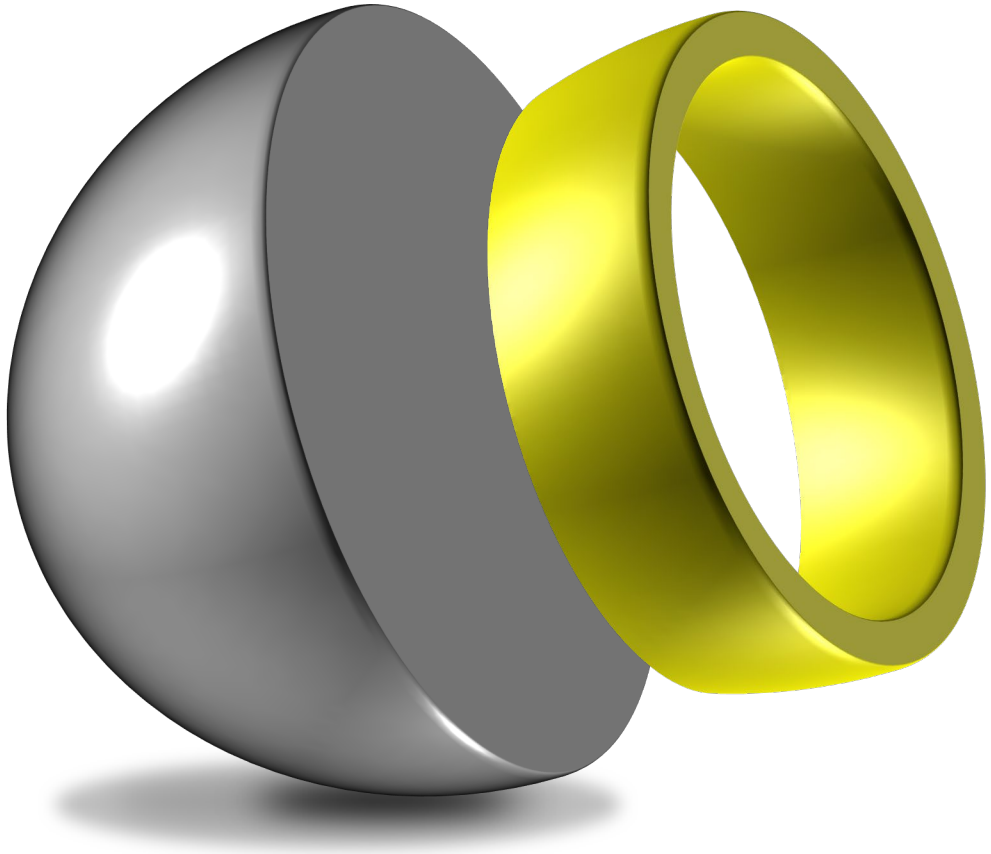
2 different simulations were performed:
- Start temperature: 25°C
- Start temperature: 40°C

Minimum and maximum cell temperatures are displayed → bus bar temperatures not included



The minimum and maximum temperatures in the module are displayed for the two simulations with different starting temperatures.

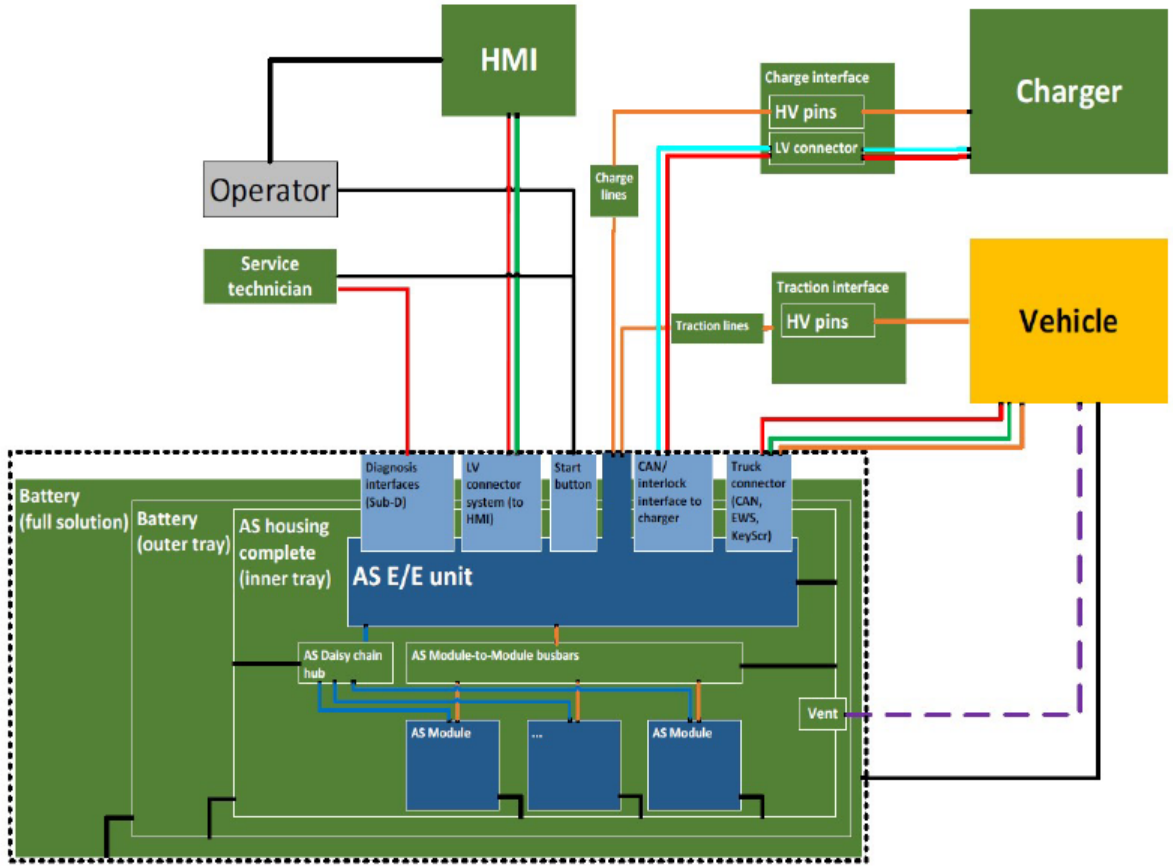
Cell temperatures



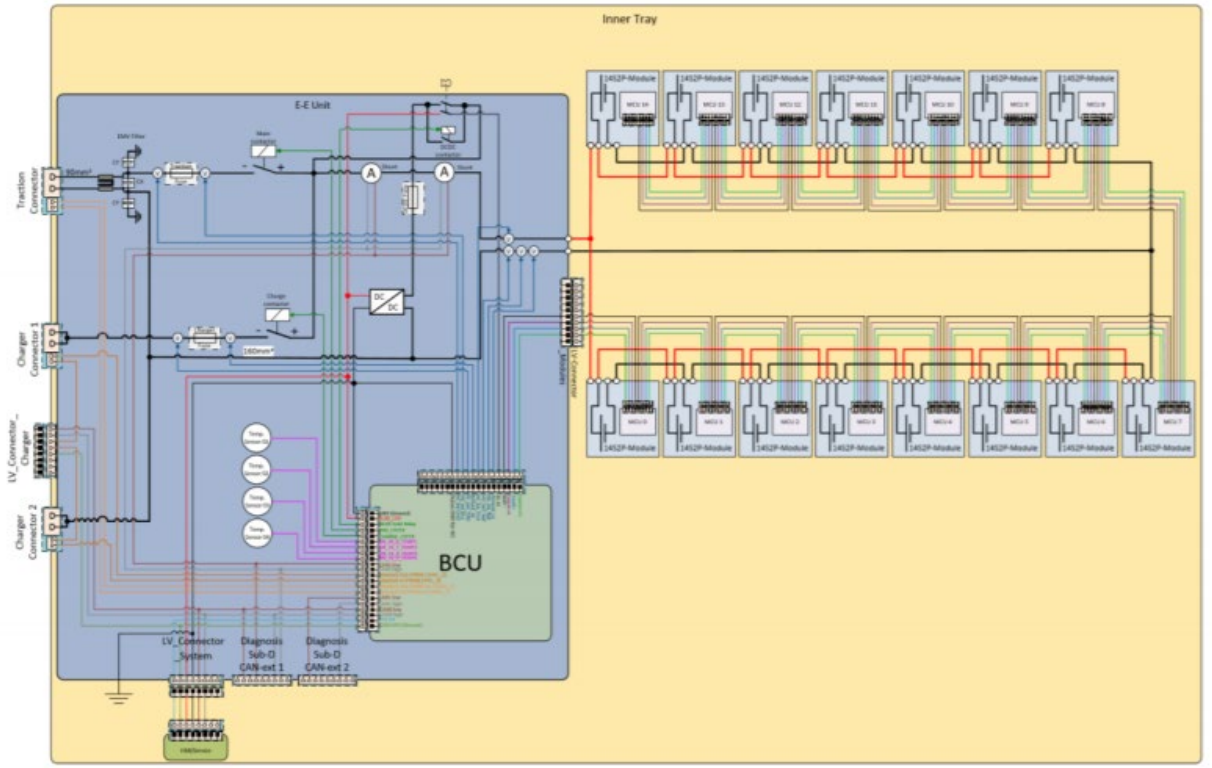
Electrical Safety System

System Architecture

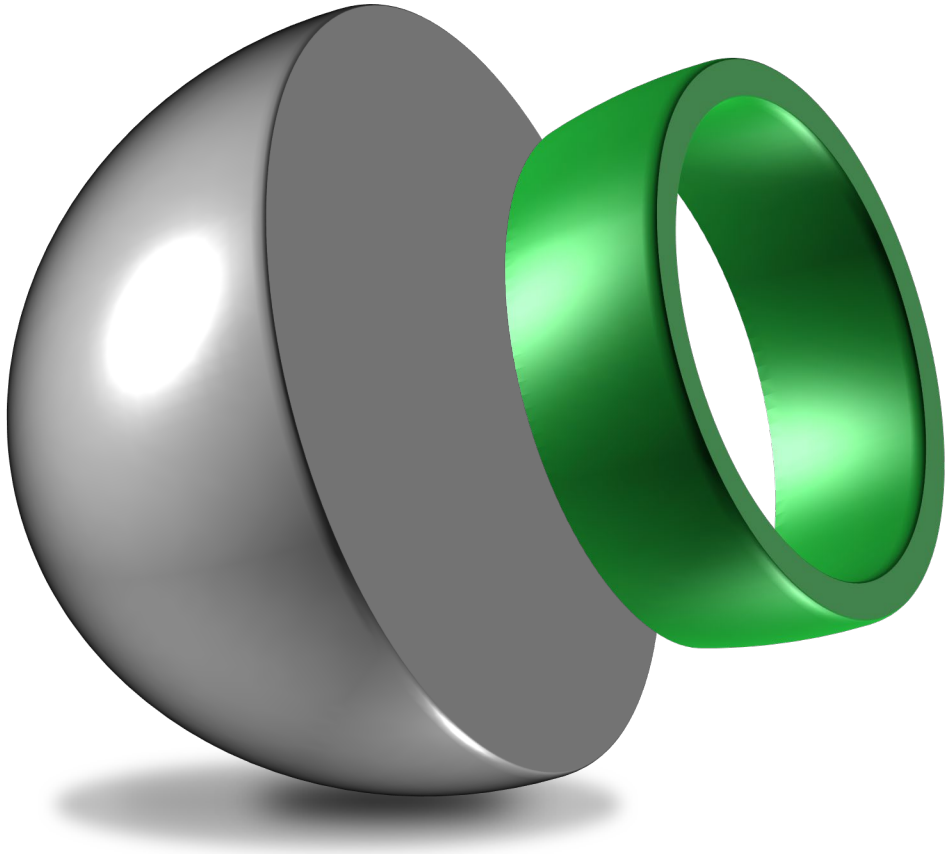
Interfaces and architecture



Interfaces



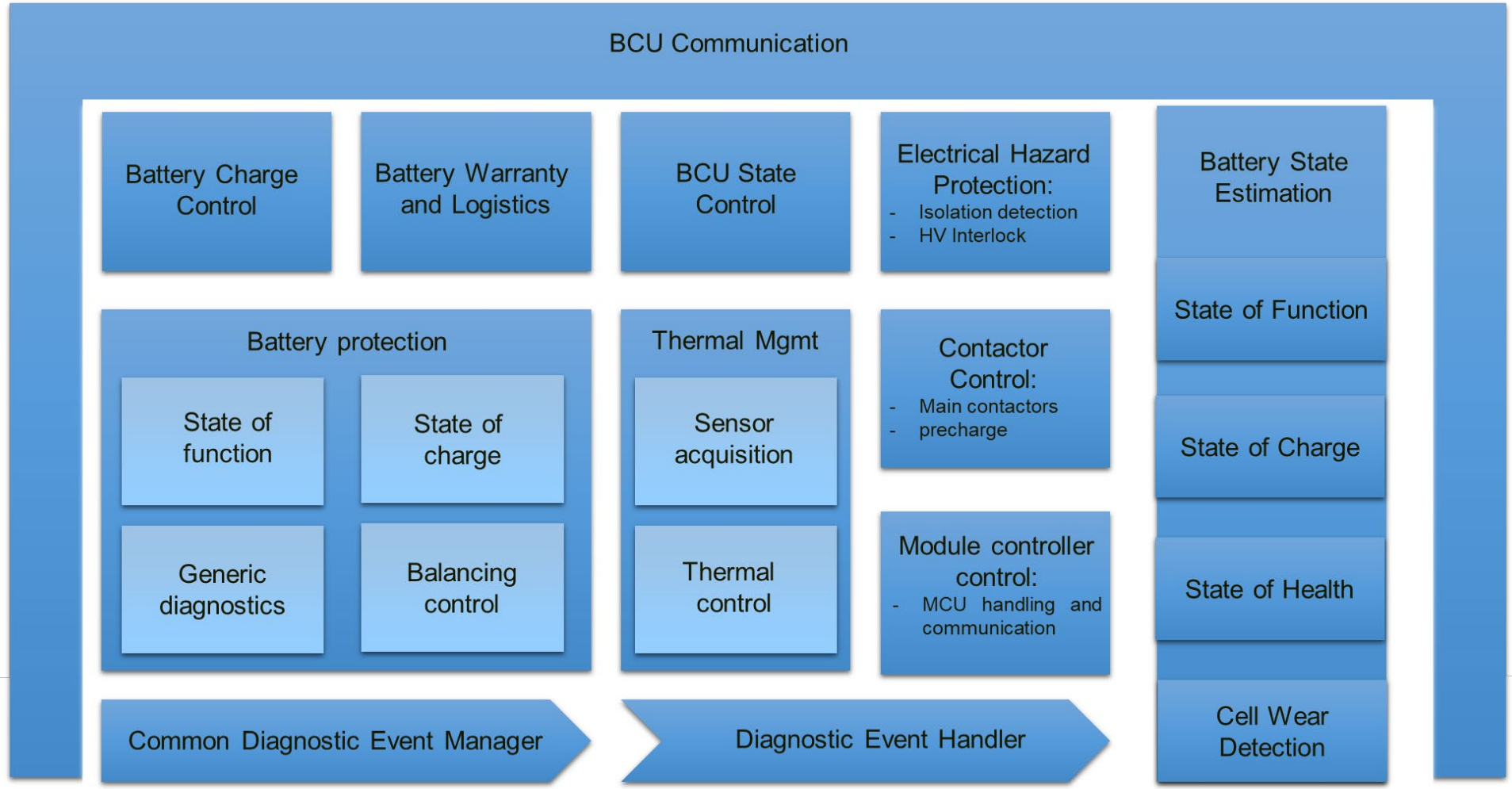
System architecture



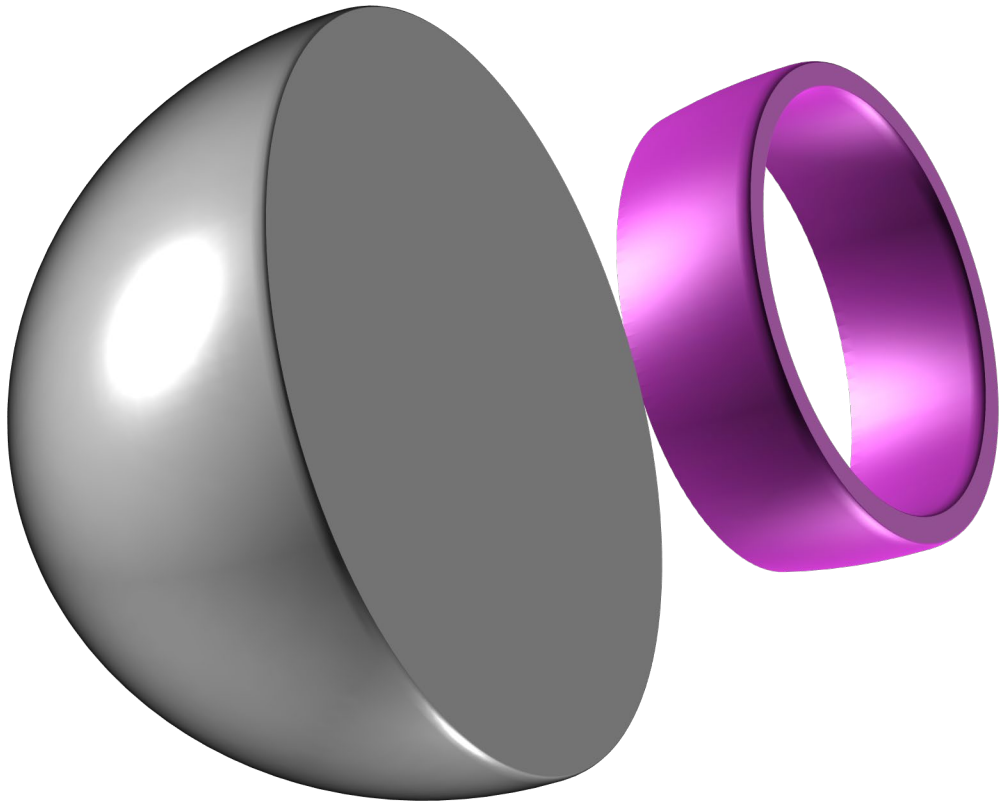
Application Software Layer

EnerSys 2019 All Rights Reserved.

Application Software Layer

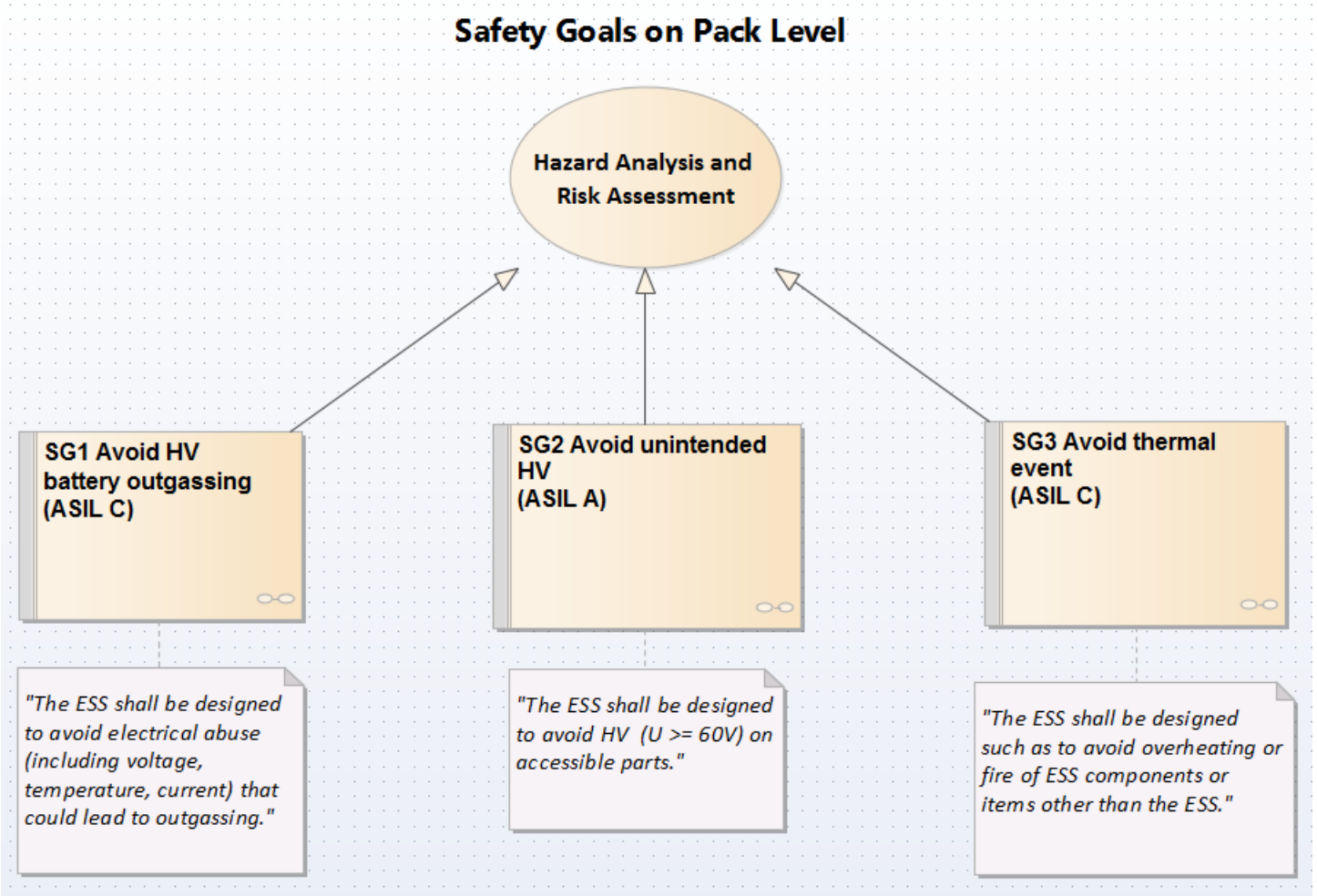


Functional Safety (FuSa) Layer



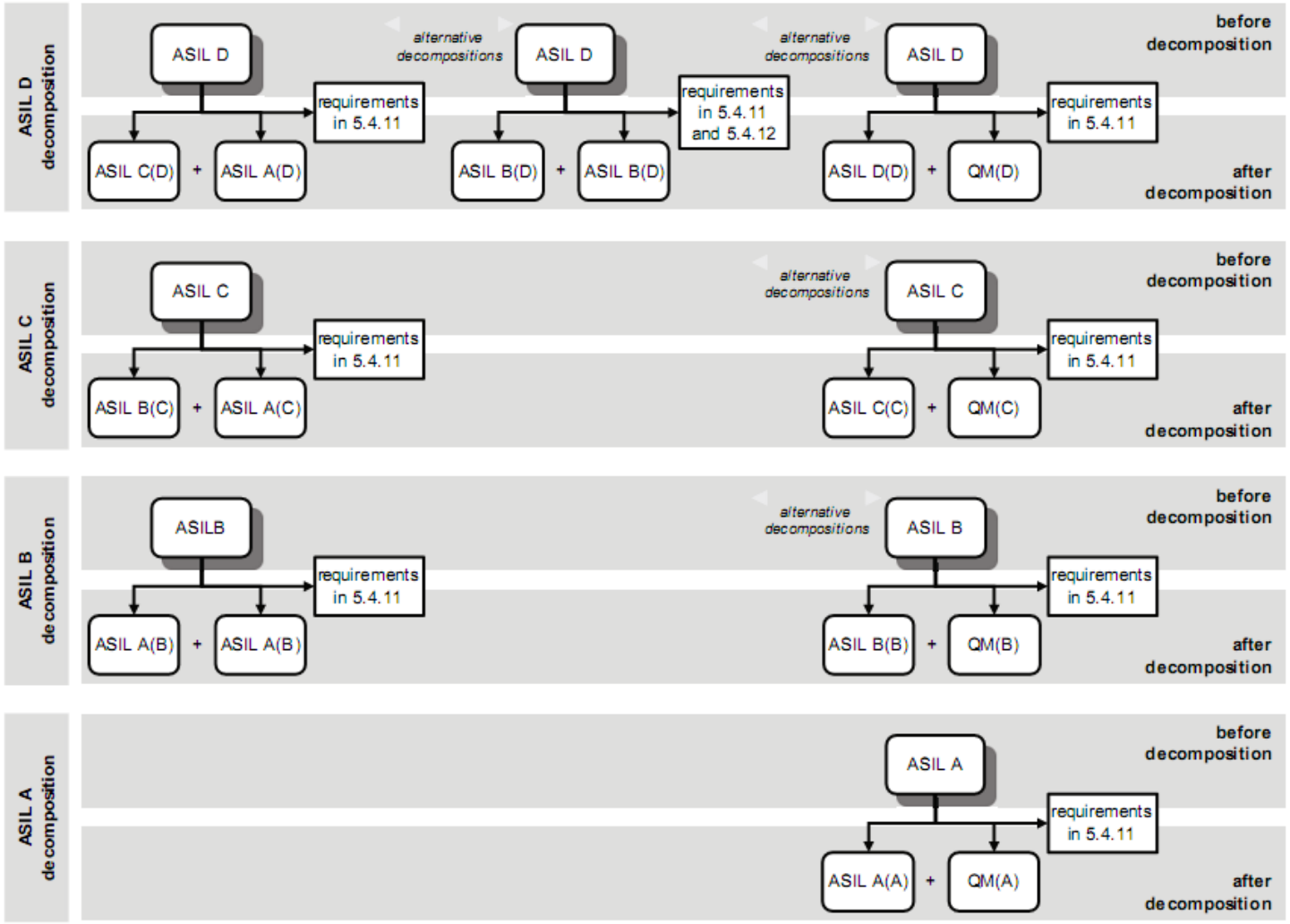
HARA

Hazard Analysis and Risk Assessment



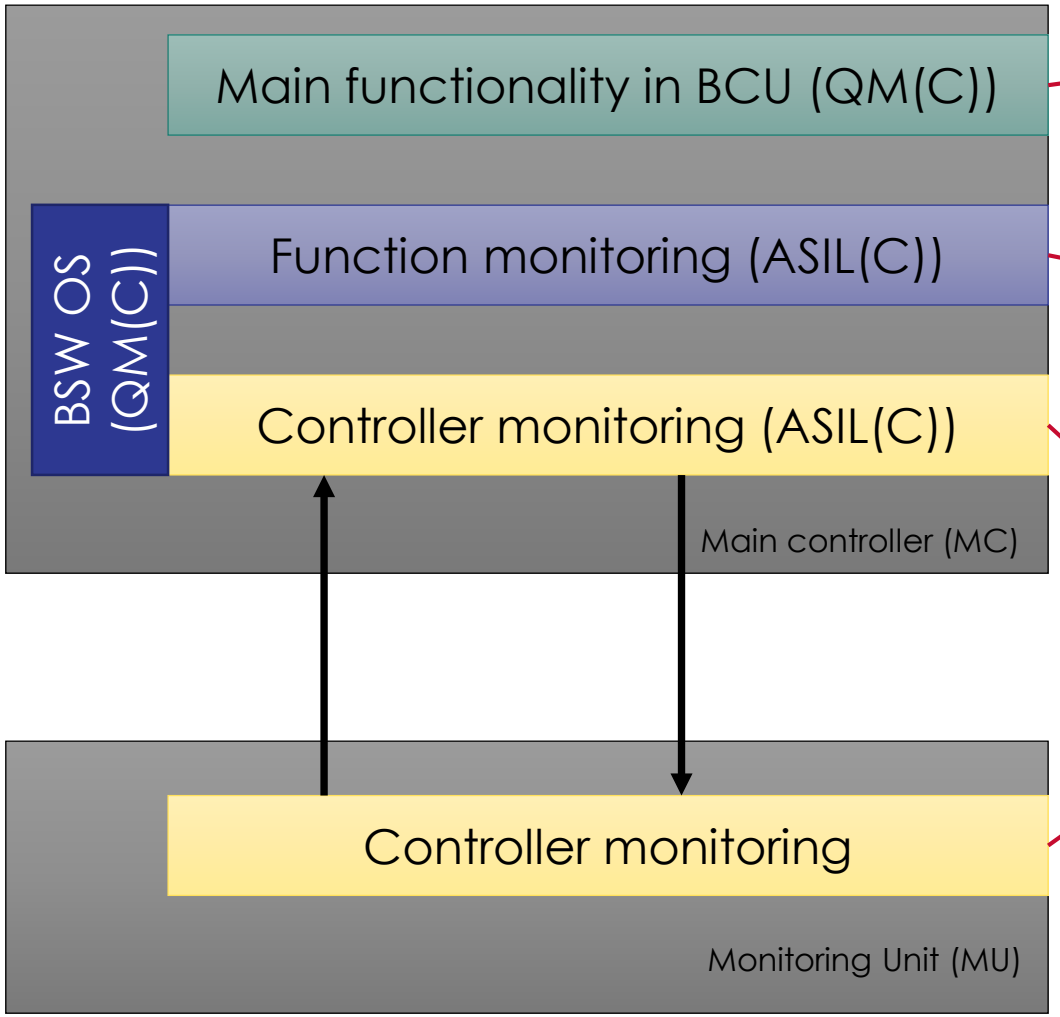
ASIL Decomposition

Distribution of ASIL requirements to more item elements



Safety Architecture

3 Level concept



Level 1
safety-critical function and diagnosis

Level 2 - physical
function monitoring
(e.g. over temperature monitoring)

Level 3 –
Controller monitoring

Thank you for your time.

Manuel Rabl

www.enersys.com