NEW TECHNOLOGY

CHALLENGE OR THREAT?
IN ANY CASE-
WE CAN NOT DO AS WE HAVE ALWAYS DONE!!

CTIF
INTERNATIONAL ASSOCIATION OF FIRE AND RESCUE SERVICES

-MIKKO SAASTAMOINEN-

SAFER CITIZENS THROUGH SKILLED FIREFIGHTERS

Mikko Saastamoinen

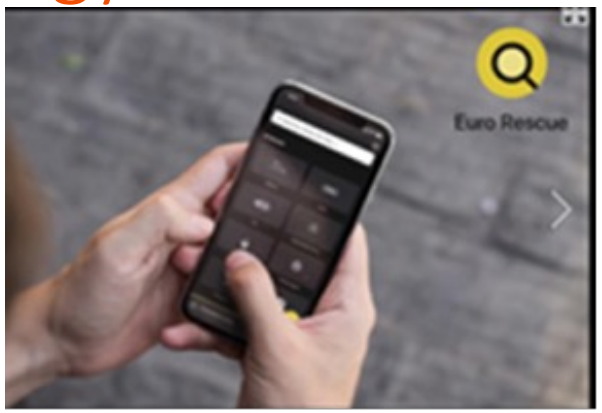
- Hello everyone
- Fire officer in Rescue department of South Savo, Pieksämäki (town is called ”spankhill”)
- Chairman of CTIF commission for Extrication & New Technology → CTIF.org (also in facebook and twitter)
- International extrication instructor

CTIF commission for Extrication & New Technology

Commission has 20 members from different countries all around world

-Some ongoing projects

- **Project EuroNCAP**
- **Project ISO 17840**
- **Project Robotics**
- **Project Drones**
- **Project Solar panels**
- **Project Li-ion batteries**
- **Project C.E.R.S**
- **Project exoskeleton**
- **Project E-rescue**



CTIF
INTERNATIONAL ASSOCIATION OF FIRE AND RESCUE SERVICES

SAFER CITIZENS THROUGH SKILLED FIREFIGHTERS

Let’s get down to business.
These ”harmless”, nice eco-friendly, new way of transporting- are true challenge-because they’re everywhere- inside & outside

Project ISO17840
We NEED to recognize propulsion--with standardized system

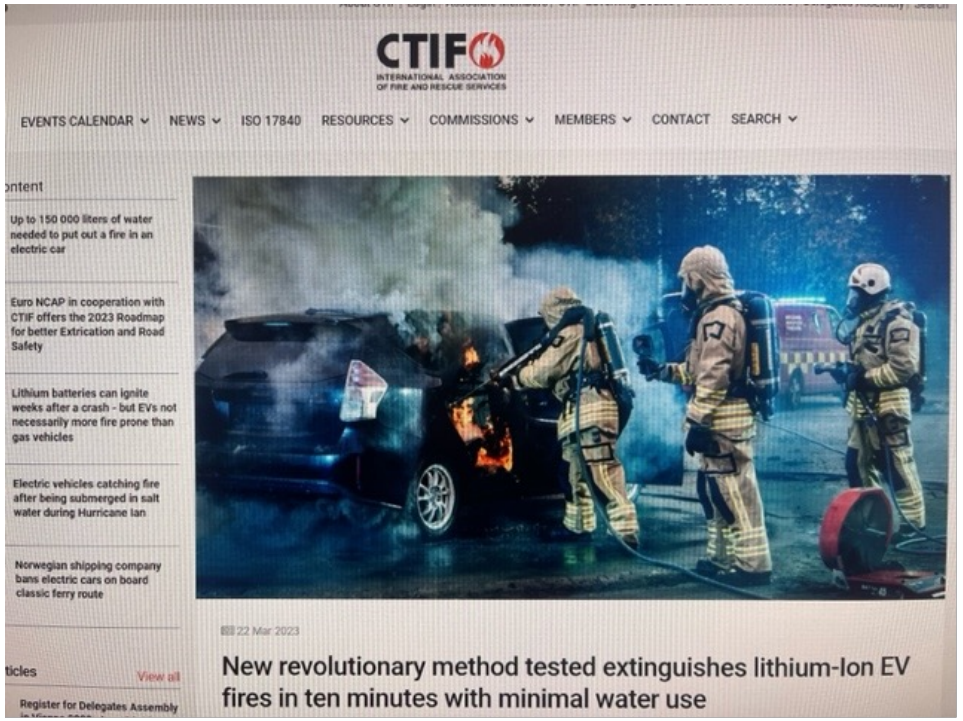
CTIF
INTERNATIONAL ASSOCIATION
OF FIRE AND RESCUE SERVICES

SAFER CITIZENS THROUGH SKILLED FIREFIGHTERS

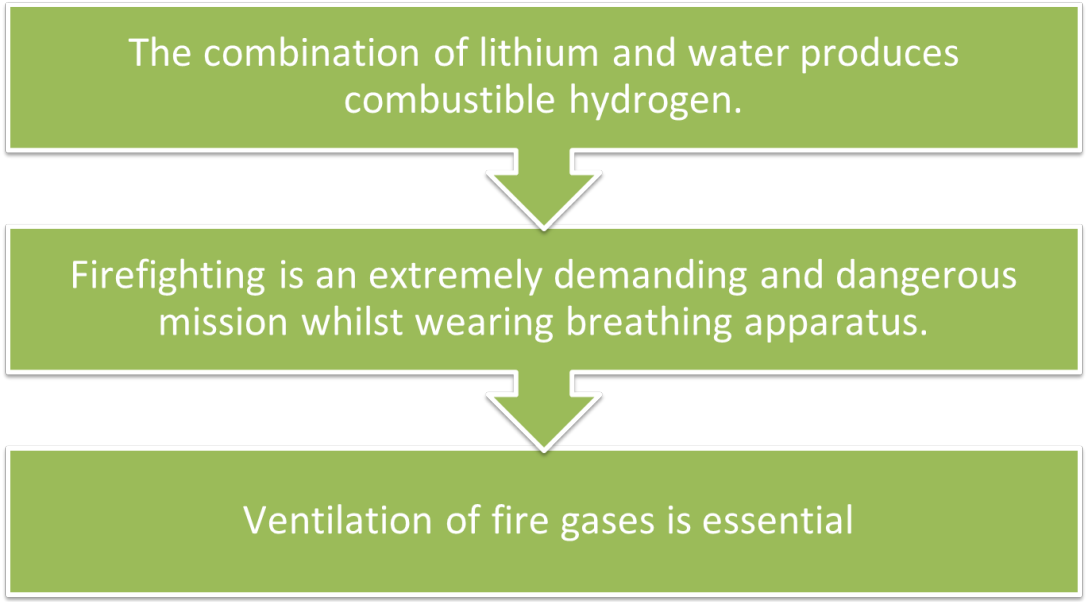
Legislations- is there anything??

- Firefighter associations are sharing material in different forums and networks /platforms
- CTIf is trying to gather and share useful material.

- https://ctif.org/news/new-revolutionary-method-extinguishes-lithium-ion-ev-fires-ten-minutes-minimal-water



Special features of electric car fires from the point of view of firefighters



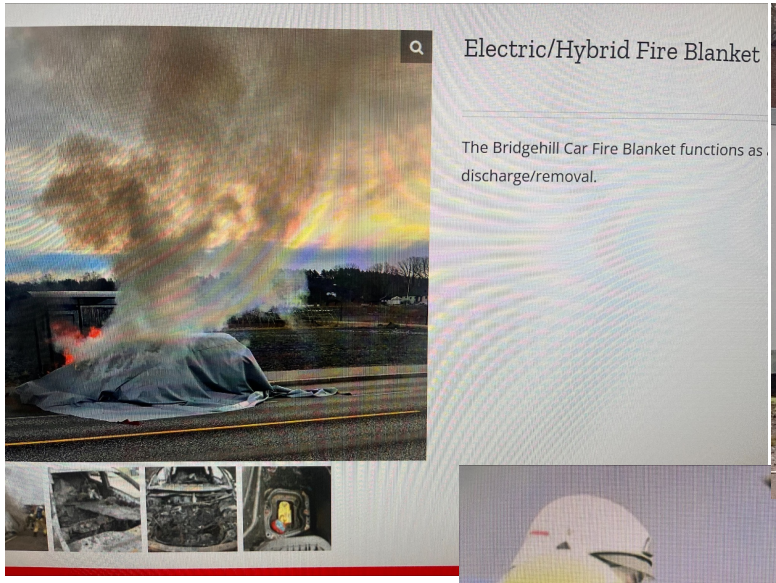
1 firefighters working time limited to 20 mins max! (Breathing apparatus-limitation)

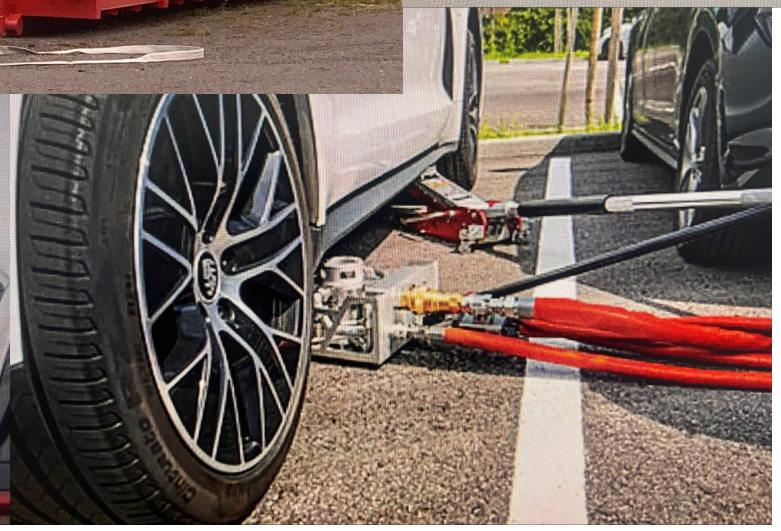
3 rounds of smokediving can exhaust a very fit professional firefighter

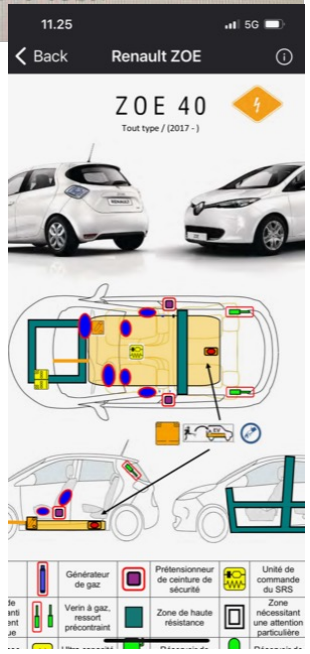
Firefighting equipment and clothing may including the use of a Hazmat suit! (in some cases)

Health risk to Firefighters within 10 mins whilst wearing normal firefighting suits.

Some solutions/innovations. We are not salesman, but we need to find best possible solutions , and share that information-which is useful and which is not







CTIF
INTERNATIONAL ASSOCIATION
OF FIRE AND RESCUE SERVICES

SAFER CITIZENS THROUGH SKILLED FIREFIGHTERS

One innovation, which is from Finland, is developed especially for ships and parking houses
https://evfspool.com/

Easy to use,
assembled from a few pieces

Firesea equipment Oy (pat pend) evfs pool

workshop

EVFS
ELECTRIC VEHICLE FIRE SAFETY

MERITURVA
Maritime Safety Training Centre

Report 1 (2)

23 February 2021

1 Contents of the report EVFS POOL (electric vehicle fire safety pool)

This report presents the results of the evaluation of the EVFS POOL electric car extinguishing method developed by Firesea Equipment Oy. The results of the evaluation include a study on the usability of the EVFS POOL in electric car fires ignited on car decks of ships. At the event, the extinguishing method and the patented extinguishing devices developed for the purpose were evaluated. The burning electric car was not extinguished in the experiment. The only known safe method of extinguishing a burning electric car is drowning, on which the system mentioned in the report is based.

The Maritime Executive

INTELLECTUAL CAPITAL FOR LEADERS

res Podcasts Magazine Newsletter Blogs Directory Jobs Adve


Research Aims to Cut Cost of Offshore Wind Farm Fabrication


South Korea's First Smart, Electric Ship Begins Service

935 Views 0 Shares

Wasaline Improves the Fire Safety at Sea with an EVFS Pool

PELASTUSOPISTO

FireSea Equipment Oy

Electric vehicle fire safety pool – experimental testing

IFV Instituut Fysieke Veiligheid

Onderzoek dompelcontainers

Een beoordeling van de dompelcontainer en mogelijke alternatieven

The conclusion was that in the event of an electric car fire,

where the lithium-ion battery (probably) gets hot, the best solution is to place the car on a platform and fill the platform with water.

Immersion in water with a pallet is a safe, effective and environmentally friendly method.

The liberated gases and loosened metal particles remain to a large extent in the water that is treated later.

The prerequisite, however, is that the electric car can easily be moved to the exchange platform.

EVFS
ELECTRIC VEHICLE FIRE SAFETY

Firesea equipment Oy (patented) evfspool

Does the sprinkler extinguish the fire?

Fact:The sprinkler system can not extinguish the electrical vehicle (or other electric) fire.

NOTE: That all EV fires are NOT caused by thermal runaway

Short summary:

-If possible, try to extinguish battery with water. (cooling is best possible way to control it)

-in any circumstances: DO NOT breathe smoke

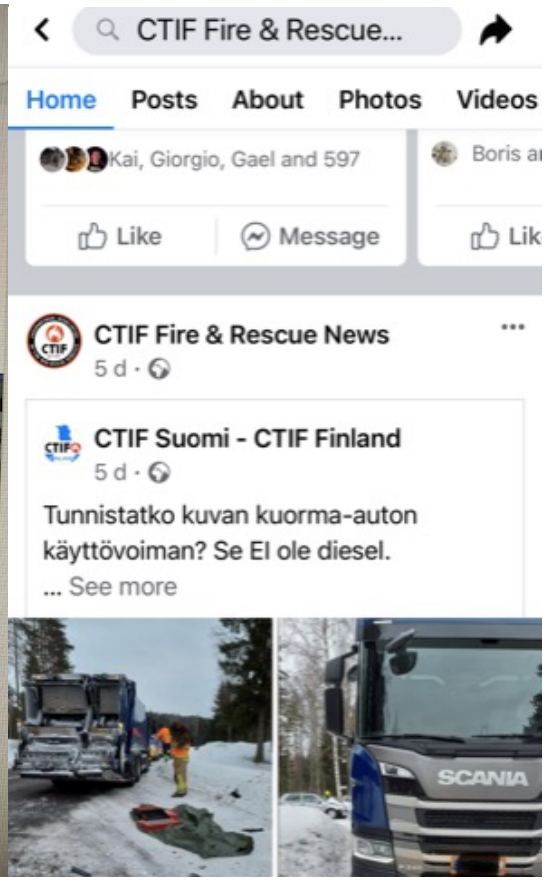
-Beware of re-ignite of electric device

----nothing will stop thermal runaway. It will stop-when moment is right – or then not.

Accidents happen- and this case- rescuers didn’t identified propulsion- because we never need to do it-(because they’re all diesel-aren’t they)

In march they add stickers to one new CNG vehicle...

…and couple weeks later, another one from same company, was involved in accident-without stickers!



EURO RESCUE

Iso –project is not just stickers

CTIF collaboration with EuroNCAP has produced application, where YOU can see X-RAY and instructions, how to deal with YOUR car

YOU can download it from appstore:

EURORESCUE

CTIF
INTERNATIONAL ASSOCIATION OF FIRE AND RESCUE SERVICES

Questions? (after the webinar)

- Thank you

CTIF
INTERNATIONAL ASSOCIATION
OF FIRE AND RESCUE SERVICES

SAFER CITIZENS THROUGH SKILLED FIREFIGHTERS

EuroSPI/ASA Certified Battery Engineer

Basic Level

U2 Battery engineering

U2.E3 Battery Safety

Content: R. Messnarz, D. Ekert, ISCN GesmbH, rmess@iscn.com, G. Macher, ISCN Group

Design and Course Integration: L. Aschbacher., T. Zehetner

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Learning objectives

- LO BATTENG.U2.E3.PC1 The students knows how a HARA is performed.
- LO BATTENG.U2.E3.PC2 The student knows about ASIL and target FIT and target Diagnostic Coverage.
- LO BATTENG.U2.E3.PC3 The student knows what an FMEA/FMEDA is.

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

BATTENG.U2.E3.PC/LO1

The students knows how a HARA is performed.

Co-funded by the Erasmus+ Programme of the European Union

Defining an Item – Precondition for a Hazard and Risk Analysis

- An item contains electronics elements, software elements, mechatronic interfaces, interfaces to hydraulics etc.
- An item has a list of functions for which the impact at vehicle level needs to be analysed
- An item represents a signal flow from sensors to ECUs (Electronic Control Units), actuators, mechatronics and impact on the vehicle level
- Attention: While the item analyses the impact on vehicle level, the ISO 26262 standard focuses on errors caused by electronics and software that lead to hazards

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Focusing on unintended vehicle behavior

Functional hazards

are based on the functional behavior of E/E safety-related systems at vehicle level, e.g.

Unintended Electric shock > 60V

Unintended
Vehicle Burning

Unintended battery explosion

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

States List e.g.

- Start Up
- Operational Mode (providing electric power to the inverter)
- Charging (loading the battery)
- Diagnostic Mode
- Shutdown
- Safe State (Main Power Line off, asc active short circuit)
  - Difference between (1) main relay open and (2) active short-circuit operation is that (1) the creates a strong brake torque (danger of rear collision accident) and (2) leads to a large increase of the amount of current when reaching the safe state, so that controllers and power electronics require higher current tolerances.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

System Functions List

- Vehicle Charging
- Vehicle Electric Drive
- Vehicle Safe State (open relays)
- Fast Discharge
- Battery Control
  - SOH State of Health
  - SOC State of Charge
  - Temperature Monitoring
  - Voltage Monitoring
  - Cell Balancing
- Etc.

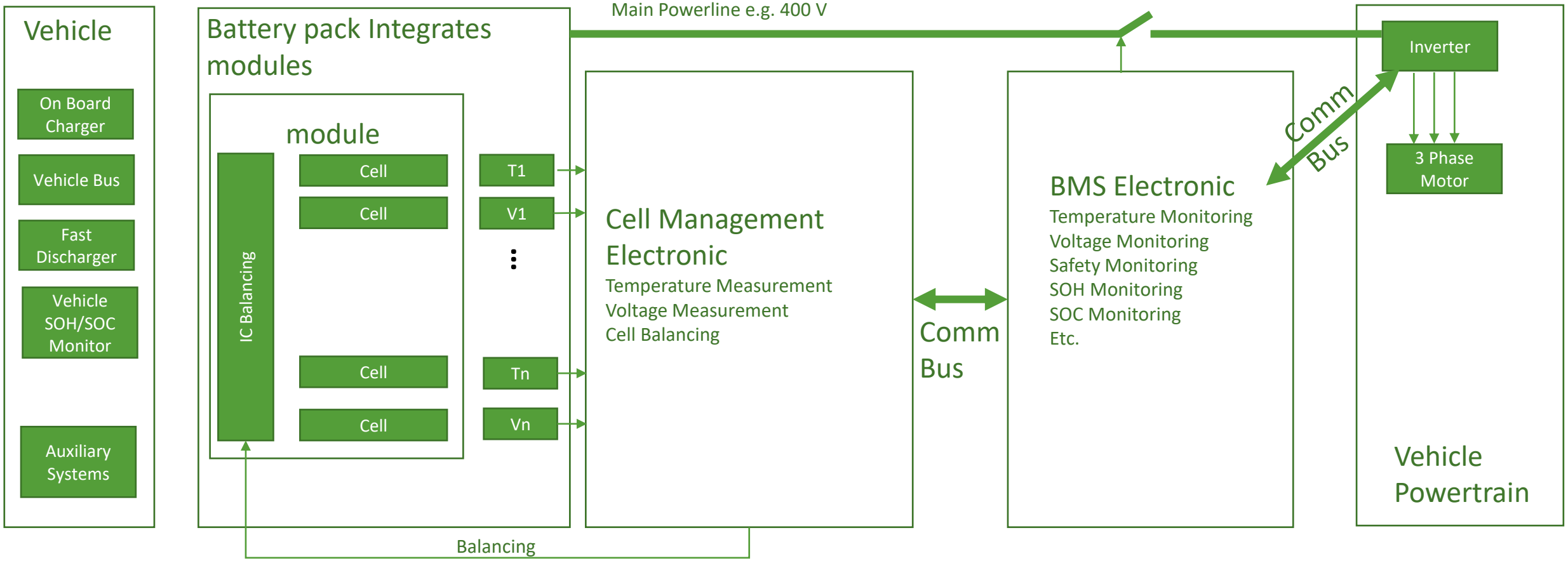
Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Item – Conceptual Architecture Picture

- Elements and Main Interfaces – Functional Concept (… Functional Safety …)

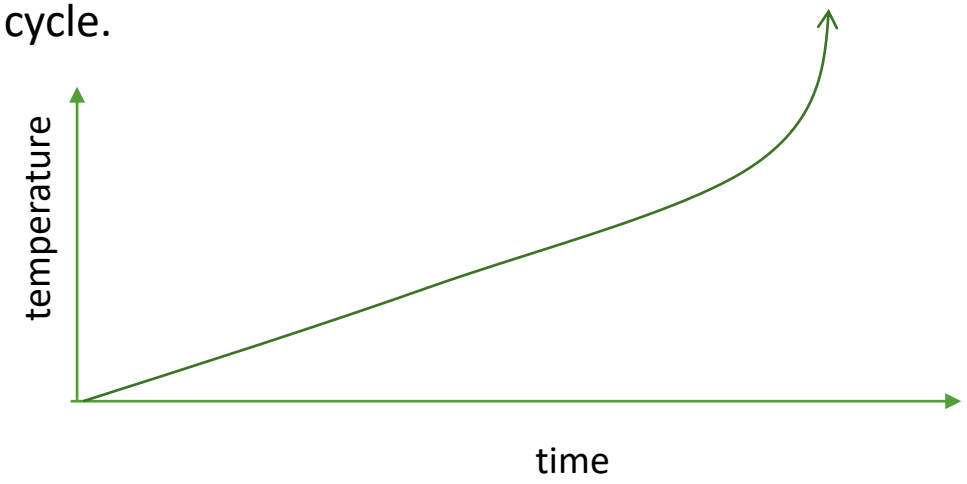


Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECPPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the activity Agreement n° 2019-1-CZ01-KA203-064430 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Functional Understanding 1/5

- Every cell (depending on the manufacturer, e.g. Northvolt, Samsung, CATL etc.) has its own characteristic behaviour. As a battery system integrator, you get specifications of the cells including:
  - Size, voltage, loading capacity etc.
  - AND (important) characteristic measurements and curves.
    - E.g. a mathematical model showing the relationship about cell temperature and temperature runaway. After a certain limit of temperature over time the cell gets a self-accelerating temperature cycle.



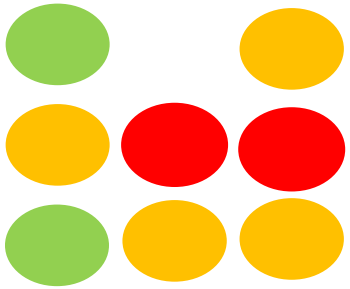
Note: this characteristic curve is manufacturer specific and has to be determined/provided. Some start to accelerate at 100 C, some much earlier. Look at the spec!

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECPPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Functional Understanding 2/5

- Every cell (depending on the manufacturer, e.g. Northvolt, Samsung, CATL etc.) has its own characteristic behaviour. As a battery system integrator, you get specifications of the cells including:
  - Size, voltage, loading capacity etc.
  - AND (important) characteristic measurements and curves.
    - E.g. In cooperation with battery integrator the battery cell production companies test the typical thermal runaway behaviour to learn about counter strategies.



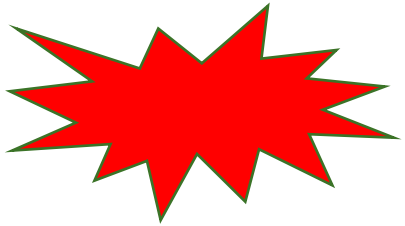
Note: Such a test under load is done with the packages to see the thermal relationships. Also testing includes the behaviour testing of a thermal runaway.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Functional Understanding 3/5

- Every cell (depending on the manufacturer, e.g. Northvolt, Samsung, CATL etc.) has its own characteristic behaviour. As a battery system integrator, you get specifications of the cells including:
  - Size, voltage, loading capacity etc.
  - AND (important) characteristic measurements and curves.
    - E.g. cells depending on temperature show an outgasing of H-Gas behaviour which is manufacturer specific (depends on their chemical design).



Attention: if you have H-gas concentration of > 2% in an enclosed space in the vehicle this can lead to explosion and fire.

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.motor1.com%2Fnews%2F575950%2Fvolkswagen-torn-apart-gas-cylinder%2F&psig=AOvVaw35dRcklffzPlgY_TbE5Y_Q&ust=1673259348327000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCMjI6P7et_wCFQAAAAAdAAAAABAD

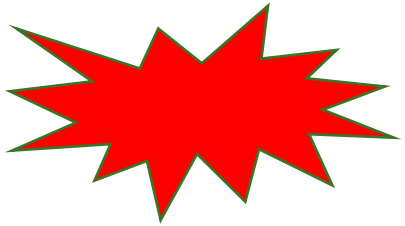
Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the Grant Agreement 2019-1-CZ01-KA203-064430 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Functional Understanding 4/5

- Every cell (depending on the manufacturer, e.g. Northvolt, Samsung, CATL etc.) has its own characteristic behaviour. As a battery system integrator, you get specifications of the cells including:
  - Size, voltage, loading capacity etc.
  - AND (important) characteristic measurements and curves.
    - E.g. cells depending on temperature and operational state (loading, operating and providing power, fast deactivation etc.) show a different physical size (e.g. can grow in their size).



Attention if the cell grows in size, this increases pressure inside the battery module, pressure creates heat, and heat creates outgasing.

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.motor1.com%2Fnews%2F575950%2Fvolkswagen-torn-apart-gas-cylinder%2F&psig=AOvVaw35dRcklffzPlgY_TbE5Y_Q&ust=1673259348327000&source=images&cd=vfe&ved=0CA0QjRxqFwoTCMjI6P7et_wCFQAAAAAdAAAAABAD

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Functional Understanding 5/5

- IMPORTANT MESSAGE
  - In practice always form a system team of electronic, battery cell (chemistry), software and vehicle experts and collect all understanding of characteristic battery behaviour before you start the HARA and safety design decisions.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of the publication under the activity reflects only the author's views. The European Commission is not responsible for any use that may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of the publication under the activity reflects only the author's views. The European Commission is not responsible for any use that may be made of the information contained therein.

Hazard and Risk Classification

H&R: Classification of hazardous events by estimating

- **severity** of potential harm to each person
- **probability** of exposure of each operational situation
- **controllability** of each hazardous event to avoid the specific harm

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Hazard analysis & risk assessment - Classification of hazardous events

Estimation of severity

- potential injuries
- each person potentially at risk

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: HARA- Abbreviated Injury Scale (AIS) to classify the severity of injuries

AIS 0: no injuries;

AIS 1: light injuries such as skin-deep wounds, muscle pains, whiplash, etc.;

AIS 2: moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures, etc.;

AIS 3: severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing, etc.;

AIS 4: severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing;

AIS 5: critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding;

AIS 6: extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities), etc.

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Examples of Secerity Classification Table

	S0	S1	S2	S3
Reference for single injuries (from AIS scale)	- AIS 0 and less than 10 % probability of AIS 1-6 - Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	- Bumps with roadside infrastructure - Pushing over roadside post, fence, etc. - Light grazing damage - Damage entering/ exiting parking space - Leaving the road without collision or rollover	- Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with very low speed - Rear/front collision with another passenger car with very low speed - Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) without passenger compartment deformation	- Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with low speed - Rear/front collision with another passenger car with low speed - Pedestrian/ bicycle accident with low speed	- Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with medium speed - Rear/front collision with another vehicle with medium speed - Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) with passenger compartment deformation

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Hazard analysis & risk assessment - Classification of hazardous events

Estimation of probability of exposure

- **number of vehicles equipped is not relevant**
- **evaluation of the driving, operating and/or environmental situations**
- **duration of a given scenario – and/or**
- **frequency of a given scenario**
- **Is related only to the given scenario not the failure situation**

Class					
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

according to ISO 26262-3

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Examples of probability classification (informative) – regarding duration

		E1	E2	E3	E4
Duration (% of average operating time)		Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time
Examples	**Road layout**	—	- Country road intersection - Highway exit ramp	- One-way street (city street)	- Highway - Country road
	Road surface	—	- Snow and ice on road - Slippery leaves on road	- Wet road	—
	Vehicle stationary state	- Vehicle during jump start - In repair garage (on roller rig)	- Trailer attached - Roof rack attached - Vehicle being refuelled - In repair garage (during diagnosis or repair) - On hoist	- Vehicle on a hill (hill hold)	—
	Manoeuvre	- Driving downhill with engine off (mountain pass)	- Driving in reverse - Overtaking - Parking (with trailer attached)	- Heavy traffic (stop and go)	- Accelerating - Decelerating - Stopping at traffic light (city street) - Lane change (highway)

according to ISO 26262-3

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Examples of probability classification (informative) – regarding frequency

		E1	E2	E3	E4
Frequency of situation		Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples	**Road layout**	—	- Mountain pass with unsecured steep slope	—	—
	Road surface	—	- Snow and ice on road	- Wet road	—
	Vehicle stationary state	- Stopped, requiring engine restart (at railway crossing) - Vehicle being towed - Vehicle during jump start	- Trailer attached - Roof rack attached	- Vehicle being refuelled - Vehicle on a hill (hill hold)	—
	Manoeuvre	—	- Evasive manoeuvre, deviating from desired path	- Overtaking	- Shifting transmission gears - Executing a turn (steering) - Using indicators - Driving in reverse

according to ISO 26262-3

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Hazard analysis & risk assessment - Classification of hazardous events

Estimation of controllability

- **avoidance of harm or damage through timely reactions**
- **by the driver or other persons**
- **is influenced by the design of the item**

Class				
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

according to ISO 26262-3

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Examples of controllability (informative) 1/2

according to ISO 26262-3

Driving factors and scenarios		Class of controllability			
		C0	C1	C2	C3
		Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm
Examples	Example situations that are considered distracting e.g. unexpected radio volume increase or warning message - fuel low	- Maintain intended driving path	—	—	—
	Example for unavailability of a driver assisting system that does not affect the safe operation of the vehicle	- Maintain intended driving path	—	—	—
	Example for unintended closing of window while driving	—	- Remove arm from window	—	—
	Example for blocked steering column when accelerating from standstill	—	- Brake to slow/stop vehicle	—	—
	Example for failure of ABS during emergency braking	—	—	Maintain intended driving path	—
	Example for propulsion failure at high lateral acceleration	—	—	Maintain intended driving path	—

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Examples of controllability (informative) 2/2

according to ISO 26262-3

Driving factors and scenarios		Class of controllability			
		C0	C1	C2	C3
Examples	Example for inadvertent opening bus door while driving with passenger standing in doorway	—	—	- Maintain intended driving path, stay in lane	—
	Example for failure of brakes	—	—	—	- Steer away from objects in driving path
	Example for faulty driver airbag release when travelling at high speed	—	—	—	- Maintain intended driving path, stay in lane, or - brake to slow/stop vehicle
	Example for excessive trailer swing during braking potential for jacknifing	—	—	—	- Driver counter-steers and brakes in an attempt to maintain intended driving path
	Example for function with high automation where driver is not in the loop	—	—	—	- No attempt to maintain intended driving path

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ISO 26262: Hazard analysis & risk assessment - Determination of ASIL -

albatts

Determination of ASIL

Note: QM requires a quality management system if at least one function is rated ASIL A or higher

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
Severity	Exposure	Controllability		

according to ISO 26262-3

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Derivation of Safety Goals and ASIL

			HAZARD IDENTIFICATION		CLASSIFICATION OF HAZARDOUS EVENTS							
Nr.	Component		possible malfunction	Situation	S	Argument	E	Argument	C	Argument	ASIL	Safety Goal
1	Battery System	1.1	Battery temperature control failing, temperature runaway, outgasing and explosion	Fully occupied vehicle; higher speed; motorway. Or: Average speed; city traffic; pedestrians ahead (e.g. crosswalk)	3	The vehicle exploding will lead to a rear end collision with other vehices at high speed.	4	Basic powertrain functions to acclerate and decelerate are required in every drive. Also motorway and city drive are in E4 range.	3	A car with an explosion and no working powertrain is not controllable.	D	Avoid unintended temperature runaway, outgasing and explosion.
		1.2	Battery temperature control failing, temperature runaway, outgasing and explosion	Car is loading at the charging station.	3	If a person remained in the car and the car explodes this will lead to a severe harm.	2	Vehicle being refuelled according to duration table in ISO 26262 is E2.	3	A car with an explosion and no working powertrain is not controllable.	B	Avoid unintended temperature runaway, outgasing and explosion.

			HAZARD IDENTIFICATION	
Nr.	Component		possible malfunction	Situation
1	Battery System	1.1	Battery temperature control failing, temperature runaway, outgasing and explosion	Fully occupied vehicle; higher speed; motorway. Or: Average speed; city traffic; pedestrians ahead (e.g. crosswalk)
		1.2	Battery temperature control failing, temperature runaway, outgasing and explosion	Car is loading at the charging station.

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Derivation of Safety Goals and ASIL

			HAZARD IDENTIFICATION	
Nr.	**Component**		**possible malfunction**	**Situation**
1	**Battery System**	1.1	Battery temperature control failing, temperature runaway, outgasing and explosion	Fully occupied vehicle; higher speed; motorway. Or: Average speed; city traffic; pedestrians ahead (e.g. crosswalk)
		1.2	Battery temperature control failing, temperature runaway, outgasing and explosion	Car is loading at the charging station.

CLASSIFICATION OF HAZARDOUS EVENTS							
S	**Argument**	**E**	**Argument**	**C**	**Argument**	**ASIL**	**Safety Goal**
3	The vehicle exploding will lead to a rear end collision with other vehices at high speed.	4	Basic powertrain functions to acclerate and decelerate are required in every drive. Also motorway and city drive are in E4 range.	3	A car with an explosion and no working powertrain is not controllable.	D	Avoid unintended temperature runaway, outgasing and explosion.
3	If a person remained in the car and the car explodes this will lead to a severe harm.	2	Vehicle being refuelled according to duration table in ISO 26262 is E2.	3	A car with an explosion and no working powertrain is not controllable.	B	Avoid unintended temperature runaway, outgasing and explosion.

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Example Safety Goals in Automotive Battery Systems

- Safety Goal 1: avoid battery over-temperature
- Safety Goal 2: avoid thermal runaway
- Safety Goal 3: avoid cell outgassing
- Safety Goal 4: avoid battery explosion
- Safety Goal 5: avoid electric shock
- Safety Goal 6: avoid immediate loss of power leading
- Safety goal 7: avoid battery overcurrent
- Etc.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

BATTENG.U2.E3.PC/LO2

The student knows about ASIL and target FIT and target Diagnostic Coverage.

Co-funded by the Erasmus+ Programme of the European Union

Safety Design Patterns

- ASIL D : 10 Fit, 99% DC for SPF
- ASIL C : 100 Fit, 97% DC for DPF
- ASIL B : 100 Fit, 90% DC
- ASIL A : no targets (Daimler sets e.g. 1000 Fit)

Fit (Failure in time) is a Hardware metric based on the used HW parts. 1 Fit = 1 fault in 10^9 operating hours in the fleet

DC stands for **Diagnostic Coverage** of the faults related to hardware parts which cab cause the hazard.

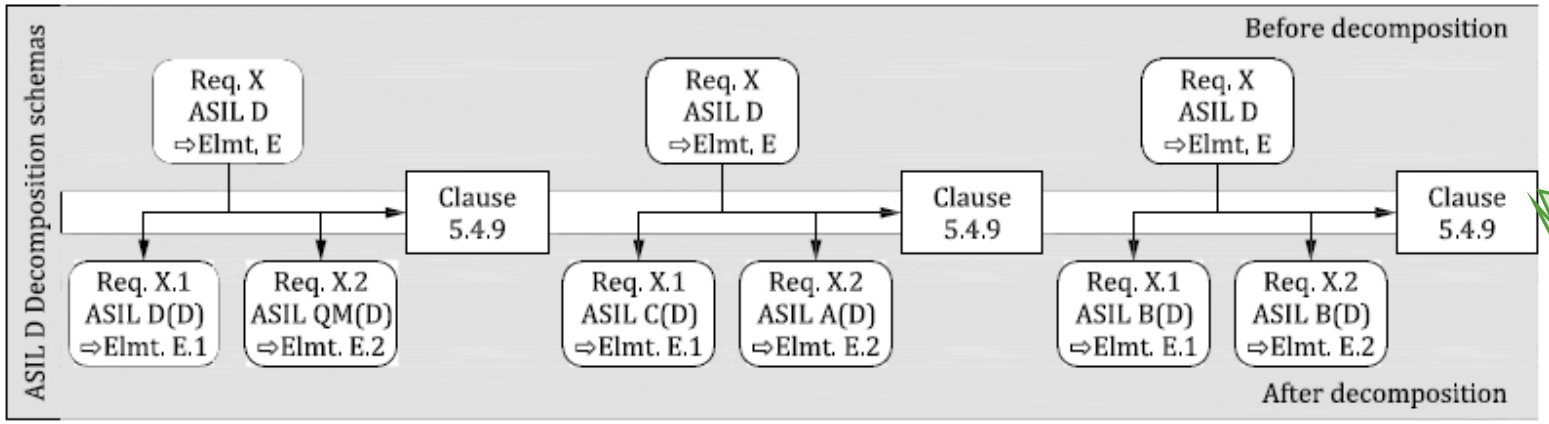
This is applied on the safety related signal and monitoring path, not the entire electronic.

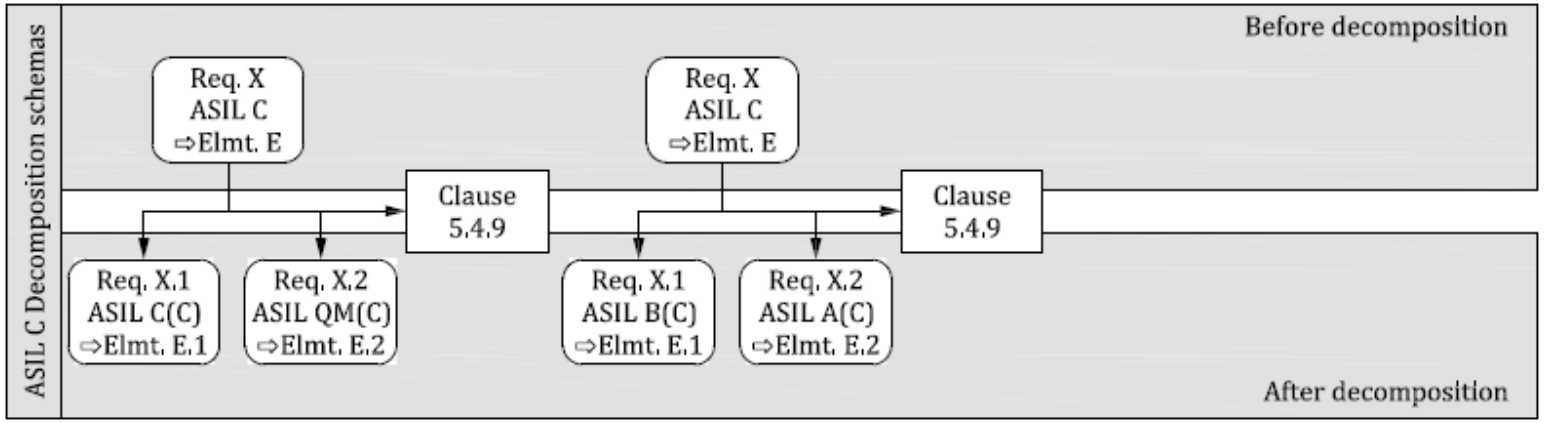
Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the activity reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Architecture: ASIL Decomposition [ISO26262-9, 5.4.9]





Independence of elements after decomposition:
- No dependent failures
  or
- Dependent failures have safety mechanism

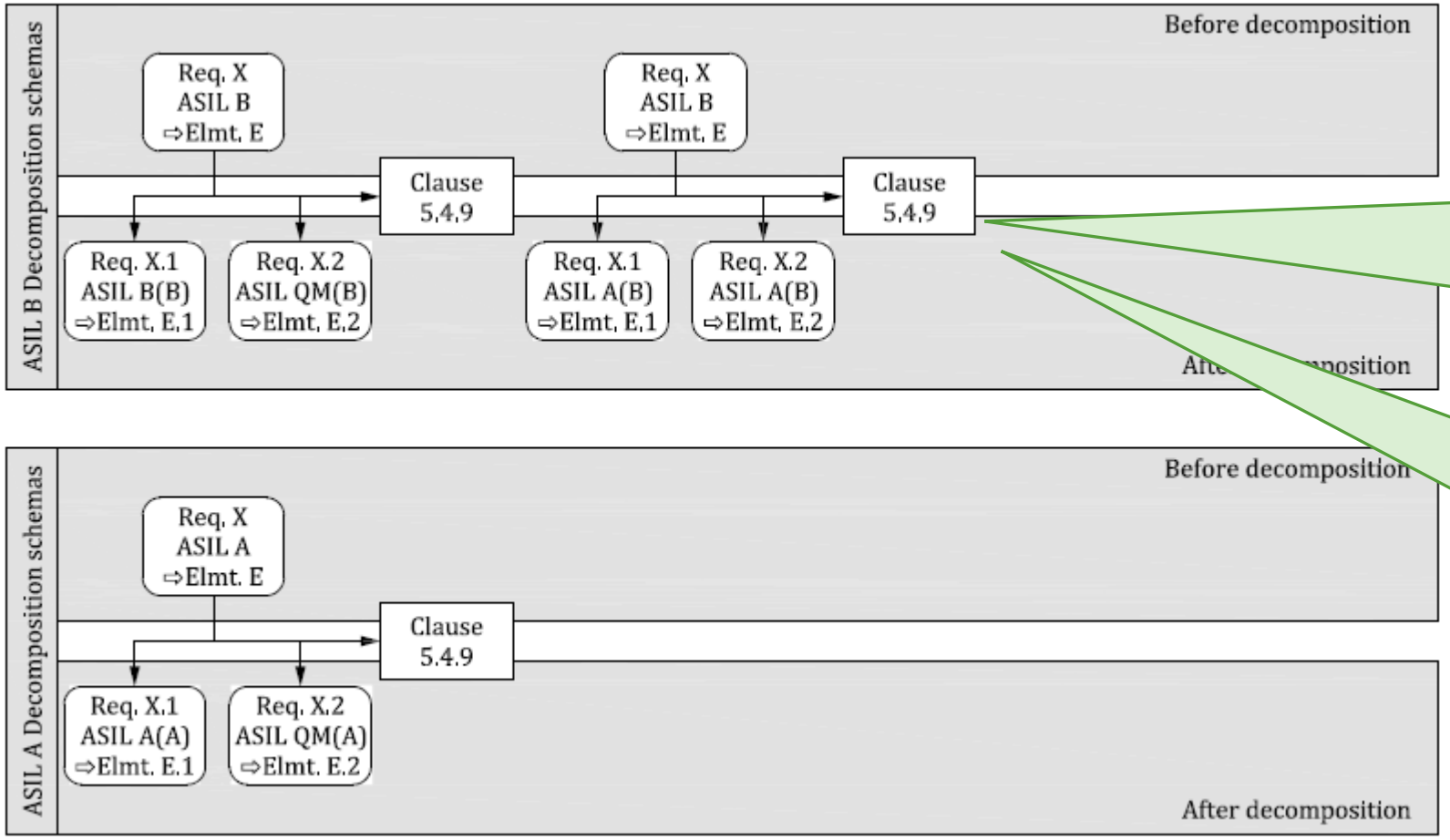
Independent confirmation measures [ISO 26262-2, 6.4.9 Tab1]:
- Confirmation reviews
- F.Safety audit
- F.Safety assessment

Recursive (A)SIL decomposition
- ISO26262: yes
- IEC61508/DO-178C: not allowed

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Architecture: ASIL Decomposition [ISO26262-9, 5.4.9]



Independence of elements after decomposition:
- No dependent failures
  or
- Dependent failures have safety mechanism

Independent confirmation measures [ISO 26262-2, 6.4.9 Tab1]:
- Confirmation reviews
- F.Safety audit
- F.Safety assessment

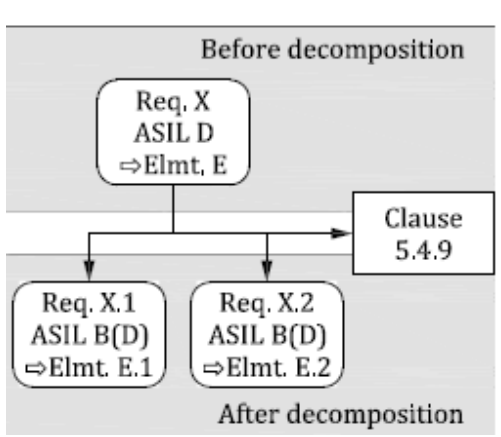
Recursive (A)SIL decomposition
- ISO26262: yes
- IEC61508/DO-178C: not allowed

Co-funded by the Erasmus+ Programme of the European Union

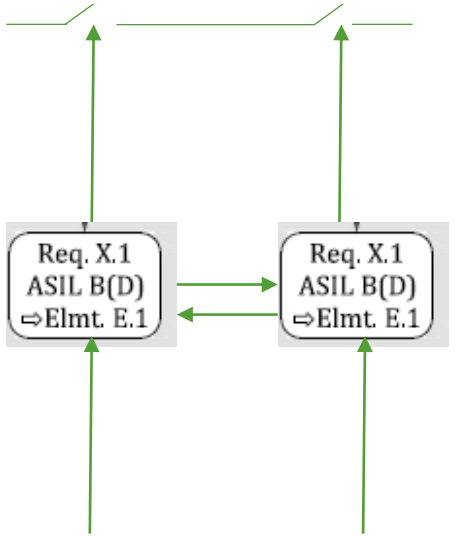
Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Design Pattern Example

- ASIL D Example



Independence of elements after decomposition:
- No dependent failures
  or
- Dependent failures have safety mechanism



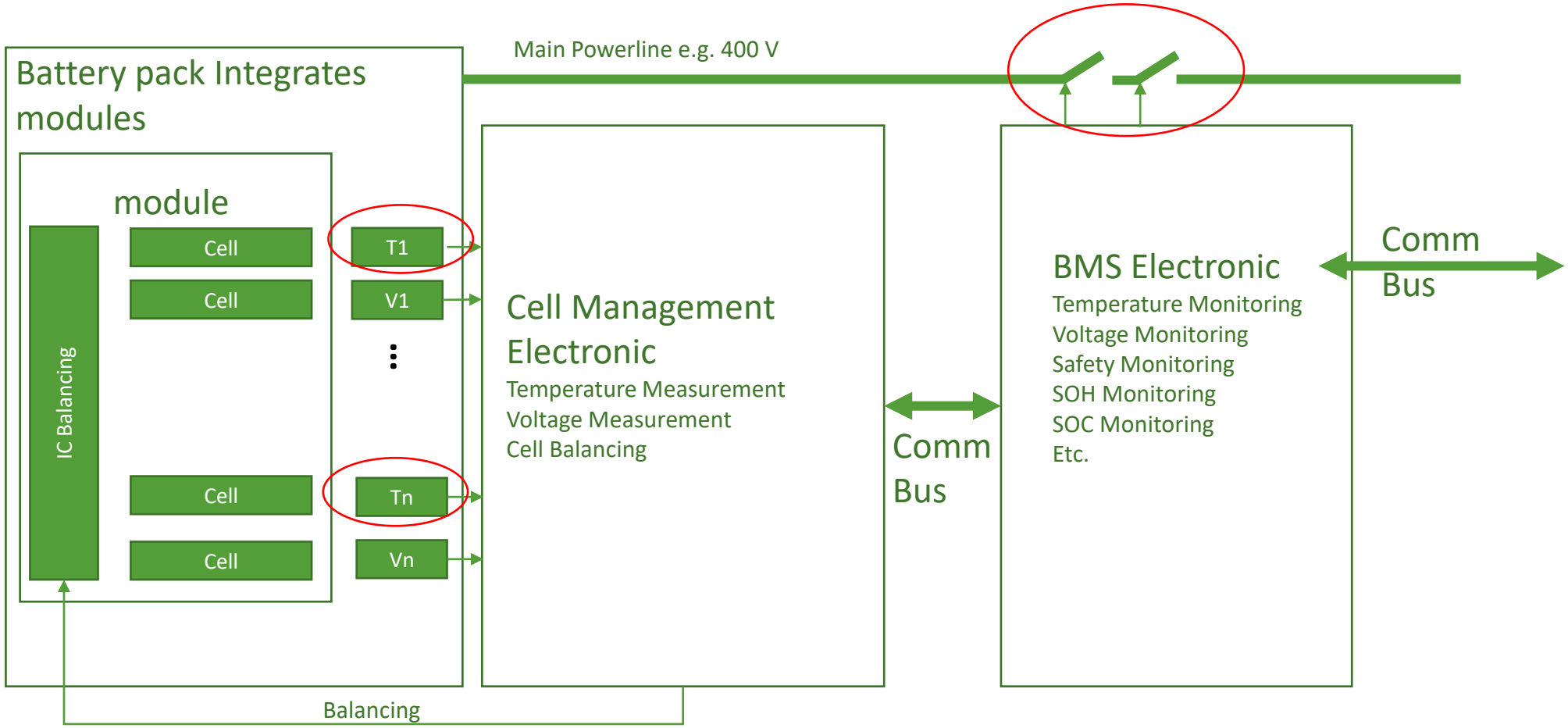
- Two independent paths
- Two independent measurements
- Each path 90% DC separately
- In the integration 99% DC must be achieved (usually by having a comparator concept, and complete independence)

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS – Project Number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Design Decisions Example

- Safety Goal 1: avoid battery over-temperature - Decomposition



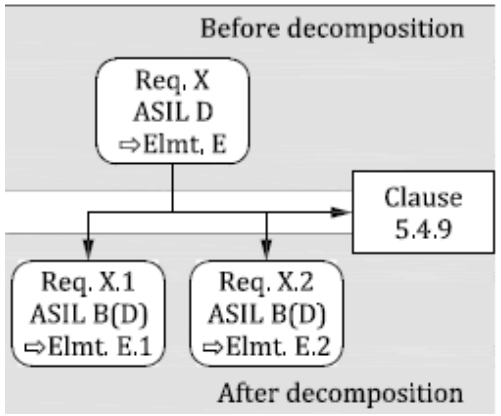
Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Design Decisions Example

- Safety Goal 1: avoid battery over-temperature - Decomposition



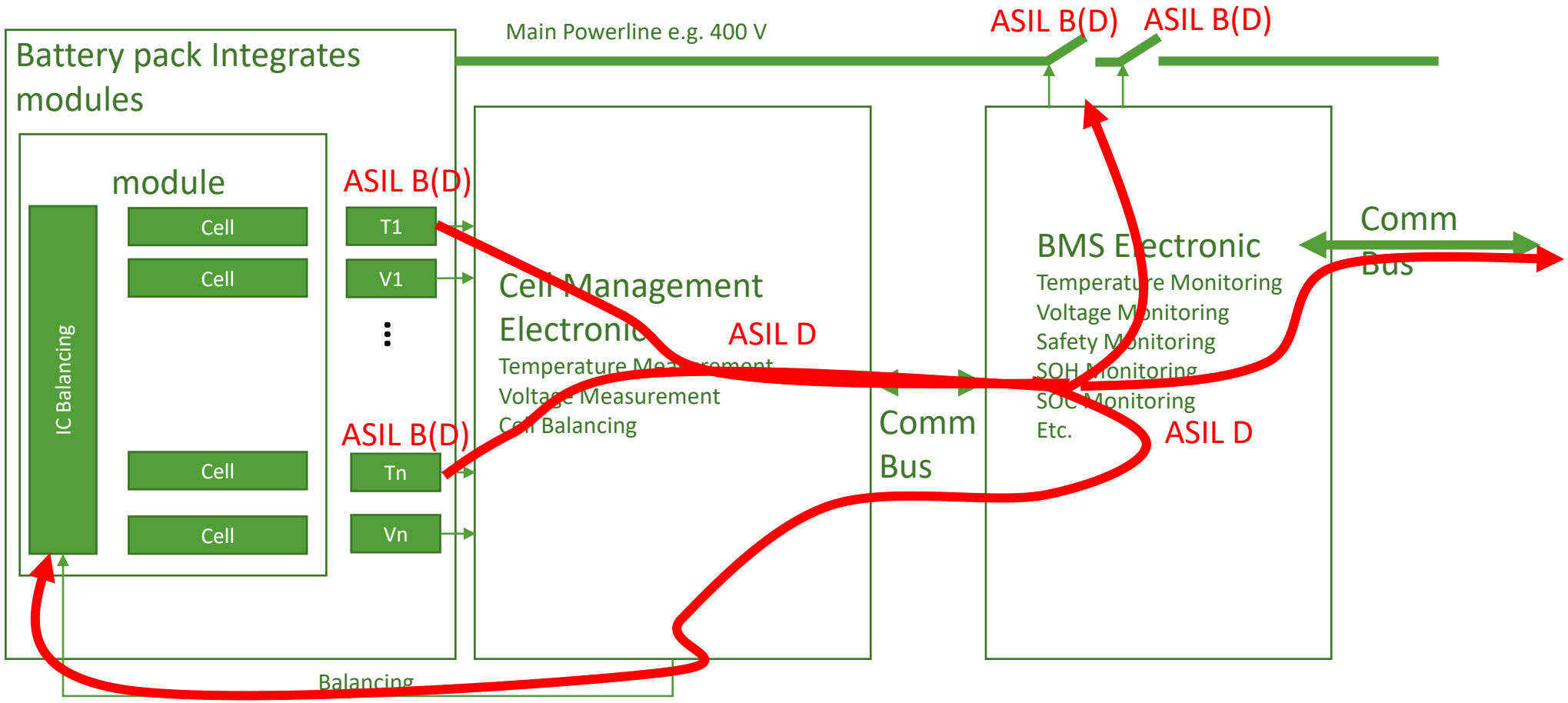
- Decomposition of Temperature
  - Min. 2 reference measurements
  - Comparing reference measurements between cells
  - Comparing measurements with a characteristic model of the cell (usually provided by the cell manufacturer)
  - Implementing a comparator diagnostic
    - 99% DC Diagnostic Coverage in case of argument of freedom from interference
      - E.g. there could be an interference
        - if the same type of temperature sensor is used
        - If they are used in the same location
    - Use of advanced diagnostics ideas to argue the independence of the comparator
      - E.g. each cell has an IC connecting it to the main powerline and each IC measures itself for temperature and can switch off in case of thermal event. This is in addition to the cell manager temperature measurements and the comparisons explained above.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication does not constitute an endorsement of the contents which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Design Decisions Example

- Safety Goal 1: avoid battery over-temperature – Safety Effect Chain per Safety Goal

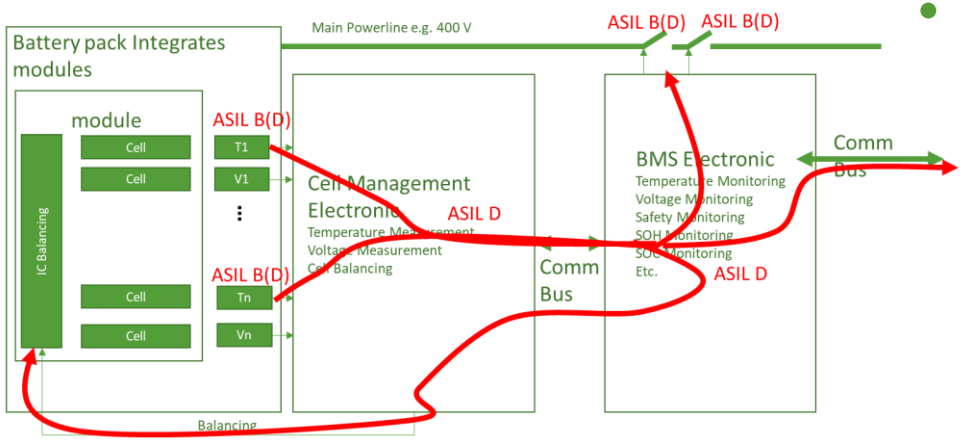


Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Safety Design Decisions Example

- Safety Goal 1: avoid battery over-temperature – Safety Effect Chain per Safety Goal



- Typical Technical Safety Concept / Effect Chain Understanding
  - Measuring temperature with ASIL D quality
  - Comparing temperature/models/IC Integrated Circuit status and detecting a thermal event
  - Either degrading (see in picture link back to the balancing) by excluding cells from the battery pack main powerline
  - Or switching to safe state (main powerline off)
  - Decomposing the switch off function into 2 channels so that more than a double fault must happened before the hazard will appear
  - Sending the thermal event data tro the vehicle to set inverter to safe state
  - Etc.

Co-funded by the Erasmus+ Programme of the European Union

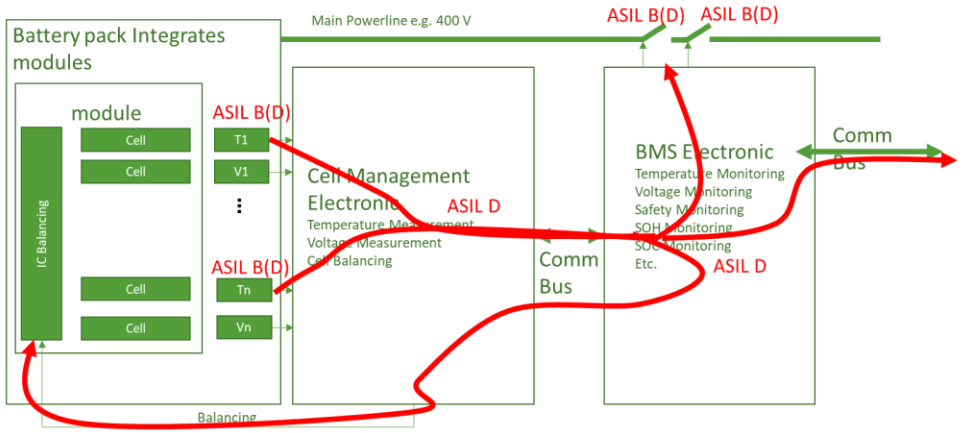
ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

BATTENG.U2.E3.PC/LO3

The student knows what an FMEA/FMEDA is.

Co-funded by the Erasmus+ Programme of the European Union

FMEDA Failure Modes Effects and Diagnostic Analysis



- An FMEDA is done per safety goal
  - All electronic parts which are impacted by a safety effect chain of a safety goal (including the part for safe state actuation) needs to be entered to the FMEDA sheet (see red flow in the picture left).
    - This red flow is also carried forward to the electronic and electronic circuit design at lower level of design.
  - For every such electronic part the known FIT (Failure in Time Rate, based on 10^9 hours basis) is entered to the FMEDA sheet.
  - For every part the implemented diagnostic functions (see previous design decisions) are mapped and judged for their efficiency.
    - E.g. DC Diagnostic Coverage 90% means that 90% of faults known for that part would be detected.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS Project Number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Basic Diagnostics Value Understanding

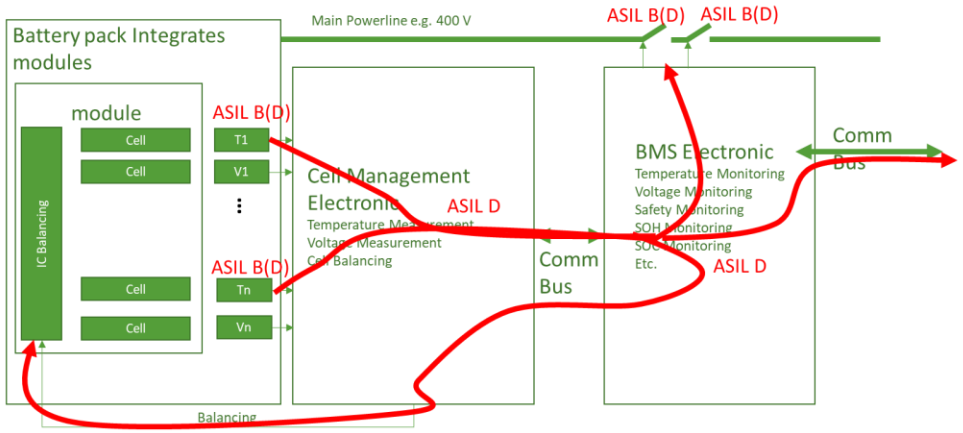
- ISO 26262 Part 5 Annex D describes a rough understanding of 60%, 90% and 99%. From that a kind of general design understanding is as follows:
  - 60% - the part is measured, and it can be judged if it is in range. Still if it would be in range but incorrect, this could not be discovered.
  - 90% - the part is measured, and a drift can be measured. Usually this is by comparison with another measurement. It can be now judged if it is in range and if the value in range is correct within a tolerance.
  - 99% - presumes the 90% and adds that now the 2 values to compare are diverse, and peaks and oscillations are handled as well to assure diagnose and stability at the same time and have no common cause fault (due to diversity common cause is not likely).

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of the publication under the Grant Agreement n° 2019-1-CZ01-KA203-064430 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

FMEDA Calculation Basics 1/4



- The sum of Single Point Fault FIT of all parts in the safety effect chain of a safety goal shall not be higher that the ASIL target FIT.
- Example:
  - Safety Goal 1: avoid battery over-temperature with ASIL D
  - ASIL D requires max. 10 FIT and 99% DC Diagnostic Coverage
  - All parts along the safety effect chain (see red flow in the picture left) together shall not exceed 10 FIT.

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union - 2019-1-CZ01-KA203-064430. The production of this publication under the ALBATTS Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

FMEDA Calculation Basics 2/4

- Single Point Fault and Single Point Fault Metric SPFM
- Example selecting parts one Thermistor and the cell management controller
- This needs to be extended by all parts for the safety goal in a real case

Hardware Architectural Metrics (ISO26262-5, C2)

albatts

Safety Goal:									
TOTAL FIT		407							
TOTAL FIT safety relevant		**325,2**							**3,36**
Metrics						**Single Point Fault Metric**			**99,0%**
							ASIL B >=90%	ASIL C >=97%	ASIL D >=99%
Component Name	**Failure rate/FIT [10^{-9}]**	**Safety-related component** to be considered in the calculations?	**Failure Mode**	Failure rate distribution	Failure mode that has the potential to **violate the safety goal** in absence of safety mechanisms?	**Safety mechanism(s)** allowing to prevent the failure mode from violating the safety goal?	**Failure mode coverage** wrt. violation of safety goal	**Residual or Single-Point Fault failure rate/FIT**	
Thermistor 1	2	YES	open (no measurement)	40%					
			drift resistance (measures incorrect)	40%	X	Temp Comparator	90%	0,08	
			short circuit (measures zero)	20%	X	Temp Comparator	90%	0,04	
Cell Management Controller	405	YES	see FMEDA sheet Aurix TC36x	80%	X	see FMEDA sheet Aurix TC36x	99%	3,24	

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of the publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

FMEDA Calculation Basics 3/4

- Thermistor
  - Raw FIT 2
  - 3 failure modes with a distribution open (40%), drift (40%), short (20%), data come from spec. sheet of supplier
  - Marking with x which mode is a hazard
  - Assigning the temperature comparator diagnose with 90% value (not 99% because the measurement principle is not diverse)
  - Calculating SPF for drift case:
    2 * 40% * (1-90%) = 0,08 FIT

Hardware Architectural Metrics (ISO26262-5, C2)

Safety Goal:									
TOTAL FIT		407							
TOTAL FIT safety relevant		**325,2**							**3,36**
Metrics						**Single Point Fault Metric**			**99,0%**
							ASIL B >=90%	ASIL C >=97%	ASIL D >=99%
Component Name	**Failure rate/FIT [10^{-9}]**	**Safety-related component** to be considered in the calculations?	**Failure Mode**	Failure rate distribution	Failure mode that has the potential to **violate the safety goal** in absence of safety mechanisms?	**Safety mechanism(s)** allowing to prevent the failure mode from violating the safety goal?	**Failure mode coverage** wrt. violation of safety goal	**Residual or Single-Point Fault failure rate/FIT**	
Thermistor 1	2	YES	open (no measurement)	40%					
			drift resistance (measures incorrect)	40%	X	Temp Comparator	90%	0,08	
			short circuit (measures zero)	20%	X	Temp Comparator	90%	0,04	
Cell Management Controller	405	YES	see FMEDA sheet Aurix TC36x	80%	X	see FMEDA sheet Aurix TC36x	99%	3,24	

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECPPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

FMEDA Calculation Basics 4/4

- Cell Management Controller
  - Has usually its own FMEDA by a sub-team done and totals are entered/integrated at system level.
  - Controllers have their own FMEDA tool and you select parts used and diagnostics to activated and configure and this delivers a calculated FIT AAND DC for the controller.
  - Here assumed a typical situation:
    - Raw FIT 405
    - 80% parts of controller used
    - Based on activated diagnostics 99% DC
    - Calculating SPF:
      405 * 80% * (1-99%) = 3,24 FIT

Hardware Architectural Metrics (ISO26262-5, C2)

Safety Goal:									
TOTAL FIT		407							
TOTAL FIT safety relevant		**325,2**							**3,36**
Metrics						**Single Point Fault Metric**			**99,0%**
							ASIL B >=90%	ASIL C >=97%	ASIL D >=99%
Component Name	**Failure rate/FIT [10^{-9}]**	**Safety-related component** to be considered in the calculations?	**Failure Mode**	Failure rate distribution	Failure mode that has the potential to **violate the safety goal** in absence of safety mechanisms?	**Safety mechanism(s)** allowing to prevent the failure mode from violating the safety goal?	**Failure mode coverage** wrt. violation of safety goal	**Residual or Single-Point Fault failure rate/FIT**	
Thermistor 1	2	YES	open (no measurement)	40%					
			drift resistance (measures incorrect)	40%	X	Temp Comparator	90%	0,08	
			short circuit (measures zero)	20%	X	Temp Comparator	90%	0,04	
Cell Management Controller	405	YES	see FMEDA sheet Aurix TC36x	80%	X	see FMEDA sheet Aurix TC36x	99%	3,24	

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of the publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

FMEDA Calculation Basics 4/4

- Thermistor
  - SPFM metric then calculates the share of dangerous FIT in percent which are detected by the safety concept.
  - In this example (simplified with 2 parts):
    - Dangerous not detected FIT are 3,36 (0,08+0,04+3,24)
    - Total dangerous FIT are 325,2 (2*40%+2*20%+405*80%)
    - SPFM 99% = (325,2-3,36)/325,2
  - So far we stay in ASIL D limits: 99% DC (here SPFM called) and 3,36 FIT. Still we need to add the other parts to come to a total
  - Note 2: ISO 26262 also requires a multiple point fault metric / latent fault metric, beside the SPFM targets.

Hardware Architectural Metrics (ISO26262-5, C2)

albatts

Safety Goal:									
TOTAL FIT		407							
TOTAL FIT safety relevant		**325,2**							**3,36**
Metrics						**Single Point Fault Metric**			**99,0%**
							ASIL B >=90%	ASIL C >=97%	ASIL D >=99%
Component Name	**Failure rate/FIT [10^{-9}]**	**Safety-related component** to be considered in the calculations?	**Failure Mode**	Failure rate distribution	Failure mode that has the potential to **violate the safety goal** in absence of safety mechanisms?	**Safety mechanism(s)** allowing to prevent the failure mode from violating the safety goal?	**Failure mode coverage** wrt. violation of safety goal	**Residual or Single-Point Fault failure rate/FIT**	
Thermistor 1	2	YES	open (no measurement)	40%					
			drift resistance (measures incorrect)	40%	X	Temp Comparator	90%	0,08	
			short circuit (measures zero)	20%	X	Temp Comparator	90%	0,04	
Cell Management Controller	405	YES	see FMEDA sheet Aurix TC36x	80%	X	see FMEDA sheet Aurix TC36x	99%	3,24	

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Summary

- Electronic faults can lead to failures which cause a hazard. Batteries have a number of life-threatening hazards which need to be avoided.
- A HARA defines the risk level by an ASIL A to D, a battery has a number of ASIL ratings, many at ASIL D.
- The higher the ASIL the more diagnostic coverage needs to achieved.
- The higher the ASIL the less the Fit rate of hardware parts related to safety monitoring and switching to safe state can have

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union - 2019-1-CZ01-KA203-064430. The production of this publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

References

- Messnarz R., Ekert D., Grunert F., Blume A. (2019) Cross-Cutting Approach to Integrate Functional and Material Design in a System Architectural Design – Example of an Electric Powertrain. In: Walker A., O'Connor R., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science, vol 1060. Springer, Cham. https://doi.org/10.1007/978-3-030-28005-5_25
- Rodic M., Riel A., Messnarz R., Stolfa J., Stolfa S. (2016) Functional Safety Considerations for an In-wheel Electric Motor for Education. In: Kreiner C., O'Connor R., Poth A., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2016. Communications in Computer and Information Science, vol 633. Springer, Cham
- G. Macher, R. Messnarz, C. Kreiner, et. al, Integrated Safety and Security Development in the Automotive Domain, Working Group 17AE-0252/2017-01-1661, SAE International, June 2017
- Messnarz R., Sporer H. (2018) Functional Safety Case with FTA and FMEDA Consistency Approach. In: Larrucea X., Santamaria I., O'Connor R., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2018. Communications in Computer and Information Science, vol 896. Springer, Cham. https://doi.org/10.1007/978-3-319-97925-0_32
- Messnarz, R; Kreiner ,C.; Riel, A.; et.al, Implementing Functional Safety Standards has an Impact on System and SW Design - Required Knowledge and Competencies (SafEUr), Software Quality Professional, 2015
- Messnarz R. et al. (2013) Implementing Functional Safety Standards – Experiences from the Trials about Required Knowledge and Competencies (SafEUr). In: McCaffery F., O'Connor R.V., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2013. Communications in Computer and Information Science, vol 364. Springer, Berlin, Heidelberg
- Messnarz R., König F., Bachmann V.O. (2012) Experiences with Trial Assessments Combining Automotive SPICE and Functional Safety Standards. In: Winkler D., O'Connor R.V., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2012. Communications in Computer and Information Science, vol 301. Springer, Berlin, Heidelberg
- Messnarz R., Much A., Kreiner C., Biro M., Gorner J. (2017) Need for the Continuous Evolution of Systems Engineering Practices for Modern Vehicle Engineering. In: Stolfa J., Stolfa S., O'Connor R., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2017. Communications in Computer and Information Science, vol 748. Springer, Cham

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Further reading

- **Safety Chapters in**
  - O'Connor, R.V. Akkaya, M., Kemaneci K., Yilmaz, M., Poth, A. and Messnarz R. (Eds), Systems, Software and Services Process Improvement, **CCIS 543, Springer-Verlag**, (2015).
  - Kreiner, C., Poth., A., O'Connor, R.V., and Messnarz R. (Eds), Systems, Software and Services Process Improvement, CCIS 633, Springer-Verlag, (2016).
  - Stolfa, J, Stolfa, S., O'Connor, R.V., and Messnarz R. (Eds), Systems, Software and Services Process Improvement, **CCIS 633, Springer-Verlag**, (2017).
  - Larrucea, X., Santamaria, I., O'Connor, R.V., Messnarz, R. (Eds), Systems, Software and Services Process Improvement, **CCIS Vol. 896, Springer-Verlag**, (2018).
  - Walker A., O'Connor, R.V., Messnarz, R. (Eds), Systems, Software and Services Process Improvement, **CCIS Vol. 1060, Springer-Verlag**, (2019).
  - Murat Yilmaz, Jörg Nieman, Paul Clarke, (Eds), Systems, Software and Services Process Improvement, **CCIS Vol. 1252, Springer-Verlag**, (2020).

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication under the activity Erasmus+ 2019-1-CZ01-KA203-064430 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Alliance for Batteries Technology, Training and Skills ALBATTS - Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Further reading

- Videos
  - How does a BMS work - https://www.youtube.com/watch?v=q4wDa_m9-8E
  - What is a BMS - https://www.youtube.com/watch?v=GXYJ1xC10j4&t=1s
  - Calculating the SoC - https://www.youtube.com/watch?v=rOwcxFErcvQ
  - Introduction to EIS - https://www.youtube.com/watch?v=Pk7SVcRIWac
  - How does EIS work for batteries - https://www.youtube.com/watch?v=xaimI9w-egQ
- Further links to relevant training materials.
  - https://de.wikipedia.org/wiki/Elektrochemische_Impedanzspektroskopie
  - https://www.mpoweruk.com/safety.htm
  - https://www.avl.com/battery/

Co-funded by the Erasmus+ Programme of the European Union

Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication under the Grant Agreement № 2019-612675 does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Reference to authors

- Dr Richard Messnarz
  - Google Scholar Profile: https://scholar.google.com/citations?user=v2xVlnwAAAAJ&hl=de&oi=ao
  - VDA Certified Principal Assessor and Instructor Competent Level Automotive SPICE
  - Functional Safety Trainer for ISO 26262
  - Director ISCN GesmH

- Dipl Ing Damjan Ekert
  - Google Scholar Profile: https://scholar.google.com/citations?user=4Sf3jdIAAAAJ&hl=de&oi=ao
  - VDA Certified Principal Assessor Automotive SPICE
  - Functional Safety Trainer for ISO 26262
  - Manager and Senior Expert ISCN GesmbH

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE) The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The Alliance for Batteries Technology, Training and Skills ALBATTS – Project number 612675-EPP-1-2019-1-SE-EPPKA2-SSA-B. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Reference to authors

- Tobias Zehetner
  - Google Scholar Profile: https://scholar.google.com/citations?hl=en&user=9tDGAe4AAAAJ
  - Developer Capability Adviser Assessment Tool
  - The assessment tool integrates ISO 26262 assessment

- MA, BA Laura Aschbacher
  - Google Scholar Profile: https://scholar.google.com/citations?hl=de&user=8-zYXjUAAAAJ
  - Designer Capability Adviser Assessment Tool
  - The assessment tool integrates ISO 26262 assessment

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-064430. The production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

albatts

Follow ALBATTS project at:

twitter

linkedin

facebook

More information:

https://www.facebook.com/pages/category/Not-a-Business/Project-Albatts-104780274397590/

Co-funded by the Erasmus+ Programme of the European Union

ECQA Certified Electric Powertrain Engineer (ECEPE). The project is co-funded by the Erasmus+ Programme of the European Union – 2019-1-CZ01-KA203-061430. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.