



## 2<sup>nd</sup> use application of battery cells: functional safety requirements

Workshop: Regulatory Qualification Requirements for Battery Storages

March 3<sup>rd</sup> 2018



WHEN YOU NEED TO BE SURE



### AGENDA

- Introduction of project MiBZ
- What means functional safety
- Standards for Functional Safety
- Comparison of functional safety requirements
- Outlook project results MiBZ

## PROJECT MiBZ: MULTIFUNCTIONAL INTELLIGENT BATTERY CELL

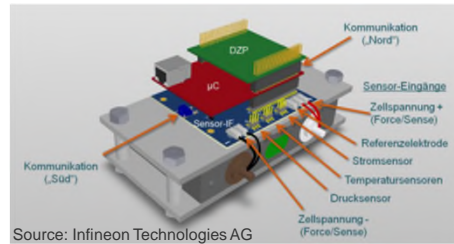
funded project of  
 Bundesministerium  
 für Bildung  
 und Forschung

- German federal funded project to research a multifunctional intelligent battery cell (MiBZ)

- PHEV2 NMC/ Graphite Cell

- Integrated sensors

- BC-Unit on cell level



Source: Infineon Technologies AG

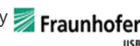
- Digital cell pass to store specific battery information

## CONSORTIUM PROJECT MiBZ

- BMW & VARTA-Storage (key user)**
  - Definition of requirements
  - Demonstration, Validation and industrial evaluation
- VARTA MB (cell manufacturer)**
  - manufacturing of „state-of-the-art“ cells incl. developed functionality
  - Test & evaluation
- Infineon Technologies (supplier)**
  - Sensors & electronics for analysis, communication and control
  - Functional model: digital cell pass
- SGS TÜV-Saar (testing organization)**
  - Functional Safety (automotive & stationary)
  - Verification & Test
- FhG Institute for Integrated Systems and Device Technology**
  - Communication between MiBZs and BMC
  - Sensorless cell temperature measurement and hybrid total current sensor
- Technical University of Munich**
  - Condition monitoring, modelling and simulation
  - Test & Evaluation



VARTA Storage



PROJECT MiBZ:  
FOCUS FUNCTIONAL SAFETY

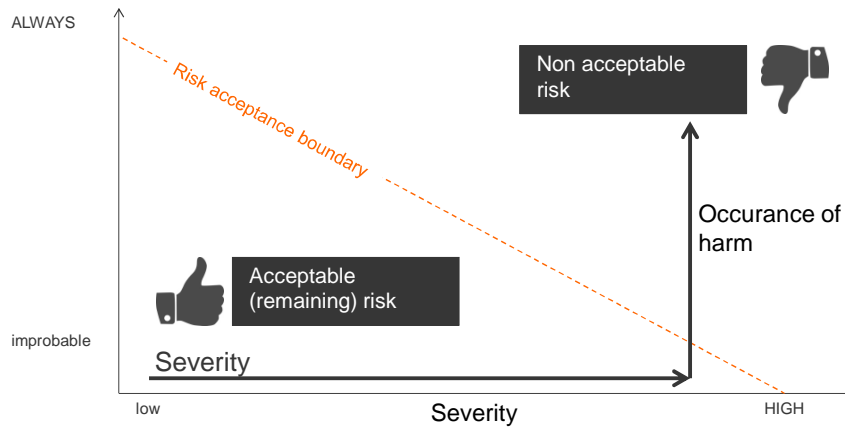
- SGS-TÜV examines the applicable standards for functional safety
- Comparison of requirements for automotive and stationary application to reduce development effort during the design phase of the MiBZ
- Assessment of the used electronic architecture  
→ statement due to qualification of industrialization and early detection of conceptual relevant issues.

## WHAT MEANS FUNCTIONAL SAFETY?



- Definition Functional Safety

absence of **unreasonable risk** due to **hazards** caused by **malfunctioning behavior** of E/E systems.



- At project start it was not clear which standard for FS of a stationary app shall be used
- ICE 62619 is reworked and published in 02-2017
  - standard addresses: Safety requirements for secondary lithium cells and batteries, for use in industrial applications
  - For functional safety the IEC 62619 recommends IEC 61508
- In the project MiBZ a hazard analysis and risk assessment was carried out, result is a SIL incl. the necessary safety functions

**INTERNATIONAL STANDARD**  
**NORME INTERNATIONALE**

Secondary cells and batteries containing alkaline or other non-acid electrolytes – Safety requirements for secondary lithium cells and batteries, for use in industrial applications

Accumulateurs alcalins et autres accumulateurs à électrolyte non acide – Exigences de sécurité pour les accumulateurs au lithium pour utilisation dans des applications industrielles

IEC 62619:2017 – 18 –

Table 1 – Sample size for type tests

Category	Test item	Opt. test No.	Refer. test No.
Primary cells	7.1 External short-circuit test	4	1
	7.2.1 Impact test	6 (see Note 3)	1
	7.2.2 Free fall	6	2
	7.2.3 Thermal abuse test	6	3
	7.2.4 Overcharge test	6 (see Note 4)	1
Rechargeable cells and battery systems	7.2.1 External short-circuit test	4	1
	7.2.2 Free fall	6	2
	7.2.3 Thermal abuse test	6	3
	7.2.4 Overcharge test	6 (see Note 4)	1
Rechargeable cells and battery systems	7.3.1 Temperature of electrolyte	7	1
	7.3.2 Internal short-circuit test	7	2
	7.3.3 Temperature of electrolyte	7	3
Rechargeable cells and battery systems	7.4.1 Overcharge control of voltage	8	1
	7.4.2 Overcharge control of current	8	2
	7.4.3 Overcharging control	8	3

NOTE 1 – The manufacturer can use “half battery” instead of “battery” at any test that specifies “battery” and not “cell” or “battery system”. The manufacturer clearly indicates the test used for each test.

NOTE 2 – If a battery system is divided into smaller units, the cell can be replaced as representative of the system. The manufacturer can indicate which are present in the final battery system. The battery manufacturer clearly indicates the method used.

NOTE 3 – Charging and discharging currents for the tests are based on the type of cell used. These currents are defined in a function of C<sub>10</sub>, where C<sub>10</sub> is the 10 h rated capacity (see IEC 61966).

NOTE 4 – The test is performed with final battery systems that are protected with only a single protection for overcharge (voltage control).

**7 Specific requirements and tests**

**7.1 Charging procedures for test purposes**

Prior to charging, the battery shall be discharged to an ambient temperature of 25 °C at a constant current of 0.2 C<sub>10</sub> for a specified test voltage.

Unless otherwise stated in this document, only for batteries shall be charged in an temperature of 25 °C ± 5 °C, in using the method specified by the manufacturer.

NOTE 1 – Charging and discharging currents for the tests are based on the type of cell used. These currents are defined in a function of C<sub>10</sub>, where C<sub>10</sub> is the 10 h rated capacity (see IEC 61966).

NOTE 2 – The battery system shall not be charged at a constant current of 0.2 C<sub>10</sub> for the duration of the specified test voltage.

**7.2 Rechargeability (rechargeable release)**

**7.2.1 External short-circuit test (cell or cell block)**

**a) Requirements**

Short-circuit between the positive and negative terminals shall not cause a explosion.

IEC 62619:2017 © IEC 2017 – 21 –

**8.1 Battery management system (in battery management unit)**

**8.1.1 Requirements for the BMS**

The BMS evaluates the condition of cells and batteries, and it monitors safety and balance when the battery is operating in operating region. The BMS shall be designed according to the safety, integrity and ISO 26262 defined in 11. Any failure of the cell operating region are voltage, temperature and current. (See Figure 6.1)

To evaluate the charge control that affects safety, the battery system manufacturer shall perform the tests mentioned in 9.2.3.10, 9.2.4.

NOTE 1 – The function of the BMS can be assigned to the battery pack or to the equipment that uses the battery (see Figure 6).

NOTE 2 – The BMS can be shared and it can be located partially in the battery pack and partially on the equipment that uses the battery. (See Figure 6)

NOTE 3 – The BMS is a subunit also referred to as a BMS (battery management unit).

- since 11-2011 ISO 26262 is the relevant standard
- this standard is accepted and established in the automotive industry
- Specific requirements on top level are available for project MiBZ

Note:

2<sup>nd</sup> edition of ISO 26262 will be published mid of 2018. Scope of the standard extends to motorcycles, heavy duty vehicles and busses.

## DERIVATION OF TOP LEVEL REQUIREMENTS

Safety related requirements are available for both apps on top level

- stationary app
  - Hazard analysis and risk assessment
  - SIL (safety integrity level)
  - definition of safety functions
  
- Automotive app
  - Hazard analysis and risk assessment acc. ISO 26262 Part 3
  - ASIL (automotive safety integrity level)
  - Definition of safety goals

Comparison shows, that different requirements result out of the standards (e.g. on SW-, HW-Level ...)

## COMPARISON FUNCTIONAL SAFETY REQUIREMENTS

- The selected standards for functional safety include different requirements on System-, HW-, and SW-Level
- A comparison is necessary and carried out to find out the differences in detail
- Assumptions:
  - 2<sup>nd</sup> use in a stationary app
  - system is 1<sup>st</sup> used in an automotive environment
  - System fulfills the requirements of ISO 26262
  - Perspective of comparison ISO 26262 → IEC 61508
- Result of comparison shows that 100 requirements are similar

## RESULT OF COMPARISON

overlapping requirements

~ 100 requirements are similar.

~ 260 requirements are not similar.

Part	Chapter	Typ	IEC	ISO	Requirements IEC61508	Result	Filtered Req
[0]	SLZ-general	Req	[1] 7.1.4.2	[2] 6.4.6.1	The requirements for the management of functional safety (see clause 6) shall run in parallel with the overall safety lifecycle phases.	-	-
[1]	SLZ-general	Req	[1] 7.1.4.3	[2] 6.4.6.1	Unless justified, each phase of the overall safety lifecycle shall be applied and the requirements met.	-	-
[1]	SLZ-general	Req	[1] 7.1.4.4	[2] 6.4.6.1	Each phase of the overall safety lifecycle shall be divided into elementary activities with the scope, inputs and outputs specified for each phase.	-	-
[1]	SLZ-general	Req	[1] 7.1.4.5	[2] 6.4.6.1	The scope and steps for each overall safety lifecycle phase shall be as specified in ISO1508-1 Table 1.	-	-
[1]	SLZ-general	Req	[1] 7.1.4.6	[2] 6.4.6.1	Unless justified in the functional safety planning or specified in the application sector standard, the outputs from each phase of the overall safety lifecycle shall be those specified in Table 1.	-	-
[1]	SLZ-general	Req	[1] 7.1.4.7	[2] 6.4.6.1	The outputs from each phase of overall safety lifecycle shall meet the objectives and requirements specified for each phase (see 7.2 to 7.3).	-	-
[1]	SLZ-general	Req	[1] 7.1.4.8	[2] 6.4.6.1	The verification requirements that shall be met for each overall safety lifecycle phase are specified in 7.18.	-	-
[1]	concept	Gen	[1] 7.2.1	[3] 8	The objectives of the requirements of this subclause is to develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out.	-	-
HW-overview		Row	[1] 7.2.2.1	[3] 8	A thorough familiarity shall be acquired of the EUC, its required control functions and its physical	-	-

Part	Chapter	Typ	IEC	ISO	Requirements IEC61508	Result	Filtered Req
[1]	Overall installation and commissioning planning	Gen	[1] 7.9.1.2		7.9.1.2 The second objective of the requirements of this subclause is to develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.	-	-
[1]	Overall installation and commissioning planning	Req	[1] 7.9.2.1		A plan for the installation of the E/E/PE safety-related systems shall be developed, specifying the installation schedule, the responsibilities for different parts of the installation, the procedures for the installation, the elements in which the various elements are integrated, the criteria for declaring all or parts of the E/E/PE safety-related systems ready for installation and for declaring installation activities complete, and the procedures for the resolution of failures and incompatibilities.	-	0
[1]	Overall installation and commissioning planning	Req	[1] 7.9.2.2		A plan for the commissioning of the E/E/PE safety-related systems shall be developed, specifying the commissioning schedule, the responsibilities for different parts of the commissioning, the procedures for the commissioning, the relationships to the different steps in the installation, and the relationships to the validation.	-	0
[1]	Overall installation and commissioning planning	Req	[1] 7.9.2.3		The overall installation and commissioning planning shall be documented.	-	0
		Row	[1] 7.9.3.1		The objective of the assessment of this subclause is to define the E/E/PE system safety	-	-

© SGS-TÜV Saar GmbH 2018 ALL RIGHTS RESERVED 13

## NEXT STEPS

- Next steps in the project MiBZ are:
  - Detailing the differences of requirements
    - HW metrics
    - HW/ SW diagnostic measures
    - Type of faults on HW-, SW-level
  - Statement how to handle specific HW- and SW requirements
  - Break down of requirement from system level

Part	Chapter	Typ	IEC	ISO	Requirements IEC61508	Result	Filtered Req
[2]	E/E/PE system design and development	Req	[2] 7.4.4.3.4		<b>Hardware safety integrity architectural constraints: Route 2</b> All Type B elements used in Route 2H shall have, as a minimum, a diagnostic coverage of not less than 90%.	-	0
[2]	E/E/PE system design and development	Req	[2] 7.4.5.1		<b>Requirements for quantifying the effect of random hardware failures</b> For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10).	-	0



## MANY THANKS

- Thank you very much for your attention
- German Ministry of Education, Science, Research and Technology (BMBF), for financial funding the project (Förderkennzeichen 03XP0027G)
- BEVS for the invitation and the chance to show the results

© SGS-TÜV Saar GmbH 2018 ALL RIGHTS RESERVED 15



## SGS - SOCIÉTÉ GÉNÉRALE DE SURVEILLANCE



- Founded: 1878 in Rouen – France
- Head quarters: **Geneva**
- **World leading testing organization** with more than **95.000** employees
- **Global network** more than **2.000 locations und laboratories** in more than 140 countries

© SGS-TÜV Saar GmbH 2018 ALL RIGHTS RESERVED 16



SGS LOCATIONS GERMANY



- Functional Safety
- Homologation
- Battery Test House
- EMC

SERVICES SGS-TÜV SAAR  
FUNCTIONAL SAFETY



Training Personal qualification	Consulting	Safety analysis	Assessment Certification
------------------------------------	------------	-----------------	-----------------------------





## CONTACT

SGS-TÜV Saar GmbH  
E-Mobility/ Functional Safety  
Michael Vogt  
Hofmannstraße 50  
81379 München, Germany  
t +49 89 787475 - 273  
f +49 89 787475 - 217  
[michael.vogt@sgs.com](mailto:michael.vogt@sgs.com)

© SGS-TÜV Saar GmbH 2018 ALL RIGHTS RESERVED 19

[WWW.SGS.COM](http://WWW.SGS.COM)  
[WWW.SGSGROUP.DE](http://WWW.SGSGROUP.DE)  
[WWW.SGS-TUEV-SAAR.COM](http://WWW.SGS-TUEV-SAAR.COM)



WHEN YOU NEED TO BE SURE

