Random Hardware failure compliance of a cell balancing circuit with the requirements of automotive functional safety

Gerhard Hofmann
Unterdietfurt, Germany
gerhard.hofmann@scienceandengineering.de

Prof. Georg Scharfenberg
OTH Regensburg
Regensburg, Germany
georg.scharfenberg@oth-regensburg.de

***Abstract* Lithium ion batteries have become established as an energy storage for electric vehicles. An essential component for optimal utilization of the stored charge is a cell balancing between the individual cells. There are several standard applications on the market now. In this paper it is shown by an example that a standard cell balancing circuit is compliant with the requirements of ISO 26262 with respect to random hardware failure. As an example the circuit is being evaluated whether it satisfies the requirements of the safety goal "overcharging shall be prevented" with respect to random hardware errors.**

Keywords: ISO 26262, Lithium Ionen cell balancing, random hardware failure

I. Introduction

Electric mobility (e-mobility) is becoming increasingly important. For hybrid vehicles, electric mobility was introduced as a supplement to conventional internal combustion engine. Meanwhile, even pure electric cars are available on the market. In the year 2014 400 000 electric vehicles have been sold worldwide. The largest markets are USA, Japan and China.[i] On the other hand, there is the lower range, shorter life time of the battery and greater demand of electronic control functions of the vehicle. The biggest challenge is the energy storage. So far, the lithium ion battery has prevailed in this area. To get the maximum charge stored in the batteries a function in a battery management system provides the cell balancing. With this, an attempt is made to compensate for manufacturing and life-related differences in charge of the individual cells of a battery. The use of lithium-ion batteries also means increased risks, e.g. by thermal effects.

In 2011, the ISO 26262 for functional safety was published. The objective of this standard is to reduce the entire product life cycle risks due to malfunction of the electrical / electronics to a manageable level.

II. Basics ISO 26262[ii]

A. Overview

The ISO 26262 deals with the functional safety of electrical / electronic systems for production vehicles up to 3.5 tons. The standard covers all aspects of the entire product life cycle. The standard is based on an item definition whose functions are examined. An automotive safety integrity level (ASIL) rating A to D is assigned to the individual hazards. This ASIL classification takes into account the probability of exposure, severity and controllability in a hazard and risk analysis (part 3). The standard describes the methods required for system design (part 4), for hardware development (part 5) and software development (part 6) depending on the associated ASIL. The area of production, operation and decommissioning is described in part 7. The support processes such as requirement management, configuration management or change management are described in part 8. Part 9 deals with a safety analysis. Finally part 10 includes a guideline for the individual parts.

Prior to intended evaluation the following activities are required. For the determination of the objectives to be achieved, the ASIL classification of the hazards and risk analysis (ISO 26262 part 3 clause 7) is to be determined. Especially for the hardware development the following sequence is indicated. From the Item definition (ISO 26262 part 3 clause 5) safety goals based on the ASIL classification are to be defined (ISO 26262 part 3 clause 7). From the safety goals a functional safety concept is to be developed. Based

ISBN 978-80-261-0386-8, © University of West Bohemia, 2015

on this concept functional safety requirements are then derived (ISO 26262 part 4 clause 6), which provide the basis for the technical safety concept.

B. *Hardware requirements according ISO 26262 part 5*[iii]

After these preparations, the requirements of ISO 26262 part 5 can be addressed. This part deals with the "product development at hardware level". Starting from the safety plan (ISO 26262 part 4) a "planning of hardware-specific activities"[iv] becomes necessary. In clause 5 three main activities are enumerated.:

- "the hardware implementation of the technical safety concept;
- the analysis of potential hardware faults and their effects;
- the coordination with software development."[v]

Based on a technical safety concept (ISO 26262 part 4) hardware safety requirements are derived. Starting from there evidence must be found that the hardware safety requirements are complied with. This is carried out through metrics for the hardware architecture (clause 8) and on the estimation, whether random hardware faults lead to a safety hazard. Two methods are described for the safety hazard: first, whether in the part 3 specified safety goals are achieved or, as described in the standard as objective, "the residual risk of a safety goal violation, due to random hardware failures of the item, is sufficient low". The first method uses a rating based on failure rates metric, called "probabilistic metric for random hardware failures (PMHF)". The second method evaluates each single-point failure, residual failure and related dual point failures. Since the second method is the preferred method[vi] it is also applied to the cell balancing circuit. For this purpose, proof is provided that a single fault does not exceed the thresholds of the standard. The residual risk of a failure is evaluated by considering "the occurrence of a fault and the efficiency of the safety mechanism". The occurrence is expressed with a failure rate class and the efficiency of safety mechanism is expressed by a diagnostic coverage. Dual point failures are evaluated similar to residual faults, with different limits. Part 5 closes with requirements on the hardware integration and testing.

III. CELL BALANCING CONCEPT

Cell balancing is a part of the battery management system (BMS) and provides an optimal charge distribution between the individual cells in order to save the maximum charge in the cells and also get a maximum back, since normal charging algorithms shut down as soon as a cell has reached the maximum charge.

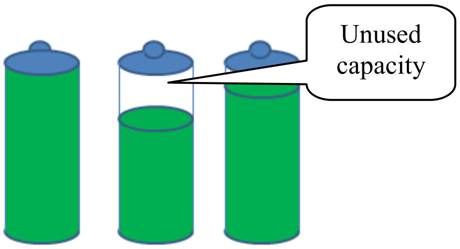


Figure 1. Need for cell balancing

The reason for the different charge levels of the individual cells can firstly be due to scattering of the manufacturing process, which is reflected in different internal resistances or capacitances. Also, different temperatures of the individual cells lead to a different behavior. The causes for different temperatures are determined inside the cell or by the thermal management of the entire package. In addition to the temperature, the State of Charge (SOC) imbalance, the total capacity or the impedance imbalance are the electrical reasons for the differences. The SOC imbalance can be compensated. The other two are generated by the construction of lithium ion cells and must be considered by the evaluation algorithm. [vii]

The greatest risk in case of error behavior is the "thermal runaway" effect of lithium-ion batteries. Here, the lithium within the cell becomes unstable and there is a strong oxidation with excessive heat.[viii] This reaction can lead to additional hazards of fire, explosion or smoke. [ix] Within lithium ion batteries, there is no overvoltage protection.[x]

The causes that can lead to thermal instability are internal or external short circuit, overload, deep discharge or excessive heating.[xi] As a threshold 4.35V may not be exceeded during charging. Deep discharges should not fall below 2.7V to 2.2V.[xii]

The reasons for cell balancing are the following:[xiii]
- Increased safety by avoiding thermal overload (thermal runaway) due to overvoltage;
- Extending the life-time;
- Loss of capacity while loading;
- Loss of capacity while unloading.

There is a distinction between passive and active cell balancing. Passive cell balancing uses resistors to dissipate energy out of weak cells during loading to reach the desired load capacity for the whole battery. During unloading this concept cannot cope the limited capacity of weak cells.
During loading the cell with a restricted capacity will reach at first the maximum threshold voltage. To prevent the shutdown of the charging process the

active balancing structure will transfer load to a cell with a higher capacity. While unloading the battery this structure can balance the other way to prevent the minimum voltage of the weak cell. As a basic principle the active balancing structure uses capacitances and inductances to transfer the energy from one cell to the next. This means much less energy is wasted as in passive cell balancing and a greater amount of usable battery capacity.

The algorithm for cell balancing can have following approaches:[xiv]

- Cell voltage based algorithm;
- State of Charge based algorithm;
- State of Charge and total capacity based algorithm.

IV. Compliance of random Hardware failure for an example circuit for cell balancing according ISO 26262

Chipsets BQ20Z80 [xv] by Texas Instruments was investigated as an example concerning the applicability of ISO 26262 part 5 clause 9 method 2 in random hardware failure during cell balancing.

For the hazard „overcharge causes thermal event“[xvi] the information of the paper „System Safety and ISO 26262 compliance for automotive Lithium-Ion Batteries“ is used[xvii]. The ASIL C classification arises at this point. The required 3 classes are explained by the aid of the Annex B of ISO 26262 part 3.

- Severity – S3 – Life threatening injuries(survival uncertain), fatal injuries;
- Probability of exposure in operational situation – E3 (“occurs once a month or more often for an average driver”);
- Controllability is rated with C3 according to the definition that less than “90% of all drivers…, are usually able or barely able to avoid harm.”

For the hazard of overcharging, the safety goal[xviii] „Battery overcharging shall be prevented“ is used. Based on the safety goal, inter alia, the functional safety requirements (FSR) "indication of overcharge shall be computed and communicated to the powertrain controller" and "if overcharge condition is detected, current shall be interrupted in x ms" are derived. As example of a cause of overcharging an over voltage is applied, that can lead to thermal runaway effect.

For the implementation of the functional safety requirements in technical safety requirement (TSR)[xix] the two TSR “overcharge condition shall be detected within y ms” and “current to battery shall be interrupted within z ms” are used. These two functions of the corresponding hardware are then allocated in the circuit.

To evaluate whether a violation has occurred, the safety goal method 2 of the ISO 26262 part 5, clause 9 for the recommended circuit for the chipset BQ20Z80 and 4 lithium ion cells are used. [xx]

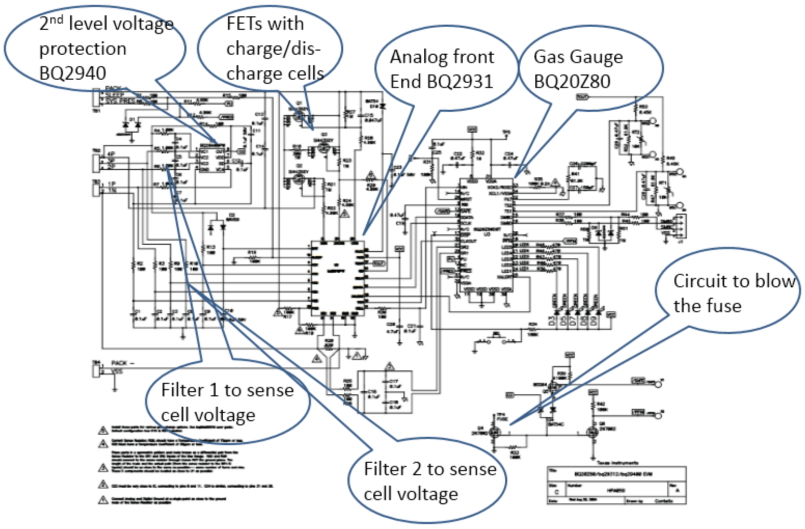

2nd level voltage protection BQ2940
FETs with charge/dis-charge cells
Analog front End BQ2931
Gas Gauge BQ20Z80
Circuit to blow the fuse
Filter 1 to sense cell voltage
Filter 2 to sense cell voltage

Figure 2. sample schematic for a cell balancing application[xxi]

It is not scope of this paper to develop or describe the schematic. Therefore the reference schematic from Texas Instrument is used. For a detailed understanding of the function of the circuit please see the application book[xxii]. The figure 2 is only added to get an understanding of the scope of the circuit and it is not intended to be readable. The core of the schematic is the gas gauge IC BQ20Z80, which computes the charge calculation and some safety function. As an analog front end (AFE) the BQ2931 is used. As a second safety overvoltage protection the BQ2940 is used. The understanding of the schematic is necessary to assign the components to the functions.

As an example for overvoltage detection the assessment for random hardware failures should be carried out for the safety goal "Battery overcharging shall be prevented". For this purpose, the method 2 of the standard is used. This method uses an individual assessment of the individual components and their errors. The method takes into account not only the error probability of occurrence but also the effectiveness of the safety mechanism. Exemplarily the BQ2940 and the cell voltage sensing of the BQ2931 are evaluated in this paper.

The targets for the evaluation can be read in the standard in the corresponding charts. Depending on the type of error, the standard takes into account, both the ASIL level, as well as the failure rate class and the diagnostic coverage.

The failure rate class reflects „the failure occurrence rate“[xxiii] The failure rate class 1 gets calculated from the corresponding target for ASIL D divided by 100. The following failure rate classes are times 10 from the previous failure rate class. In Table 1, the values for failure rate class targets are specified.

TABLE I. FAILURE RATE CLASSES ACCORDING ISO 26262 PART 5[xxiv]

Failure rate class	Random hardware failure target	Remark
FRC 1	$<10^{-10}h^{-1}$	Target for ASIL D ($<10^{-8}h^{-1)}$ divided by 100
FRC 2	$<10^{-9}h^{-1}$	Ten times the FRC 1 value
FRC 3	$<10^{-8}h^{-1}$	100 times the FRC 1 value or the Target for ASIL D
FRC i; i > 3	$<<10^{-10+(i-1)}h^{-1}$	$10^{(i-1)}$ times the FRC 1 value

Depending on the type of error, single point failure, residual failure or dual point failure other failure rate classes are defined as a target. For a single point failure of the ASIL C classification of the standard can be found in the FRC 1 or FRC2 with dedicated measures.[xxv]

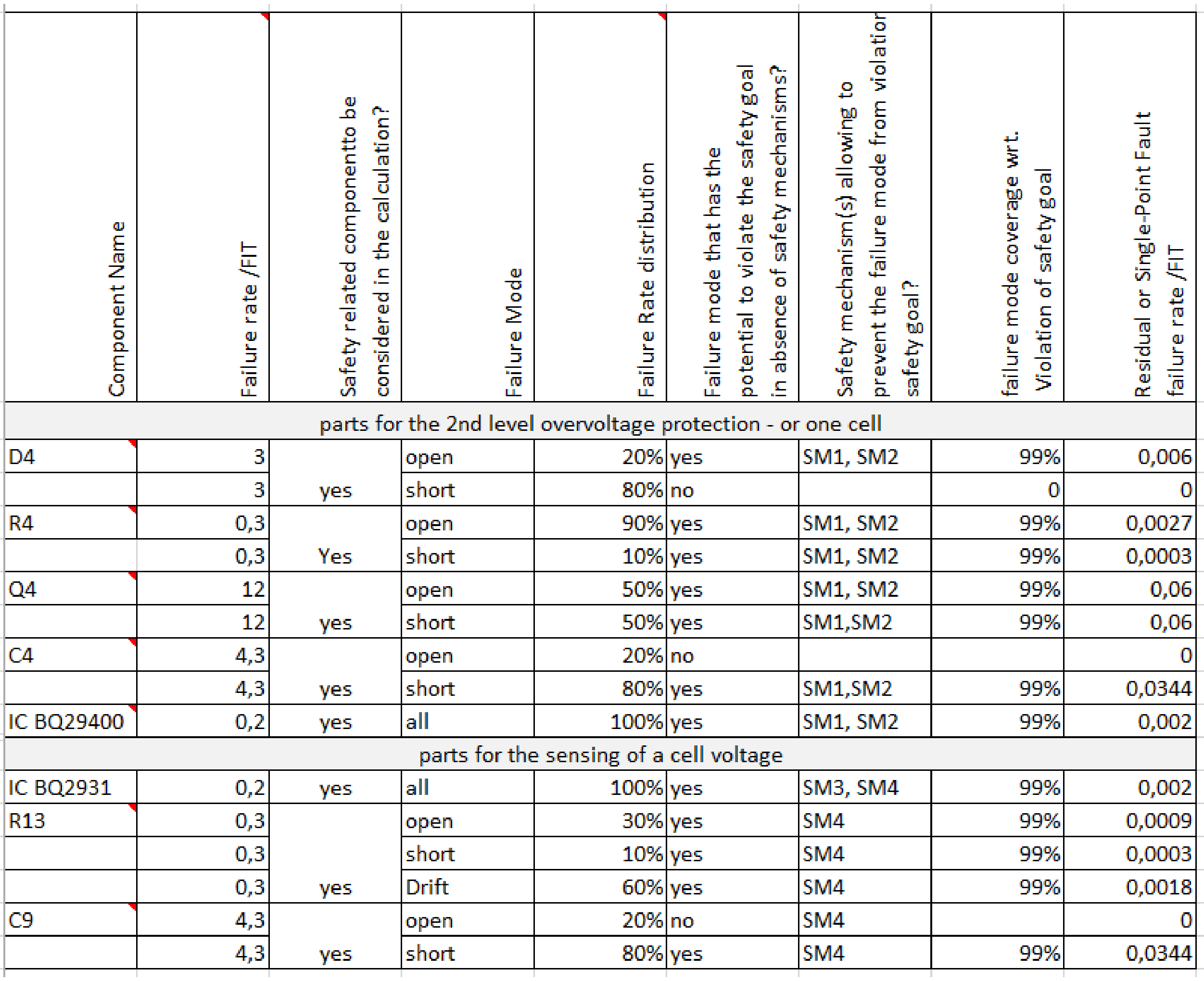
In the following table possible safety mechanism for overvoltage prevention are summarized.

TABLE II. IN THE FOLLOWING TABLE THE DIFFERENT SAFETY MECHANISM APPEAR.

Safety mechanism 1	AFE – overcurrent protection by turning Charge/Discharge FETs off
Safety mechanism 2	AFE –instructed by Gas Gauge BQ20Z80 to AFE to turn Charge/Discharge FETS off
Safety mechanism 3	Gas Gauge (BQ20Z80) indicate implausible FET or Watchdog of AFE and blows fuse
Safety mechanism 4	2nd level overvoltage protection by BQ2940 blow fuse

To find the default failure in time (FIT) values for each of the implementation the standard references in Section 8.4.3 to Industry standards such as „IEC/TR 62380, IEC 61709, MIL HDBK 217 F notice 2, RIAC HDBK 217 Plus, UTE C80-811, NPRD 95, EN 50129:2003, Annex C, IEC 62061:2005, Annex D, RIAC FMD97 and MIL HDBK 338”.[xxvi]. For carrying out the evaluation, the basis failure rate values of the MIL HDBK 217[xxvii] and the specifications of the supplier were used. The division of the failure mode was geared to the example in the ISO 26262 part 5 in Appendix E and the diagnostic coverage is assumed with 99%. The following table shows exemplarily the evaluation of the random hardware failure rate of the overvoltage protection of 2nd level protection and the series cell voltage sensing of the analog front end. The 2nd level overvoltage protection senses the voltage (R4, C4) and the BQ2940 decides by itself to blow the fuse, over the Diode D4 and the transistor Q4. The series cell voltage sensing is done by the AFE BQ2931 and the Resistor R13 and Capacitor C9.

TABLE III. EVALUATION OF THE RANDOM FAILURE RATE ACCORDING ISO 26262 PART 5 CLAUSE 9



Component Name	Failure rate /FIT	Safety related componentto be considered in the calculation?	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 violatior safety goal?	failure mode coverage wrt. Violation of safety goal	Residual or Single-Point Fault failure rate /FIT
parts for the 2nd level overvoltage protection - or one cell								
D4	3	yes	open	20%	yes	SM1, SM2	99%	0,006
	3		short	80%	no		0	0
R4	0,3	Yes	open	90%	yes	SM1, SM2	99%	0,0027
	0,3		short	10%	yes	SM1, SM2	99%	0,0003
Q4	12	yes	open	50%	yes	SM1, SM2	99%	0,06
	12		short	50%	yes	SM1,SM2	99%	0,06
C4	4,3	yes	open	20%	no			0
	4,3		short	80%	yes	SM1,SM2	99%	0,0344
IC BQ29400	0,2	yes	all	100%	yes	SM1, SM2	99%	0,002
parts for the sensing of a cell voltage								
IC BQ2931	0,2	yes	all	100%	yes	SM3, SM4	99%	0,002
R13	0,3	yes	open	30%	yes	SM4	99%	0,0009
	0,3		short	10%	yes	SM4	99%	0,0003
	0,3		Drift	60%	yes	SM4	99%	0,0018
C9	4,3	yes	open	20%	no	SM4		0
	4,3		short	80%	yes	SM4	99%	0,0344

Comparing the FIT rates in the residual or single point fault column with the valid fault rate class it can be seen that all values are lower than the target and the circuit meets the requirement of the safety goal. However, it only fulfills the requirement because the safety mechanisms grab.

CONCLUSION

- ISO 26262 part 5 is a useful method to evaluate random hardware failures also in cell balancing circuits.
- The hardware- design of this example is adequate to the ISO 26262 requirement, because it reaches the targets in part 5 (hardware). Without additional safety mechanism it would not reach the requirements.
- The example of the cell balancing circuit shows that a “not very complex” function has to be well deliberated to fulfill the requirements of ISO 26262
- To evaluate the circuit it is also necessary to understand the battery basics to define the safety goals

REFERENCES

[i] compare http://ecomento.tv/2014/04/01/weltweit-ueber-400-000-elektroautos-bestand-2013-verdoppelt/ accessed on 04.03.2015

[ii] Compare ISO 26262 part 1-10, 1 Edition, Genf, 2011

[iii] Compare with ISO 26262 part 5, 1 Edition, Genf, 2011

[iv] ISO 26262 part 5, 1 Edition, Genf, 2011 page 3

[v] ISO 26262 part 5, 1 Edition, Genf, 2011 page 4

[vi] Chitra, T., automotive functional safety compliance requirments with ISO 26262 HW architectural

metrics with an example, SAE-China and FISITA (eds), Springer, 2013

[vii] http://www.artechhouse.com/static/sample/barsukov-491_ch04.pdf accessed on the 22.02.2015– page 138

[viii] Korthauer, Reiner [editor], Handbuch Lithium-Ionen Batterien, Berlin, Springer, 2013, page 22

[ix] Korthauer, Reiner [editor], Handbuch Lithium-Ionen Batterien, Berlin, Springer, 2013, page 315

[x] Compare http://e2e.ti.com/support/power_management/battery_management/m/videos__files/528845 page 17 of file D1 - Track 1 - 1 keynote_battery_fundamentals_2011_part1.pdf accessed on 27.03.2015

[xi] Compare Korthauer, Reiner [editor], Handbuch Lithium-Ionen Batterien, Berlin, Springer, 2013, page 315

[xii] http://www.artechhouse.com/static/sample/barsukov-491_ch04.pdf accessed on the 22.02.2015– page 123-124

[xiii] http://www.artechhouse.com/static/sample/barsukov-491_ch04.pdf accessed on the 22.02.2015– page 111-112

[xiv] http://www.artechhouse.com/static/sample/barsukov-491_ch04.pdf accessed on the 22.02.2015– page 134ff

[xv] compare http://www.ti.com/product/bq20z80a-v110/description from 29.03.2015

[xvi] Compare Taylor, William; Krithivasan, Gokul; Nelson, J. Jody, System Safety and ISO 26262 Compliance for automotive Lithium Ion Batteries, IEEE Paper, 2012Paper LIIon – figure 5

[xvii] Compare ISO 26262 part 3, 1 Edition, Genf, 2011, clause 7

[xviii] compare ISO 26262 Part 3, 1 Edition, Genf, 2011, clause 7

[xix] compare ISO 26262 Part 4, 1 Edition, Genf, 2011, clause 6

[xx] http://www.ti.com.cn/general/cn/docs/lit/getliterature.tsp?baseLiteratureNumber=slua340&fileType=pdf page 3 accessed on the 29.03.2015)

[xxi] http://www.ti.com.cn/cn/lit/an/slua340c/slua340c.pdf accessed on 29.03.2015

[xxii] https://www.ti.com/seclit/an/slua380/slua380.pdf accessed on 29.03.2015

[xxiii] ISO 26262 part 5, 1 Edition, Genf, 2011, page 23

[xxiv] ISO 26262 part 5, 1 Edition, Genf, clause 9.4.3.3

[xxv] Compare ISO 262621 part 5 Edition, Genf, 2011 page 24, Table 7

[xxvi] ISO 26262 part 5, 1 Edition, Genf, 2011, page 15

[xxvii] http://www.sre.org/pubs/Mil-Hdbk-217F.pdf accessed on 11.03.2015