

Development of Safe Energy Storage System for Small Electric Vehicles

Martin R. Hammer¹, Udo Steininger², Lothar Wech², Georg Walder¹, Richard Eckl¹,
Moritz Steffan¹, Markus Lienkamp¹

¹Institute of Automotive Technology, Technische Universität München
Boltzmannstraße 15, 85748 Garching bei München

²TÜV SÜD AG, Daimlerstraße 11, 85748 Garching bei München
Hammer@ftm.mw.tum.de

Abstract— To ensure the safety of small electric vehicles, both the established safety instrumented systems and the challenges of weight-related compatibility have to be considered. Furthermore, the requirements of the electric power train have to be ensured. Attention has to be directed to the energy storage system due to the usage of lithium-ion-technology which on its upside has superior performance during vehicle operation, but on the downside can represent a possible threat to vehicle safety. Impulsive electric loads due to longitudinal and lateral driving maneuvers, permanent mechanical stress in daily use as well as the threat of a car crash necessitate a thorough, holistic safety concept for energy storage systems.

The paper at hand suggests a safety concept conforming to ISO 26262-3 specifications for energy storage systems in small electric vehicles. The analysis considers in addition to the designated electronic components relevant mechanical elements, supplementary loads and hazards that could cause a threat due to malfunction during daily operation. The acquired safety goals form the basis for the conceptual design of a safe energy storage system suggested subsequently.

The safety goals derived from the hazard analysis and risk assessment highlight the importance of accurate cell monitoring. Measurable cell data needs to be processed for failure detection and prevention such as thermal conditioning and overvoltage protection. Controllability of the high voltage circuit decreases the hazard probability of high electric or thermal loads. Furthermore, the analysis reveals that mechanical shocks and vibrations as well as thermal loads affect the battery safety significantly, particularly with regard to the battery cells. Hence, a shock damping bonding technique, an individual cell fusing and an effective cooling method is presented in the energy storage system concept. Furthermore the battery system needs to be placed in the zone between the axis behind the front seats to provide good protection against front-, side- and bottom impacts.

Keywords—Energy storage system, ISO 26262, safety, Hazard Analysis and Risk Assessment, Bonding Technique

I. INTRODUCTION

The trend towards electromobility will have a crucial impact on future automotive engineering. Especially micro cars with their extremely low weight make an interesting argument for urban mobility. Due to the low weight of such vehicles like the MUTE [1], they only require a small and on that account

inexpensive energy storage system for an acceptable operating range.

Battery Management Systems (BMS) are intended to ensure overall battery safety by monitoring every single cell both thermally and electrically and by communicating with the vehicle control system. These systems use integrated circuits and algorithms that may commit errors in the hardware and software throughout their lifecycle. The ISO 26262 standard focuses on the development of safe electronic systems to maintain the functionality of the system according to defined criteria and to ensure functional safety [2]. In its third part, the hazard analysis and risk assessment methodology is used to discover near-threatening situations involving electronic systems. This process assists the deduction of functional safety goals which result in functional requirements. In the final step, these requirements form the basis for deriving the safety concept of the energy storage system.

The scope of the ISO 26262 standard only focuses on electronic systems such as sensors and BMS but omits malfunctions or hazards relating to non-electronic components such as cell junctions, interconnections, cell brackets or mountings. The selection of the battery cell and its positioning in the vehicle package is not considered directly either, even though these aspects have a significant impact on vehicle safety.

Therefore, system safety is not exclusively substantiated on the functional safety covered by ISO 26262, but also depends on nonfunctional safety requirements. This enables an expansion of the scope for a safe battery system concept. Martin et al. mention the electric and mechanical safety as further relevant fields. According to his paper, various hazards are evoked indirectly by electronic failure, meaning that the energy storage system cannot be described ambiguously as an E/E-system [3].

II. FUNCTIONAL SAFETY AND SAFETY IN USE

A consistent definition of the term *safety* is not possible. Nonetheless, it can be noted that the terms *safety* and *risk* are associated with each other. The dependency is illustrated by the definition provided in DIN ISO 31000-2 [4]. The standard is internationally adapted to any risk and therefore does not focus on specific products or industries. However, it states a general approach to treat certain hazards by supporting specialized

standards. The term safety is directly related to the following expressions:

<i>Risk</i>	Measure for the probability of occurrence of malfunctions and its severity
<i>Tolerable risk</i>	Technical condition which is hazardous if the risk is increased The maximal acceptable risk of a technical state
<i>Danger</i>	Transgression of the tolerable risk
<i>Protection</i>	General description of actions that reduce the probability of occurrence of malfunctions and their consequences

These terms allow a definition of safety according to DIN ISO EN 31000-2:

Safety The risk of a technical condition is inferior to the tolerable risk

Thus, every safety related step targets a positive influence on limiting the risk to the tolerable risk when implemented. For ensuring safety, precautions are established to decrease the remaining risk even more than the necessary risk reduction postulates.

A. Functional Safety

According to Börcsök, functional safety implies that a component or system accomplishes its safety related tasks correctly in accordance with the relevant risks. The function will be performed even in case of internal failure and breakdown or transitions into a defined safe state [5].

Along with the development of a new product, both specific industrial guidelines and standards have to be considered for a methodical realization of functional safety [6]. The EC 61508 *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)* is an international standard for all types of programmable systems that can cause a threat to property, environment or people due to a single malfunction or combined malfunctions [7]. Functional safety is a partial aspect of the overall safety and is attended to focus on the correct execution of functions [5,8]. ISO 26262 has been adapted from its parent standard IEC 61508 to react to the particular needs of the automobile industry.

The functional safety is characteristic of a product and has to be developed systematically and implemented constructively. The ambitious goal to establish a high functional safety standard requires a widespread collaboration of safety experts, product designers, quality managers and process management within the development process. The principle is to develop schemes and technical solutions early on to avoid failures and associated hazards. The main requirement is identifying potential dangerous situations. By doing so, an appropriate reaction for a safe state is executed [8].

B. Safety in Use

In contrast to the functional safety, which focuses on potential malfunctions, the scope of the safety in use is justified by focusing on operational functions in working order.

The purpose of a *safety in use analysis* is to identify hazards that may occur during use due to inadequate sizing or designing of components. The analysis allows making changes to the system at an early stage of the development process to avoid failure of functions that may undermine the vehicle safety [9]. For instance, the choice of cell design can help to ensure safety in use since the failure rate of cells is in relation to the active material masses due to normal production variations [10]. On that account a large cell is more failure-prone than a small cell. Furthermore the impact of cell failures such as internal short-circuits caused by thermal runaways is a significant threat to the battery safety and can be partially ensured by the system design if a suitable cell design is chosen.

The impact of short circuits is dependent among others factors on the cell capacity, respectively the cell size, and the type of the short circuit. According to Kim et Al. a high impedance short circuit results in the same local localized heating and a negligible global heating for both the large and small cells. On the contrary, a low impedance short circuit causes a high heat generation which can evolve to a safety critical situation depending on the cell size and the location of the short circuit. For a large cell a low impedance short circuit results in a localized heating, small cells have to endure a global heating [25]. Nevertheless both cells can become explosion-prone, but with its smaller capacity respectively smaller chemical energy content, the severity of a small cell failure is likely to be less critical.

The energy storage system development with large cells in one single serial string may lead to a breakdown of the entire system due to just one large cell. But using small cells, connected in parallel to obtain an equal capacity, can improve the safety during use respectively the operational availability. Since the defective cell impedance becomes high or the cell is detached from the electric interconnection, the circuit can be compensated by other parallel cells. Thus the availability of the vehicle is maintained as well [10].

Therefore one important decision is to select the right cell design and subsequently the corresponding bonding technique to ensure a high availability of the energy storage system and the safety in use [10].

III. BATTERY SYSTEMS – COMPONENTS AND SETUP

The key element of an electrified power train is the battery system. It consists of electrochemical energy storage units, also called battery cells, various BMS components as well as a variety of sensors, electric conductors, housings and mountings.

The favored Lithium-Ion technology with its high performance and energy density compared to the NiMh technology gives electric vehicles a driving range up to 500 km and a performance of more than 350 kW in series vehicles [11]. By combining different active cathode and anode materials, it is possible to select the power and energy density as well as safety features. However, every combination shows a precarious safety behavior both regarding over- and undervoltages, extreme temperatures or high current loads. The mechanical penetration of the active material can lead to internal short circuits and result, especially in combination with the stated reasons above, in venting or thermal runaway. This sudden release of energy in terms of an explosion can cause fatal damage to the energy storage system and poses a high hazard to passengers and environment.

A. Stresses and Strains in Use

The usage of energy storage systems in electric vehicles entails besides the hazard of destruction in an accident risks due to shocks and vibrations affecting the energy storage components. Chassis investigations executed by the Technische Universität München with a lightweight electric car of 650kg showed that accelerations of 9g along the vertical z-axis and up to 2.5g along the horizontal x- (longitudinal) and y- (lateral) axis could occur in the most likely position of the battery system. The stress emerged predominantly at low frequencies among 4 Hz, see figure 1. In case of an accident, the values easily can exceed 50g [12]. Regarding an accident of a micro car with a heavy vehicle, the acceleration could be even greater.

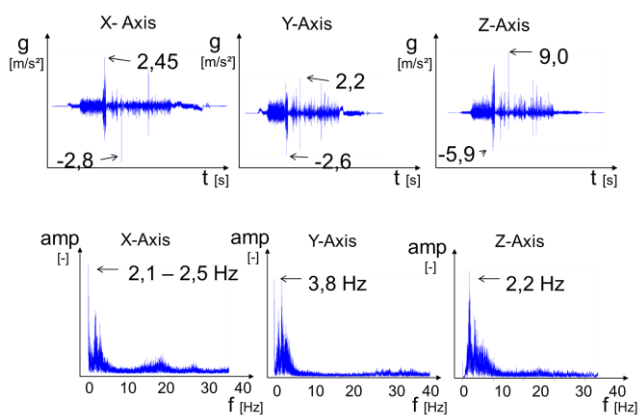


Figure 1: Accelerations and Frequencies at the B-pillar of chassis investigations executed by the Technische Universität München

Thermal stresses of the battery cell due to high ambient temperatures and/or heat generation of the ohmic losses in its interior damage the battery cell over the long term and increase the hazard of thermal destruction.

The performance requirements during use necessitate the battery to provide high current values on a short term basis or even alternating currents. If the current value exceeds the maximum tolerable limits by charging and discharging, the risk of under- or overvoltage becomes more likely which results in a hazardous situation. Conclusively, the monitoring of the measurable cell data such as voltage, temperature and state of charge is of utmost importance for the overall safety since occasional hard- or software failures cannot fully be prevented.

B. Size and Design of Battery Cells

Currently, there are three different cell designs of lithium-ion-batteries that are applicable.

The prismatic cell has a rectangular shape which allows a tight package. The metal housing provides good protection for the sensitive active materials against mechanical impacts that could provoke internal short circuits. The positive and negative poles are located on top. The heat dissipation primarily is realized by bottom cooling. The standardized VDA prismatic cell (115 mm x 173 mm x 32 mm / 45 mm) provides an electric energy capacity between 40 and 66 Ah [10]. The high volume compared to the cooling surface (Ratio volume/cooling surface: 115) shows disadvantages for optimal heat dissipation. This results in high temperature gradients within the cells that affect aging, performance and reliability negatively.

Pouch cells possess a flexible aluminum shell that provides little protection to the active materials and allows the cell to expand under electric and thermal loads. The high surface to volume ratio allows good heat dissipation, but pouch cells show disadvantages of leakage and inflation through pressure build-up [13]. The electric bonding is realized via tabs which are clamped to a bus bar. Cooling is also realized via the tabs. The pouch cell format of the VDA has a capacity between 50 and 54 Ah [10].

The third cell design is the cylindrical battery cell, specifically the format 18650 (diameter 18mm, length 65mm) that is in use in all Tesla Motors vehicles [4]. The coiled active materials are inserted into a metal cup that provides a similar stability as the prismatic design. The current drain is realized via the poles on the faces of the cylinder. The robust cup can resist an increasing internal pressure caused by chemical side reactions. However, the conditioning, due to the commonly used cylinder-shell-cooling, does not allow the tightest arrangement of these cells. The volume/cooling surface ratio with shell cooling results in the value 9 assuming only one side of the shell being in direct contact with the cooling fluid. But even though the surface to volume ratio is better than the ratio offered by prismatic cells, the efficacy is worse [13]. This can be explained by the 20 times higher heat transfer resistance in radial direction of 18650 cells [24]. Bottom cooled prismatic cells use the relatively low internal resistance of the active materials to conduct the internal heat directly to the cooling surface whereas the heat in shell-cooled 18650 cells has to overcome several contact resistances in radial direction. The capacity of an 18650 cell is between 1 Ah and 3.2Ah, with other cylindrical sizes delivering up to 6.8Ah [10].

Small cylindrical cells with their little reactive masses generally can be seen as safer compared to large cells. In different studies and simulations, scientists have shown that a cascading failure of cells and therefore the hazard increase with cell dimensions [10].

C. Package and System Configuration

The energy storage system has to be integrated into a safe area to ensure protection from intrusion. A vehicle package provides the three suitable locations - *bottom sandwich integration*, *T-shape integration* (transmission hump/ below rear seat row) or *distributed integration* (below the seats / back of the car). Regarding the necessary crash elements and to increase the customer benefit through large stowage and interior space, the *bottom sandwich integration* is suggested [13]. Nevertheless, the proximity of the energy storage system to the ground is problematic, since some battery accidents involving Tesla Model S have occurred. For instance, the battery system in the bottom of the car was punctured by a piece of metal while driving and caught fire [14].

For conditioning the energy storage system, the peripheral equipment has to be integrated properly to the application. Conceivable cooling systems are passive cooling methods without additional components, active air cooling systems and liquid cooling systems requiring a detached cooling circuit, including heat exchanger. Yet, the system's error-proneness increases with its complexity and therefore the hazard of a system failure becomes more likely.

D. Interconnection and Bonding

Using large cells reduces the effort of interconnecting, bonding and integrating the energy storage system into the vehicle package. However, flexibility decreases with the cell size, because existing space can be utilized less compared to systems with small cells. Pouch cells require a costly bonding and package integration due to the significant volume increase with rising cell temperature [10]. Regarding a predefined capacity of the energy storage system, the usage of small cells necessitates a higher number of cells connected in parallel by far.

The electric cell bonding is determined by the cell design, either via screwed contacts (prismatic design), clamping or ultrasonic welding (pouch design) or resistance welding (cylindrical design), see Fig. 2. Persistent electric, thermal and mechanical loads require a safe and long life fatigue strength bonding. The three techniques named have disadvantages when subjected to vibrations and shear stress.

Screwed connections reveal even with lock washers or plastic inserts in the Junker vibration test in accordance with DIN 65151 a clear preload force drop in just a couple of hundreds load changes [15]. Resistance welding bondings have at a number of four welding points a loadability of about 3.5N [10]. The experimentally recorded shocks in conjunction with the weight of a single cell result in loads of up to 5N which reveal a possible weakness and danger spot of the battery system.

With regards to safety requirements a distinct designation cannot be given since stresses vary with the field of application. However screwed connections have useful premises to dimension and to safeguard the connection to the occurring loads.



Soldering

Heat input into cell,
Limited vibration resistance



Clamping

Limited vibration resistance,
high contact resistance



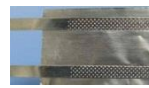
Resistance welding

High Bonding resistance, corrosion of
connection, limited vibration resistance



Screwed Connection

Danger of loose screws,
only available for large cells



Ultrasonic /Laser Welding

Heat input into cell,
only possible for large cells

Figure 2: Disadvantages of bonding technologies [10]

E. Battery Management System (BMS)

The Lithium Ion / Lithium Polymer technology with its advantages in long-term stability, power and energy density has a downside relating to explosions and ignition in case of misuse such as high voltages, high temperatures or high current loads. Electronic monitoring units are intended to protect the cells from hazardous conditions. They monitor cell parameters like voltage and temperature and calculates the state of charge (SOC) whilst taking the current load into account to ensure a safe state.

The BMS often is arranged in a master-slave-architecture where every subunit (battery module) is equipped with a BMS slave, who gathers all the module information. The data is transmitted to the BMS master unit that supervises the overall safety and communicates with the car control device and adjusts the cooling. A safety mechanism called pilot line can be looped through every BMS so that every component is able to directly actuate the electric contactor. This fall back level can help to ensure the safe state of the system.

IV. HAZARD ANALYSIS AND RISK ASSESSMENT ISO 26262

The third part of the ISO 26262 standard mentions a hazard analysis and risk assessment as a systematic approach for the development of a safety concept for electronic components. The focus is set to the malfunctioned behavior of electronic systems. Hazards caused by electric shock, fire, crashes, vibrations or other reasons is not in the scope of ISO 26262 unless these hazards result from the malfunctioning of electronic components [2]. Nevertheless the hazard analysis

and risk assessment highlights nonfunctional hazards that may influence the overall safety. The hazard analysis and risk assessment is a qualitative approach with the objective of detecting system risks and assessing the system or its subsystems according to automotive safety integrity levels (ASIL) [2]. TÜV SÜD defined a systematic analysis scheme of the hazard analysis and risk assessment on which the developed safety concept for electric storage system is based. A precondition of the shown scheme in Fig. 3 is a defined item definition.

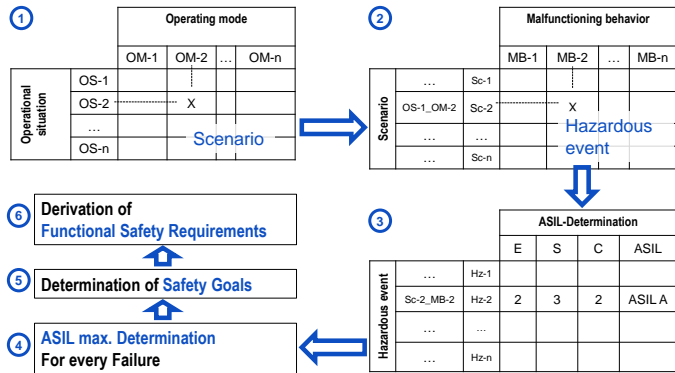


Figure 3: ISO 26262-3 scheme of TÜV SÜD

To develop a holistic safety concept for an energy storage system, both the functional and nonfunctional requirements acquired in the hazard analysis and risk assessment of ISO 26262 were taken into account. The nonfunctional requirements for safety during use cover the location of the energy storage system, cell design, mechanical influences such as shocks and vibrations as well as nonelectrical components.

A. Process of Hazard Analysis and Risk Assessment ISO 26262-3

The third part of the ISO 26262 describes the concept development of electronic systems. This process can be divided according to Loew et al. into six steps [7] which inherently match with the scheme shown in Fig. 3.

In the first step, all analysis necessary data such as application descriptions, system configuration and boundary constraints are gathered. Then relevant scenarios are set up by combining operation conditions with operational situations of the vehicle. The next step targets the preparation of possible malfunctions of all system components. Input data and expertise shall be considered to obtain a thorough list of all possible malfunctions. In the fourth step according to Loew et al. the scenarios are linked with the malfunctions to hazardous scenarios which are assessed by references to the following three factors:

- Frequency of the situation (Exposure E)
- Severity of possible threats (Severity S)
- Controllability by the driver (Controllability C)

Depending on the factors, each hazardous situation is assessed by three or four increments. The rating of the severity

of a possible threat ranges from S0 (no injuries) to S3 (life threatening injuries). Appendix A2 of ISO 26262-3 provides examples for the assessment that have been taken into account [1]. Subsequently, the fifth step determines the necessary risk minimization of every malfunction according to the assessed triple. Each of those names a certain classification of the ASIL which in its lowest characteristic is described as QM (Quality Management, no further risk minimization necessary) up to ASIL D (high requirements for risk minimization), see Fig. 4.

S	E	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

Figure 4: ASIL-assessment

The last step defines the safety goals for each individual function. This results in functional safety requirements for the system that can be allocated to different components in the following development process. The requirements serve as input for the development of the software and hardware of each component in accordance with ISO 26262.

B. Item Definition

The assessment begins with the definition of the system’s scope and the allocation of the system boundary. Hence, the list of all relevant components as well as all signals within the system and crossing the system boundary is performed. For the assessment of energy storage systems, multiple schematic diagrams beginning from superordinate groups to each component were issued. Fig. 5 shows the top of four levels.

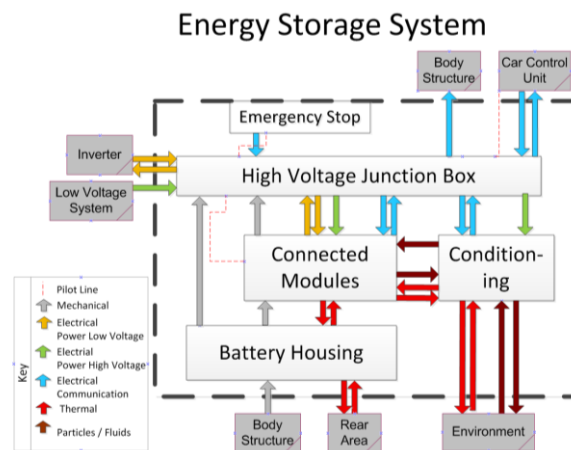


Figure 5: Signals within the energy storage system

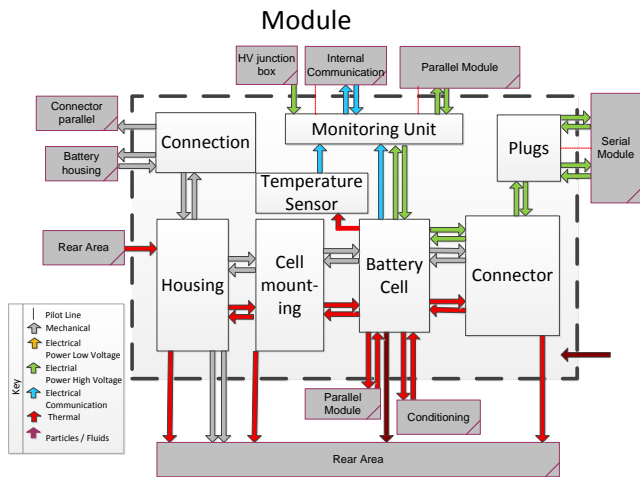


Figure 7: Signals of a module

The system boundary (grey dotted line) defines the energy storage system to the surroundings. The signals were divided into seven categories:

No.	Category	Description
1.	Pilot line	Signal to interrupt the high voltage circuit
2.	Mechanical	Mechanical loads (shocks, vibrations, ...)
3.	Electrical Power High Voltage	Energy signals for power transmission using high voltage potentials ($U > 60V$)
4.	Electrical Power Low Voltage	Energy signals for power transmission using low voltage potentials ($U < 60V$)
5.	Electrical Communication	Data and signal transmission
6.	Thermal	Exchange of thermal energy (Radiation, Convection)
7.	Particles/Fluids	Influence of gas, fluids, foreign bodies

Table 1: Signals of energy storage system

The analysis considers the mentioned signals for the component clusters *high voltage junction box*, *connected modules*, *conditioning* and *battery housing* as well as for the definition of malfunctions. Each component cluster has been structured into multiple levels down to the single components to obtain a detailed and clear view of the transmitted signals. Fig. 6 displays the component relations of the component cluster *connected modules*.

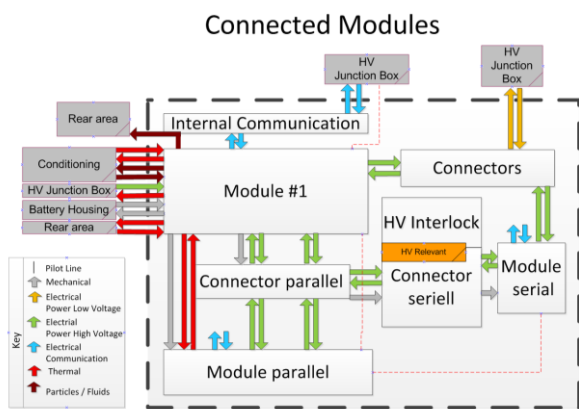


Figure 6: Signals within the component cluster connected modules

This approach takes advantages obtaining traceable pathway of all signals. For example, it is possible to track the signal *temperature of modules* from the *temperature sensor* to the *electronic monitoring unit module* via the *internal communication* to the *electronic monitoring unit master* that transmits the signal across the system boundaries to the car control device.

Fig. 7 illustrates that many different signals are initiated by the battery cell. Thermal signals are linked to *temperature sensor*, *connectors* and *cell mounting* as well as mechanical loads caused by vibrations between *connectors*, *cell mountings* and *battery cells*. At the same time, electrical signals for cell monitoring (*electronic monitoring unit module*) and the power signals (*connectors*) are relevant. The battery cell has a certain potential of different malfunctions that entitles the cell to be considered intensively in the assessment of the functional safety and the safety in use.

Table 2 shows the range of the item definition, the number of component functions as well as the amount of determined malfunctions.

Component cluster	Component(s)	No. Fct.	No. Mal-Fct.
Battery housing	Battery housing	6	6
High-voltage junction box	Isolation guard, electronic monitoring unit master, current sensor, fuses, contactor „Drive +“, contactor „Drive -“, contactor „pre“, contactor „DCDC“, Preload resistance, plugs, housing	44	62
Con-ditioning	Fan, air duct components	6	7
Emergency stop	Emergency stop	3	4
Connected modules	Internal data transmission, electronic monitoring unit module, connection, housing, cell mounting, connectors, plugs, temp. sensors, board connectors parallel, board connectors serial, HV-Interlock	34	57
28 components		93	136

Table 2: Scope of the hazard analysis and risk assessment

C. Scenarios and Hazardous Scenarios

By linking the six operational situations *subterranean garage*, *small streets*, *middle streets*, *large streets*, *highway* and *motorway* with 23 operational conditions, a total number of 21 relevant scenarios have been selected for further analysis. The scenarios display a realistic summary of the electric vehicle application throughout its life cycle.

The consolidation of the scenarios incorporates the frequency of the situations and its severity to limit the scenarios to the most relevant ones. Consultations with experts have been conducted and recorded. The relevant scenarios cover the four scenarios at stop (“parking, ignition off” to “vehicle ready, gear engaged, brake actuated”); slow/middle/fast driving (“rolling, acceleration, braking/regeneration, Stop and Go traffic, maneuver with full lock, constant driving”) and special situations (lifting platform).

A separate climatic classification was not realized but the influence of different temperatures, humidity and other environmental impacts have been considered by lining up the hazardous events and the ASIL assessment. The combination of the relevant scenarios with 136 malfunctions yield 3128 possible hazardous events. After detailed consideration, 142 hazardous events were selected since a large number of potential hazardous events have a similar threat potential.

D. ASIL-Assessment

The hazardous situations have been assessed regarding its potential hazard on the basis of the three factors E, S and C mentioned above by an expert committee of engineers with experience in lithium-ion cells, BMS, battery system design and field application and professionals in the methodological approach of hazard analysis and risk assessment. The assignment of ASIL to each malfunction gives a clear view of the most hazards that could counteract the safety of the battery system. Table 4 lists the major malfunctions that cause a threat to the overall safety.

<i>Malfunction</i>	<i>max. ASIL</i>
Destruction of housing	B
Possible threat of high voltages	C
Failure of cell monitoring	D
Unknown current load	QM
Interruption of HV circuit not possible	D
Overcharging	D
Insufficient cooling	A
Failure activation of emergency stop	B
Failure of data transmission	C
Destruction of cell mountings	C
Mechanical, electrical or thermal overload of cell	D
Tear off bonding, sense and sensor conducts	D
High temperatures in energy storage system	C

Table 4: ASIL-Assessment of major malfunctions

Electronic monitoring of the energy storage system is assessed to the highest safety classification ASIL D. This is justified by the importance of a correct monitoring of the cell status, especially voltage and temperature. Even the triggering of safety elements such as contactors or pilot line is of high importance to have a reliable disconnection of the loads from the battery system.

The accurate conditioning of the energy storage system contributes to a high operating safety and is of high significance to the overall safety, see table 4. Low temperatures below 15°C reduce the power provision and driving range due to sluggish electrochemical processes. High temperatures over 35°C on the other side hinder the power provision to prevent the battery cells from overheating [16]. Various components such as temperature sensors, fans and electronic components can contribute to this necessary state. A priori conceptual

decisions concerning the cooling principle and the arrangement of the fans have a high impact on the safety concept.

By additional consideration of non-electronic failure, the safety evidently is prejudiced by the mechanical stability of the system, the fans, the energy storage cells as well as the connectors and sense lines. The two above-mentioned components in particular have an enormous impact on the overall safety.

The battery cell being an electrochemical energy storage unit contains approximately eleven times more chemical energy than the stored electric energy [17]. That implies that an internal cell short circuit can release eleven times its electric capacity as thermal energy. Therefore, a significant safety hazard exists which prompts the discussion of cell size and the quantity of stored electrical energy per cell.

Vibrations may lead to internal short circuits within the battery cell or system [18]. The trigger is supposed to be impurities on the electrode active materials which cause a piercing of the separator under vibration. This leads to a cell short circuit causing a thermal runaway [19]. However, loosened connectors or tabs that connect cells to a bus bar are a significant hazard for external short circuits or overload for the cells. In 2008 a refitted Toyota Prius caught fire because of a loose connector [20].

With reference to the vehicle body, fatigue failure occurs predominantly near welded spots. The failure develops on significantly lower loads than the critical load of strength tests. The weak spot of a weld is its complexity. Its functionality is dependent on various parameters like residual stresses, welding point dimensions, material properties of the heat affected zone as well as on the materials, coatings and loads [21]. Corrosive mediums can augment this effect and have to be prevented. In summary, a safe, durable and low-vibrational bearing and connection is of great importance.

E. Determination of Safety Goals

According to the ASIL assessment, safety goals were derived for every malfunction. For reasons of clarity and comprehensibility, only an extract is listed below and a separation of functional and nonfunctional safety goals was made.

The main functional safety goals were determined as:

- High voltage circuit must be interruptible (ASIL B)
- Direct and indirect contact of high voltage components must be prevented (ASIL B)
- Predefined battery conditions have to be satisfied (ASIL C)
- Loads on the battery system are not allowed to exceed battery cell limit values (ASIL D)
- State of high voltage circuit has to be safeguarded by at least one element (ASIL D)
- All measureable cell data has to be monitored and used for failure detection (ASIL D)
- Incorrect current loads in case of short circuit or overload must be prevented (QM)

- Disconnection of loads from high voltage circuit must be possible (ASIL D)
- Thermal heating of cells may not exceed predefined values and must be monitored (ASIL D)
- Cell balancing must be monitored (ASIL A)

By focusing on further requirements for safety during use commonly to the functional safety aspects, a holistic battery safety concept can be developed by fulfilling the functional and nonfunctional safety goals.

- Vibrations have to be kept from the battery system (ASIL B)
- Resistance to piercing and electrical safety of the battery housing must be provided (ASIL B)
- Electric load of cells is permitted to harm cells (ASIL C)
- Internal short circuits or thermal runaways are prevented from harming people in or around the vehicle (ASIL D)
- Electrical connection of the cells is not allowed to be torn off or causing sparks (ASIL D)
- Cells may not overheat (ASIL D)
- Mechanical piercing of cells must be prevented (ASIL B)

The classification shows that there is a major need to consider nonfunctional aspects besides all functional requirements. A technically correct development sometimes is not sufficient due to fundamental deficiencies of state-of-the-art techniques. Therefore new approaches, for example for cell bonding or prevention of cooling, have to be discovered.

The hazard analysis and risk assessment reveals that safety depends on the battery concept determined by the safety goals. Changes or adaptations contributed retrospectively often cannot compensate mistakes in the development process. An example would be the position of the energy storage system in the package or the package of the conditioning fans.

The analysis was carried out according to ISO 26262-3 even though the considered system is not directly intended for serial automobiles. The conclusions and assessment have to be reconsidered for a serial application due to several high ASIL assessments that would cause enormous efforts for the development of the corresponding hardware and software within the ISO 26262 cycle.

V. DEVELOPMENT OF A SAFE ENERGY STORAGE SYSTEM

Regarding the acquired safety goals, a holistic concept for a safe energy storage system for micro electric vehicles was elaborated. The concept is guided by both functional and nonfunctional hazards revealed in the analysis. Beginning with the definition of the package to the reduction of hazardous stresses and the importance of the monitoring of each battery cell, the presented energy storage system shows conceptual, technical and electrical guidelines to ensure an overall battery safety.

A. Battery System

To guard the sensitive battery cells against intrusions, the battery system has to be located in a deformation-free area. The zone between the axis behind the front seats, which already has been recognized as optimal during the MUTE project [1], provides high protection in terms of front, rear and side impacts. Moreover, the battery system is not placed in the underfloor so that potential hazards from all directions are minimized.

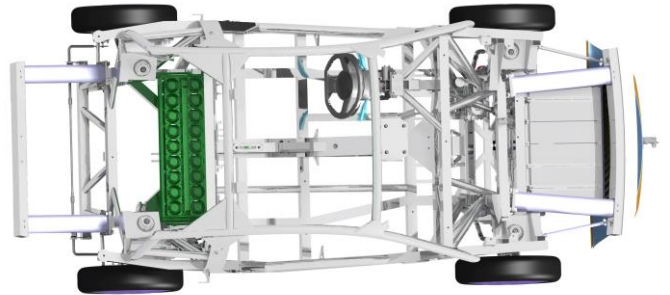


Figure 8: Package of the Battery System (green)

To protect the battery system from shocks, a vibration-damping bearing is expedient. Vulcanized machine footing with additional tear-off securing in the vertical axis absorb forces in all directions, decreasing the vibrations significantly.

The battery housing is built mainly of glass fiber reinforced plastic (GFRP) sandwich panels which are very stiff and electrically insulating. They are hold in place by an aluminum space frame. Hence, there is a high stability with simultaneously low weight.

The failure of the active cooling system, which has been conceptually selected for air cooling due to the low car classification, has to be prevented. Therefore, the air supply is diversified from a low number of big fans to one fan per module. Safety during use is maintained due to mutual use of air slots that allow the compensation of single failure of fans by surrounding modules' fans.

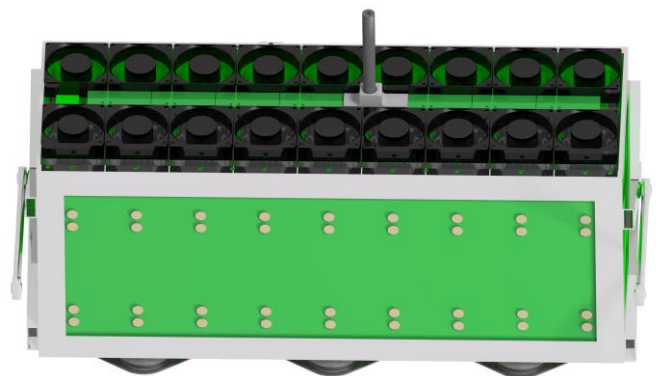


Figure 10: Diversification of air supply

The necessary high voltage components contactors, the current sensor, the precharge resistance, the isolation guard and all fuses are located in a high voltage junction box on top of the

battery housing. This positioning advantageously prevents the accessibility of unfused cables on outside. Furthermore an opening of the HV junction box automatically disengages the HV interlock. Two switches trigger the interruption of the HV circuit redundantly if the lid is opened.

In case of electric short circuits, several components can interrupt the high voltage circuit. Both the electronic monitoring unit master and the isolation guard are able to trigger the pilot line from system view. Additionally, the electronic monitoring unit slave possesses a separate pilot line to interfere independently.

To ensure the correct status of the HV circuit, both the positive and negative cables have contactors for redundancy.

B. Battery Module

Due to the energy signals, both the schematic figure of the energy storage system and its subsystems reveal, that the battery cell itself is of greatest importance when it comes to overall safety. Due to production-technical fluctuation in quality and possible internal failures over the life cycle cannot be eliminated completely, the 18650 small cell design was selected for a safe battery module. The usage of standardized cylindrical cells minimizes in consequence to its small energy content the severity of a possible cell failure. Moreover, 18650 cells have been established in production and development over the last decades, which ensure a high quality and safety of the single cell. The solid shell assures good mechanical stability, see Fig. 11. To obtain the demanded capacity of the system, several cells have to be connected in parallel. This benefits the reliability respectively the safety in use because the failure of single cells can be compensated by the other cells.



Figure 11: 18650-Cells on aluminum based circuit board

To prevent the thermal runaway of cells, every 18650 cell is fused individually. The application of aluminum based circuit boards allows an individual design of the parallel and serial interconnection. Furthermore, customized circuit board fuses can be applied to protect the cell from high current loads or to isolate a cell with an internal short circuit from the system, see Fig. 12. This requires a distinct sizing as well as a

specific board surface treatment to ensure a safe state in case of overload or short circuit [22].

Integrated sense wires are used to detect the triggering of the fuse and enable the cell monitoring unit slave to report a warning to the cell monitoring unit master that initiates power reduction.

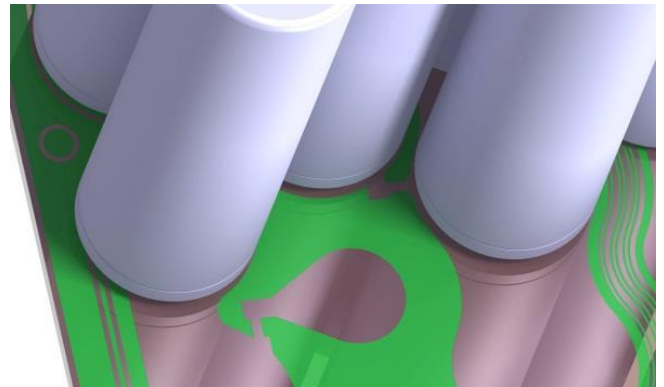


Figure 12: Individual cell fusing and sense cables

The malfunction *electrical connection of the cells is not allowed to be torn off or causing sparks* assigned to ASIL D has been safeguarded with an innovative bonding technology (*Conchifera*) that abandons a welding connection. Instead, a force-fitted method is applied to connect the cells electrically and thermally to the circuit board.

To obtain a vibrationless electric connection, a new bonding technology (*Conchifera*) has been developed. The cells are pressed to the aluminum based circuit board with a flexible, electrical conductive material in between, see Fig. 13. The flexibility of the material is developed to dampen relevant mechanical loads and shocks efficiently. Fluctuations in contact resistance can be eliminated through a defined composition of the material. A tear off of the connectors or the sense wires can be excluded, so cell monitoring and depiction of power can be maintained even under rough conditions which consequently results in benefits compared to other bonding techniques such as welding. Additionally, the process of connection can be performed easily and quickly compared to sequentially conducted welding or screwing processes.

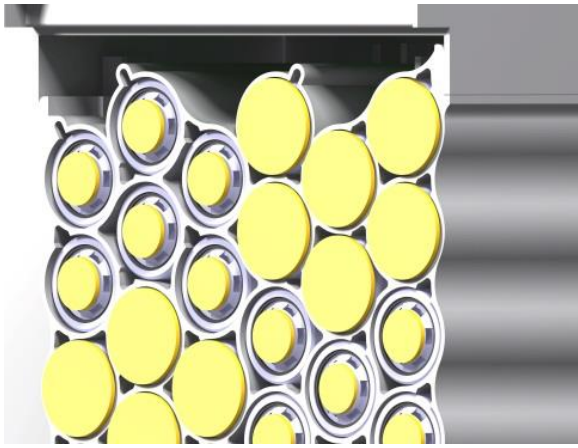


Figure 13: Flexible cell connection (yellow) on 18650 Cells

To ensure an optimal conditioning of the battery system, that has to be realized with an active air cooling, the cells dissipate internal heat via the positive and negative poles. The *Conchifera* bonding technology allows a unique thermal and electrical connection. The heat loss arising in the inner parts of the cells is conducted over the positive and negative pole through the flexible bonding material to the aluminum based circuit board. Since the heat transfer resistance in axial direction is only 1/20 of the radial resistance [24], the cooling of the 18650 cells is maximized. The on rushing cooling air dissipates the heat efficiently. The module therefore gains a homogeneous temperature distribution minimizing disadvantageous aging effects and increasing the power distribution of the battery system.



figure 14: Cooling of battery modules

Two temperature sensors are integrated in every module. Their data are evaluated by a redundant monitoring unit slave. In combination with the aluminum based circuit board, the exact temperature of the cells can be monitored. The distributed fans on each module are actuated by the monitoring unit slave. This allows an autonomous regulation of fan performance according to the module temperature. This concept can provide a homogenous temperature over the entire battery system, especially in large systems, where inner modules are surrounded by several heat sources.

Each module has an individual battery management system (slave) to monitor the battery data subvoltages, temperature and

SOC. It is a part of the master-slave-BMS-System which has obvious advantages in terms of surveillance and efficiency enhancement of battery systems [23]. The BMS slave in the module itself consists of two boards. The first BMS-board monitors the absolute limits of cell voltages and cell temperatures to ensure the overall safety. The second BMS board additionally offers intelligent functions such as temperature and voltage monitoring, adaption of the fan power according to the actual temperature, calculation of SOC and the communication to the BMS master. For safety reasons, both boards monitor the voltage and temperature simultaneously. In case of a critical cell status each board is able to trigger a pilot line which cuts off the load immediately to protect the battery module. This design of a two-layer BMS-Slave allows verifying the functionality of both boards and gives the BMS-slave a high safety thanks to its redundant structure.

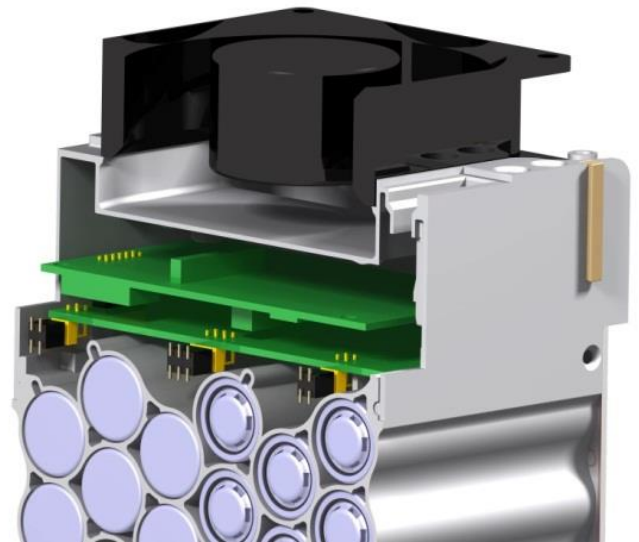


Figure 15: Dual Battery Management System in the Module

VI. ACKNOWLEDGMENT

The generation of the hazard analysis and risk assessment as well as the review was supported by Michael Hüttinger (TÜV SÜD) and the TÜV SÜD Battery Testing employees. The chassis investigation data was contributed by Andreas Schulze, Institute of Automotive Technology, Technische Universität München. Additionally the research of Dominik Pelerin and Adrian Melzer about functional safety was included into this paper.

- [1] Burda, Peter; Keil, Peter; Lienkamp, Markus; Jossen, Andreas: Development of a modular lithium-ion battery for a sub-compact electric vehicle. in: EVS26, Los Angeles, 2012
- [2] Norm ISO 26262-3: Road vehicles – Functional safety – Part 3: Concept phase, 2010.
- [3] Martin, Helmut; Winkler, Bernhard; Leitner, Andrea: Investigation of the influence of non-E/E safety measures for the ASIL determination. 39th Euromicro Conference Series on Software Engineering and Advanced Applications. CPS, 2013
- [4] Czichos H.; Hennecke M.: Ingenieurwissen. Springer-Verlag, 32. Auflage, Berlin 2004.

- [5] Börcsök, Josef: Funktionale Sicherheit. Grundzüge sicherheitstechnischer Systeme. 3. Auflage. Berlin: VDE-Verl., 2011.
- [6] Schlummer, Marco: Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie. Bergische Universität Wuppertal, Diss. 2012.
- [7] Loew, Peter; Pabst, Roland; Petry, Erwin: Funktionale Sicherheit in der Praxis: Anwendung von DIN EN 61506 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten. Heidelberg: dpunkt, 2010.
- [8] Hillenbrand, Martin: Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik Elektronik Architekturen von Fahrzeugen. Zugl.: Karlsruher Institut für Technologie, KIT, Diss., 2011. Karlsruhe Baden: Universität Karlsruhe Universitätsbibliothek, 2012.
- [9] Krüger, Richard; Ganzheitliche Sicherheitsbetrachtung am Beispiel von E-Fahrzeugen, Vortrag in: Safety in Transport, 2011, Braunschweig
- [10] Burda, Peter: Entwicklung und Auslegung von Energiespeichersystemen für Elektrofahrzeuge, München, Technische Universität München, Lehrstuhl für Fahrzeugtechnik FTM, Dissertation, 2014
- [11] Tesla Motors Inc. Internetzugriff: 14.01.2014. http://www.teslamotors.com/de_DE/models/features#/performance
- [12] Johannsen, Heiko: FIMCAR; Frontal Impact and Compatibility Assessment Research. Seventh Framework Programme, April 2012
- [13] Kampker, Achim, Vallée, Dirk, Schnettler, Armin: Elektromobilität: Grundlagen einer Zukunftstechnologie. Berlin. Springer 2013
- [14] Musk, Elon: Model S Fire, Blog. URL: www.teslamotors.com/de_DE/blog/model-s-fire, Zugriffsdatum: 16.,1.2014
- [15] Nord Lock GmbH; NORD-LOCK Bolt securing system: Technische Informationen. Produktinformation. Westhausen, 2010
- [16] Rugh, John; Pesaran, Ahmad; Smith, Kandler: Electric Vehicle Battery Thermal Issues and Thermal Management Techniques. SAE 2011 Alternative Refrigerant and System Efficiency Symposium. Scottsdale, Arizona USA, 2011.
- [17] Groß, René; Jossen, Andreas: Sicherheitsaspekte beim Testen von Lithium-Ionen Batterien. PDF von URL: www.basYTEC.de: Internetzugriff: 14.01.2014.
- [18] Doughty, Dan; Roth, E. Peter: A General Discussion of Li Ion Battery Safety. The Electrochem. Society. Interface. 2012, p. 37–44 .
- [19] Spiessberger, Christian, Tammer, Christoph: Partikeldetektion auf Elektroden für Lithium-Ionen-Batterien mit laserangeregter Thermographie. Thermographie-Kolloquium 2013, Vortrag 16. 2013.
- [20] Beauregard, Garrett: Report of Investigation: Hybrids Plus Plug in Hybrid Electric vehicle – prepared for: National Rural Electric Cooperative Association, Inc. and U.S. Department of Energy, Idaho National Laboratory, June 26, 2008.
- [21] Donders, Stijn; Brughmans, Marc; Hermans, Luc: The Effect of Spot Weld Failure on Dynamic Vehicle Performance. Sound and Vibration April 2005, p. 16-24.
- [22] Meisel, Peter, Rupalla, Manfred: Entwicklung eines miniaturisierten Schmelzsicherungssystem für moderne Leiterplatten mit abgestimmtem Auslösungsverhalten zur gleichzeitigen Verbesserung der Gerätesicherheit und Verinderung des Bleieintrages in die Umwelt. Abschlussbericht, DBU Deutschen Bundesstiftung Umwelt, AZ 27125-21/0. Witten,2010
- [23] G. Walder, C. Campestrini, M. Lienkamp, and A. Jossen, "Functionality and behaviour of a dual Kalman Filter implemented on a modular battery-management-system," in Conference on Future Automotive Technology: Focus Electromobility. München, 2013.
- [24] S. Al Hallaj, H. Maleki, J.S. Hong, J.R. Selman: Thermal modeling and design considerations of lithium-ion batteries. In: Journal of Power Sources 83 (1999), 1-8
- [25] Kim, Gi-Heon, Smith, Kandler, Pesaran, Ahmad: Lithium-Ion Battery Safety Study Using Multi-Physics Internal Short-Circuit Model, in: 5th International Symposium on Large Lithium-Ion Battery Technology and Application in Conjunction with AABC09, 2009, Longbeach, CA, USA.