STALLION Handbook on safety assessments for large-scale, stationary, grid-connected Li-ion energy storage systems

Arnhem, March 2015

Author(s): Nynke Verhaegh (DNV GL), Jos van der Burgt (DNV GL), Alma Tiggelman (DNV GL), Grietus Mulder (VITO)

STALLION Project: "Safety testing approaches for large Lithium-ion battery systems"(1st of October 2012 to 31st of March 2015)

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° ENER/FP7/308800/STALLION.

LIST OF ABBREVIATIONS

AC	alternating current
BESS	battery energy storage system
BMS	battery management system
MBMS	module-level BMS
PBMS	pack-level BMS
SBMS	system-level BMS
CT	current transformer (i.e. current sensor)
DC	direct current
FMECA	failure mode, effect and criticality analysis
LRU	line-replaceable unit
LV	low voltage
MV	medium voltage
PCM	phase-change material
PTC	(resistance with) positive temperature coefficient (i.e. the resistance value increases when its temperature increases)
RPN	risk priority number
SIL	safety integrity level
SOH	state of health
SOC	state of charge
VT	voltage transformer (i.e. voltage sensor)

TABLE OF CONTENTS

1 INTRODUCTION

This Handbook is meant to guide interested parties through the relevant safety aspects of large-scale, stationary, grid-connected, Li-ion battery, energy storage systems. This Handbook is a final objective of the EU FP7 STALLION project, in which a safety assessment has been performed for a stationary, large-scale, grid-connected Li-ion storage system.

This document consists of the following sections:
Chapter 2 addresses the safety aspects of Li-ion batteries. The STALLION project is introduced (2.1), the importance of safety assessments for Li-ion systems is elucidated (2.2), and examples of (demonstration) projects with stationary, large-scale, grid-connected Li-ion storage systems are described in (2.3).
Chapter 3 introduces the STALLION method for the failure mode, effects and criticality analysis (FMECA). An introduction into the FMECA methodology is given in (3.1). The FMECA starts with a system description for all levels (3.2). Then failures are identified per component on each level (3.3). Each system design contains mitigating measures to reduce these failures (3.4). An FMECA exerts a quantification of the failures by ascribing a severity and probability to each failure. This is explained in (3.5). Additional mitigating measures are presented in (3.6). Finally (3.7) focuses on the outcomes of the STALLION safety assessment of large-scale, stationary, grid-connected, Li-ion battery, energy storage systems.
Chapter 4 contains a summary, including conclusions and recommendations for the user of this handbook.

2 LI-ION BATTERY SAFETY ASSESSMENT

In this chapter, the importance of a safety assessment for large-scale Li-ion systems is discussed. This is done with the aid of several examples of incidents with these systems, but also several projects are presented that show the feasibility of safety of these systems. After a short introduction about the STALLION project and the objective of this handbook, the need for a safety assessment is explained. In the final paragraph of this chapter, several projects are described that include a large-scale Li-ion system.

2.1 Introduction into the STALLION project

The EU FP7 project STALLION considers large-scale (≥ 1MW), stationary, grid-connected lithium-ion (Li-ion) battery energy storage systems. Li-ion batteries are excellent storage systems because of their high energy and power density, high cycle number and long calendar life. However, such Li-ion energy storage systems have intrinsic safety risks due to the fact that high energy-density materials are used in large volumes. In addition, these storage systems are most likely situated in or near residential areas. Thus it is of utter importance to guarantee the safety and reliability of this emerging application for the Li-ion battery technology.

Therefore, the STALLION project has performed a risk assessment based on a Failure Mode, Effect and Criticality Analysis (FMECA). Parts of the risk assessment performed in STALLION are used as examples throughout this handbook, the full exercise can be found in (1). This exercise was meant to identify the most critical safety risks. In the rest of the project, test protocols and system improvements have been investigated to reduce the risk of the system. There was a close collaboration with another EU project, the STABALID project (2). In the collaboration of STALLION and STABALID test procedures were developed. At the end of the project the risk assessment has been redone in order to see the impact of the proposed improvements, this exercise can be found in (3).

A final objective of the project is the publication of a Handbook describing the systematic risk assessment methodology for large scale stationary grid connected Li-ion storage systems as developed within STALLION. This Handbook will be presented to targeted audiences such as municipalities and other local authorities, end-users such as distribution network operators, or system integrators by dedicated training.

2.2 Importance of safety assessment of large-scale Li-ion battery systems: unfavorable conditions

Li-ion batteries are excellent storage systems because of their high energy and power density, high cycle number and long calendar life. As a consequence, all lithium-ion batteries entail hazards that arise when the battery is used outside of its safe operating area. These hazards become more severe in larger battery systems. Therefore, Li-ion battery systems require effective management systems to ensure that uncontrolled release of that energy does not occur (4).

Li-ion batteries are used in a large scale in consumer electronics, almost every laptop and mobile phone contains a Li-ion battery. These applications have proven to be relatively safe, due to the small size of the batteries and the maturity of these applications. However, large Li-ion batteries have not yet been applied on a large scale and little is known about their risks.

Although safety and reliability of Li-ion cells increase continuously, so do the density of the stored energy and the power capability. Therefore Li-ion batteries are also developed for applications such as electric vehicles and grid support. These are systems with significantly higher power and energy densities, which may lead to higher and more severe potential hazards if things go wrong. Therefore these larger energy storage systems require development of appropriate management systems and new standards.

Misuse or abuse of a battery may lead to fire, explosion, release of toxic and flammable substances, and electric arc and shock. Therefore there is a need to use batteries in a controlled manner and to prevent abuse. This is why the battery management system (BMS) has to be present, which should prevent the battery from being misused and mitigate hazards that arise with a severe event such as

exposure to extreme heat. A good BMS measures the battery parameters, determines the condition of the battery and controls the system to ensure that it operates as desired. However, a good BMS is not sufficient to ensure a safe battery system. Battery safety involves several aspects within different layers of the battery system. The extent to which a battery can withstand abuse varies widely for different types. Several abuse conditions exist, which will briefly be discussed below.

When a battery is charged to a state of charge (SOC) greater than 100%, *overcharge* occurs. Overcharge causes degradation of the chemistries inside the cell which can lead to thermal runaway*, cell swelling, venting of gases, and other severe events. Vice versa, when a cell is discharged beyond 100% depth of discharge, *over-discharge* occurs. This results in a rapid fall of cell voltage or even polarity reversal, causing potential failure of management electronics. Over-discharge can lead to significant internal cell damage which results in safety risks. Due to the self-discharge of the battery cell, even when it is not connected to its load, over-discharge is particularly a challenge. Even overcharge or overdischarge of a single battery cell in a large system can lead to dangerous situations because thermal events can propagate from one cell to another. *Overcurrent* is an excessive current during charge or discharge, causing overcharge or overdischarge and leading to the same types of reactions. Overcurrent also leads to internal heating, which may lead to high temperature conditions (4).

Exposure to *high temperatures* can lead to thermal runaway*. High temperatures can be caused by high ambient temperatures, exposure to sources of heat or battery overload (excessive charge or discharge power levels). An incident illustrates this risk. A Boeing 787 passenger flight from Japan Airlines caught fire in its lithium-ion batteries while on the ground in 2013. This happened because Boeing's safety assessment did not consider the possibility of cell-to-cell fire propagation as a result of an internal short circuit. Also, because the battery description did not contain a specific requirement for battery behavior with a cell in thermal runaway, the need for a thermal runaway qualification test appeared less urgent to Boeing. This also shows that safety measures to prevent cell-to-cell fire propagation are valuable. Luckily, no injuries or fatalities were caused by this incident (5).

Figure 1 Fire incident Japan Airlines

On the other hand, most lithium-ion batteries have limited performance at *low temperatures*. Charging at low temperatures may cause plating of lithium on the anode which leads to irreversible capacity loss and possibly internal short circuit.

* Thermal runaway is a process where an increase in temperature changes the internal chemical conditions in a way that causes further increase in temperature, leading to venting of cell contents, fire, or explosion.

Penetration of foreign matter and other *internal cell defects* may cause internal short circuits which can cause heating. The risks associated with these defects can be minimized with advanced manufacturing techniques. Furthermore, *mechanical damage* to batteries can cause internal or external short circuit leading to venting of cell contents, thermal runaway or fire, and shock hazards due to electric arcing. Ensuring safety against mechanical defects is complex with no certainty of preventing a dangerous condition. An incident with a Tesla model S electric vehicle illustrates the importance of this issue. The car caught fire after penetration of a metal object into the battery pack. Luckily, the fire was contained by the separation units inside the car, which shows the benefits of such a safety measure. The car gave a safety risk alarm well before the actual incident. The driver was asked to put his car at the side of the road by the board computer. Only one battery compartment caught fire and no flames came into the driver's compartment. The firefighters however cut open the steel plate covering the battery pack to apply water for extinguishing the fire. Due to this action flames came upwards and into the car, worsening the fire as the fire could spread inside the vehicle. This also demonstrates that although the battery system can be very safe, external factors such as objects and people's actions are also very important aspects to consider (6).

Figure 2 Fire incident Tesla car

The probability of most failure modes associated with lithium-ion batteries increases with *age*. In addition, lithium-ion battery chemistries are much less tolerant to abusive conditions such as overcharge, over-discharge, high temperature and excessive current as compared to other battery types. Furthermore, there is a wide variety of materials and electrochemistries used in lithium-ion batteries, each having their own implications for performance, lifetime, and safety. This variety of materials has a significant impact on the requirements of battery management systems and further complicates their development.

Figure 3 Fire incident at recycling site G&P Batteries

On top of these hazards, large lithium-ion battery systems are often placed within or near a residential area. This poses additional challenges for safeguarding the safety of nearby residents and/or employees.

The issues mentioned above mostly apply to the stage in which the Li-ion system is in operation. However, there are also risks related to other stages over the lifetime of the battery, i.e.: storage, transport, installation, commissioning, operation, maintenance, repair, decommissioning and recycling. These stages can have different risks due to different circumstances. Therefore, it is also important to perform risk

analyses in different life stages of the system. A good example is an incident that occurred at the recycling company G&P. This company had a fire in 2014 due to lithium-ion batteries. A spokesperson for the company said that the fire broke out when workers were sorting through damaged waste batteries which involved 700 kg of material. As it contained lithium waste batteries, the material had been taken to a safe lithium waste battery store area to be dealt with, and while this was happening it is believed an internal short circuit in one of the cells caused the fire (7). Another example which underlines the importance of assessing risks in different life stages of the system is an incident which occurred while transporting thousands of Li-ion batteries. In 2010, a cargo airplane of UPS Airlines crashed near Dubai due to fire of a cargo container with thousands of lithium batteries. The two shipments of lithium batteries were not declared as hazardous materials, which should have been the case. Therefore the batteries were not handled in the way they should have been handled, decreasing the safety. Unfortunately, both pilots did not survive the crash (8).

Figure 4 Crash site of cargo airplane in Dubai

Although these accidents seem quite catastrophic, there are also a number of projects which prove that the application of large scale Li-ion systems can be safe. A selection of these projects will be discussed in the next section.

2.3 Examples of projects with large-scale Li-ion systems

Although large scale Li-ion systems are not yet commercially produced, there are several demonstration projects with these systems. These exist mainly in the USA, but also in Europe and other continents. Some of these projects are mentioned in this section.

In 2014, the installed capacity worldwide for electrochemical storage systems was 518 MW according to the DOE Global Energy Storage Database (9). Although this is only a marginal fraction of the total installed capacity for pumped hydro storage (over 140 GW worldwide in 2014), it is a growing field since another 639 MW was planned at the same time (either under construction or announced). The major part of this installed electrochemical storage capacity consists of Li-ion systems, that is 256 MW (and 388 MW was planned). The USA is leading with 116 MW installed Li-ion capacity and 193 MW planned capacity.

Because STALLION is a European project, the remainder of this paragraph will focus on European projects. For more information on the discussed projects and other projects, the DOE database can be addressed (9).

2.3.1 Nice Grid project

Nice Grid is the first smart solar-energy district demonstration project to be conducted in France. The objective is to develop a smart electricity grid that integrates a high proportion of solar panels, energy storage batteries and intelligent power meters installed in the homes of volunteer participants. The Nice Grid project will test several types of lithium-ion storage technologies and will involve the deployment of 2.7 MWh of batteries installed at three distinct levels of the electricity distribution network. One 560 kWh/1.1 MW lithium-ion battery at the Carros primary substation, that will link ERDF's distribution network to RTE's transmission network; three 106 kWh/33 kW lithium-ion batteries installed in medium/ low-voltage distribution substations, that will control peak generation of PV installations and manage peak demand periods, while also allowing for operation in islanded mode; several 4 kWh/4.6 kW lithium-ion batteries installed in volunteering customers' homes to facilitate load shedding (10).

2.3.2 WEMAG Younicos Battery Park

In Schwerin, Germany a large grid-connected battery park of 5 MWh is constructed. This battery park serves in the primary frequency regulation market, thus helping to balance the grids and integrate green energy. This project claims to be Europe's first commercial battery park (11).

Figure 5 WEMAG Younicos Battery Park

2.3.3 The Zurich 1 MW BESS

The Utility of the Canton of Zurich (EKZ) and ABB have installed a 1 MW battery in Dietikon, Switzerland. The battery can store up to 500 kWh and is the largest of its kind in Switzerland. The energy storage system is connected to the low and medium voltage grid of EKZ and its surroundings include a photovoltaic plant, an office building and electric vehicle charging stations, allowing to test various different smart grid applications. The battery cells were provided by LG Chem and are located inside an air conditioned outdoor container. The various applications investigated include primary frequency control, peak shaving, microgrid control including the office building, and voltage control using active and reactive power supplied by ABB's converter (12).

Figure 6 The Zurich BESS

2.3.4 Younicos and Vattenfall Project

In a joint pilot project, Younicos and Vattenfall have commissioned a large-scale battery for integration into the European electricity balancing market. Since the end of 2012, a 1 MW sodium-

sulfur (NaS) battery based at the Younicos headquarters in Berlin-Adlershof balances short-term fluctuations in the power grid. This is the first time a battery is employed in maintaining the mains power frequency of the transmission system operator 50 Hertz Transmission GmbH (Germany). Today, the hybrid battery consists of a 1 MW/6 MWh sodium sulfur unit and a 200 kW/200 kWh lithium-ion unit (13).

2.3.5 Bosch Braderup ES Facility

One of Europe's largest hybrid batteries stores the electricity generated at a community wind farm in the northern German municipality of Braderup and feeds it back into the power grid as needed. Bosch and the community wind farm run by BWP Braderup-Tinningstedt GmbH & Co. KG brought the stationary energy storage facility on-line on July 11, 2014. Bosch designed, built and operates the hybrid system, which has a total capacity of 3 MWh. The energy storage plant consists of a 2 MWh lithium-ion storage unit and a 1 MWh vanadium redox flow battery (14).

Figure 7 Bosch Braderup ES Facility

2.3.6 Orkney Storage Park

The Orkney Storage Park is an energy storage system demonstration project. It is connected to the distribution grid of UK's Orkney Islands, which has a high penetration of renewable energy. The goal of the project is to demonstrate power supply stabilization in the region by introducing containers which contain large capacity energy storage systems using Li-ion rechargeable batteries. The whole system has a power output of 2MW. When there is too much renewable energy, exceeding the export capacity of the cable to the mainland, the energy storage system will import part of the excess energy, reducing the need to constrain renewable generation on the islands, by reducing or stopping generator export (15).

Figure 8 The Orkney Storage Park project

2.3.7 Smarter Network Storage

The Smarter Network Storage (SNS) project claims to carry out a range of technical innovations to tackle the challenges of the transition to low-carbon and facilitate the adoption of energy storage. It demonstrates storage across multiple parts of the electricity system, outside the distribution network.

The goal is to determine the cost effectiveness of storage and with that to provide a more sustainable, efficient and flexible way to reinforce electricity networks (16).

Below, an overview table is given of the seven projects that are discussed in the previous sections.

Table 1 Overview of the discussed projects in this paragraph

Name	Location	Application	Power [kW]	Capacity [kWh]
WEMAG Younicus Battery Park	Schwerin Germany	Primary control	5000	5000
Nice Grid project	Carros, France	Smart grid	1100/33/4.6	2700
The Zurich 1 MW BESS	Zurich, Switzerland	Grid support	1000	500
Younicos and Vattenfall project	Berlin, Germany	Frequency regulation	200	200
Bosch Braderup ES Facility	Braderup, Germany	Transmission Congestion Relief Onsite Renewable Generation Shifting Frequency Regulation	2000	2000
Orkney Storage Park	Orkney Islands, United Kingdom	Demonstration of power supply stabilization	2000	500
Smarter Energy Storage	Leighton Buzzard, United Kingdom	Support security of supply, investment deferral, ancillary services	6000	10.000

3 FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS

In this chapter, the failure mode, effects and criticality analysis (FMECA) to assess risks will be explained. This will be done with the aid of examples from the STALLION project. Before the FMECA is explained in detail, an introduction is given about this risk assessment method.

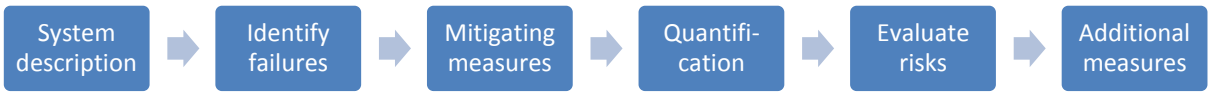
3.1 Introduction on FMECA

In general risk analyses are performed to identify potential risks, so that mitigating measures can be taken when necessary. Many methods for (quantitative) risk analysis exist, such as Hazard and Operability Study (HAZOP), Preliminary Hazard Analysis (PrHA), Probalistic Risk Analysis (PRA), etc. These methods are partly similar to each other but all have their own properties.
In STALLION the Failure Mode, Effect, and Criticality Analysis (FMECA) is chosen as the risk assessment method. FMECA is a roadmap for a risk analysis to assess and evaluate a system. It comprises three assessment criteria: severity, occurrence and detectability. Severity is the maximum possible level of danger, damage or injury that may occur. Occurrence is the frequency or probability of failures, i.e. the likelihood that the failure will occur. Detectability is a measure of the likelihood that the failure will be detected before it has catastrophic effects.
FMECA is the most widely used risk analysis technique in the initial stages of product/system development. FMECA is chosen because of its thoroughness and structured nature as compared to other risk analysis techniques and because of its reliability. Also, the concept and application of this method are relatively easy to learn. Furthermore, FMECA makes evaluating even complex systems relatively easy to do. Drawbacks may be that it is tedious, time-consuming, expensive, and that it is easy to forget human errors in the FMECA. (17)

FMECA is a technique used to identify, prioritize and eliminate potential failures of the system. Therefore a dedicated expert group should be involved who together identify and quantify the failures of the system under study. This expert group should ideally contain a variety of ‘experts’ such as designers, manufacturers, integrators, operators to have a complete picture of the system and its application during all stages of its lifecycle.
The outcomes are relative values for risks, so that they can be compared. It has to be noted that the FMECA does not result in absolute numbers of risks, i.e. the outcomes of different FMECAs cannot be easily compared. It is a technique to resolve potential problems in a system before they occur. In FMECA, failure modes are systematically identified for as many components as possible and on different levels within a system. The effects that these failures may have on the whole system are also investigated. Additionally, FMECA can be used to chart the probability of failure modes against the severity of their consequences. Thereafter, measures to mitigate the effects of the failures on the system can be identified. As mentioned before, it is important to identify risks within different stages of the lifetime of a system (transport, commissioning, operation, etc.). In this Handbook the FMECA will be explained with examples from the operational stage.

There are two approaches for an FMECA: the bottom-up and top-down approach. The *bottom-up approach* is used when a system concept has been decided. Each component on the lowest level is studied one-by-one. The analysis is complete since all components are considered. The *top-down approach* is mainly used in an early design phase before the whole system structure is decided. This analysis starts with describing the main system functions – and how these may fail. Functional failures with significant effects are usually prioritized in the analysis. The top-down approach may also be used on an existing system to focus on problem areas. The bottom-up approach will be used in this handbook to explain FMECA.

In short, the steps in a bottom-up FMECA are: describing the system and its potential failures, quantifying these failures and comparing the outcomes of the quantification. In the remainder of this chapter, these steps are explained in more detail. These steps can be represented in the following blocks:



1. System description

Define the scope of the system, what is considered to be inside the system and what is outside of the system under study. Define system specifications: application, services, size, rate of charge and discharge, capacity, power output, lifetime, etc. Identify different system levels, components within these levels and functions of the components. This step will be elaborated in paragraph 3.2.

2. Identify failure modes

Identify all possible failure modes for each component. The expert group evaluates what happens in case of malfunctioning components and formulates what the causes and effects are. This will be explained in more detail in paragraph 3.3.

3. Identify present measures

Several measures (prevention, detection, mitigation) to enhance safety are integrated in a large-scale battery system in any case, these are measures which are usually already in the system design. These measures need to be identified so that they can be taken into account in the risk analysis. The step of identifying measures will be described in paragraph 3.4.

4. Quantification of failures

Severity, occurrence and detectability are quantified for each failure mode with the expert group. This is a difficult process because quantification will largely be based on expertise especially when historical data is not available. This step will be further elaborated in paragraph 3.5.

5. Evaluation of risks

After the quantification of important parameters, the risks can be compared and evaluated. This is discussed together with the quantification in paragraph 3.5.

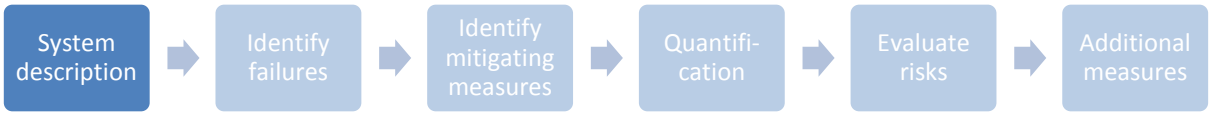
6. Take additional mitigating measures

When risks are known and their gravity is recognized by the quantification process, appropriate additional measures can be taken to mitigate part of the risks. This step is discussed in paragraph 3.6.

As mentioned before it is essential to involve a **group of experts** in the whole process in order to do a complete and correct analysis.

In the following sections, the above mentioned steps will be discussed in more detail together with examples from the STALLION project.

3.2 System description



Large battery storage systems, such as grid-connected storage, contain various components besides the battery cells themselves, including converters, switches, sensors and actuators. These large systems also incorporate sophisticated electronics and software that together measure the battery parameters, determine the condition of the battery and control the system to ensure that it operates as desired. This electronic system is called the battery management system (BMS). Many modern BMSs are expected to do more than monitor battery condition and calculate performance data, such as measure data from additional sensors and inputs, and control actuators and outputs which drive auxiliary functions. Systems may use the BMS to monitor temperature sensors throughout the system and control heating/cooling devices to maintain the appropriate temperature. It is also common for the BMS to control contactors and relays to maintain safety by disconnecting the battery when necessary.

In order to perform a risk assessment, the specifications of the battery system have to be defined. Systems specifications are for example application, services, size, rate of charge and discharge, capacity, power output, lifetime, etc. In STALLION a fictional system is described, which gives a good example for the different specifications that have to be known. The system considered in STALLION is a grid-connected energy storage system that supports the operation of a 2 MW PV plant. The system contains battery cells with lithium iron phosphate cathodes (which are intrinsically safer than e.g. lithium cobalt oxide cathodes) and graphite anodes. It is assumed that the storage system must be able to supply power at its maximum power (design value) for 15 minutes and will then gradually ramp down within one hour. The maximum storage capacity for this application is defined as an energy supply at the maximum power of 2 MW during approximately 45 minutes, which translates into an energy content of about 1650 kWh (including a 10% safety margin). The PV plant is assumed to be connected to the medium voltage grid via a step-up transformer. The storage system should have a three-phase 400 V AC converter output, which corresponds to a storage system with a minimum voltage of 560 V DC. For more details on the system design is referred to the extensive report about FMECA of STALLION (1).

In the next sections different levels (cell, block, module, pack and system) of the large-scale, stationary, grid-connected Li-ion battery system are described. For each level the corresponding components and their functions are listed, and the design and electrical wiring diagram are given in a schematic drawing. It is emphasized that this is not an existing system, but just a hypothetical generic storage system to guide the reader through the risk assessment methodology applied within STALLION. The design of each storage system should reflect the precise system requirements (control, lifetime, application, customer requirements, etc.) and will depend on the battery supplier.

3.2.1 Battery cell

The smallest storage component is a battery cell. The Li-ion cell is an electrochemical storage unit which consists of an anode, cathode, electrolyte, separator and enclosure, see Figure 10 for the example from STALLION. Both electrodes (i.e. anode and cathode) are coated onto a metal foil that acts as a substrate and current collector. They contain active material that stores lithium, substances to increase conductivity of both Li-ions and electrons and binders and other materials to provide structural integrity and good adhesion to the metal foil. The separator is a porous polymer film used to separate the two electrodes while providing a barrier through which lithium ions can travel. The entire cell must be enclosed in a container which prevents loss of the electrolyte and contamination. The most common shapes of a battery cell are: cylindrical, prismatic (used for small devices) and pouch (see Figure 9). During charging Li-ions migrate away from the cathode towards the anode and, vice versa, during discharge Li-ions migrate towards the cathode. The electrolyte serves as conductor during these processes.

Figure 9 Consecutively, cylindrical battery cells, a prismatic cell and a pouch cell.

The selection of the materials used in the two electrodes, as well as the composition of the electrolyte is referred to as the battery chemistry. However, the term “battery chemistry” most often refers to the choice of cathode material. Generally, the anode is often made of carbon and the cathode of a lithium metal oxide or phosphate. The exact composition of the materials has various possibilities and depends on the manufacturer. It is important to note that the choice of both anode and cathode materials has significant effect on battery behavior in normal *and abnormal* conditions.

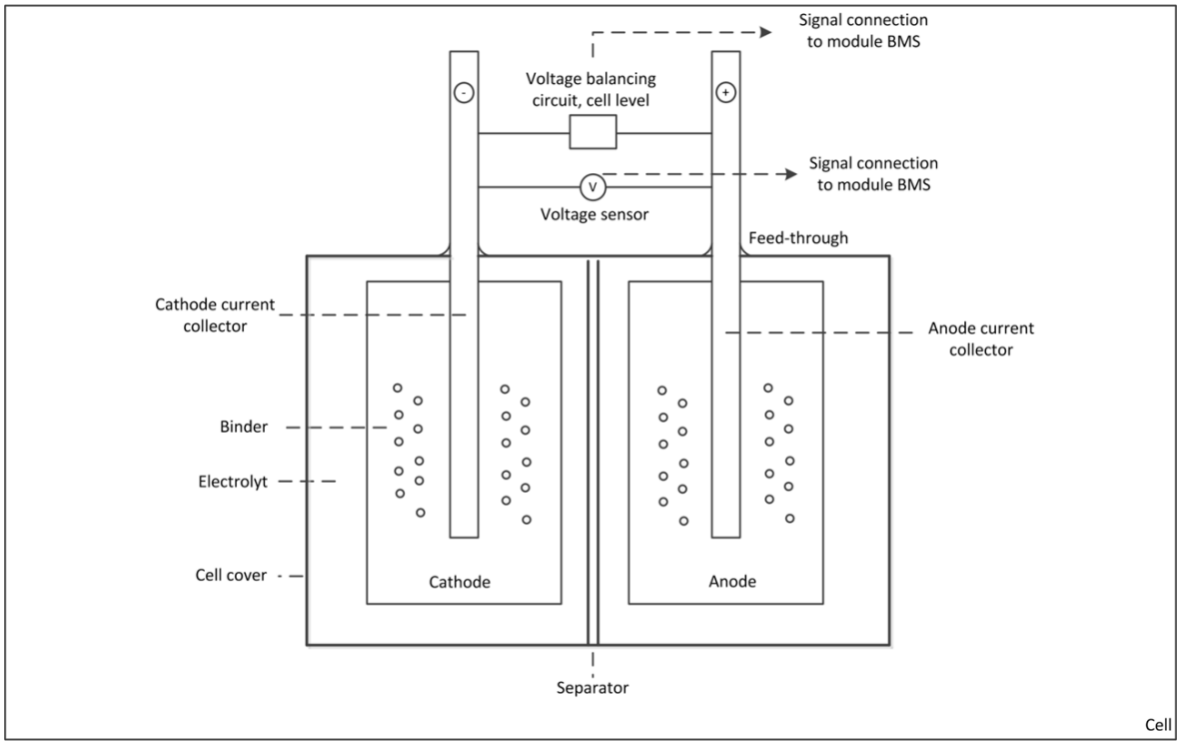


Figure 10 Schematic drawing of battery cell in STALLION

The cathode material of a lithium-ion battery cell is in general sensitive to very low and very high temperatures. When exposed to very low temperatures the cathode material is unstable (i.e. it can easily undergo chemical changes). Too low temperatures may result in internal shorts and too high temperatures may result in a burst of the cell. Therefore, the cell temperature has to stay within safe limits. This is monitored with temperature sensors[†] around the cells, connected to the BMS. The anode material (graphite) is in general very dangerous when a fire occurs because it is more flammable as compared to other anode material. Furthermore the protecting layer formed on top of the anode (SEI) is sensitive to elevated temperatures as well. Destruction of the SEI may lead to decomposition of the electrolyte and to the burst of the cell. The electrolyte is a lithium salt in an organic solvent, which may produce toxic and flammable gasses when an outburst of the cell occurs. Each cell should have a voltage sensor connected to the battery management system (BMS) so that all cell voltages stay within safe operating values and the system can balance (equalize) the cell voltages (4).

It should be noted that no battery cell is exactly the same in terms of capacity and self-discharge, therefore the state of charge of a number of connected cells which have all been exposed to the same current profile is not equal. This is why the BMS needs to have the cell balancing function.

In Table 2 the components of a battery cell and their functions are described. A schematic drawing of the battery cell as used in STALLION can be seen in Figure 10.

[†] In general, there is not one temperature sensor for each cell. In this system, a temperature sensor at the block level is assumed, see the next section.

Table 2 Battery cell components and their functions

Battery cell	
Component	**Function**
Cathode	Li-ions migrate towards cathode during discharge
Anode	Li-ions migrate towards anode during charge
Cathode current collector	Current collection: during charge current flows from anode towards cathode
Anode current collector	Current collection: during discharge current flows from anode towards cathode
Feedthroughs	Transmit current through a hermetic seal, provide a hermetically sealed environment inside the cell
Binder	Material in electrodes that provides cohesion of the electrode foils
Separator	Allow permeation of Li-ions and prevent short circuit
Electrolyte	Transport of Li-ions between cathode and anode
Voltage balancing circuit	Adjust the voltage of the cell
Cell cover	Prevent the electrolyte from reacting with moisture and air, and to ensure the integrity and functionality of the cell
Voltage sensor	Measure the cell voltage
Signal connections to module BMS	Signal transfer between cell and module BMS
Overpressure valve (in pouch cells, the pouch cover sealing acts as the overpressure valve)	Release of gas from defect cells to avoid dangerous overpressure

3.2.2 Battery block

In a battery block several cells are connected in series and/or in parallel. When placing cells in series, the voltage level becomes higher because the voltages of the individual cells sum up; the current remains the same in series connection. When cells are placed in parallel connection, the currents of individual cells sum up and the voltage level remains the same. A number of cells are connected in series and/or in parallel in a battery block to obtain the desired voltage and current level. Some blocks may have a combination of serial and parallel connections. It is important to use the same cell type and size, this is especially important in a serial configuration. Each battery block should have a temperature sensor connected to the BMS in order to monitor the temperature.

The block in the STALLION system set-up is not according to the definition of a block in battery standards like draft IEC 62620 ('Secondary cells and batteries containing alkaline or other alkaline non-acid electrolytes - Large format secondary lithium cells and batteries for use in industrial applications'). There it refers to a group of cells connected together only in parallel configuration.

In Table 3 the components of a battery block and their functions are described. A schematic drawing of the battery block as used in STALLION can be found in Figure 11.

Table 3 Battery block components and their functions

Battery block	
Component	**Function**
Cell	Electrochemical energy storage unit
Block cover including feedthroughs	Hold a number of cells together
Power connections	Wires transporting power, connecting the cells together
Signal connections	Wires transporting signals (temperature, voltage) to the module BMS
Temperature sensor	Measure the temperature on block level

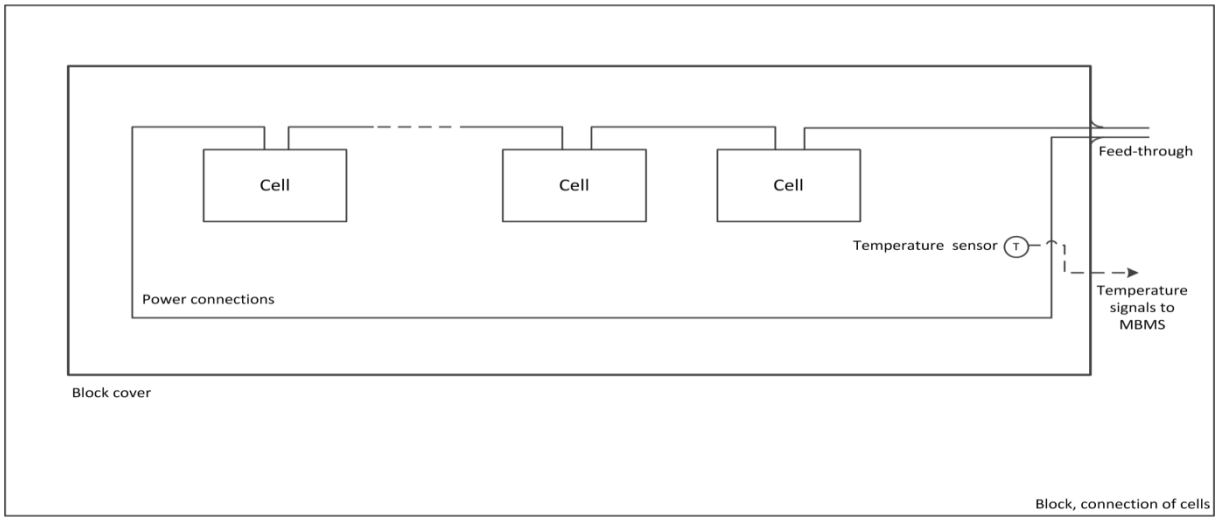


Figure 11 Schematic drawing of cell block in STALLION

3.2.3 Battery module

A battery module is a series and/or parallel connection of a number of blocks. Again, this connection is to obtain the appropriate voltage and current level. In a large battery system, there should always be a level designed to be replaced easily at the operating location, the so called line replaceable unit (LRU). The battery module is often the LRU. The LRU always requires extra components and extra attention in the design and in the risk assessment, because these units are handled by humans e.g. during maintenance or replacement. Furthermore, the LRU requires a local BMS (a BMS per module) that communicates with the system BMS. Also, a module often contains a cooling system or is cooled from outside in order to maintain the temperature within limits.

In Table 4 the components of a battery module and their functions are described. A schematic drawing of the module as used in STALLION can be seen in Figure 12.

Table 4 Battery module components and their functions

Battery module (LRU)	
Component	**Function**
Block	Connection of cells, energy storage unit
Module cover including feedthroughs	Hold a number of blocks or cells together; Protect personnel against touching live conductors; Protect module against misuse (e.g. drop, shock, EMI).
Feedthroughs	Transmit current through module cover in case of a hermetically sealed module cover
Power connections	Wires transporting power, connecting the cells and blocks to the outside of the module
Signal connections	Wires transporting signals, connecting the blocks and other components with the module BMS
Fuse	Protection; permanently disconnect the current
Mechanical disconnector	To disconnect module manually
Module BMS (MBMS)	Receive signals from temperature sensors on block level and from cell voltage sensors, communicate with balancing circuit on cell level and with pack BMS, and monitor module state of charge
Water cooling system[‡]	Protect the module against high temperatures exceeding a set limit

[‡] This is just an example, sometimes modules contain an air conditioning instead or are cooled from outside the module.

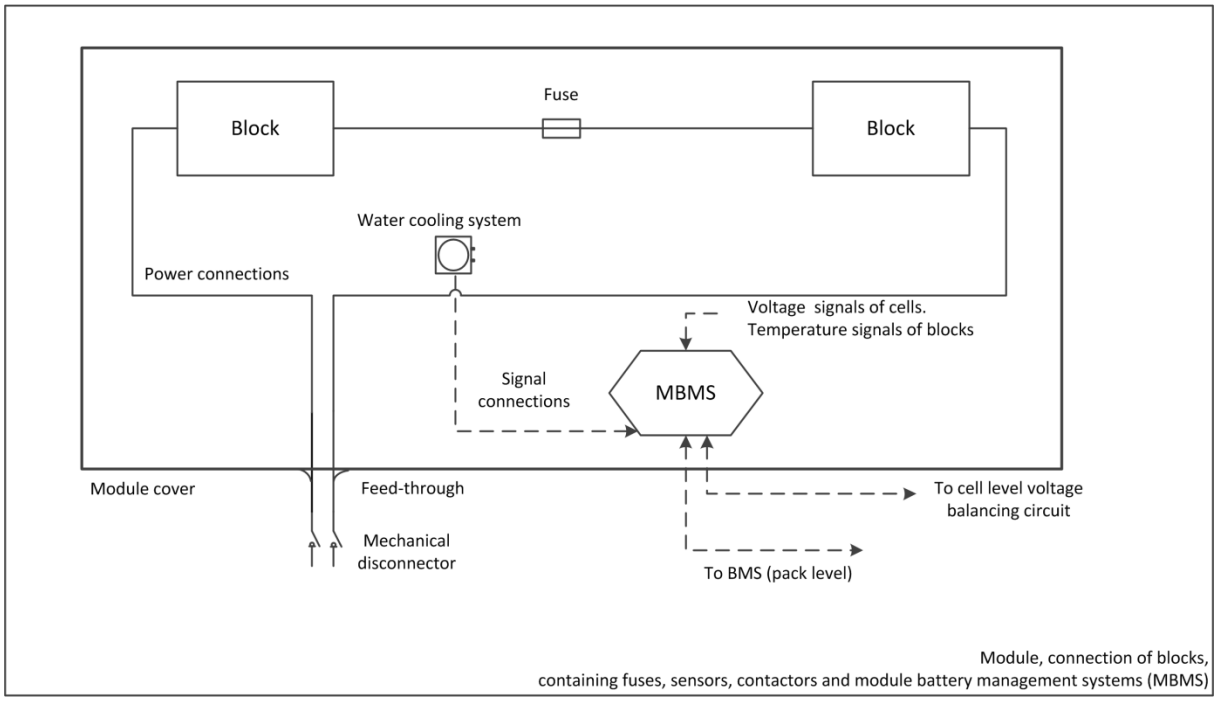


Figure 12 Schematic drawing of battery module in STALLION

3.2.4 Battery pack

The battery pack is a series and/or parallel connection of a number of modules. Because the module is often the LRU which is inside a battery pack, the battery pack can be opened. It may incorporate a protective housing and be provided with terminals or other interconnection arrangement. It may include protective devices and control and monitoring, which provides information (e.g. cell voltage) to a battery system. A battery pack often also contains elements for protection of personnel like a mechanical disconnector, an insulation resistance monitor and a fire sensor/alarm. These components are often applied on pack level because the LRU is one level lower and thus personnel is working on pack level when repairing or replacing system (parts).

In Table 5 the components of a battery pack and their functions are described. A schematic drawing of battery pack as used in STALLION can be seen in Figure 13.

Table 5 Battery pack components and their functions

Battery pack	
Component	**Function**
Module	Connection of blocks, energy storage unit, LRU
Pack cover including feedthroughs	Protect the battery pack against unintended touching
Feedthroughs	Transmit current through pack cover
Power connections	Wires transporting power, connecting the modules and other components within the battery pack
Signal connection between module BMS and pack BMS	Wires connecting the module BMS and pack BMS, communicate data
Pack BMS	Several functions with regard to safety, receive voltage, current and temperature signals from module BMS, monitor state of charge at pack level, receive signals from the current and voltage sensors and insulation resistance monitor at pack level, communicate with voltage balancing circuit at module level, control electrical contactor on pack level, send pack voltage to system BMS, communicate with system BMS, power supply for system BMS electronics
Electrical contactor (a) and (b) (aka: on/off switch / DC breaker)	Electrical contactor, connect and disconnect DC current once a command is received from system BMS (SBMS) or pack BMS (PBMS)
Mechanical disconnector	To disconnect pack manually
Fuse	Protection function, permanently disconnects the current in emergency
Current sensor	Measure current flowing through pack
Insulation resistance monitor (floating earth)	Measure insulation resistance between power connections and pack cover
Pack cover earthing	Safety earthing of pack
Signal connection between pack BMS and system BMS	Signal wires connecting the pack BMS and system BMS
Fire sensors	Detect a fire
Fire alarm	Produce an alarm signal when direct evacuation of people in the storage unit is required
Cooling tubes	Transport cooling fluid into the modules
Extinguishing gas tubes (= inert gas tubes)	Transport extinguishing gas into modules

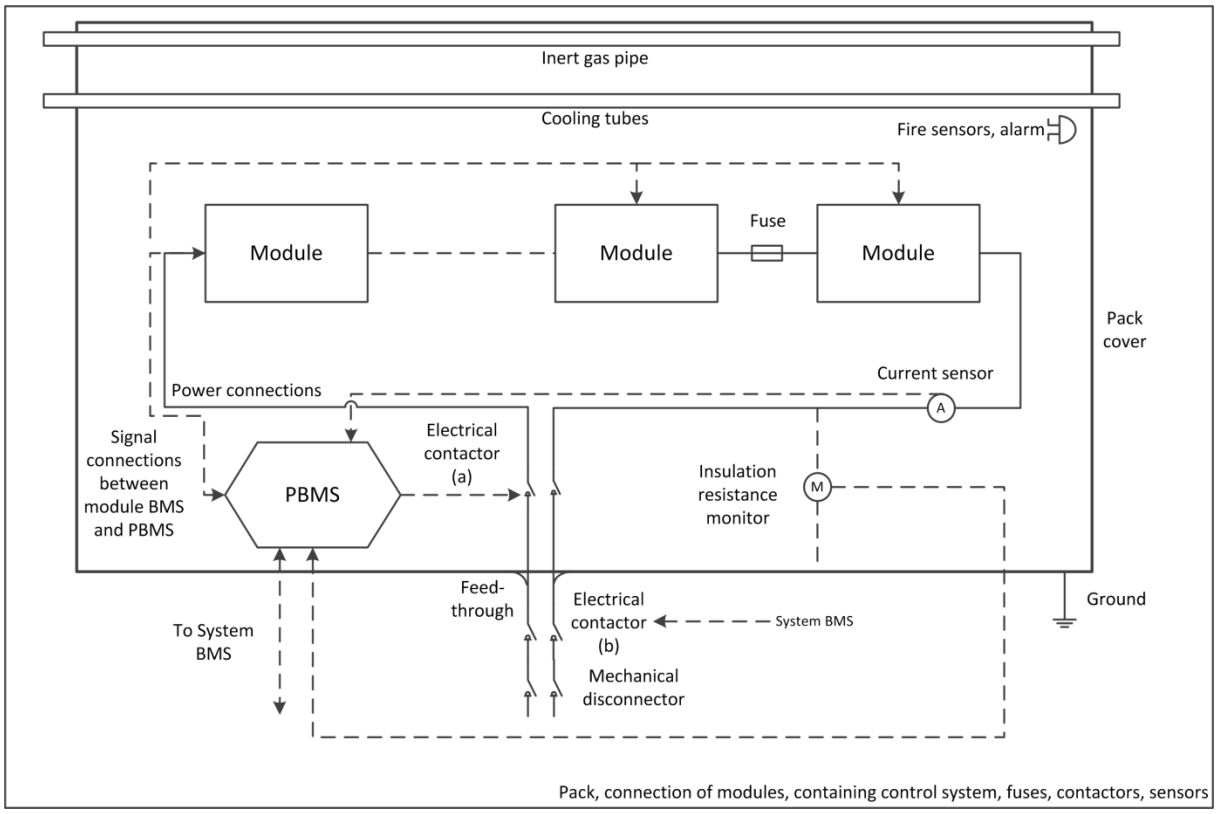


Figure 13 Schematic drawing of battery pack in STALLION

3.2.5 Battery system

The battery system incorporates several battery packs. It typically has a BMS and is connected to the outside world, therefore it needs some additional components to provide an appropriate connection.

A large battery system typically consists of the following parts:

- Storage unit: a number of battery packs connected in parallel and/or in series (depending on the specifications, supplier, design, etc.).
- Converter unit: convert AC to DC and vice versa for the grid connection.
- System BMS: two-way communication with several internal system components and with system demand controller to control the state of the entire battery.
- System demand controller: communicate with system BMS, converter unit and with external world for central control storage operation.
- Coupling transformer (step-up transformer): transform voltage to the needed grid voltage level.
- Air conditioning system: most battery systems contain an air conditioning system (for cooling and/or heating) to maintain the appropriate temperature and humidity inside the system housing.

In Table 6 the components of a battery system and their functions are described. A schematic drawing of battery system as used in STALLION can be seen in Figure 13.

Table 6 Battery system components and their functions

Battery system	
Component	**Function**
Pack	Energy storage unit
Battery system cover including feedthroughs	Protect the battery system against outside; Protect personnel from touching live parts.
Feedthroughs	Transmit power leads and signal leads through the battery system cover
Power connections	Wires connecting the battery packs and other components within the battery system
Fuses	Protection function, to permanently disconnect the current in emergency
Current and voltage sensors	To monitor the DC current and DC voltage
Electrical contactor (a)	Connects or disconnects the DC current once a command is received from the system BMS (SBMS)
Electrical contactor (b)	Connects or disconnects the DC current once a command is received from the converter master controller
Signal connections between battery system and system demand controller	Signal wires connecting the battery system to the system BMS, and connecting the SBMS and the converter master to the system demand controller
System BMS	Switch the electrical contactor, communicate with the system demand controller, run the water cooling system pump, read the voltage sensor, read the current

	sensor, communicate data from the pack BMSs to the system BMS, communicate commands from system BMS to pack BMSs
System demand controller	Communicate about required storage system operation with the converter master and the SBMS via signal connections, communicate with external world (grid operator, generator, etc.), receive the AC current and voltage signals from the grid via CT and VT
Converter unit	Provide AC-DC power conversion between grid and energy storage system
Converter master controller	Monitor and control converter unit; Communicate with system demand controller for required system operation; Command electrical contactor (b) for connection with battery system
MV AC-grid	To supply power to and absorb power from the system
System disconnector	Disconnect storage system from the MV grid (between system and coupling transformer) when a command is received from the system demand controller
Grid disconnector	To disconnect system from MV grid (between MV grid and coupling transformer) when a command is received from an external controller
Coupling transformer	To match voltage levels and transfer power
Battery system cover earthing	Safety earthing of battery system cover
Water cooling system [§]	To protect against high temperatures
Fire extinguishing system	Fire extinguishing in case of emergency
Air conditioning system	To maintain temperature and humidity inside container within prescribed limits
Container	To contain the whole system and to protect against the outside
System earthing (inside converter unit)	To set predefined voltage levels, safety provision
Inert gas tanks	Store inert gas; Release inert gas in case of fire (gas is distributed and released into the modules in the packs)

[§] This is just an example, a lot of systems have natural ventilation or air cooling instead of water cooling.

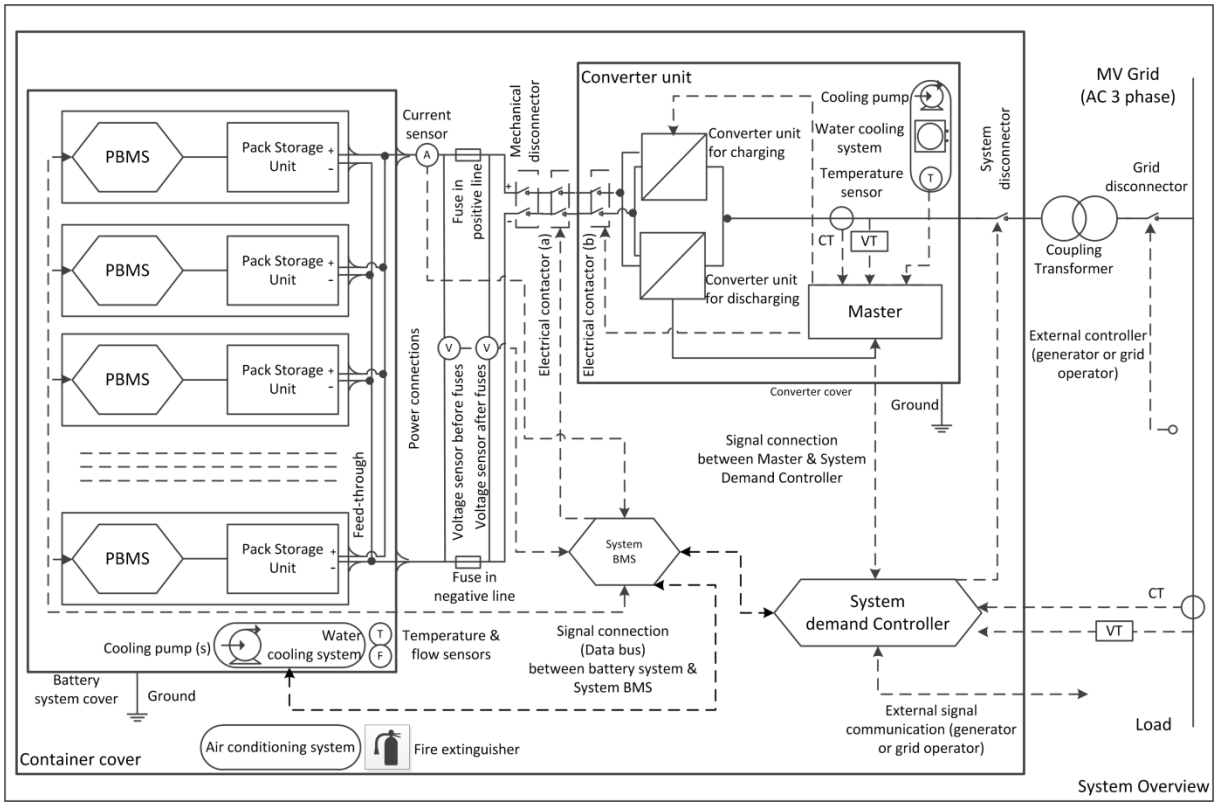
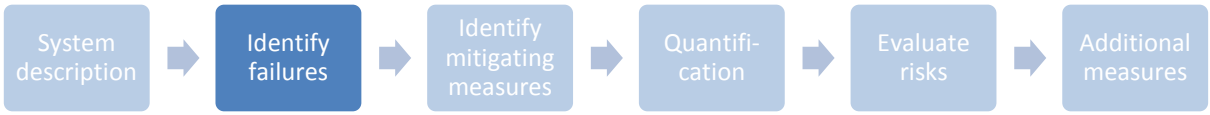


Figure 14 Schematic drawing of battery system in STALLION

3.3 Failures and their causes and effects



The next step of the risk assessment is the identification of potential failures of functional components. Functional components contribute to the operation of the storage systems. They are distinguished from safety components, which are included in the design in order to safeguard the negative effects of the storage system on life, property and the environment. Failures of safety components are not considered in this step, since there is a dependency between failure of a safety component and of a functional component, representing a 'chain of events'. Thus, the failure of safety components is processed later on in the 'effectiveness of measures'.

Each functional component has one or several functions in the system. We consider a *failure* mode to be a way in which a component can fail to perform these functions. Typically this is done using expert judgment, but as a source of inspiration, guide words (from the HAZOP) methodology can be used (Appendix B). These guide words suggest a number of ways in which a component can fail to perform its function. Secondly, each of these failures has one or more *causes*, which have to be described separately to keep a good overview. Finally, every failure has a *local effect*, e.g. 'cell on fire' and an *effect on system level*. For example, the separator is a component on cell level. Its function is that it should prevent contact between anode and cathode. A failure of this component (unwanted event) could be that the separator does not prevent contact between anode and cathode. The failure cause could be heating-induced shrinkage of the separator. The local effect is 'short-circuit' which could lead to 'cell on fire'. The effect on system level could be 'system fire'. As an example, in Table 7 some failures are listed.

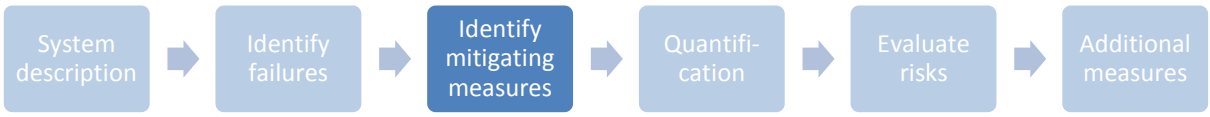
Table 7 Example of a number of failure modes on cell level

Battery cell					
Component	**Function**	**Failure**	**Failure cause**	**Local effect**	**System effect**
Cathode	Li-ions migrate towards cathode during discharge	No/limited intercalation of Li-ions into/out of cathode during discharge/ charge	Bad SOH, low quality cells	Low performance	Reduced functionality
		Overdischarge	BMS failure	Cell on fire	Risk of fire when the cell is discharged next time
		No/limited electron transfer from/to anode during discharge/	Delamination	Low load capacity	Reduced functionality

		charge			
Anode	Li-ions migrate towards anode during charge	No/limited intercalation of Li-ions into/out of anode during charge/ discharge	Bad SOH, low quality cells	Low performance	Reduced functionality
		Overdischarge	BMS failure	Cell on fire	Risk of fire when the cell is discharged next time
		Overcharge	BMS failure	Risk of lithium plating, risk of electrolyte decomposition (gas formation), cell on fire	Risk of opening of a cell and fire due to reaction of anode with moisture and air
		Lithium plating	Charging too fast, charging at too low temperature	Cell degradation, internal short circuit	Cell destruction, fire
		No/limited electron transfer from/to anode during discharge/ charge	Delamination	Low load capacity	Reduced functionality
		Expansion of anode may squeeze water cooling tubes	Bad design	Cell overheating	Thermal runaway, fire

Table 7 shows that several failures (unwanted events) on cell level have the same local effect. On the next level (i.e. block level), cell failures are considered with these local effects. For example, at block level ‘cell on fire’ is considered to be a single failure mode for a cell. The failure rate for this specific failure on block level is derived by summing all the single failure rates corresponding to the local effect on cell level. This is done for all levels (e.g. block on fire is a failure on module level with a failure rate calculated by summing the failure rates of all ‘block on fire’ failures on block level, etc.).

3.4 Present measures



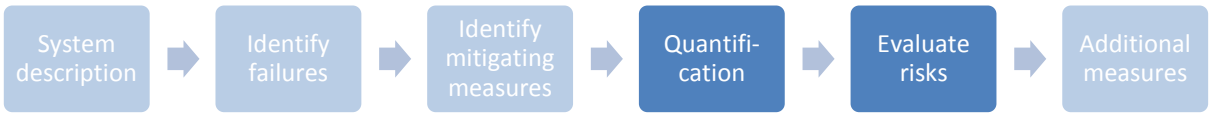
A normal design contains measures to prevent, detect and/or mitigate risks and thus increase safety. When quantifying risks, these present measures should be taken into account. It is therefore convenient to look at each failure mode and evaluate whether a measure is already present on that component level. See Table 8 for some examples of present measures.

Battery cell				
Component	**Function**	**Failure**	**… ***	**Present measure**
Cathode	Li-ions migrate towards cathode during discharge	No/limited intercalation of Li-ions into/out of cathode during discharge/charge	…	Manufacturing Quality system
		Overdischarge	…	BMS
		No/limited electron transfer from/to anode during discharge/charge	…	Quality system
Anode	Li-ions migrate towards anode during charge	No/limited intercalation of Li-ions into/out of cathode during discharge/charge	…	Quality system
		Overdischarge	…	BMS
		Overcharge	…	BMS
		Lithium plating	…	BMS
		No/limited electron transfer from/to anode during discharge/charge	…	Quality system
		Expansion of anode may squeeze water cooling tubes	…	-

Table 8 Example of a number of present measures

* Columns ‘failure cause’ and ‘effects’ omitted for clarity.

3.5 Quantification and evaluation of risks



The next step of the risk assessment is the quantification of risks. This should be done by an expert group with thorough knowledge of the energy storage system and its application. Quantifying risks means assigning a probability and severity to an unwanted event or failure and an effectiveness to each measure. This *probability* of a risk is expressed as a rate of events, e.g. number of failures per hour (this is the case in STALLION) or per year. *Severity* is a measure for the possible consequences of a hazard resulting from a failure. It indicates the worst potential (but realistic) effect of the failure considered on the system level, for example the number of fatalities. In general risk assessments, also functional risks are addressed, but in this case we are only interested in safety risks.

3.5.1 Generally used risk quantification

Probability, severity and the effectiveness of measures (detectability) are often expressed as a scale of integers, for example ranging between 1 and 10. The resulting risk priority is typically presented by a risk priority number (RPN). The RPN is the product of probability score and severity score. Depending on the range of numbers chosen for probability score and severity score, the RPN has a minimum and maximum outcome. The expert group should define thresshold values for acceptability of RPN values, e.g. RPN below x are considered to be acceptable, and above x are unacceptable. The RPN gives a relative number and not an absolute number. So outcomes of different FMECA's differ, as would be expected regarding the freedom of choosing the scales and ranges of the different parameters. A drawback of using RPN as a risk priority is the fact that very different risks (with different probability, severity and detectability) may end up having the same RPN.

A risk matrix shows the separate dimensions (probability, severity, detectability) on separate axes and therefore doesn't have this drawback of 'mixing' them. A 2D risk matrix typically has the probability on the X-axis and the severity on the Y-axis. Each failure is assigned a value for probability and for severity; therefore each of these failures can be entered into this matrix. In such a risk matrix areas can be identified which are more 'risky' than others. See for example Figure 15 where colors indicate different areas: catastrophic, unacceptable, undesirable, acceptable, desirable.

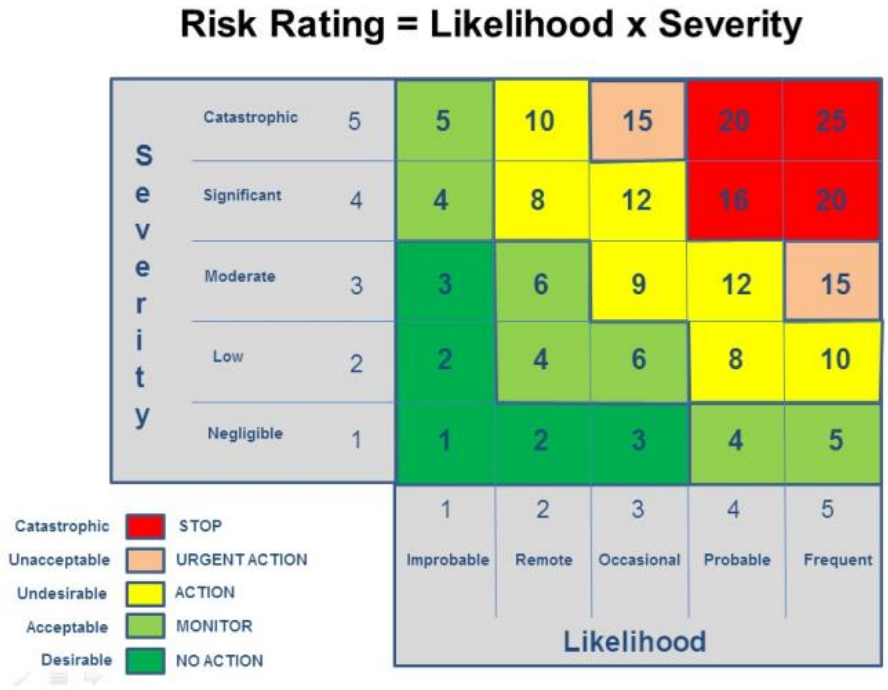


Figure 15 An example of a risk matrix

3.5.2 Risk quantification in STALLION

The Risk Priority Number (RPN) is the product of severity and probability score, where severity and probability normally are expressed in a range of integers. In STALLION, the RPN values have not been used due to the limited range in severity and probability applied. For example, an RPN of 8 could be the result of probability=2 and severity=4 or of probability=4 and severity=2. Thus, it is questionable whether two failures with RPN '8'should be ranked similarly. Therefore the two-dimensional representation of a risk matrix is preferred.

In STALLION the probability and severity are shown in a 'bubble' graph (see Figure 16). The bubble graph contains a bubble for each combination of severity and probability where the size of the bubble indicates the amount of failures with this combination.

Bubble graphs have been created for each level in the system. STALLION distinguishes between three risk classes: Risk class 1 is considered as acceptable (green), Risk class 2 is considered as noticeable (yellow) and Risk class 3 is considered as critical (red).

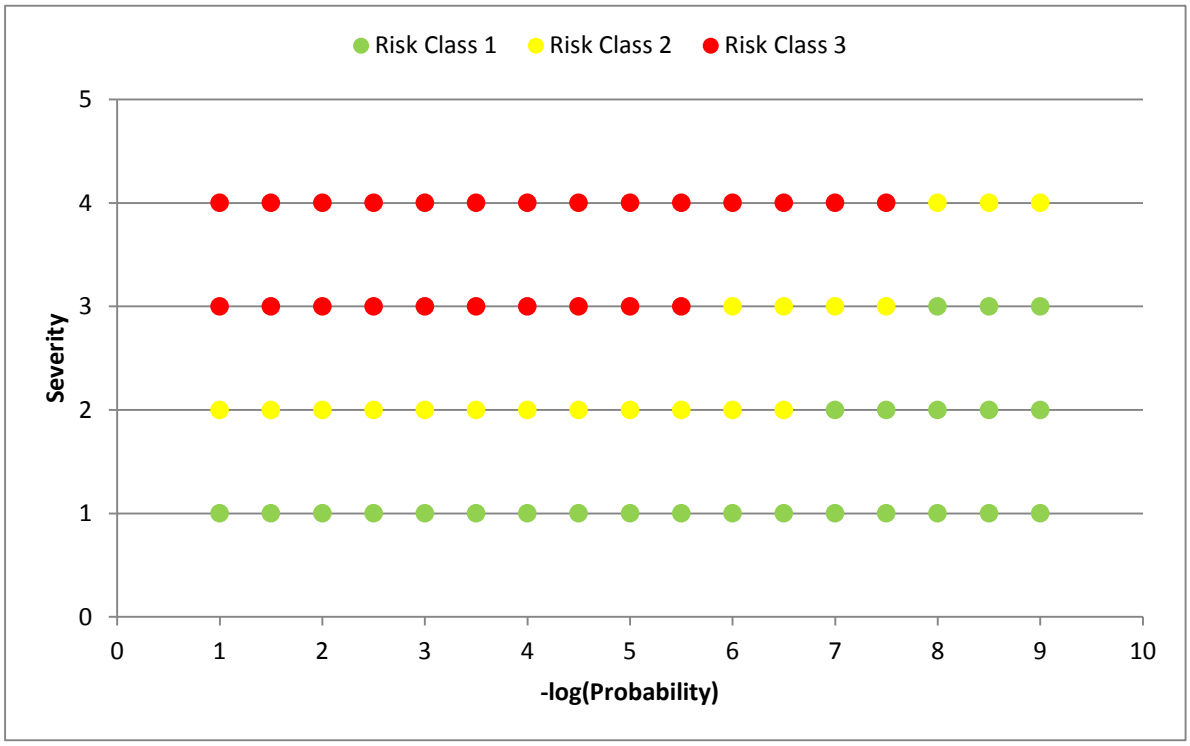


Figure 16 Configuration of the bubble graph as used in STALLION

Now the quantification of severity and probability within STALLION will be discussed.

Severity should be quantified by an expert group. Each failure is classified in a severity class, ranging from 1 (minor injury) to 4 (more than one person deceased). See Table 9 for an overview of the severity classes as used in STALLION.

Table 9 Quantification of severity of failures

severity	description	example
1	minor injury	e.g. when someone touches a conductor at lower voltage
2	severe injury (loss of limb)	e.g. when someone touches a conductor at higher voltage
3	one person deceased	e.g. when something happens while someone carries out corrective maintenance
4	more than one person deceased	e.g. when there is an explosion during maintenance

Probability is in STALLION considered as the rate of failures of a component for a failure mode with a specific cause. Probability is calculated for each cause of a failure, because one failure may have several causes. We consider failures and their probability on each level and do not transfer them directly to system level. So instead of taking the number of components on system level into account, the number of components of one level up is taken into account. This will be further elaborated on page 36.

The formula for probability is in STALLION defined as:

Probability = basic failure rate * percentage of failure causes * (1 - effectiveness of measures) * number of components

Below, these four contributors to Probability will be discussed in further detail.

The *basic failure rate* states how many times (per hour) a single component will fail in general. In STALLION these rates are defined by the expert group for components of a certain type (e.g. mechanical rotating component, electrical component, etc.). The defined failure rates for the different components in STALLION are depicted in Appendix C. These basic failure rates typically have a value between 10^{-8} and 10^{-3} per hour, where the latter for example means: 'component fails once in every 1000 hours'.

The *percentage of failure causes* indicates the relative proportion of the different causes of a single failure mode of a certain component. This means that the sum of all of these values for one failure mode of a component is 100%. If this number is not taken into account it would mean that a failure mode with several causes would automatically have in total a greater probability of occurring as compared to a failure mode with a few causes, while this is not necessarily the case. In other words, the probability of a failure mode is made independent of the number of causes of that failure mode.

As mentioned before every design contains safety measures intended to increase safety. Present measures related to the failure modes are defined as those designed in in the system design. Thus, in this step the safety components are included as present mitigating measures. The *effectiveness of (present) measures* is a percentage which indicates how well the present measure could prevent the failure from occurring. This means that the safety components reduce the risk to a certain extent. This is derived from the SIL approach, which focusses on the integrity of safety components. Appendix D gives a short description of the SIL methodology.

These numbers are defined by the expert group. In the determination of the effectiveness, also detectability of failures is taken into account. It is convenient to consider for example 99.99% as 'the present measure is not effective on 1 in 10.000 times'. When a risk turns out to be unacceptable according to the expert group, additional mitigating measure(s) are necessary, which should decrease

Table 10 Values of effectiveness of present mitigating measures used in STALLION

Effectiveness of measures		Present measure is <u>not</u> effective in one out of x events	Reasoning
Very limited	0%	1:1	No present measure, thus no effectiveness
Fair	50%	1:2	For example: quality management, preventive maintenance, operational procedures
Rather effective	90%	1:10	For example: design of operational limits
Quite effective	99%	1:100	…
Very effective	99,9%	1:1000	For example: BMS, electronic back-ups, fuses, back-up sensors
Almost perfect	99,99%	1:10.000	Process and quality control

the probability by increasing the effectiveness of the measures. See **Table 10** for the auxiliary table for effectiveness of mitigating measures used in STALLION. The additional mitigating measures will be discussed in paragraph 3.6.

If one component does not fail very often, but there is a large number of that component present in the system, then the probability of such a component failing increases (if we assume components failing independently). Therefore, the *number of components* at the level considered is taken into account in the calculation for the probability. In other words, probability is derived on each level by multiplying with the number of components on that specific level. For example, when considering failure of a module on pack level, the number of components is 16 (because there are 16 modules inside a pack), see Figure 17.

	# cells per level	# blocks per level	# modules per level	#packs per level
cell				
block	7			
module	14	2		
pack	224	32	16	
system	28000	4000	2000	125

Figure 17 Number of components in STALLION

The failure rate indicates how many times per hour a component is expected to fail. Probability is also a measure for the failure rate, but taking into account improving and worsening parameters of that failure. Some failures cause a failure on levels higher up. In other words, a chain of events may occur through the different battery levels (cell – block – module – pack – system). When considering a failure that is part of a chain of events, i.e. a failure on one level causes a failure on higher levels, the probability of that event is equal to the failure rate of the failing component on the next level. A fire which starts on cell level is a good example: there is a possibility that this fire will grow bigger until the whole system is on fire. This inheritance of failure rates is graphically displayed in Figure 18.

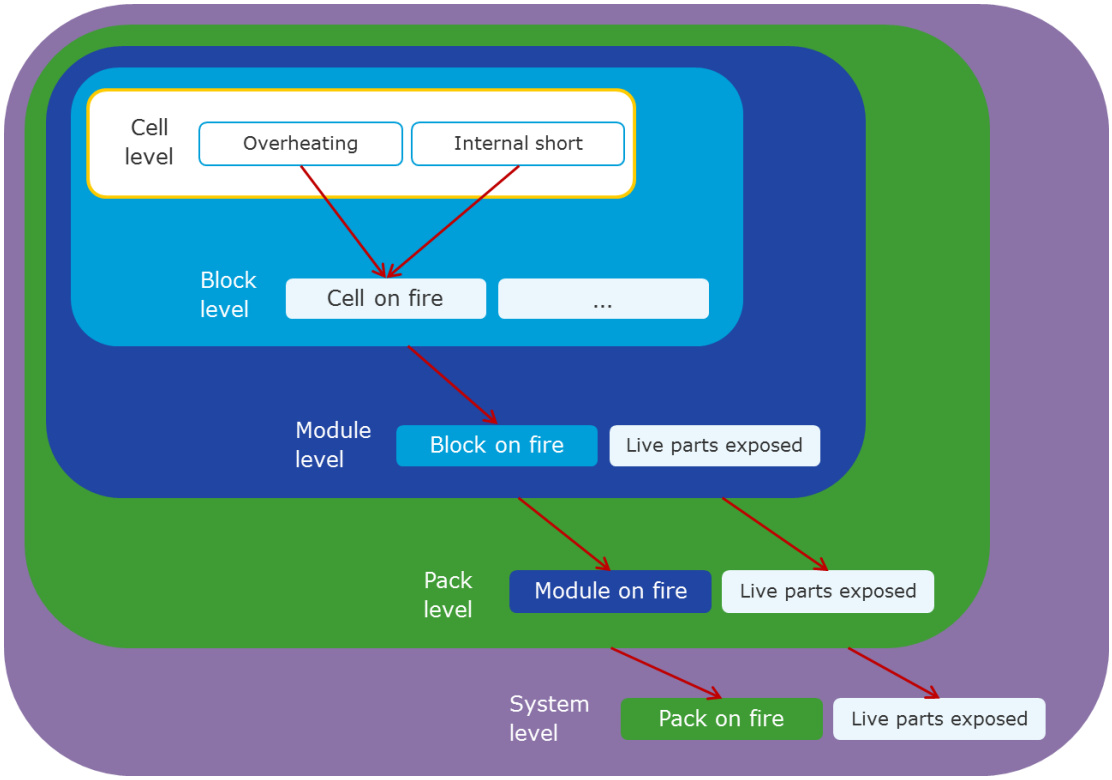


Figure 18 Graphical representation of inheriting failure rates within a chain of events (propagating fire)

To summarize, a simplified representation of the bubble graph with the contributors to probability are shown in Figure 19. The failures can be plotted by using the severity level and probability as axes. In STALLION, the $-\log_{10}$ of the probability is plotted to visualize the failures in a convenient way. The size of the bubbles indicates the number of failures on that x-y coordinate in the graph.

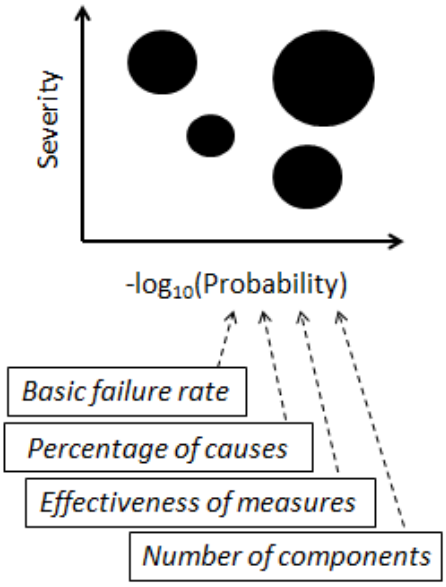


Figure 19 Configuration of bubble graph and contributing parameters

Below (Figure 20), an example of a bubble graph on system level of the STALLION FMECA. As can be seen, several risks are risk class 1 or 2, which thus do not require immediate action. However, there are several risk class 3 risks, which is not acceptable. These risks require additional measures; the approach for additional mitigating measures will be discussed in the next paragraph.

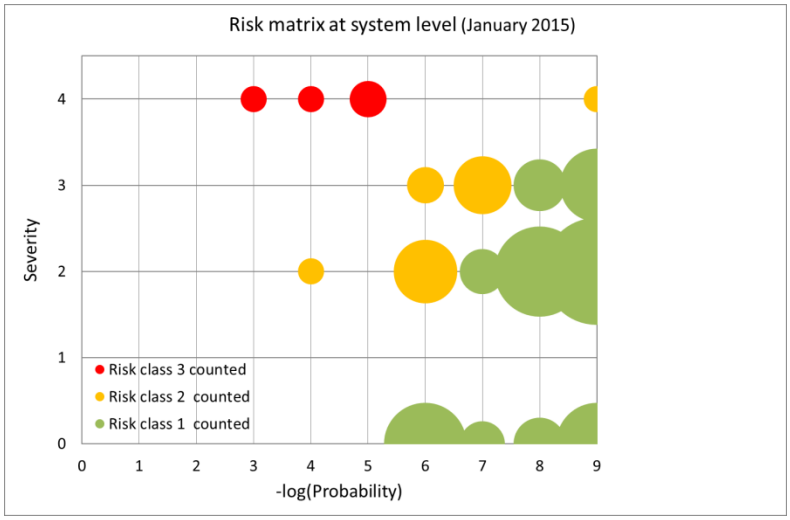
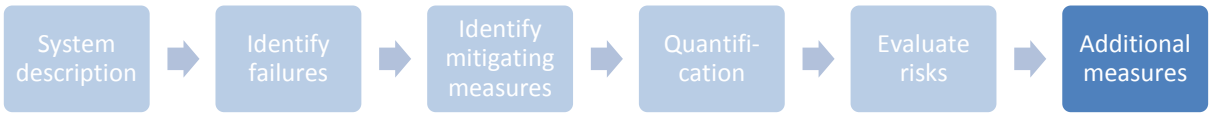


Figure 20 Resulting bubble graph on system level in STALLION

3.6 Additional mitigating measures



After the risk analysis is performed, additional measures can be taken into account to increase safety, especially on risks which proved to be highly dangerous.

The risk may be reduced by introducing one or more of the following general aspects:

- Design changes
- Increased manufacturing quality control
- Engineered safety features
- Safety devices
- Safety-relevant electronics and software, that have separate, redundant safety functions, apart from the operational functions
- Warning devices
- Procedures/training

Based on the characteristics of these new measures, the calculation of the previous chapter can be redone to assess whether these new measures decrease the probability enough to get to a safe system.

3.7 STALLION risk assessment

At the beginning of the STALLION project an FMECA risk assessment was performed within STALLION. Details of the system description are given in (1). For all components the above described steps necessary within the risk assessment are given in appendix A.
Below shows the bubble graph on system level of the Stallion FMECA (Figure 21) and the assumptions used (Table 11).

Table 11 Assumptions for FMECA on system level in STALLION

Functional component	Basic failure rate [1/hr]	Safety components	Effectiveness of measure [%]
Cell materials	$1x10^{-6}$	MBMS, PBMS, SBMS	99
		Quality system	99,9
		Fuses	99
		Backup power supply	90
		System and pack cover	90

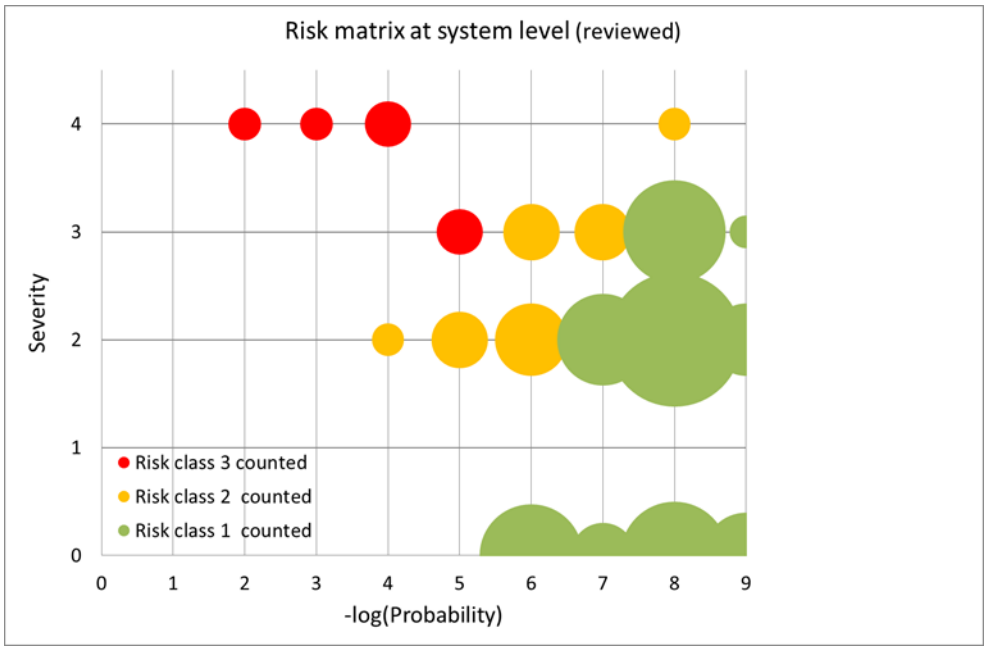


Figure 21 Bubble graph on system level in STALLION

Figure 21 shows that there are six risk class 3 failures, which are listed in

Table 12.

Table 12 Risk class 3 failures for reviewed FMECA

[-log(Prob); Sev]	component	failure	Present measure	Effectiveness of measure
[2.1;4]	Battery pack	pack on fire	Fire extinguishers	50%
[5.2;3]	Battery pack	Insulation fault	Pack cover	90%
[3.9;4]	Battery pack	Release of explosive gas	Airco / ventilation	90%
[3.4;4]	Battery pack	Release of poisonous gas	Airco / ventilation	90%
[4.2;4]	Battery pack	Electrocution	-	0%
[5.3;3]	System demand controller	No power supply	Back-up power supply	90%

At the end of the STALLION project the FMECA risk assessment was reviewed, based upon lessons learned from STALLION. Therefore, additional mitigating measures derived from the STALLION project have been incorporated in the risk assessment. For example, we have improved the failure rates of cell materials, assuming that a dedicated selection methodology will be applied at the initial stages of product design. For this, we refer to the selection methodology developed by Umicore within STALLION (18), which leads to an optimized material choice taking costs, safety and product specifications into account.

In addition, the STALLION project has learned that the effectiveness of safety measures has to be increased. This applies for the BMS and the quality system, and for backup power and system cover, as is summarized in Table 13. Figure 22 shows the corresponding bubble graph. Four risk class 3 failures remain, although the probability has decreased. This is also quantified in Table 14.

Table 13 Assumptions for FMECA including additional measures

Functional component	Basic failure rate [1/hr]	Safety component	Effectiveness of measure [%]
Cell materials	$1x10^{-8}$	MBMS, PBMS, SBMS	99,9
		Quality system	99,99
		Fuses	99,9
		Back-up power supply	99
		System and pack cover	99

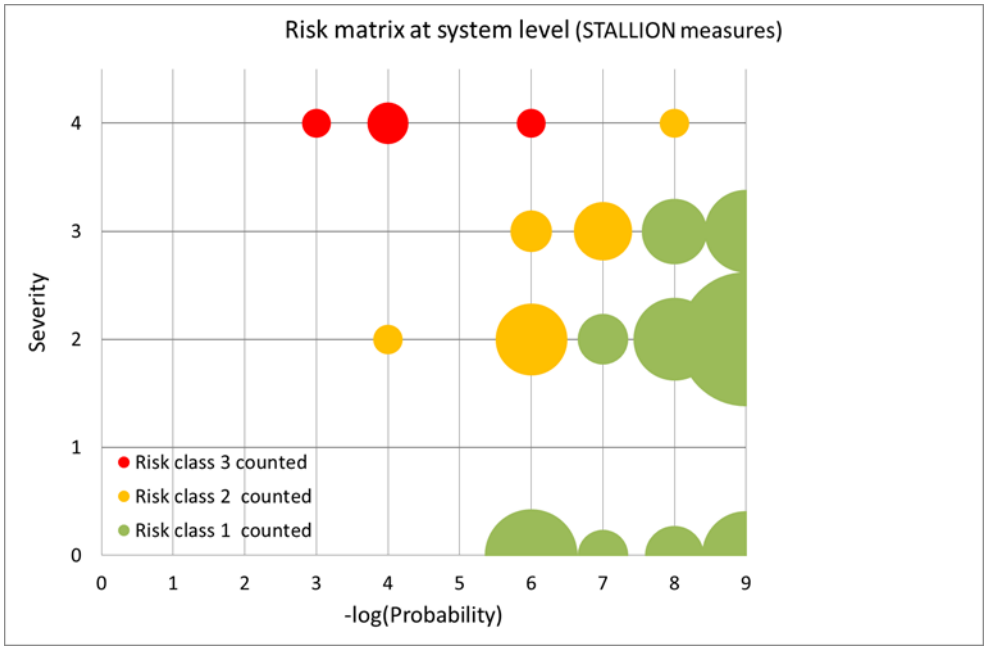


Figure 22 Bubble graph on system level including additional measures

Table 14 Risk class 3 failures for FMECA including additional measures

[-log(Prob); Sev]	component	failure	Additional measure	Effectiveness of measure
[3.0;4]	Battery pack	System on fire	Fire extinguisher	50%
[3.6;4]	Battery pack	Release of poisonous gas	Airco/ventilation	90%
[5.9;4]	Battery pack	Release of explosive gas	Airco/ventilation	90%
[4.4;4]	Battery pack	Risk of electrocution	-	0%

Risk class 3 failures of FMECA including additional measures

1) Failure of power supply for system demand controller is no longer a risk class 3 failure, but a risk class 2 failure because the [-log(Prob);Sev] has changed into [6,3;3]. This is mainly due to an improved backup power system with an effectiveness of measures of 99% instead of 90%.

2) The insulation fault failure has become a risk class 2 failure, since the [-log(Prob);Sev] has changed into [6,2;3]. This is mainly due to an improved pack cover with an effectiveness of measures of 99% instead of 90%.

3) System on fire is still a risk class 3 failure. Within STALLION we proposed the following final recommendations to cope with these potential risks:
    - Apply thermal barrier between cells in module and between modules

- More data from cell manufacturer is needed, e.g. runaway inception temp
- The system design should include thermal insulation layers between cells and/or modules to prevent the spread of thermal runaway (or fire) outside the module.
- Cells and modules should pass fire propagation test procedures to guarantee the use of safe cells and modules.
- There is a need for safety-relevant electronics and software that have separate, redundant safety functions, apart from the operational functions (BMS at all levels, system demand controller, converter master controller).

4) So far no additional measures have been implemented in order to reduce the risk of release of poisonous or explosive gas. Within STALLION we proposed the following final recommendations in order to cope with these potential risks:
    - Apply detector for toxic and/or flammable gases
    - Implement improved ventilation or airco systems

5) So far no additional measures have been implemented in order to reduce the risk of electrocution. Within STALLION we propose the following final recommendations:
    - Provide a checklist of requirements for a safe system design and a manufacturing quality control
    - Provide strict handling/maintenance procedures.

For a more detailed evaluation of the final STALLION risk assessment we refer to (3).

4 CONCLUSIONS AND RECOMMENDATIONS WITH RESPECT TO RISK ASSESSMENTS FOR LARGE, STATIONARY, LI-ION, GRID-CONNECTED, STATIONARY STORAGE SYSTEMS

This Handbook is a guide for interested parties into the world of large-scale, stationary, Li-ion, grid-connected, energy storage systems and the relevant safety aspects. It explains the need for dedicated risk assessments, it describes the risk assessment methodology applied within STALLION and it gives examples of major risks. This chapter summarizes conclusions and recommendations from the Handbook.

Since there is a growing interest in large-scale, stationary, Li-ion, grid-connected, energy storage systems in order to support the grid in case of large penetration grades of renewables, it is of utter importance to guarantee the safety and reliability of such storage systems. Especially since Li-ion energy storage systems have intrinsic safety risks due to the fact that high energy-density materials are used in large volumes. In addition, these storage systems are most likely situated in or near residential areas.

A Failure Mode Effect and Criticality Analysis (FMECA) is a suitable tool to perform a risk assessment. In order to start with a dedicated system description, a close involvement of the system designer and the system operator, defining the system specifications, is required. An FMECA should consider all components on all relevant levels (system, pack, module, block and cell level). For all these components their functions should be specified. Each system contains functional components, contributing to the storage functionality of the system, and safety components, which are included in the system to guarantee safety.

In the risk assessment a dedicated expert group should explore ‘failures’ of these functional components. Failures of safety components are not directly considered since they should only operate in case of failure of a functional component. Safety components are considered as ‘measures’ in the design to guarantee safety.

Failures of functional components are referred to as ‘unwanted’ events. Of course, failures may have one or more causes. The impact of these failures on local level and on system level should be estimated. The expert group has to quantify these failures by assigning a ‘severity’ and a ‘probability’. The severity indicates the worst potential (but realistic) effect of the failure considered on the system level, for example the number of fatalities. The probability is the rate of failures of a component for a failure with a specific cause. It is a function of the basic failure rate of each component (how often does this component fail in general), the effectiveness of a mitigating measure (i.e. safety component) already designed in on this specific level (how well does a safety component work on this level) and the number of components on this level.

Since all sub-level component (cell, block, module, pack) failures can propagate to the next level, this should also be taken into account in the risk assessment. For example, fire on cell level could lead to fire on block level, etc.

The Handbook gives examples from the FMECA risk assessment performed in the STALLON project with respect to the safety of large-scale, Li-ion, grid-connected, energy storage systems. Major risks identified were system on fire, release of poisonous and explosive gases, and the risk of electrocution.

In order to reduce the risk of system on fire, propagation of fire from lower levels towards a system fire should be prevented. Therefore, it is recommended to select cell materials in accordance with the final system specifications. A detailed data sheet from cell manufacturers, including e.g. runaway inception temperatures should be required. In addition, the system design should include thermal insulation layers between cells and/or modules to prevent the spread of thermal runaway (or fire) outside the module. And cells and modules should pass fire propagation test procedures to guarantee the use of safe cells and modules. Finally there is a need for safety-relevant electronics and software, which have separate, redundant safety functions, apart from the operational functions (BMS at all levels, system demand controller, converter master controller).
In order to reduce the risk of release of poisonous or explosive gases, it is recommended to apply detectors for toxic and/or flammable gases or to implement excellent ventilation or air-conditioning systems.
Finally the risk of electrocution could be reduced by a check list of requirements for a safe system design and a well-documented manufacturing quality control. In addition a checklist providing strict handling and maintenance procedures are required.

5 BIBLIOGRAPHY

1. **Verhaegh, N. & van der Burgt, J.** Failure Mode, Effect anc Criticality Analysis for stationary, grid-connected, large-scale, Li-ion storage systems. *Deliverable 1.2 for the STALLION project.* 2013.
2. **STABALID.** STABALID: STAtionary Batteries LI-ion safe Deployment. [Online] http://stabalid.eu-vri.eu/.
3. **DNV GL, VITO, ABB, Umicore, VDL.** FMEA updated report. *Deliverable 7.1 for the STALLION project.* 2015.
4. **Weicker, P.** *A Systems Approach To Lithium-Ion Battery Management.* 2014.
5. **National Transportation Safety Board.** *Aircraft Incident Report: Auxiliary Power Unit Battery Fire, Japan Airlines Boeing 787-8, JA829J.* 2013.
6. **Lavrinc, D.** Tesla Cleared By Feds After Fires, Add Additional Armor Anyway. *WIRED.* [Online] http://www.wired.com/2014/03/tesla-feds-armor/.
7. **Date, W.** G&P Batteries suffers second fire in weeks. *letsrecycle.com.* [Online] http://www.letsrecycle.com/news/latest-news/gp-batteries-suffers-second-fire-in-weeks/.
8. **Ranter, H.** Report: UPS Boeing 747F uncontained cargo fire likely caused by lithium batteries. *Aviation Safety Network.* [Online] http://news.aviation-safety.net/2013/07/25/report-ups-boeing-747f-uncontained-cargo-fire-likely-caused-by-lithium-batteries/.
9. **DOE.** DOE Global Energy Storage Database. [Online] http://www.energystorageexchange.org/.
10. **Grid4EU.** Demo 6 in Carros, France (Nice Grid). *Grid4EU.* [Online] http://www.grid4eu.eu/project-demonstrators/demonstrators/demo-6.aspx.
11. **U.S. Department of Energy.** WEMAG Younicos Battery Park. *DOE Global Energy Storage Database.* [Online] http://www.energystorageexchange.org/projects/563.
12. —. The Zurich 1 MW BESS. *DOE Global Energy Storage Database.* [Online] http://www.energystorageexchange.org/projects/584.
13. **Younicos.** Balancing the German grid. *Younicos.* [Online] http://www.younicos.com/en/projects/08_vattenfall/.
14. **U.S. Department of Energy.** Bosch Braderup ES Facility: Li-Ion Battery. *DOE Global Energy Storage Database.* [Online] http://www.energystorageexchange.org/projects/1453.
15. —. Orkney Storage Park Project. *DOE Global Energy Storage Database.* [Online] http://www.energystorageexchange.org/projects/474.
16. **Networks, UK Power.** Smarter Network Storage. *UK Power Networks.* [Online] http://innovation.ukpowernetworks.co.uk/innovation/en/Projects/tier-2-projects/Smarter-Network-Storage-%28SNS%29/.
17. **Rausand, M.** Presentation. *Chapter 3 System Analysis: Failure Modes, Effects, and Criticality Analysis.* [Online] http://frigg.ivt.ntnu.no/ross/slides/fmeca.pdf.
18. **Merchin, D. (Umicore).** Report on methodology for selecting appropriate cathode/anode materials. s.l. : Conducted within the STALLION project.

APPENDIX A - LEGEND OF STALLION FMECA SPREADSHEET

Column	Title	Explanation
A	Level	Level name (cell/block/module/pack/system)
B	Components	Component name
C	Initiating frequency [per hour]	Basic failure rate [hour $^{-1}$] of the component. These values are copied from the sheet 'Basic failure rates' in the Excel file.
D	Number of components	Number of components at the level of interest
E	Number of components at system level	Total number of components in the system
F	Function	Intended function of the component, separate lines for each function.
G	Failure (unwanted event)	This is the failure mode: what can go wrong. Separate lines for each failure.
H	Potential failure cause	Cause of the failure. Either use a separate line for each cause of the failure (ideal), or mention the most probable cause.
I	Percentage of failure causes	What is the probability of the failure with a particular cause for a certain component, compared to all failure causes of this failure? The sum of these percentages for a certain failure should be 100%.
L	Local effect	Local effect of unwanted event (column G)
M	Effect on system level	Effect of unwanted event (column G) on system level.
N	Present measures	Description of present measure(s)
O	Effectiveness of measures	Effectiveness in of present measures in percentage. An effectiveness of 90% reduces the occurrence by a factor of 10.
P	Probability of failure to be dangerous on system level	Probability is a function of basic failure rate, percentage of failure causes, effectiveness of measures and number of components
Q	Negative log of Probability	-log(Probability)
R	Severity	Severity of system effect: value is 1, 2, 3 or 4. See also sheet 'Severity'.
T	RPN / Safety	Risk priority number calculated by multiplying values of Columns L and Q.
U	Additional measures	Recommendations for additional measures. These are not taken into account in the scoring! If they need to be taken into account, they should be under 'Present measures' (column O).

Figure 23 FMECA spread sheet

APPENDIX B - GUIDE WORDS

Guide word	Meaning
No or Not	Complete negation of the design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification / increase
Part of	Qualtitative modification / decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution
Early	Relative to the clock time
Late	Relative to the clock time
Before	Relating to order or sequence
After	Relating to order or sequence

APPENDIX C - BASIC FAILURE RATES

COMPONENT	ROUGH FAILURE ESTIMATE (INITIAL FAILURE FREQUENCY PER HOUR)
SYSTEM DEMAND CONTROLLER	1,00E-04
CONVERTER UNIT	1,00E-05
AC-SIDE SYSTEM EARTHING	1,00E-06
AIR CONDITIONER SYSTEM	1,00E-03
BATTERY SYSTEM COVER EARTHING	1,00E-06
BATTERY SYSTEM COVER INCLUDING FEEDTHROUGHS	1,00E-06
CONTAINER	1,00E-05
COUPLING TRANSFORMER	1,00E-06
CURRENT SENSOR	1,00E-06
DC-SIDE SYSTEM EARTHING	1,00E-06
MV AC-GRID	1,00E-05
POWER CONNECTIONS	1,00E-06
SBMS ELECTRICAL CONTACTOR	1,00E-06
SIGNAL CONNECTION BETWEEN BATTERY SYSTEM AND SYSTEM DEMAND CONTROLLER (DATA BUS)	1,00E-06
SIGNAL CONNECTION BETWEEN CONVERTER MASTER AND SYSTEM DEMAND CONTROLLER	1,00E-06
VOLTAGE SENSOR AFTER FUSES	1,00E-06
VOLTAGE SENSOR BEFORE FUSES	1,00E-06
SIGNAL CONNECTION BETWEEN MODULE BMS AND PACK BMS	1,00E-06
CURRENT SENSOR PER PACK	1,00E-06
COOLING TUBES	1,00E-05
SIGNAL CONNECTIONS	1,00E-06
MODULE BMS (MBMS)	1,00E-04
BLOCK COVER INCLUDING FEEDTHROUGHS	1,00E-06
CATHODE	1,00E-08
ANODE	1,00E-08
CATHODE CURRENT COLLECTOR	1,00E-09
ANODE CURRENT COLLECTOR	1,00E-09
BINDER	1,00E-08
SEPARATOR	1,00E-06
ELECTROLYTE	1,00E-08
VOLTAGE BALANCING CIRCUIT	1,00E-06
CELL COVER	1,00E-06
INERT-GAS-TANKS	1,00E-06

APPENDIX D - SIL APPROACH

The Safety Integrity Level (SIL) is a reduction factor for risks. In other words, it is a relative level of risk-reduction provided by a safety function. In simple terms, SIL is a measurement of performance required for safety instruments. It has 4 levels: from light safeguard (1) to very heavy safeguard (4). The latter should be avoided. The necessary SIL levels result from a risk assessment such as FMECA.

Once a required SIL level is established, it should be proven that a control loop attains this SIL level. However, also a failure redundancy is necessary that is based on the reliability of the used instruments. The calculation invokes the so-called Probability of Dangerous Failure (PFD). It takes into account the undetected dangerous failure rate, the failure redundancy, common cause failure, test interval and common causes.

With the standard IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems), safety integrity can be certified to a SIL. According to the standard there are two methods to determine SIL levels (in Annex D and E of part 5 of the standard).

The SIL method may provide a good completion to a risk assessment such as FMECA, because it focusses on the integrity of safety components.