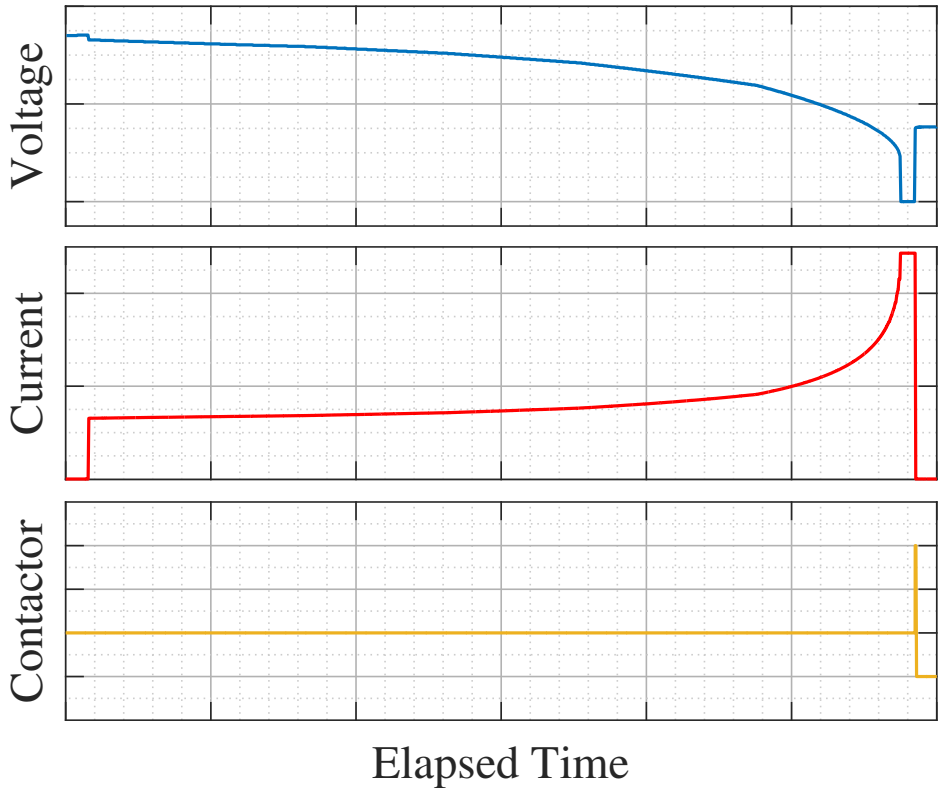
CHALMERS
UNIVERSITY OF TECHNOLOGY



Test case analysis of system safety regarding degraded Li-ion battery

Validation and verification of BMS safety functions in HIL environment with focus on ISO 26262

Master of Science Thesis in Electric Power Engineering

CARL BIERICH
EMIL MAGNUSSON

Department of Electrical Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2019

Master's thesis 2019

Test case analysis of system safety regarding degraded Li-ion battery

Validation and verification of BMS safety functions in HIL environment with focus on ISO 26262

CARL BIERICH
EMIL MAGNUSSON

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Electrical Engineering
Division of Electric Power Engineering
Chalmers University of Technology
Gothenburg, Sweden 2019

Test case analysis of system safety regarding degraded Li-ion battery
Validation and verification of BMS safety functions
in HIL environment with focus on ISO 26262

CARL BIERICH
EMIL MAGNUSSON

Supervisor: Lucas Bergman, Volvo Car Corporation
Examiner: Torbjörn Thiringer, Department of Electrical Engineering

Master's Thesis 2019
Department of Electrical Engineering
Division of Electric Power Engineering
Chalmers University of Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: Measurement of current, voltage and contactor status for overdischarge test.

Typeset in LaTeX
Gothenburg, Sweden 2019

Test case analysis of system safety regarding degraded Li-ion battery
Validation and verification of BMS safety functions
in HIL environment with focus on ISO 26262
CARL BIERICH
EMIL MAGNUSSON
Department of Electrical Engineering
Chalmers University of Technology

Abstract

As lithium ion batteries become a larger part of the vehicle propulsion system, the testing of the battery management system software becomes increasingly important. This thesis focuses on evaluating the existing hazard and risk analysis to find test cases that can be further investigated in order to find alternative test methods. The new test methods are supported by the latest version of the ISO 26262:2018 standard. The tests that are conducted are stress tests of aged cells in a HIL environment which are used to verify the functional safety of the current and voltage limits.

The results show that the safety functions stated in the early version of the technical safety requirements are working for the applied stress tests. It is however questioned if the limits implemented in the software at the time of testing is sufficient to ensure full safety of the battery system. Some tests, especially for aged cells, reaches voltages that are far beyond the safety limits and the exposure time is discussed if long enough to risk significant damage. Solutions are presented that could mitigate the issues that are found during the testing process.

Keywords: Functional safety, HIL, Verification, Validation, 26262 , BMS, Automation, BEV.

Acknowledgements

First of all, we would like to express our gratitude to Anna Niemi who gave us the opportunity to conduct our thesis work at Volvo Cars Corporation. We are really appreciative of our supervisor Lucas Bergman for his guidance and consulting throughout the thesis work to lead us in the right direction. A special thanks to Karthik Hitavalli Prakash who have helped us to implement our modifications in the HIL model, despite his busy schedule, and Simon Torstenson who have helped us with practical issues regarding the HIL simulator.

We would like to express our appreciation to Torbjörn Thiringer who agreed to be our examiner and provided us with useful feedback and support throughout the thesis work. We would also like to thank Alberto Isernia, Alma Ciric, Bengt-Inge Larsson, Kristian Frenander, Naresh Reddy and Shivadeep Maheswar for their help and support in providing necessary information and experience for the thesis work.

Carl Bierich, Gothenburg, June 2019
Emil Magnusson, Gothenburg, June 2019

Acronyms

ASIL	Automotive Safety Integrity Levels
BEV	Battery Electric Vehicle
BMS	Battery Management System
CAN	Controller Area Network
ECU	Electronic Control Unit
ECM	Engine Control Module
EOL	End Of Life
E/E	Electrical and/or Electric
FSR	Functional Safety Requirements
FTTI	Fault Tolerance Time Interval
GUI	Graphical User Interface
HARA	Hazard And Risk Analysis
HIL	Hardware-In-The-Loop
ICE	Internal Combustion Engine
ICM	Inverter Control Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISTQB	International Software Testing and Qualification Board
I/O	Input and Output
LCO	Lithium Cobolt Oxide
LIB	Lithium Ion Battery
Li	Lithium
OCV	Open Circuit Voltage
SEI	Solid Electrolyte Interface
SFC	Sequential Function Chart
SOC	State of Charge
SOH	State of Health
TSR	Technical Safety Requirements

Contents

1
Introduction

To ensure the safety of the battery, the battery management system (BMS) needs to operate the battery within certain limits. These limits are expressed as safety conditions within the BMS software. For each new software that is introduced in the BMS one or a series of tests need to be performed in order to verify that the safety conditions are not compromised. To verify the functional safety of the system, tests can be performed in a hardware-in-the-loop (HIL) environment. The control unit of the battery is then connected to hardware which is running a simulation environment, making it possible to perform tests on the BMS software implemented in its dedicated hardware. This increases the credibility that the testing in the simulation environment has the same consistent outcome as for a physical test and that it follows the safety standards.

1.1 Problem background

Electrification of vehicles is a part of Volvo Cars future and the ambition is to have 50% of the sales volume to be fully electric by the year 2025. One of the most important aspects of going electric is to embrace a cleaner mobility. By going electric it is possible to regenerate energy from braking, which is one benefit that improves the overall energy efficiency of the powertrain. When comparing an internal combustion engine (ICE) and an electric motor it is also clear that the later is much better in terms of energy efficiency [1]. The higher overall energy efficiency results in a lower energy consumption, which can also be replaced with electric energy from renewable energy sources instead of energy from combustion of fossil fuels.

The BMS controls the battery to operate optimally and within safe limits to protect it from abuse situations. The vehicle performance can in this way be secured and the batteries lifetime increase. If a failure or malfunction of the system occurs, the BMS should make sure that the battery is disconnected from the electrical system and prevent hazardous events. It has several important functions such as monitoring the state of the battery, balancing the battery cells and reporting data. One of the most important parameters the BMS has to monitor is the temperature of the battery. The battery should operate within a certain temperature range to avoid degradation of the cells, which temperature range depends on the chemistry [2]. To ensure that the control unit is robust and reliable, tests of the system is necessary.

As all new developed software must be tested, the procedures can be repetitive and costly. The executed code used for operation of the vehicle increases exponentially, which leads to a need for more software verification[3], [4]. To be certain that safety is guaranteed, many of the tests are performed both in a simulated environment and physically in the car. To reduce the costs of the tests it is favourable to automate as many as possible of the tests performed in the simulated environment. In order to do so the standards regarding functional safety must be interpreted and integrated in the testing.

Safety within the automotive industry have always been a topic of great importance. In order to be sure that all car manufacturers performs validation and verification of their electrical/electronic (E/E) systems, the international organization for standardization (ISO) has published the standard ISO 26262, titled "Road vehicle - Functional safety". It is an adaptation of the international electrotechnical commissions (IECs) standard IEC 61508 which provides a framework for functional safety related systems in vehicle development, which should be followed to verify that tests are performed correctly. As the technical complexity of automobiles increases, ISO 26262 includes guidance for appropriate requirements and processes to avoid the increasing risk of systematic failures.

1.2 Previous work

Research in order to understand the degradation and hazards with LIBs is a hot topic as the automotive market is going electric. All vehicle and battery manufacturers are competing to develop the most efficient BEV, with a competitive range and price against the ICE vehicles. Batteries are tested in abusive conditions in order to examine how they behave and what the effects are. The effects are still uncertain as the battery development leads to new designs, materials and chemistries used in the battery cells. Due to this, the full understanding of how a LIB ages and degrades with time is never accomplished while still being relevant. To make sure that the battery operates correctly, the battery must be tested when integrated with the electrical system. This research has been specifically hard to find as vehicle manufacturers do not want to share their research.

1.3 Purpose

The purpose of the thesis is to test alternative test methods to trigger faults in the BMS in simulation environment, to broaden the test coverage and improve the troubleshooting of the system. The test methods will be investigated if possible to use to confirm that aged battery cells still fulfills the functional safety requirements in accordance with ISO 26262.

1.4 Scope

Standards related to automotive system safety, where the focus will be regarding validation and verification of tests on system and functional level for the BMS. The standards should be interpreted, taking into account how they impact the testing procedure. To keep the scope of this thesis feasible, the following will be considered:

- ISO 26262-4:2018 Road vehicles – Functional safety – Part 4: "Product development at the system level" will be taken into account when designing tests. Other parts of the standard might be reviewed if necessary.
- The BMS system will particularly be considered, but other control units in the vehicle will be observed if necessary.
- A test scope will be defined at a high level, which will then be decomposed to lower levels to find and select the most suitable test and validation methods.
- Tests for battery electric vehicles (BEVs) will be in focus.
- Changes will be performed on parameters through scaling factors in the existing model. Changes in the existing model structure will not be performed.
- The testing will be performed on voltage and current limits only, as a thermal model is not yet implemented in the HIL simulator available for this thesis.
- Testing at different temperatures will include 20 °C, 0 °C and -10 °C. More temperatures was not included to minimize the amount of tests.
- A script for automated testing will be constructed and executed for one of the test methods that are suitable for automation as a proof of concept.
- Evaluation of the social and ethical aspects will mainly focus on the risks and benefits of performing safety tests in a simulated environment.
- The sustainability aspects of this thesis will be focused around the limits of the safety functions and how they may affect the lifetime of the battery.

1.5 Ethical and sustainable aspects

Volvo has always been a car manufacturer with a focus on the safety of the driver and passengers. The company has a vision that no fatalities or severe injuries should occur in a new Volvo car by 2020 [5]. Ensuring that cars are safe involves rigorous testing which is a field where Volvo has a lot of experience [6]. Testing can be performed both on hardware and software, where both are important parts of battery testing. As an example; both needs to be tested so that the energy in the battery is utilized sufficiently within safe limits. It is the software of the BMS which is tasked with keeping track of the operation of the battery and ensure that it is done safely. As the battery contains large amounts of energy and is constructed using materials that are highly reactive, using it outside of the limits may cause reactions that are uncontrollable. However, the car should utilize as much of that energy as possible without infringing on the safety, to supply the driver with the best possible performance. Performance in this case referring to power output, energy content and life time of the battery. Setting the safety limits is therefore a balance between safety and performance but safety should always maintain top priority.

Testing of the BMS should give evidence of safe operation of the battery under normal conditions but also prove that safety measures are taken if a hazardous event is predicted. Expanding the different scenarios that are tested can bring further assurance that the safety is sustained under various circumstances. The end goal is for occupants of an electric vehicle to feel as safe or safer than in a conventional ICE vehicle. If standards are used during the development and testing, it provides assurance that the product is engineered using processes that are planned, executed and documented carefully. Implementing tests in a simulated environment, where it is possible to automate tests, can free up time for testers to perform other tests which makes the work more efficient [7]. If the testing is done efficiently then this can save cost of the product which means that final prizes can be reduced. As lower costs will make the BEVs more competitive against ICE vehicles, this is a valuable development process to improve in order to motivate people to buy BEVs.

Volvo also has a goal that 50% of the sales volume in 2025 is to be fully electric [5]. Electrification is part of the sustainability goals as BEVs has a lower emissions of green house gases compared to conventional ICE vehicles [8], [9]. The emission of green house gases does however depend on the lifetime of the vehicle, which in the case of BEVs depend on the lifetime expectancy of the battery. This relates back to the operation of the battery as the extent of degradation relates to how harshly the battery has been operated. If the limits are too high or too low then operation close to the limits may cause accelerated degradation. Setting the limits with some safety margin may mitigate this problem as long as the allowed operation time beyond the limits is not long.

Increasing the lifetime of the battery is of importance as it means that the resources, such as lithium or cobalt, are used in a sustainable way. An aged battery also has a higher internal impedance which causes more losses within the battery, decreasing the efficiency. Keeping the battery at a healthy state longer prolongs the time span in which the battery is utilized with lower losses.

2

Theory

In the following chapter the working principle of a lithium ion battery (LIB) will be explained, as well as factors which leads to degradation of battery cells. The purpose of the BMS and working principals in order to prevent degradation and hazardous events will be described. Finally, the ISO 26262 series of standards and verification methods will be presented.

2.1 Li-ion battery

The LIB stores energy electrochemically by transferring lithium ions (Li-ions) back and forth between the cathode and anode material. When the LIB is discharged all Li-ions are located in the cathode material. The cathode material often contain a mixture of transition metals to minimize the weight and to be able to store as many Li-ions as possible, in order to increase the energy density [2]. When the LIB is charged the Li-ions will be transferred through the separator, which prevents the cathode from getting in contact with the anode. A direct contact between the anode and cathode would result in a short circuit, which could lead to a fire. The Li-ions can move freely in the electrolyte which the cathode, separator and anode are soaked in. As the Li-ions are transferred to the anode, electrons will flow in an external circuit through the aluminum and copper current collector which connects the cathode and anode. The separator, which consist of a thin porous paper film, galvanically isolates the cathode and anode from each other. This forces the electrons to move through the external circuit, as the Li-ions move through the separator. When the Li-ions have passed the separator they will be stored in the anode material which usually consists of hard carbon or graphite. When all cyclable lithium is located in the anode the battery is fully charged. If the battery is instead discharged, the Li-ions and electrons will move in the opposite direction and the Li-ions will be stored in the cathode material. A simple structure of a battery cell can be seen in Figure 2.1.

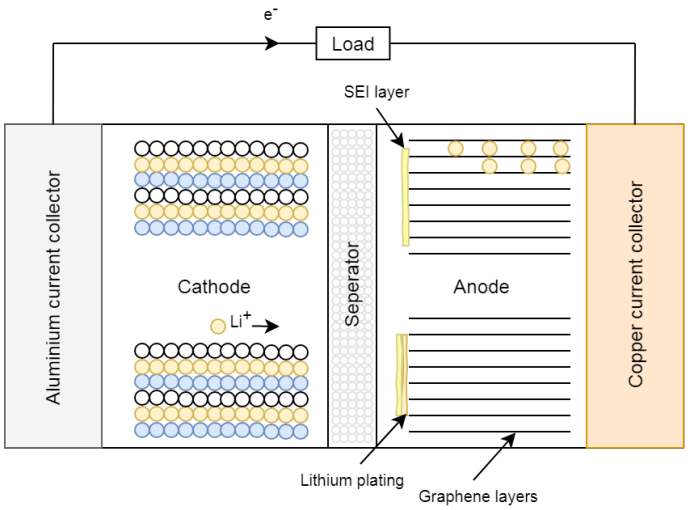


Figure 2.1: Structure of a battery cell [10].

A battery pack is constructed using a number of modules. Each module contains several cells that can be connected in series to increase the voltage across the module, in parallel to increase the capacity or a combination of both. To describe how the cells of a module is connected an annotation like 3P4S is used. This means that three cells are connected in parallel and four of these parallel connections in series. As three cells in parallel has trice the capacity but the same voltage as one cell they are often referred to as a logical cell. Figure 2.2 shows the layout of a 3P4S battery module which consists of four logical cells.

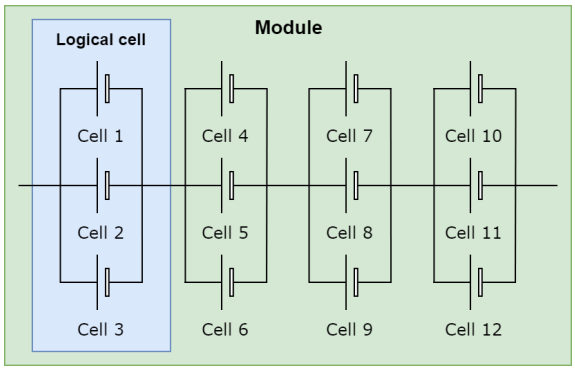


Figure 2.2: Illustration of a 3P4S module.

2.1.1 Variance in Li-ion battery impedance

The impedance of the battery depends on several factors, such as structure and material compositions, which can be presumed constant during operation. It is also affected by aspects that are dynamic in time, such as temperature and state of charge (SOC), where the temperature has the largest impact, which has been shown in [11] and [12]. This is mainly due to the ionic conductivity of the electrolyte being strongly temperature dependant. Due to these dependencies, the usage of the battery can vary largely depending on the climate in which it is operated.

2.1.2 Degradation of Li-ion battery cells

As batteries are used, the chemical reaction changes over time and the characteristics of the battery is altered due to different mechanisms. The main factors that degrade a LIB is material degradation in the electrodes and side reactions in the interface between electrodes and electrolyte. Both of these result in less cyclable Li-ions [2]. The first part of this degradation occurs already in the first couple of cycles.

The degradation of a LIB is related to the amount of cycles experienced, which will have a negative impact on capacity and performance of the battery [2]. As can be seen in Figure 2.3, the capacity of the battery decreases rapidly in the beginning and at the end of life (EOL). In the first region the capacity fade mainly occurs due to formation of the cell and loss of cyclable lithium which builds up the solid electrolyte interface (SEI) layer. During cycling of the battery the SEI layer may crack which will result in new exposed electrode material and more lithium will be consumed to form the SEI layer. This results in the capacity fade in region 2 and 3, but in region 3 loss of active material is also accountable for the capacity fade. However the formation of the SEI layer is the dominant factor for the loss of cyclable lithium. In region 4 the amount of cyclable lithium is greater than the active material in the cathode, which will increase the rate of Li-ions trapped in the negative electrode. At this point the capacity of the battery will decrease faster. The EOL for vehicle application is usually defined at 80% of the initial capacity, which is located before region 4.

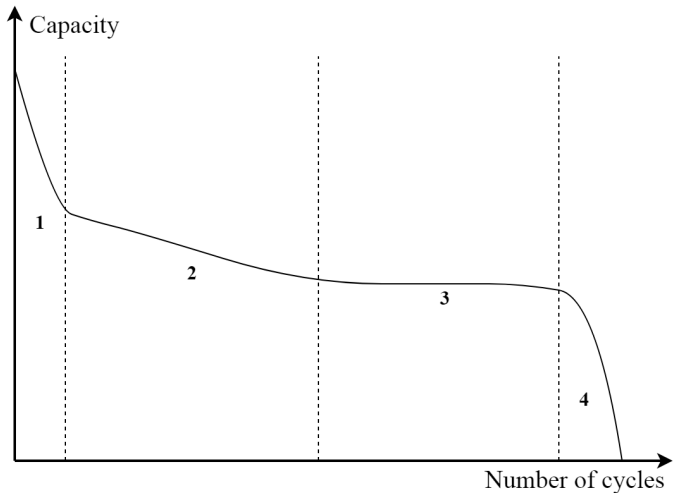


Figure 2.3: Capacity vs number of cycles with regions with different characteristics of degradation [2].

This degradation happens in all cells but can be accelerated if the battery is used outside of optimal conditions. Such causes can be overcharge or overdischarge and overcurrents. If cells are overcharged, i.e. voltage across the cell is to high, then there are no more Li-ions to be moved from the cathode to anode, which will increase the impedance. In turn the energy put into the cell will be converted to heat which accelerates side reactions [13]. These side reactions consumes some of the cyclable lithium, reducing the cells capacity. Another disadvantage of overcharging cells is that if excessive amounts of Li-ions are extracted from the cathode the structure of it might become deformed, leading to less ions being inserted into the cathode during the discharge following an overcharge [2]. One of the largest potential risks of overcharge is lithium plating of the anode, which occurs when lithium ions cannot be inserted into the anode [14], [15]. Lithium plating may cause dendrites as the current is no longer uniformly distributed over the electrode surface. The dendrites are basically whiskers of lithium metal stretching out from the anode material that can lead to an internal short circuit of the battery.

The effects during overdischarge is that the SEI layer of the anode starts to dissolve and expose new active electrode material to the electrolyte. This will initiate the development of new SEI during the subsequent charge to repair the damaged areas, which will consume cyclable lithium [2]. When cells are overdischarged there is a reaction that dissolves the current collector of the anode. This reduces contact between electrode and current collector ,which increases the resistance. The dissolved particles from the current collector can also stick to the separator or penetrate it, forming metal plating on the separator or cathode. This metal plating can create conducting paths or support lithium plating which leads to decreased capacity and internal short circuits [16], [17]. The worst case scenario is that a short circuit occurs between the aluminum collector and the anode. The low electrical resistance of the anode and the low thermal conductivity makes it possible for a high current to flow, but the heat will be trapped in the anode material [18]. Overdischarge may also cause thermal stability changes which can make it more sensitive to abuse conditions.

Overcurrents will deplete the lithium ions from the surface of the electrodes faster than the ions can diffuse within the electrode material. This causes an increased impedance which will increase the temperature of the battery, that in turn accelerates unwanted side reactions that reduces the capacity [2]. Depending on the SOC of the battery an overcurrent may also be the cause of an over or undervoltage.

Apart from degradation inside the cell, the degradation can be accelerated if one cell connected in parallel has degraded faster due to the production lot [2]. This will impact all cells connected in parallel and converge all cells to age according to the cell with lower state of health (SOH) [19]. The reason is that the lower SOH cell experience lower current compared to the cells connected in parallel, as it has an increased resistance. The higher currents in the healthy cells will result in increased ohmic heat generation and faster ageing until they reach the same SOH as the degraded cell. According to [19], a 60% difference in peak cell current is observed when four cells are connected in parallel with a 30% difference in impedance.

2.2 Battery management system

The BMS is responsible for managing the correct functional performance of the battery. To prevent hazardous events the BMS monitors the voltage, current and temperature to operate these parameters within a safe operational window [20]. If the BMS detects any safety risks, which can lead to a thermal or gassing event in the vehicle, safety measures should be taken to prevent this from occurring. These safety actions can be to limit the operational load, and if that does not work the contactors that connect the battery to the rest of the high voltage system should be open by the BMS. Therefore it is of high importance that the BMS is robust and has consistent and correct implementation. Another important objective of the BMS is to estimate different parameters, such as the SOC, SOH and power limits. This allows the system to estimate the driving range of the vehicle and the power losses in the battery, which leads to degradation of the battery cells. As it is difficult to measure the exact internal temperature of the battery cells the estimated power losses in the battery cells makes it possible to estimate the internal temperature as well [2].

2.2.1 Battery cell model

The battery cell model implemented in the BMS to estimate the state of the battery consists of RC-links. The electrochemical reactions which occurs in a battery cell depends on polarization and diffusion [2]. These effects can be explained by the movement of the ions in the electrolyte and how they interact with the electrodes. To represent these effects in a battery cell, which determines the characteristic impedance, cascaded parallel RC-links can be used. There is also an internal resistance in the battery which is represented by a single series resistance. An example of a 2 RC-link model is presented in Figure 2.4.

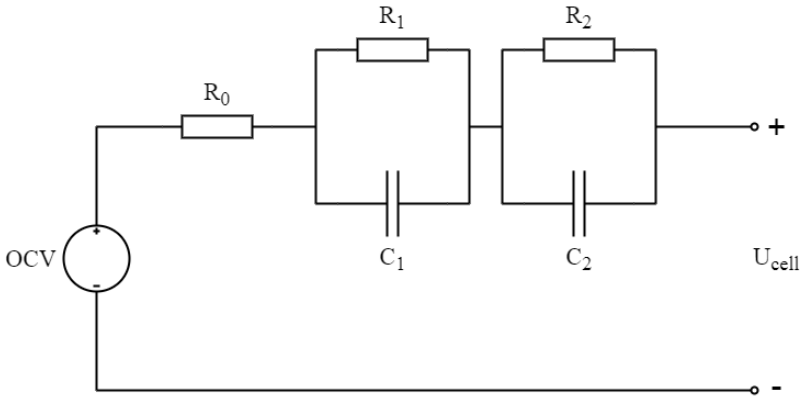


Figure 2.4: The electric circuit of a battery cell model.

The RC-links gives the model its dynamics and by choosing appropriate values for the resistance and capacitance in parallel, the desired time constant τ can be determined according to

$$\tau_1 = R_1 \cdot C_1 \tag{2.1}$$

$$\tau_2 = R_2 \cdot C_2 \tag{2.2}$$

where R_1 is the polarization resistance, C_1 the polarization capacitance, R_2 the diffusion resistance and C_2 the diffusion capacitance. The series resistance R_0 in the model represents the ohmic resistance in the battery which results in an initial voltage drop. The battery cell model is used to determine how the cell voltage varies over time according to

$$U_{cell} = OCV - I(R_0 + R_1(1 - e^{\frac{t}{\tau_1}}) + R_2(1 - e^{\frac{t}{\tau_2}})) \tag{2.3}$$

where U_{cell} is the cell voltage, OCV is the open-circuit voltage and I the current.

A Nyquist plot demonstrates how the different chemical reactions in the battery cell impacts the impedance. In Figure 2.5 the characteristic impedance can be seen for a common LIB. The semi-circle represents the polarization, where the charge transfer at the electrode has the biggest impact on the impedance phenomena. It also depends on the concentration gradient of ions at the surface of the electrode, but it does not have as much impact as the charge transfer. When the impedance drastically increase and becomes highly capacitive depends on diffusion. The process of polarization and diffusion occurs at different rates, which is represented with the different time constants in the model [21].

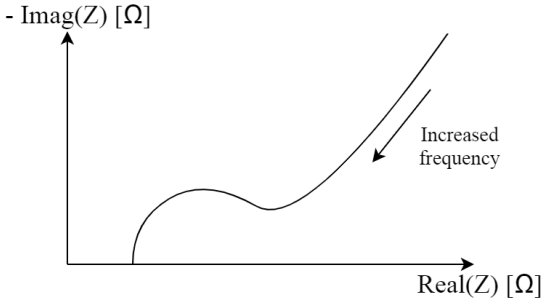
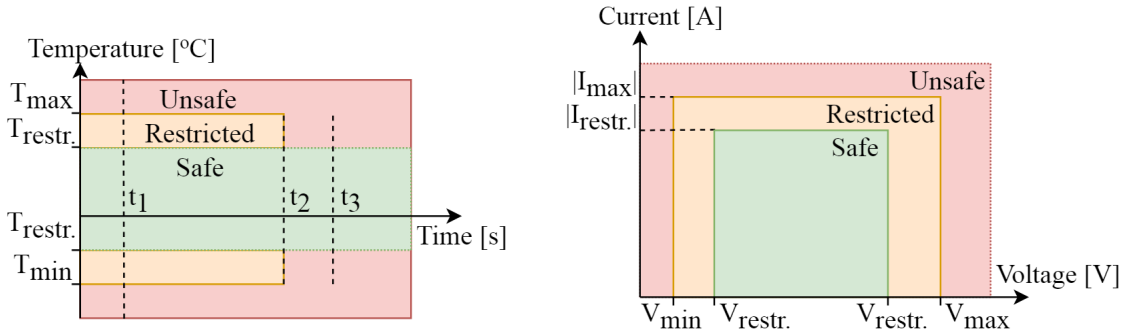


Figure 2.5: Nyquist plot for a common Li-ion battery.

The impedance of the battery cell is influenced by several different parameters. The battery behaviour depends on temperature, SOC, current level, previous short-term history, pressure and ageing [2], [22]. The factors that are considered in the model is the temperature and SOC, as these are the parameters that affects the impedance the most. The parameters in the cell model can be changed for each battery cell so that the characteristic impedance looks different for each of them. By increasing the impedance for one of the battery cells it is possible to emulate a degraded or defect battery cell in an otherwise healthy battery pack.

2.2.2 Operational window

In order to use the battery safely, it should be operated within certain temperature, voltage and current limits [2]. These limits provide the conditions for normal operation and for restricted operation, where the battery can be used for a limited time with restricted power input or output. If the battery is operated outside these limits longer than a certain time it can be considered as unsafe. The limits can be provided by the battery manufacturer and are based on their risk analysis. Internal testing at the company, together with calculations performed by the computer-aided engineering team is used to complement the recommended limits from the manufacturer. Figure 2.6 shows how this type of operational window can be set by the voltage, current, temperature and time limits in two different ways.



(a) Operational window of the battery set by temperature and time limits in the BMS.

(b) Operational window of the battery set by current and voltage limits in the BMS.

Figure 2.6: Example of how operational windows can be defined by limits in the BMS.

The times in Figure 2.6a represents the maximum time that the battery is allowed to be operated in that temperature interval, were t_1 is the time before disconnection of the battery if the temperature is in the unsafe temperature range. The second time, t_2 is the time the battery is allowed to operate in the restricted operational window and t_3 is the maximum time allowed for disconnection if the battery is in the restricted operational window longer than t_2. These types of time limits are also defined for the voltage and current limits in Figure 2.6b.

The voltage of the operational window is based on the OCV profile of the battery. How the OCV profile looks depends on the battery chemistry, its internal resistance, capacity, hysteresis and relaxation of the battery [2], [23]. The voltage profile of a common Li-ion battery can be seen in Figure 2.7.

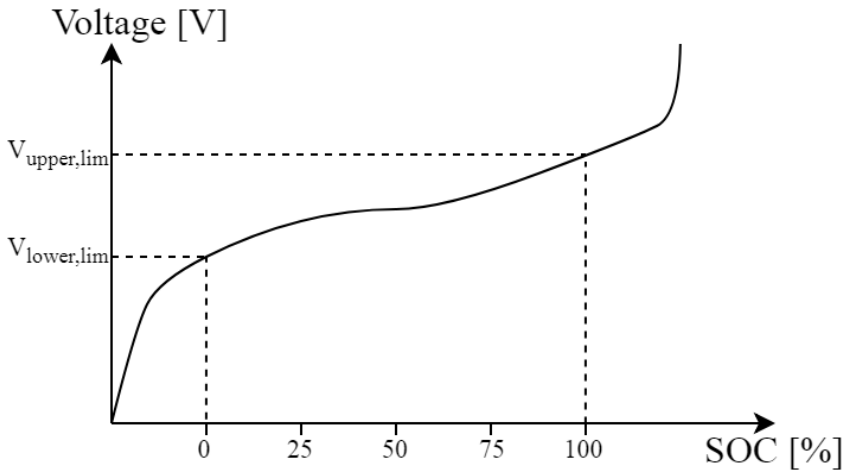


Figure 2.7: The voltage profile of the battery and the set voltage limits.

The reason of investigating the voltage during operation is due to the risk of lithium plating and the build up of dendrites, which rapidly degrades the performance of the battery and is a safety issue [14]. As the LIB gets damaged, if operated outside its operational window, it will eventually lead to a short circuit inside the LIB. A short circuit in the battery is a major concern as it may lead to a thermal runaway and start a fire. This should be prevented with active safety, therefore it is of importance that the voltage limits and fault tolerance time interval (FTTI) are chosen properly.

2.2.3 Thermal runaway

If a malfunction of the BMS occurs it is possible that the battery is overcharged or overdischarged [2]. These events can trigger a thermal runaway, as well as too high currents, mechanical abuse, internal short circuits in the battery and overheating. During an overcharge condition, heat generation can lead to a temperature rise of about 60-80 °C. When the temperature reaches 120-130 °C the separator deforms or partially melts and Li-ions cannot be transferred through it, which is a safety mechanism to prevent any further charging of the battery. When a temperature of 180-190 °C is reached the active electrode material is decomposed and a thermal runaway is unavoidable. Decomposition reactions are often of exothermic character, which means that even more heat will be generated from these reactions. Safety vents in the battery casing will then open and there is a substantial risk that gas will emit from the battery cell. When a thermal runaway occurs the temperature will increase rapidly due to the heat generation inside the battery cell and the risk of cell rupture will lead to a fire. The different failure pathways for a LIB can be seen in Figure 2.8.

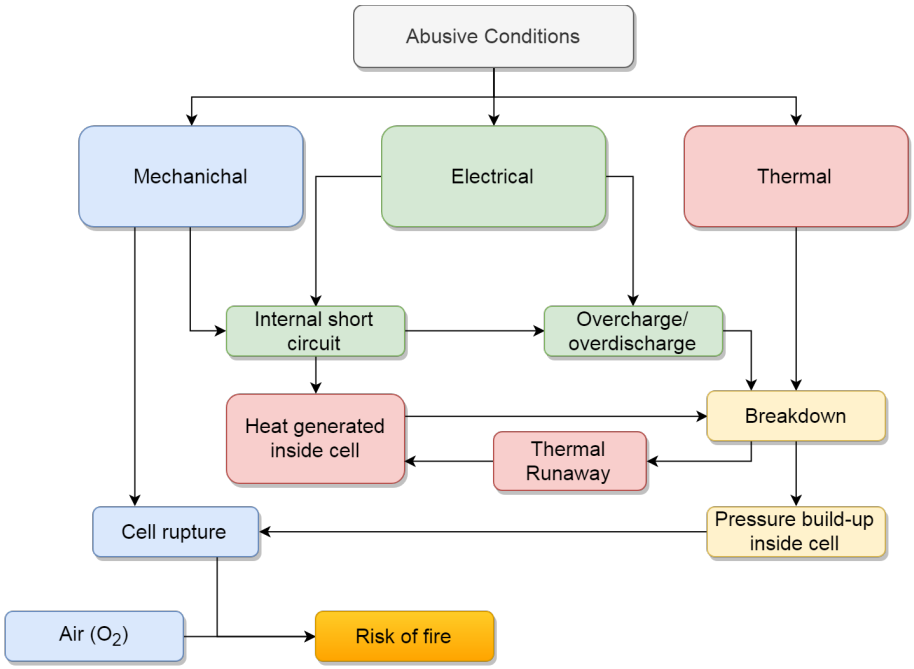


Figure 2.8: The failure pathways for LIBs [24].

Internal short circuits that occur due to manufacturing defects are unavoidable, as the BMS does not have the possibility of detecting these defects [2]. The heat generation of an internal short circuit can be extreme and lead to a rising temperature of several hundred degrees per second. Impure particles originates from the manufacturing and at the time of the inspection of the newly manufactured battery it is impossible to observe. The impure particles will degrade the battery cells in a faster pace and build up dendrites which will eventually short circuit the battery. The risk of a thermal runaway is higher for internal short circuits which slowly builds up over time compared to external abuse. All impurities and internal short circuits will not lead to a thermal runaway, but the impurities increase the risk of internal short circuits, which in turn increase the risk for a thermal runaway.

An aged battery has an enhanced effect to trigger a thermal runaway due to ageing conditions [2]. As the internal resistance of an aged battery increases, the battery becomes more sensitive to overcharge and overdischarge. The increased resistance also results in higher losses in the battery cell which generates heat. Internal short circuits are more common on an aged battery as well, as dendrites have had the time to build up during the battery lifetime.

2.2.4 Discharge of the battery

The voltage across a cell is determined by the OCV and the voltage drop across the internal impedance, which is current dependant. The BMS can extract the energy from the cell either by requesting a constant current or constant power from the battery. Both will reduce the charge in the battery, thus reducing the voltage over time. Requesting a constant power will therefore lead to increasing currents to

compensate for the decreasing voltage. A constant current request will instead lead to a power that decreases with the voltage, This is understood by

$$P = U \cdot I \tag{2.4}$$

were P is the power, U is the voltage and I is the current. Since an increase in current will lead to faster discharge of the battery the voltage will reduce quicker. The rate of discharge of the battery for a constant power request therefore increases with time.

2.3 ISO 26262 series of standards

The ISO 26262 series of standards can be used for guidance to achieve functional safety for E/E systems in road vehicles throughout their lifetime [25]. It is an adaptation of IEC 61508 series of standards and it applies for all safety-related E/E systems. It contains different parts regarding guidance for different stages in the development of a product. The ones that are of interest for tests at system and functional level is part 3: *Concept phase* and part 4: *Product development at the system level*. The concept phase will be considered to validate that the functional and technical requirements fulfill the safety goals, but most focus will be on part 4. If the product development is in accordance with the standard, the functional safety objectives should be fulfilled.

2.3.1 Concept phases

The first step in the concept phase is to define the items purpose, functionality and interface with other systems. To identify potential flaws on the defined item and faults that can occur, a hazard analysis and risk assessment (HARA) is performed. The HARA should identify all the safety risks and classify its severity, probability and controllability [25]. Based on the hazard event and the items functional behaviour, an automotive safety integrity level (ASIL) is determined. Depending on the hazard events ASIL and which safety goal it is categorized under, the safety goal will be assigned the same ASIL. When hazards and risks are identified for the E/E system, specific safety goals are specified to prevent any malfunctioning behaviour through safety-related functions. Such a safety goal could be that the battery should not catch fire under normal operating conditions. The functional safety requirements (FSRs) are derived from the safety goals and can be more specific, for example that the battery should not catch fire during driving. The FSRs which are on an item level are then divided into system level specific technical safety requirements (TSRs). The TSRs could be such that the battery is disconnected if a voltage, current or temperature limit is exceeded.

2.3.2 Functional and technical safety requirements

The safety goals are the top-level safety requirements which are based on the HARA. The FSRs should define the required functionality to ensure that the safety goals are satisfied. A fault tree analysis can be used to identify potential violations of the FSRs and to improve the traceability. It should contain all faults that could possibly occur and the dependencies between them. To determine all faults that can occur in a complex system might be hard, but as many as possible should be ruled out [26]. The faults that are broken down from the FSRs are the basis for the TSRs. These requirements are more specified to a certain fault that must be prevented by the active system and are given ASILs to specify its risk and hazard. In the TSRs there are both functional and non-functional requirements. A functional safety requirement specifies an action that should occur if a certain criteria is fulfilled to achieve or maintain a safe state [27]. A non-functional requirement just specifies a constraint or restriction on the system design that should be satisfied [28]. The TSR states if testing is needed to confirm that the requirement is satisfied or if other verification methods are better suited, like failure mode, effects, and diagnostics analysis. Which environment the test should be performed in depends on the implemented functionality and complexity. It might therefore be adequate to perform the test in other integration sub-phases [29].

2.4 Verification methods

Verification is done in order to ensure that a product complies with the specified requirements [30]. The verification can be done using various methods in several stages of the product development and testing. During development the verification is essentially the evaluation that the items requirement specification, design and models follows the requirements of correctness, consistency and completeness. In the testing process the verification is performed in a testing environment to evaluate that the item comply with the requirement specification. The verification should in both cases be planned, specified, executed, evaluated and documented systematically.

The testing performed in this thesis will be focusing on the system integration, which is addressed in ISO 26262-4:2018 7.4.3 [29], however much of the system will be simulated. This is further explained in Section 3.2.1. The paragraphs of Subsection 7.4.3 in the standard focus on different stages of the system integration, the first being correct implementation of functional and technical safety requirements. The recommended test methods for each paragraph are presented in tables similar to Table 2.1.

Table 2.1: Correct implementation of functional and technical safety requirements at system level [29]. "hr" = highly recommended, "r" = recommended, "n" = no recommendation for or against.

Methods	ASIL			
	A	B	C	D
Requirement based test	hr	hr	hr	hr
Fault injection test	r	r	hr	hr
Back-to-back test	n	r	r	hr

Other tests that are recommended for system integration are performance test, error guessing test, test derived from field experience, internal and external interface tests, interface consistency check, test of interaction and resource usage test. For this thesis the one that will be applied is stress testing. This test method as well as those of Table 2.1 will be explained further in the following sections.

2.4.1 Requirement based tests

Using requirement based testing has two major benefits: first, provide validation that the requirements are correct, concrete and logical; and second, designing sufficient and necessary sets of tests that are based on the requirements [31]. The second benefit does however introduce challenges that must be addressed. The first one is the reduction in the amount of tests that are needed to fulfill the requirements, as there are potentially endless test scenarios. The second is to ensure that the selected tests provides the correct answers for the right reasons, that is they should not provide correct answers if it is done by taking shortcuts. If the tests are selected correctly then they should reduce the ambiguity and provide a clear level of detail. Requirement based testing can be clarified by dividing it into eight parts:

- Define test completion criteria which clearly states when a test can be considered approved.
- Design a test case which sets up the initial condition of the tested function, the database for the test and the inputs, as well as stating the expected outcome, outputs and final system state.
- Build a test case which is done by assembling the data and tools needed to perform the test.
- Execute the test according to the test design and collecting and documenting the results
- Verify test results to ensure that they are as expected, or if not, then analyze why.
- Verify test coverage to track the total coverage of a test or set of tests against the full set of requirements.
- Manage and track defects to ensure that they are handled correctly. This also involves keeping track of the trends in defects.
- Manage the test library, i.e. keeping track of which test has been performed and on which software parts and versions as well as if the test has passed or failed. This is often done by a test manager.

2.4.2 Fault injection test

Fault injection testing at the system level aims at producing a fault in real time and verifying that the outcome is as expected. This can be done either internally in the software by changing values or externally, using hardware that is adapted for the specific system, by setting an interface signal [29]. One way of introducing faults by hardware interfaces without the need for a full system is using HIL, which is further described in Section 3.2.1. Fault injection is an important part when testing safety functions as such functions need to operate correctly but are not expected to be needed during normal operations.

2.4.3 Back-to-back test

Software testing performed in a simulated environment should correspond to the physical environment as closely as possible. To ensure that it does it is important to verify the simulated tests to the physical. To verify that simulation results are correct, the response of a simulation test can be compared with the response within the physical environments to detect any difference [29]. The outcome of a test should result in an equal outcome if the same input is given. However testing of this nature may not be applicable in all cases. If testing in a physical environment could have varying outcome then it will not be comparable to a simulation which produces equal results if repeated. Due to the nature of the tests performed in this thesis, back-to-back testing will not be utilized.

2.4.4 Stress test

A stress test can be performed to verify the correct behaviour of the system when it is exposed to high operational loads. This can be applied on the current, voltage and temperature of the battery and can be used as an alternative method to the fault injection test to verify that safety limit functions operates correctly. By operating the system beyond its limits and analyzing the system at the specified workloads, it is possible to evaluate if the safety is adequate [32].

2.5 Test strategies

The methods described in Section 2.4 can be used to different extent in the testing stage of development. Various verification methods can be used depending on the level of detail that is needed. The selection of verification methods used can be summarized as a test strategy. Some of these test strategies will be explained in the following sections.

2.5.1 Smoke testing

According to the definition by the international software testing and qualifications board (ISTQB) [32], a smoke test is a selection of tests that are performed for the system in order to establish that the main functionality works. These tests should

be broad and preferably simple, to test many of the functions quickly and should not be considering details. Smoke testing can be used to decide if further testing is viable or if there are major issues that needs to be addressed first. An example of a test that could be part of the smoke testing for functional safety of the BMS is if the contactors are closed and opened when requested. A smoke test can be performed at any stage of testing but is mainly performed once changes has been made to the system that could affect the functionality.

2.5.2 Regression testing

Regression testing is performed on the system if a software is updated, bug-fixed or if hardware is replaced. It could also be performed if the environment of the system is changed. The purpose of regression testing is, according to the ISTQB definition [32], to make sure that no unwanted changes or defects has been introduced due to resent changes. This mainly applies to the parts of the system that has not been subject to changes.

Since regression testing should be performed following changes in the system it may be part of many different stages in the development testing. The number of tests that are part of the regression testing may vary depending on if the full set of tests are required to be performed again or just a subset. It might be the case that a certain selection of tests needs to be prioritized in order to solve a persistent issue [33].

2.5.3 Acceptance test

Acceptance testing is part of the final stages before a product is released. According to ISTQBs definition [32], it is performed in order for the customer to determine if the system is acceptable. This is done by formal testing based on the customers needs, requirements and business process and should meet pre-defined acceptance criteria. Acceptance testing is performed once unit, integration and system testing has been performed, as illustrated by Figure 2.9. The delivery can be to customers outside of the company or to other divisions within the company.

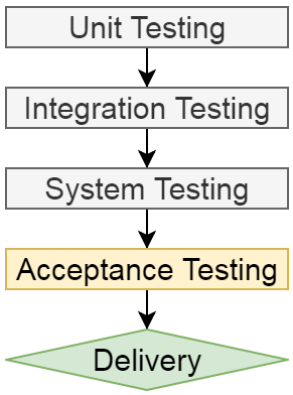


Figure 2.9: Concept of acceptance testing [34].

3
Development of testing procedure

To develop a test procedure in accordance with the relevant standard, ISO 26262, certain steps must be followed to ensure that the requirements are fulfilled. When safety-related functional tests are to be designed the hazards and risks must be considered, which are the foundation for the safety goals of the E/E system. In the following chapter the development of the functional and technical safety requirements will be explained and how they are implemented and tested. It is of high importance that the specifications are followed to guarantee safe operation of the vehicle. The specifications should be clear so that they are interpreted correctly. The set requirements will be verified in the simulation environment but not back-to-back tested in the physical environment due to the nature of the tests being destructive and hard to replicate outside of simulations.

3.1 Validation of concept phase

Initially the HARA as well as the safety goals will be reviewed to examine how the FSRs and TSRs are determined. The scope of the thesis work will be influenced depending on which hazards and risks that are taken into consideration in the analysis. The intention is to guarantee that safe operation of the battery is ensured during its whole lifetime, as its characteristics changes over time. Depending on the outcome of the results the hazards and risks will be discussed if further safety precautions can be taken.

3.2 Case set-up

The set-up of hardware units and software model will be presented in this section to study the functions of the BMS software when implemented in the BMS hardware. The set-up should have a layout and function so that it complies with [29] and [35] in order to be used for safety test verification and validation.

3.2.1 Hardware-in-the-loop

To verify that the control unit works properly it can be tested in a safe and simulated environment to detect and isolate faults before integrating a new software in the vehicles. The HIL set-up used for verification of the BMS in this project is dSPACE SCALEXIO [36]. It is a modular, real-time system that can emulate all the signals and measurements from the rest of the electronic control units (ECUs) in the vehicle, in a closed loop simulation, to represent a real car. An example of the ECU network of a BEV is shown in Figure 3.1 where the BMS is communicating with the engine control module (ECM) and inverter control module (ICM) through the controller area network (CAN) bus.

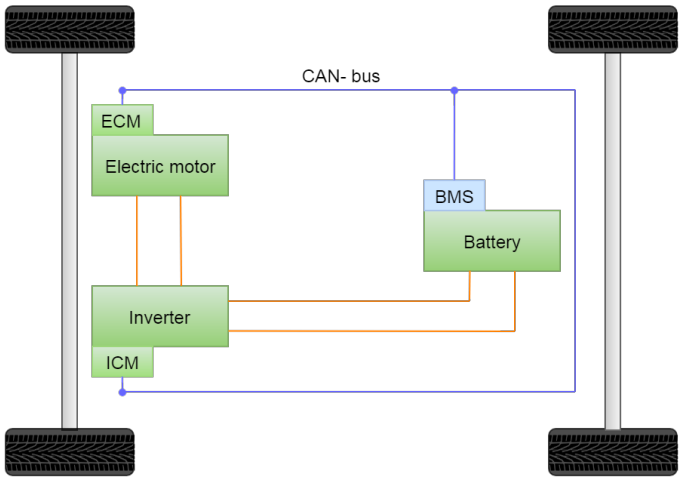


Figure 3.1: Communication connections between control units in the vehicle.

Since it is the BMS that is of interest, the other ECUs and their respective software as well as the communication are emulated in a simulation. All physical components and signals are represented in a so called environment model, which is the environment that the BMS will be implemented in. The environment model is then simulated in the HIL processor which communicates with the test object through input and output (I/O) boards. The processor can also communicate with an external PC on which parameters of the model can be changed and values can be read. The HIL set-up provides an interface between the host PC which manages the test and the object under testing. In some cases the external PC might need to have a separate communication with the test object outside of the HIL. This is because there are internal signals in the test object that are not communicated to the I/O boards. A representation of the HIL with relevant connections is shown in Figure 3.2.

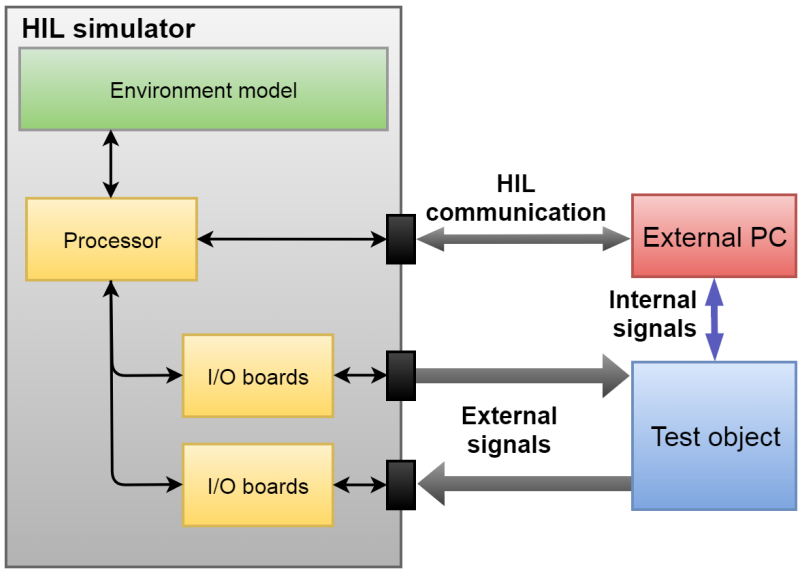


Figure 3.2: Visualization of HIL set-up.

To avoid high voltages and currents in the simulation environment, which are measured in the vehicle in reality, scaling factors are used. When performing tests on the BMS it requires real-time signals. Because of this limitation the test sequences can become time-consuming if many requirement tests should be executed. Since requirement based testing, both functional and non-functional, make up large parts of the tests performed on an ECU, it is preferable to automate these types of tests [37].

3.2.2 ControlDesk

ControlDesk is an experiment setup software from dSPACE which allows for easy ECU measurement, calibration and diagnostics as well as instrumentation layouts [38]. It is beneficial since it allows for easy use of simulation tools, such as HIL modules, as well as vehicle communications networks, such as CAN. It essentially allows for tasks that would normally require several tools to be operated by one single software. The instrumentation layout is based on a modular graphical user interface (GUI) which allows for custom layouts which are adapted to the type of testing that is performed.

3.2.3 AutomationDesk

AutomationDesk is a tool to automate test scenarios in the HIL environment for ECUs. The software is certified by TÜV SÜD, which confirms that it is suitable for testing safety related systems in the automotive industry, according to ISO 26262 and IEC 61508 [39]. The automation tool combines a GUI, for easy implementation and traceability of test scripts, and python based test development. If a specific algorithm is needed, which is not already implemented in the AutomationDesk library, python scripts can be written to add user-specific extensions. Test scripts can later on be reused if stored in a custom library to increase the time efficiency, resulting

in a development process that will speed up with time. A useful feature that can be used to evaluate the tests result is the automatic report generator. After the test script has been executed a document will automatically be generated with the specified content of the test results that is of interest.

3.2.4 Measurement software

Two types of software applications (hereafter referred to as just applications) with associated hardware are used in order to record and store measurement data, as well as write information to the BMS. One application records the signals that are communicated on the CAN-bus, thus it can record all data that is communicated between the BMS and other ECUs. Since all ECUs except the BMS are simulated in the HIL, using the environment model, the signals they communicate on the CAN-bus can be controlled by the user. Such signals can be the power requested by various systems, such as the inverters, air condition or temperature management systems.

The second application can only communicate with the BMS using the internal signals of the controller. The application therefore has access to internal software parameters of the BMS, which can then be changed by the user in real time. The software also has access to all logical cell voltages that are measured by the BMS while only the minimum and maximum cell voltages, as well as the pack voltage are communicated by the BMS on the CAN-bus.

The second software also has twice the sampling frequency which means higher accuracy for fast changing events. This is because the BMS measures a signal and then converts it before communicating it to the CAN-bus, due to this conversion the sampling rate is slower for the CAN-bus.

3.3 Base verification

A base verification is performed in order to establish that the model works as intended in regards to the theory mentioned in Section 2.2.1. Simpler tests are performed with different alterations, one at a time, in order to ensure that each change in the parameters results in the predicted outcome.

The first part of the base verification is to observe the voltage response of the battery cells when a constant current step is applied. The parameters in the battery model will be changed to simulate a highly degraded battery cell or pack, to study how it will affect the voltage response of the battery. This will be compared with simulations using the original parameters in the battery model. The tests performed on the original parameters will be presented as a new cell, meaning a test cell which has not been tampered with.

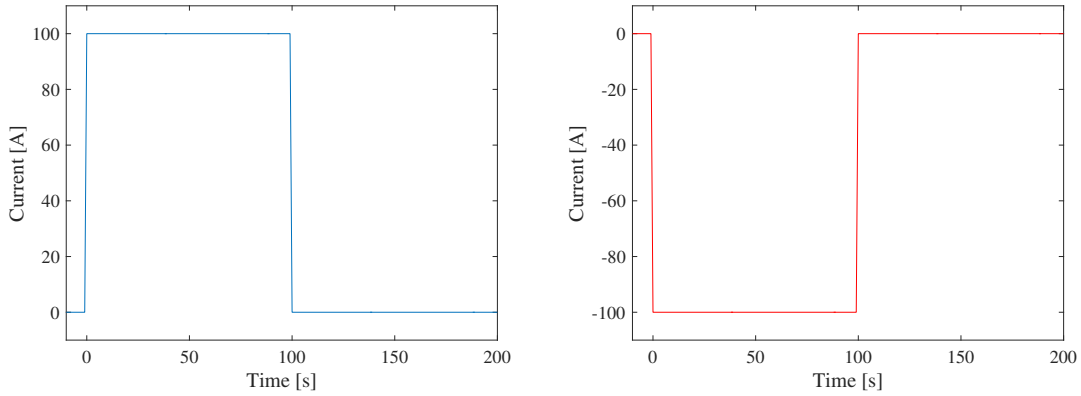
As the tests will be performed for degraded cells with impedance that has changed during the usage of the battery, the impedance parameters of the model needs to be changed. This is done by multiplying the values in the existing look-up tables of the test cell with scaling factors. The changes can however be implemented on all cells using a global variable or on individual cells using a matrix. If the entire pack is scaled to the parameters of a degraded cell this will be referred to as an aged pack. When only one cell is scaled this will be referred to as a highly degraded cell. The scaling factors have been summarized from Figures 5, 7, 8, 12 and 13 in [11] and can be seen in Table 3.1. The degraded cell that was used to establish these scaling factors has been cycled for 1900 cycles at temperatures of -10 to 40 °C and in addition to that stored for 18 months at various temperatures between 25 and 50 °C. This implies that the cell has been used close to how a BEV battery is expected to be used. It is however not a cell that has been in a car but instead the ageing is done experimentally, causing accelerated ageing, which should be considered when looking at the results.

Table 3.1: Scaling factors for the highly degraded cell.

Temperature [°C]	R_0	R_1	C_1	τ
20	2.5	8.6	5.8	50
0	3.3	4.3	11.6	50
-10	3.9	4.2	11.8	50

As the time constant changes with large variance for different temperatures as well as between new and degraded cells it was assumed that it increased 50 times for all temperatures. R_1 is calculated using C_1 and the assumed time constant scaling of 50 from [11]. The SOC dependency has a low impact on the scaling factor according to the data and is therefore not considered.

The voltage response should follow (2.3), which can be verified by looking at the initial voltage drop and the dynamic voltage response. The current should be applied for a specified time and afterwards set to zero. The voltage response once the current is zero can be seen as the relaxation time. The initial conditions for the voltage response test is a SOC of 50% and a temperature of 20 °C, if nothing else is mentioned. The current is either a charge or discharge current of 100 A which is applied for 100 s. The cell is then monitored for another 100 s to observe the voltage response which represents the relaxation of the battery. An illustration of the applied current steps can be seen in Figure 3.3 where a positive current is a discharge current.



(a) Discharge pulse. **(b)** Charge pulse.

Figure 3.3: Example of the current steps that are applied for the base verification tests.

3.3.1 Change of internal series resistance

Once the voltage response has been observed for the original parameters of the model, one or more parameters are changed to see that the model is performing as expected. The first one subjected to change is the series resistance R_0. As the initial temperature for the test is 20 °C the scaling factor is chosen as 2.5 according to Table 3.1. The resistance of each cell is multiplied by this factor and the voltage response is recorded and plotted for comparison with the results of a new cell.

3.3.2 Change of parameters in RC-link

When testing the behaviour of the RC-link both the resistance R_1 and capacitance C_1, which are connected in parallel are changed simultaneously, while the series resistance is scaled to its original value. The reason for this is that the capacitance should mainly influence the time constant and the resistance should influence both the time constant and the final voltage drop across the cell, which gives the impedance its dynamic appearance. Like for the change of internal resistance the parameters R_1 and C_1 are chosen for 20 °C from Table 3.1.

3.3.3 Simulation of aged battery cells

Once the internal series resistance and RC-link has been simulated as aged separately the two tests are combined to simulate an aged battery pack, meaning that both the internal series resistance and RC-link are scaled as they were in Sections 3.3.1 and 3.3.2. This test is performed only for the discharging pulse, with the same initial conditions as previously at 20 °C and 50% SOC. As the temperature has a great impact on the internal impedance of the battery, the test is also performed when the battery temperature is set to -10 °C to see that it affects the voltage response as expected.

3.3.4 Simulation of one highly degraded battery cell

The next part of the base verification is to see how the voltage of a logical cell reacts when one of the cells connected in parallel is simulated as degraded. This represents a worst case scenario where one cell has some form of defect from the manufacturer, causing it to degrade inconsistently with the other cells in the pack as mentioned in [20]. The response will be studied only for the complete logical cell as a voltage can only be measured across the complete parallel connection.

3.3.5 Overriding the cell voltage

To test the safety functions, the simplest method is to override a signal from the environment model with a value outside the range which is considered as safe, then wait for the BMS to act. This can be done for voltages, currents and temperatures individually or in combinations to test the safety functions at different operating conditions. Signals for voltage and current are overridden in these tests to verify that safety functions are operating correctly. The results of these tests will only be presented for overridden voltage in the base verification and if they deviate from the results of other tests in the functional safety verification.

3.4 Functional safety verification

In order to verify the functional safety of the system, tests will be performed to provide results that can be used to evaluate if the functionality is working. An approved test provides evidence that a TSR is fulfilled and ensures safe operation of the product. Different tests will be verified which are related to over- and under-voltages, as well as overcurrents in the battery. There are safety mechanisms which will prevent these from occurring, but as the functionality of the most critical events must be confirmed as well, these tests will be performed without taking all safety mechanisms into consideration. In rare occasions some safety mechanisms might not work properly and in that case the system should still be able to reach a safe state.

Safety mechanisms that should act before the safety limits are reached are the power limits. These should restrict the amount of power that can be requested from or injected into the battery. These changes dynamically based on the current through the battery and the voltage across it. However for the tests in these cases it is assumed that these power limits have stopped working or is miscalculating the limits, allowing the battery to violate the safety limits.

There are also limits as the battery enters the the restricted operation, defined in Figure 2.6b. These limits should be reached before the critical limits and if these limits are exceeded then the discharge power is limited to 15% of maximum specified power or the charging is disrupted in an attempt to get the battery back into a safe state. If the battery operates in the restricted mode for a specified duration then the contactors should open within required time, even though the critical limits has not been reached. For the tests performed in this thesis the limits for the restricted

mode is not yet implemented in the software and can therefore not be part of the tests. This also implies that the tests will focus on the functionality of the BMS for the most critical limits.

As these tests are performed to simulate cases where the voltage and current limits are exceeded, an important part of the analysis is to verify that appropriate actions are taken within the FTTI. If the BMS does not take action then the reason for this will be investigated and possible causes will be presented.

3.4.1 Cell voltage monitoring

If the voltage of the battery cell is outside the operational window, safety precautions must be taken to prevent a thermal or gassing event, but also to prevent degradation of the battery. The worst case scenario is if the battery catches fire, which can take place if a thermal runaway occurs in a battery cell.

When the battery is close to fully charged and a high charging current is applied to the battery there is a risk for an overvoltage. This also applies when the battery is close to fully discharged but the other way around, then an undervoltage can occur if a high discharge current is drawn from the battery. Since the voltage changes with time, as described in Section 2.2.1 it is dependant on the resistance of the cell which in turn changes with the SOC of the battery.

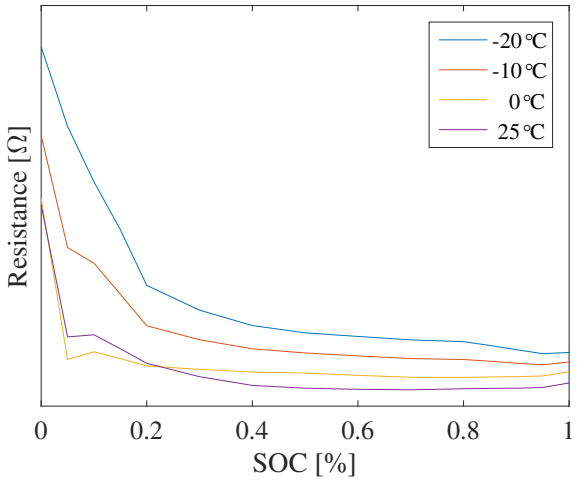


Figure 3.4: Resistance in correlation with SOC and temperature.

As seen in Figure 3.4 the resistance is higher at lower SOCs and it increases with lower temperature. The risk of a critical undervoltage is more likely to occur compared to a critical overvoltage, as the voltage drop becomes higher if the same power is requested at a low SOC compared to injected at high SOC. Therefore the testing performed for the lower voltage limits is of most interest, to see how the system reacts to abusive conditions.

3.4.1.1 Battery at low state of charge

A test is performed to simulate a battery pack which is expected to deliver moderate current/power at a low SOC. The SOC is manually set to 5% and the temperature is initially set to 20 °C. A constant power of 15% of maximum specified power is then requested. The expected outcome is that the current will increase with time as the voltage will follow the OCV curve and decrease with time. The constant power of 15% is chosen as it is the maximum allowed power once the voltage has entered the restricted operation mode described by Figure 2.6 in Section 2.2. The test will continue until the BMS opens the contactors which should be done after a specified time once the voltage reaches the critical undervoltage limit. The test will be carried out for three different temperatures; the initial 20 °C, 0 °C and -10 °C. The test is first performed for a new pack to get a reference, followed by a test performed on an aged pack. The impedance of the aged pack will be altered according to Table 3.1.

3.4.1.2 Battery at high state of charge

A test will be performed similar to the low state of charge test but for a high state of charge, where instead of requesting a constant power from the battery a constant power is fed to the battery. In this test it is expected that the voltage keeps increasing with time while the current decreases. The chosen power that is fed to the battery is 33% of maximum specified power, as this is the highest charging power from regenerative breaking. The test continues until the BMS opens the contactors which should be done after a specified time once the voltage reaches the critical overvoltage limit. The test will be carried out for three different temperatures; the initial 20 °C, 0 °C and -10 °C. The test is first performed for a new pack to get a reference, followed by a test performed on an aged pack. The impedance of the aged pack will be altered according to Table 3.1.

3.4.1.3 One highly degraded logical cell

In order to see how the system reacts if one logical cell is highly degraded, the impedance in a logical cell is changed according to the scaling factors in Table 3.1. An increased resistance over a logical cell should in theory lead to a higher risk of an under- or overvoltage or overtemperature, if the current amplitude is sufficiently high. The test is performed to study if the system opens the contactors when the degraded logical cell reaches a safety critical limit. Another part that is to be taken into consideration is how the non-degraded cells are performing once the degraded cell reaches a limit and if they are utilized poorly and to what extent.

3.4.2 Current monitoring

If the internal resistance of a battery cell is high, the losses when a high current is going through the cells will result in high power losses. The power losses will lead to an increase in temperature which is dangerous in terms of thermal stability. To prevent the cells from heating up to dangerous levels the current is limited if it reaches above a certain limit. If this limitation does not manage to decrease the current then it is cut of after a predefined time.

3.4.2.1 High power request

In order to monitor the effects that ageing of a cell will have on the current response, a test is performed where a constant power is requested from the battery. The initial SOC is set to 80% and the initial temperature set to 20 °C. The requested power is 100% of maximum specified power. As in the test for low SOC the current is expected to increase gradually as the voltage decreases. The test will then continue until the current has reached the limits set by the operational window, as described by Figure 2.6b, or until the lower voltage limit is reached. Once the current or voltage reaches the limit the BMS should open the contactors within a specified time. The test will be carried out for three different temperatures; the initial 20 °C, 0 °C and -10 °C. The test is first performed for a new pack to get a reference, followed by a test performed on an aged pack. The impedance of the aged pack will be altered according to Table 3.1.

3.5 Automation of test

The tests that have been performed for the different voltage and current limits are used to select one requirement that shows promising results which is to be automated. The objective of automating the test is to show a method for how this can be performed and that the result is equal or sufficiently close to that of the manually performed test. As the different test cases are similar, the test script will only need minor changes in order to be performed for the other tests in this thesis.

The test is implemented as a sequential function chart (SFC). A sequence controlled test is used as it is robust if a signal fails and easier to use to handle signal errors. It also gives a clear overview of how the test is performed, which will simplify further modifications. The testing tool is AutomationDesk and the GUI is used to construct the SFCs.

3.5.1 Development of tests

The development process starts with building a sequence which tests the lower voltage limit by setting a constant power request, like the manually performed tests in Section 3.4.1.1. The test should close the contactors, set the initial SOC and then request a constant power. The sequence should then detect the undervoltage, however a time limit is implemented so that the sequence does not get stuck if an undervoltage does not occur. After the voltage limit is reached, or the timer runs out, the program should check if the contactors open within the specified FTTI. Once the FTTI check is done the program restores the power request and requests the contactors to open, as a safety precaution if it is not performed during the low voltage test. Finally the test restores the faults and evaluates the test, which means that it creates a report where steps that have passed or failed are displayed and the stored signals are presented in graphs.

Section 3.4.1.1 describes how a low voltage test is performed for both new and aged cells for three different temperatures. This involves all steps of the automated test mentioned above, from the closing of the contactors to the clearing of the faults. This sequence can therefore be summarized as a low voltage test. The benefit of the automated test is that such a sequence can be performed for both new and aged cells at many different temperatures without any input from the user. An example of how the low voltage test is constructed and implemented in a loop that changes the temperature can be seen in Figure 3.5.

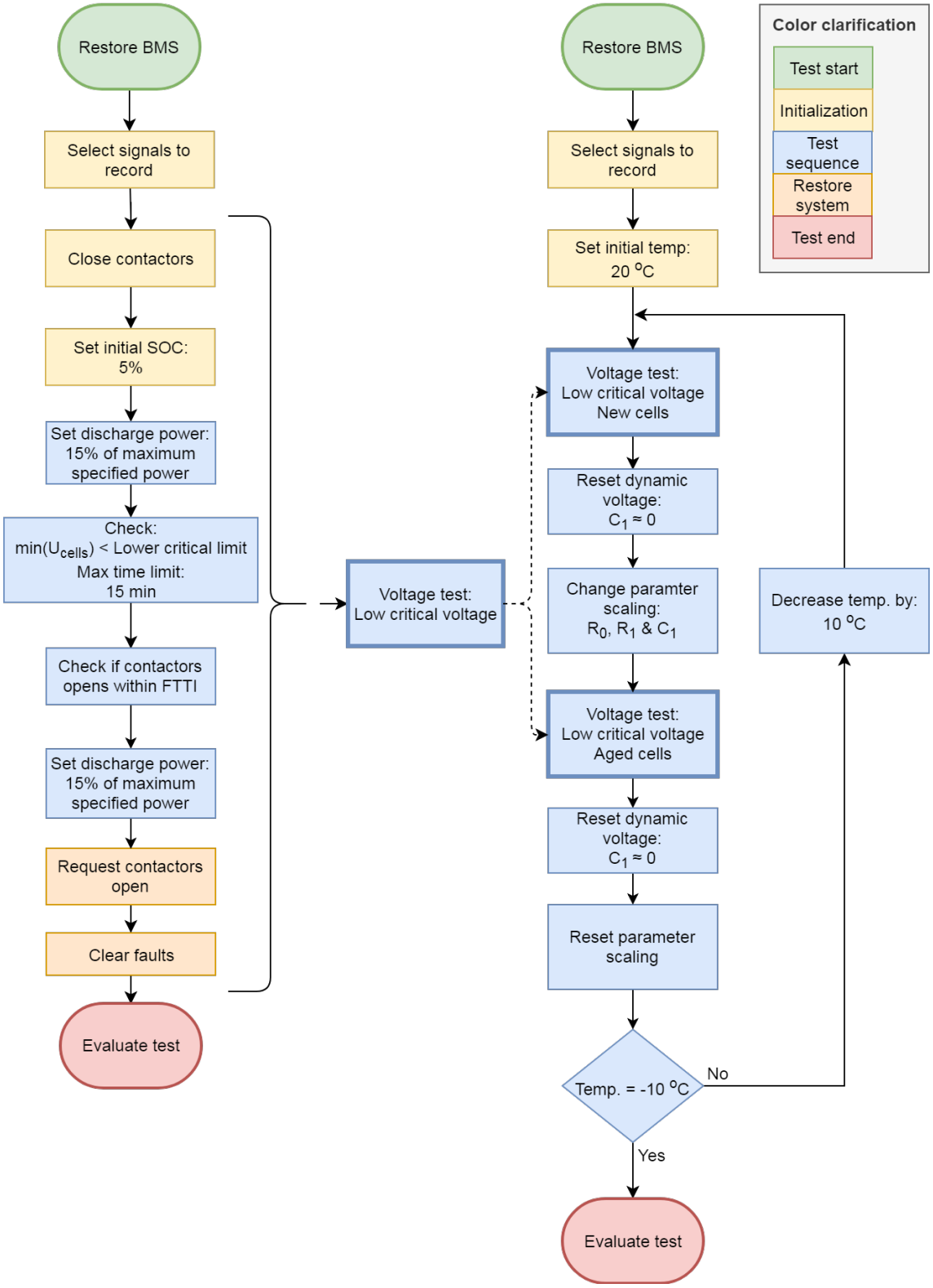


Figure 3.5: To the left: an example of a low voltage test with constant power requested from the battery. **To the right:** an implementation of the low voltage test for both new and aged cells at different temperatures.

In Figure 3.5 there are blocks that are called "Reset dynamic voltage", these are needed in order to cancel out the relaxation effect of the dynamic voltage drop in the model. It basically reduces the time constant so that the discharge in the RC-link is done immediately. This means that when a SOC of 5% is set, it results in the same voltage every time, which gives equal initial starting points for all tests.

3.6 Validation

After the tests have been performed they will be verified against the requirements to establish if they are fulfilled. Once the verification has been performed the results will be used to support the validation of the requirements towards the safety goals. The validation will establish if the requirements are sufficient to reach the safety goals or if further requirement specification and testing is needed.

3.6.1 Functional safety validation

The TSRs will be validated and the test methods that are used will be determined if adequate to prove that the set requirements, which are based on the safety goals, are fulfilled. In order to fulfill a FSR, all technical requirements that are dependent on that requirement must be approved. However, as not all tests of a FSR will be performed they can not be confirmed as fulfilled.

The validation will be based on examination of different type of tests replicating faults to provide evidence for a specified safety-related function. Depending on the outcome of the tests, the safety requirements can be evaluated if sufficient level of integrity has been achieved [27]. If any safety concern is identified, the failure shall be prevented if necessary, in order to comply with the safety goals.

When new types of tests are made the safety goals will be considered as well as variance in operation, which is recommended in ISO 26262-4:2018 8.4.1.3. By including tests on aged battery cells the E/E system can ensure safe operation of the product throughout its lifetime. Some hazards have a higher risk of appearing when the battery cells are aged and therefore it is of interest to make sure that the safety-related functions are working properly in this operational use case. In ISO 26262-3:2018 7.1 the objectives of the functional safety concept is written, which states that the degraded functional behaviour should be specified in accordance with its safety goal.

3.6.1.1 Operational use cases

In ISO 26262-4:2018 8.4.1.3 it is recommended that the safety goals shall be validated taking into consideration different operational use cases, as it might impact the behaviour of the system. By performing the tests for the BMS when the battery has aged and is close to or has reached its EOL, it is ensured that the systems safety is validated throughout its lifetime. In this thesis an aged battery packs characteristics will be used when performing the tests, to verify that the TSRs are suitable

to achieve functional safety. The parameters used are stated in Table 3.1 in Section 3.3. Performing a stress test under high operational loads will give rise to a different behaviour of the battery, this will show how robust the system is and if the correct operation is still sufficient regarding the safety.

The tests performed also differ since they are more similar to how an unsafe voltage or current might be achieved. Limits has previously been tested by overriding signals from the environment model with a value that violates the limits after which the actions of the BMS has been recorded to ensure that these are correct, as described in Section 3.3.5. In the test performed during this thesis the voltage and current response over time is considered in order to investigate how the battery may respond during the time span between fault detection and action.

3.6.1.2 Battery usage limits

The validation of the TSRs will focus on the usage limits for the voltage and current in the battery. Through different test cases, where the power is set to be constant at different levels depending on the test, the voltage and current will be analyzed if they reach unsafe limits within the time that the contactors should open. When a fault is detected there is a time interval that is defined in which the system should react. This is the FTTI and defines the time in which actions needs to be performed in order to reach a safe state once a fault occurs. An example of the FTTI and the events it may contain can be seen in Figure 3.6.

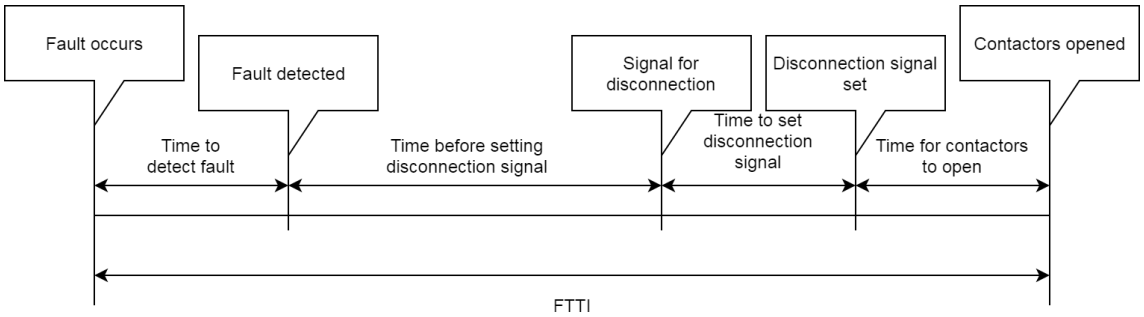


Figure 3.6: Detailed FTTI for disconnection of contactors when a fault is detected.

The fault must be consistent during the time between the detection of the fault and signaling for disconnection in order to request the contactors to open. The FTTI is also used to follow the time of the degradation limits to prevent a hazardous event. The time between fault detection and setting the disconnection signal is typically in seconds while the other time intervals are in milliseconds in Figure 3.6, but due to better visualization the figure is not properly scaled.

3.6.2 Tests in relation to safety goals

When a test has been performed, it should be analyzed to ensure that it covers the TSR from which the test is constructed. Once this is done there should be a validation to make sure that the TSR is in line with the safety goal and that it covers the parts of the safety goals that it is intended to. The results from the test should be used to support the validation of the TSR. Should a test pass in regards to the TSR but a potential safety risk is identified, then a discussion will establish if the risk violates the safety goals and the requirement should be altered. If it cannot be established if the requirement should be altered and further testing is needed, then new tests will be suggested.

4
Analysis

In this chapter an analysis will be performed of how an aged battery pack and a highly degraded logical battery cell impacts the voltage and current of the battery. As the increased impedance of the battery leads to increased voltage drops, it may result in insecure operation. Temperature increase in a battery cell can be enhanced if the battery is aged as well as it becomes more sensitive to overcharge and over-discharge. Besides from ageing, 1 out of 5-10 million cylindrical cells for the most experienced manufacturers has a defect which results in a safety incident [40]. This means that 1 out of approximately 1000 vehicles may have a defect battery cell [41]. This calculation example is related to 18650 cylindrical cells and a Tesla model S 85 kWh. For pouch cells used in this work, the failure rate may be lower or higher but it gives some perspective of the failure rate. The likelihood that battery cells have degraded functionality is most likely higher compared to a defect cell which can result in a safety incident.

The tests performed on the battery during the development stage should guarantee safe operation during its whole lifetime, in the greatest extent possible. The functional safety will be evaluated for which amount of time the voltage is allowed to stay under or over the critical voltage limit of the battery, to prevent unnecessary risks. The limits are presented as dotted lines in the figures. It should be mentioned that the software tested is not intended for production and not yet calibrated correctly. Therefore parameters in the software may differ from the final software.

As there are many safety functions in the BMS that will prevent the battery from operating outside its voltage and current window, these functions are not considered in order to evaluate the most critical safety functions. These functions must be verified as they are crucial if a software malfunction occurs. If safety functions which limits the power do not work correctly it is important that other safety functions in the system still works.

The voltage measurements shown in this chapter comes from the internal signals of the BMS, these values has better accuracy compared to the voltage signal on the CAN-bus. The mean value for 24 logical cell voltages is used to present the logical cell voltage. When a highly degraded logical battery cell is analyzed one of the cell voltage measurements differs from the rest, this voltage is also considered in the mean voltage. Voltages in the text are mentioned in percentage of nominal voltage, while figures are labeled with per unit (p.u.). The measured current is taken from the CAN-bus.

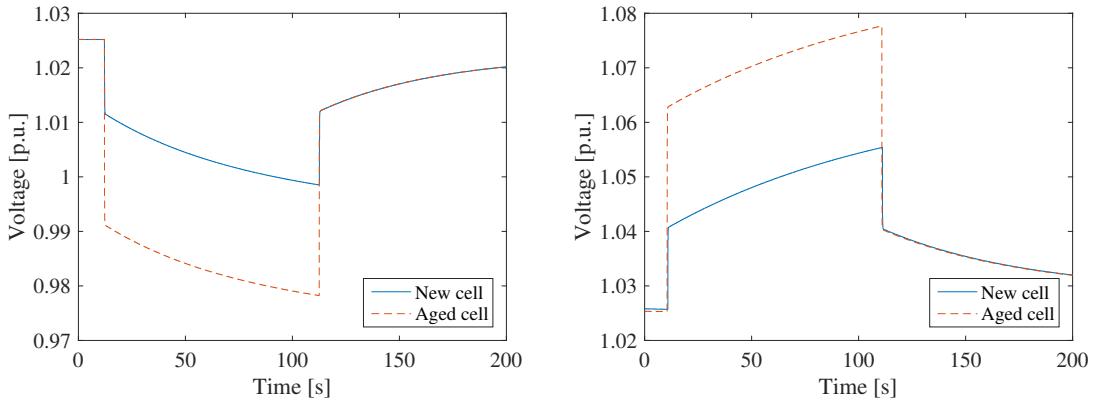
4.1 Base verification

To verify that the model responds according to what is predicted of the battery model, a base verification is performed to see how the voltage responds to a current step when the parameters of the battery cell model are changed. The expected response should follow (2.3) in Section 2.2.1 but for a single RC-link, as this is how the battery is modeled in the HIL set-up.

A charge and discharge current pulse of 100 A is applied for 100 s to analyze the voltage response of the battery cells. Due to the high current the results will be influenced by the change of SOC, but as the batteries capacity is large this will not be considered.

4.1.1 Change of internal series resistance

The first parameters that is changed is the series resistance R_0 which, in the model, represents the initial voltage drop when current is applied. In Figure 4.1 the voltage drop can be seen for a new and aged cell, only considering the internal series resistance to be aged, when a charge and discharge current pulse of 100 A is applied.



(a) Discharge current pulse.

(b) Charge current pulse.

Figure 4.1: The measured voltage drop over a new and aged battery cell for a constant current pulse of 100 A.

In this case the internal series resistance is increased with a factor of 2.5 to simulate an aged battery pack, which results in an increased initial voltage drop. The simulation was performed at a temperature of 20 °C, depending on the temperature of the battery cells the internal resistance of the LIB will vary. This will also result in a change of the voltage drop over the battery cell. When the series resistance is changed the initial voltage drop will do the same. The time dependant change in voltage during the current pulse depends on the RC-link which builds up a higher voltage drop over its impedance over time. This looks the same for both plots, which is as expected. When the current pulse is turned of the voltage will return to its relaxed state where the new and aged cell remains at the same voltage.

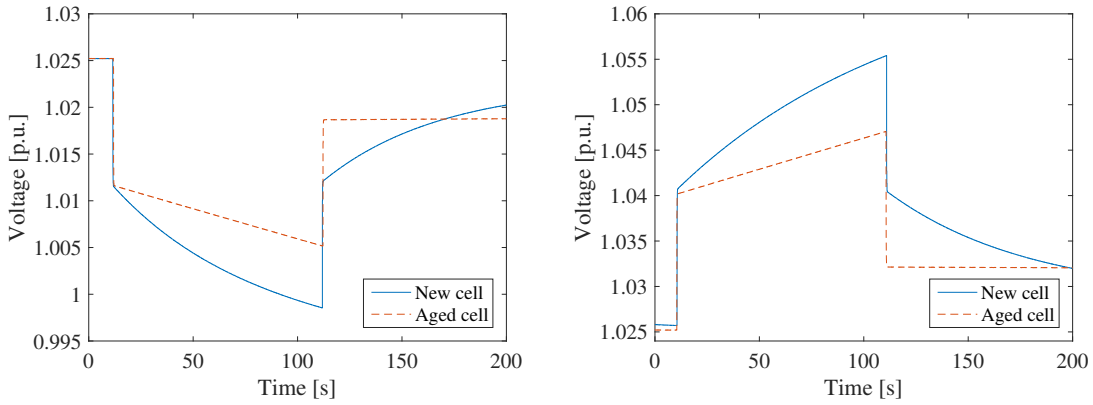
Table 4.1: Voltage drop comparison of new and aged battery cells during discharge and charge.

		Initial voltage drop [p.u.]	Dynamic voltage drop [p.u.]
Discharge pulse	New cell	0.0136	0.0128
	Aged cell	0.0342	0.0128
Charge pulse	New cell	0.0150	0.0144
	Aged cell	0.0375	0.0144

In Table 4.1, it can be seen that the voltage drop and therefore also the impedance of the battery depends on if it is charged or discharged. As both the initial and dynamic voltage drop are lower during the discharge pulse compared to the charge pulse, it indicates that the battery impedance is higher during charging. As the battery ages the initial voltage drop will have a greater impact when a charging current pulse is applied compared to a discharging current pulse. In this test case the charge pulse results in a 10% increase in the initial voltage drop compared to the discharge pulse.

4.1.2 Change of parameters in RC-link

In the second part of the base verification both the resistance and capacitance of the RC-link are changed simultaneously as described in Section 3.3.3. The results of this is presented in Figure 4.2.



(a) Discharge current pulse. **(b)** Charge current pulse.

Figure 4.2: The measured voltage drop over a new and aged battery cell for a constant current pulse of 100 A.

As can be seen in Figure 4.2 the initial voltage drop is the same for the new and aged cells as it only depends on the series resistance of the battery model. As the current pulse test is performed for the new and aged cells at the same initial SOC and temperature, the voltage should be the same before the current pulse is applied. The dynamic voltage drop for the aged cells has a linear appearance compared to the new cells. This is due to the time constant which is 50 times higher for the

aged cells, so it will take much longer time for the voltage to reach steady-state. As the resistance is 8.6 times higher, the voltage drop over the RC-link will be much higher for the aged cell when it has reached steady-state. When the current pulse is turned off the ohmic resistance voltage drop is similar as expected. When the voltage slowly reaches the relaxed state of the cell it can be seen that it will take much longer time for the aged cell to reach it.

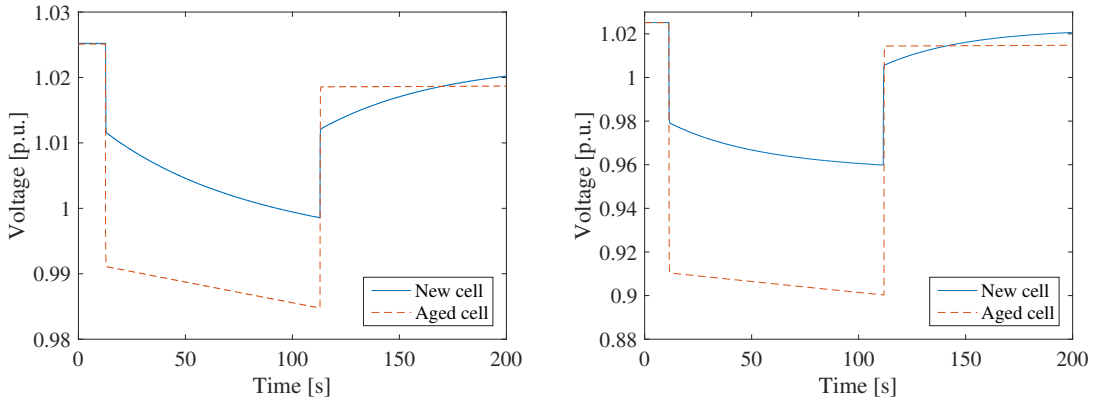
Table 4.2: Voltage drop comparison of new and aged battery cells during discharge and charge.

		Initial voltage drop [p.u.]	Dynamic voltage drop [p.u.]
Discharge pulse	New cell	0.0136	0.0131
	Aged cell	0.0136	0.0064
Charge pulse	New cell	0.0150	0.0144
	Aged cell	0.0150	0.0067

In the same manner as before, the voltage drop increases when a charging current pulse is applied as seen in Table 4.2. After 100 s the dynamic voltage drop is higher for the new cell compared to the aged cell due to the long time constant of the aged battery.

4.1.3 Simulation of aged battery cells

To verify the change in the voltage drop response between new and aged battery cells, both the static and dynamic parameters are changed in the battery model. This results in a voltage difference of 0.0206 p.u. in the voltage drop when the current pulse is applied and turned off. This is seen in Figure 4.3a when a current pulse of 100 A is applied when the temperature of the battery is 20 °C. If a higher current is drawn from the battery it will result in a higher voltage drop difference between the new and aged battery cells.



(a) At 20 °C. **(b)** At -10 °C.

Figure 4.3: The voltage drop over new and aged battery cells when a discharge current pulse of 100 A is applied at different temperatures.

In Figure 4.3b, the temperature is decreased to -10 °C. As the battery cells impedance is temperature dependent and especially sensitive to low temperatures, where the resistance will increase exponentially with decreasing temperature, it is of interest to perform tests at low temperatures. This will result in a larger voltage drop difference between the new and aged cells. The voltage drop difference now becomes 0.0686 p.u. when the current pulse is applied and turned off. The voltage difference have now increased with a factor of 3.3 compared to when the current pulse was applied at 20 °C and will increase even more if the temperature decreases.

4.1.4 Simulation of one highly degraded battery cell

Even though only one cell is defect in the logical cell it will have a small impact on the voltage over the battery cells connected in parallel, seen in Figure 4.4. The voltage drop over the logical cell including the highly degraded cell will be higher compared to the cells in the rest of the battery pack. The voltage drop difference between the highly degraded cell and the mean cell voltage is 0.0064 p.u. initially and 0.0044 p.u. at the end of the current pulse. The voltage drop difference seems to decrease over time.

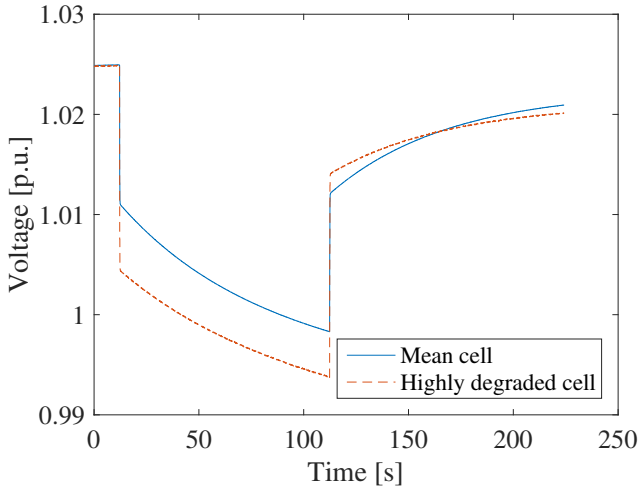


Figure 4.4: The voltage drop over one highly degraded battery cell versus the mean voltage drop over 24 logical battery cells when a discharge current pulse of 100 A is applied.

This difference may not be significant at these voltage levels. However if the SOC of the battery is low then, as known from the OCV curve of Figure 2.7, even small voltage drops across cells may have a big impact on the voltage of the cell. This can in turn lead to the afflicted cell violating the safety limits prior to the rest of the pack. In such a case the degraded cell will reduce the performance of the entire pack.

4.1.5 Overriding the cell voltage

When all cell voltage signals are overridden the voltage drops instantaneously to the set voltage at 39% of nominal voltage. This can be seen in Figure 4.5. For this test the contactors open after specified time. However this is not visible in the voltage as this restored manually after the disconnection event.

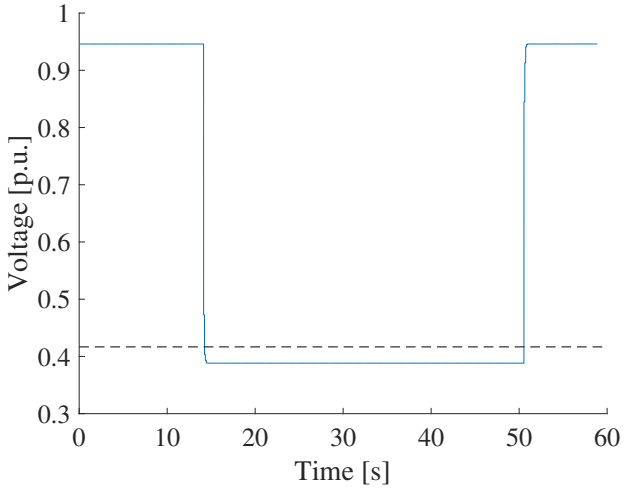


Figure 4.5: The mean voltage drop of 24 logical battery cells when the voltage is set to 39% of nominal voltage.

This is an effective method to perform requirement based tests compared to the stress test, where the voltage is forced below the voltage limit. The test is more time efficient and verifies the functionality of the system. One disadvantage is that it does not consider the batteries dynamic voltage behaviour and how low the voltage can become during a test scenario.

4.2 Functional safety verification

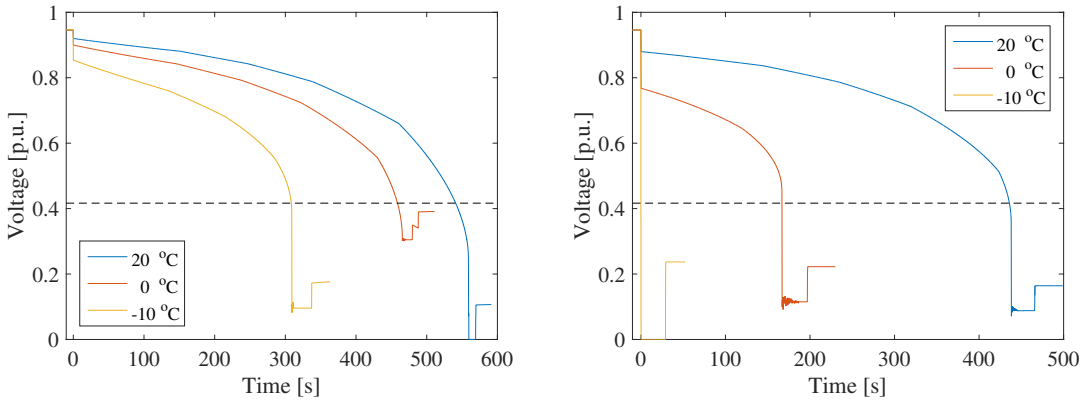
The test method used to verify the functionality of the BMS is stress testing. By verifying the system at high loads it is possible to see how extreme situations can affect the system. It is favourable to stay within the operation window, but due to different operation of the vehicle it is possible to exceed these limits. The tests will verify that the functionality of the BMS works as intended. Besides the functionality, it is also possible to examine how far beyond the limit the voltage or current reaches before the contactors opens.

4.2.1 Cell voltage monitoring

The voltage should operate within the voltage window to prevent accelerated degradation and to ensure safety. Tests are performed both at low and high SOC to evaluate if the contactors opens within the FTTI when the safety critical voltage has been exceeded. If the voltage reaches values that are considered dangerous, an evaluation will be done to assess if it is acceptable.

4.2.1.1 Battery at low state of charge

When a constant power of 15% of maxiumum specified power is requested from the battery at an initial SOC of 5%, the voltage will soon reach the point on the OCV curve where the voltage rapidly decreases. When comparing the voltage for the new and aged battery pack at 20 °C and 0 °C, seen in Figure 4.6, the voltage decreases fast and the safety critical limit at 42% of nominal voltage will be reached faster for the aged battery. At -10 °C the aged cells has such high initial resistance that the voltage drops to 0 V immediately. If the voltage is below the safety critical voltage limit for a specified duration, the BMS should send a request to open the contactors. The longest FTTI that is allowed for overdischarge is 5 seconds longer than the specified duration, it is seen however that the contactors opens after twice the specified duration which is not in line with the requirement. Within this time the voltage will reach an extreme undervoltage, but when the contactors are opened the cell voltage recovers back to a relaxed state. The software is however an early version which does not have the correct time parameters, which was known.



(a) New battery pack. **(b)** Aged battery pack.

Figure 4.6: Voltage measurement for constant power request of 15% of maxiumum specified power.

The reason for the difference in lowest voltage reached for different temperatures is a sensing fault. As the lines show the average value of a total of 24 logical cells and some cell sensors reads out as 0 V while a few seems to lock up at a previous value. It is however most reasonable that all cells would reach 0 V in this kind of tests. However, the measuring signals that reach 0 V seems to lose the measurement completely and does not show any voltage, even after the contactors open. This

would be an unlikely event for a LIB as there should be some OCV once the current is interrupted and the voltage drop across the impedance disappears. This loss of measurements also affect the new voltage after the contactors open, as the graphs show the average.

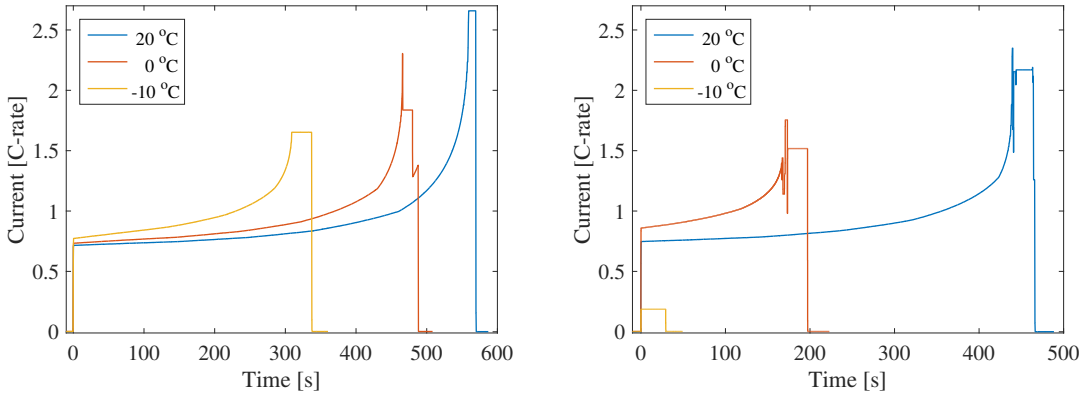
Looking at the signals that show a voltage after the contactors have opened indicates that the voltage starts relaxing as given by Table 4.3. From this it shows that the OCV for the cells becomes lower the longer it takes to reach the limit and open the contactors. This would be reasonable as the voltage drop is lower the higher the temperature becomes, which allows the cells to discharge deeper before the voltage across them reaches the limit.

Table 4.3: Relaxed voltage after contactors has opened.

Temperature	[°C]	-10	0	20
New cell	[p.u.]	0.697	0.578	0.422
Degraded cell	[p.u.]	0.947	0.889	0.656

As the internal resistance impacts how fast the voltage will decrease, a lower temperature will affect the results in the same way as the comparison between the new and aged battery pack. With decreased temperature the internal resistance will increase inside the battery cells and result in a higher voltage drop. In Figure 4.6 it can be seen that voltage decreases faster for the battery exposed to a colder climate.

As the battery cells voltage is decreasing and a constant power of 15% of maximum specified power is requested, it will lead to an increase in current, explained in Section 2.2.4. Due to the increased current when the battery is fully drained, seen in Figure 4.7, the voltage will decrease even faster as the voltage drop over the internal resistance will increase and the OCV will decrease rapidly, much like a feedback loop.



(a) New battery pack.

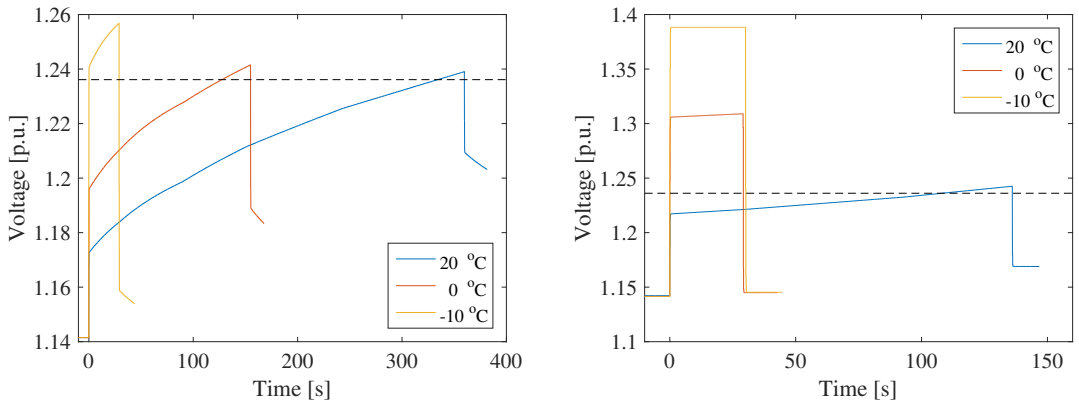
(b) Aged battery pack.

Figure 4.7: Current measurement for constant discharge power request of 15% of maximum specified power.

The fast changes in the current at 0 °C in Figure 4.7a and at 20 °C and 0 °C in Figure 4.7b is a result of the instability of the simulation model as the voltage reach extremely low voltages. As these voltage values are reached the battery pack voltage starts flickering and the model behaves incorrectly.

4.2.1.2 Battery at high state of charge

When testing the upper voltage limit a constant power injection of 33% of maximum specified power is set at an initial SOC of 95%. As previously seen for the low SOC test, the critical safety limit of the voltage will be reached faster for the aged battery cells compared to the new battery cells, seen in Figure 4.8. This is due to the increased internal resistance of the aged battery cells. When the limit is exceeded the contactors opens after a specified time. The FTTI for overcharge is exceeded, but as the software is in its development stage, the time settings are not in alignment with the specified requirements as these are updated throughout the development. When this test was performed the software was not updated to the latest safety requirements.



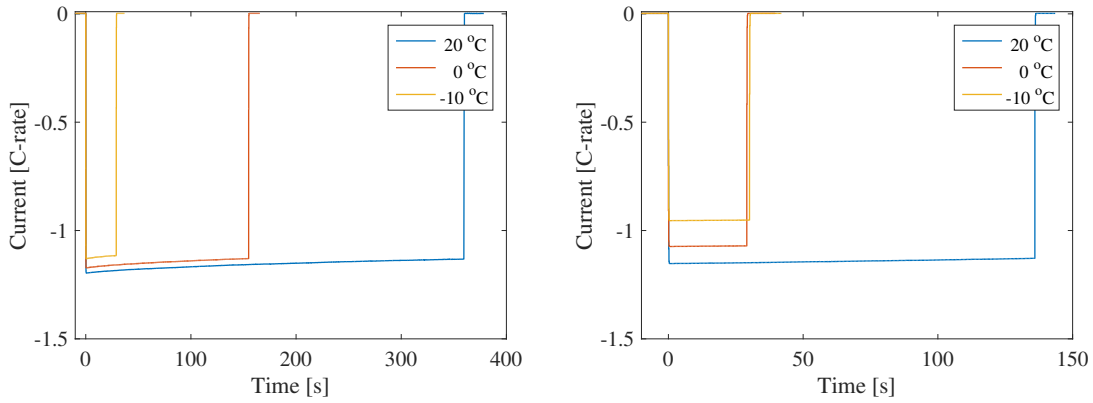
(a) New battery pack. **(b)** Aged battery pack.

Figure 4.8: Voltage measurements for constant power charging of 33% of maximum specified power.

When the battery is operating at lower temperatures it results in increased voltage drops and the critical safety levels will be reached faster. For the lower temperatures the voltage levels reached are more critical and when the battery is aged it results in much higher cell voltages. For the aged battery the voltage levels are significantly higher compared to the new battery. From a safety aspect this is important to consider during the product development.

It should also be noted that the voltage at -10 °C in Figure 4.8b seems to stay constant just below 140% of nominal voltage. This is however due to the limitations within the model as the look-up table for the OCV does not extend beyond 140%. It is therefore not a typical characteristic of a LIB which would quickly reach beyond this limit, similarly to the right hand side of the OCV curve in Figure 2.7.

Figure 4.9 compares the current in the new and aged battery pack for different temperatures. As the voltage increases the current reduces in a rate of change which correlates to the voltage. This however means that the current at -10 °C has some uncertainties as the voltage at that temperature is restricted within the model. Apart from that uncertainty the graph shows that the charging at high SOC has no significant impact on the currents in regards to the limits.



(a) New battery pack. **(b)** Aged battery pack.

Figure 4.9: Current measurements for constant power charging of 33% of maximum specified power.

The current levels reached at the critical voltage levels are not critically high. However as the current has a great impact at critical voltage levels regarding degradation of the battery or the risk of a thermal runaway. The voltage levels and time intervals reached for the aged battery pack is more reasonable to occur in reality compared to the new battery pack. This is one of the reasons it might be a good idea to perform tests of the BMS when the batteries characteristics are changed.

4.2.1.3 One highly degraded logical cell

If one battery cell is degraded in a faster pace compared to the other cells in the battery pack, it will affect the cells connected in parallel. It will accelerate the degradation of the cells connected in parallel as the current will always be higher in the parallel branch with the lowest resistance and the degraded cell has a higher resistance. Due to the higher currents flowing through the healthy battery cells the degradation will accelerate as the current will generate heat which affects the batteries SOH. Due to this ageing effect, the test will be performed assuming all cells in one logical battery cell has degraded equally.

The test case performed for one highly degraded logical battery cell is the same as for the new and aged battery pack. It is of interest to see how low the voltage over the highly degraded logical cell gets compared to the healthy logical cells. In Figure 4.10 the results of the voltage drop can be seen for the mean of the logical cells and for the highly degraded logical cell. As in previous tests it is performed for different temperatures when a discharging power of 15% of maximum specified power is requested.

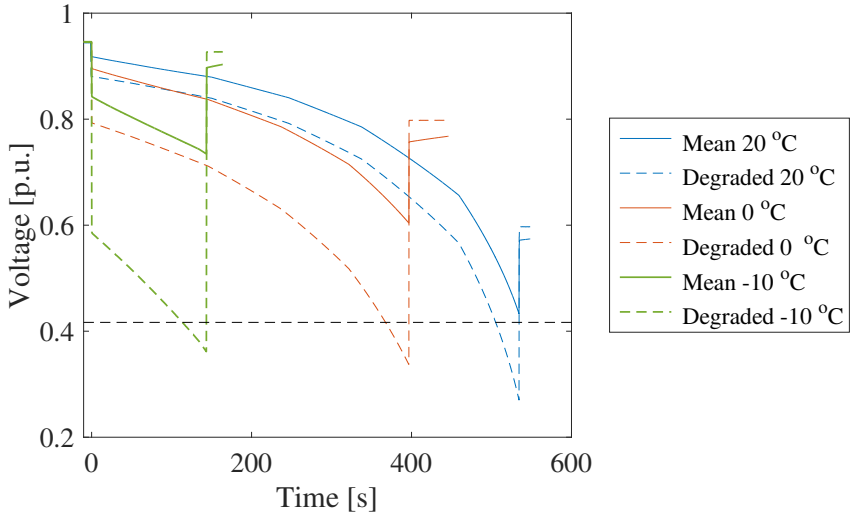


Figure 4.10: The voltage drop over one highly degraded logical battery cell versus the mean voltage drop over 24 logical cells when a power request of 15% of maximum specified power is applied at 5% SOC.

The voltage over the highly degraded logical cell reaches the critical voltage levels before the healthy logical cells, which becomes more apparent with lower temperatures. The limit is reached faster in this test than for a pack of new cells but later than for a pack of degraded cells. The voltage of the logical cell does not reach as low voltages as for a full pack of aged cells. These results indicates that the degraded logical cell would affect performance, which is anticipated, but the degraded logical cell would not suffer the same abuse as the pack in Section 4.2.1.1.

When the upper critical voltage limit is tested for the highly degraded logical cell the charging power is 33% of maximum specified power. As can be seen in Figure 4.11, this results in a larger voltage drop. However, as seen in the results from Section 4.1.1 the internal resistance is higher during charging which also contributes to the increased voltage drop. When the charging pulse is applied for the temperatures 0 °C and -10 °C the voltage limit is reached instantaneously and therefore the contactors opens at the same time. At -10 °C the voltage for the highly degraded logical cell reaches a maximum value of 139% of nominal voltage as this is the highest value of the OCV look-up table deciding the voltage value from the SOC.

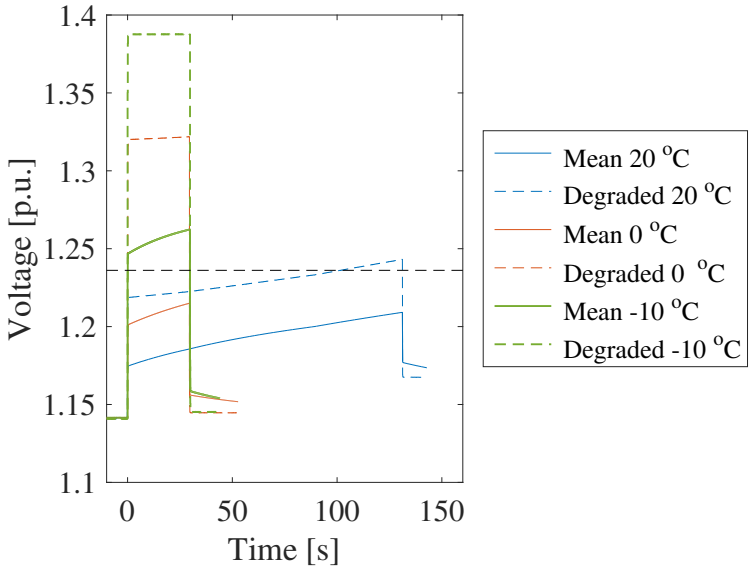
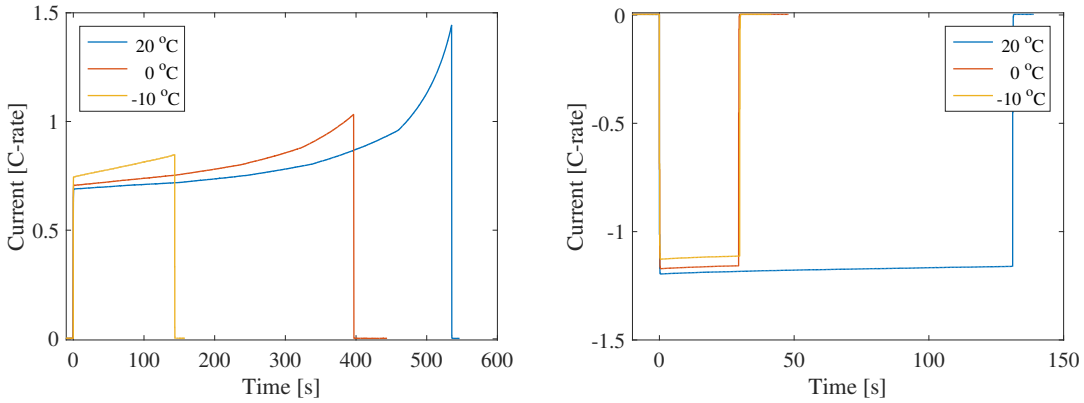


Figure 4.11: The voltage drop over one defect logical battery cell versus the mean voltage drop over 24 logical cells when a power request of 33% of maximum specified power is applied at 95% SOC.

Just like for the charging test of Section 4.2.1.2, the voltage at -10 °C for the degraded logical cell is not representative of how a physical cell would react. If the same reasoning is applied, suggesting that the voltage would rapidly increase for the degraded cell this might cause an internal short circuit. If that would be the case then the cell would enter a thermal runaway which could be a dangerous situation. The results thereby indicates that an overcharge has a potentially higher risk than an overdischarge.

The current measured for the charge and discharge test at the upper and lower SOC can be seen in Figure 4.12. The magnitude of the current does not differ significantly, even though the battery is charged with 33% of maximum specified power and discharged with 15%. The time the current is applied is significantly shorter for the charge compared to the discharge, due to the increased voltage drop during charging, as seen in Figure 4.11.



(a) Discharge of 15% of maximum specified power at 5% SOC.

(b) Charge of 33% of maximum specified power at 95% SOC.

Figure 4.12: Current response for pack with one highly degraded logical cell.

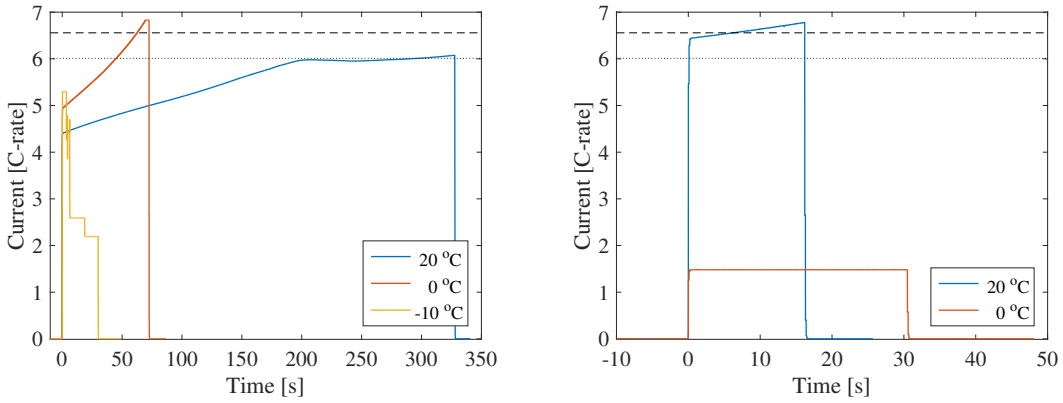
The results show clearly that the system acts by opening the contactors even when it is only one logical cell that exceeds the voltage limits, which is as intended. However, it also shows that if one logical cell has some kind of fault that causes a faster degradation this will affect the performance of the entire pack. This becomes more evident with decreasing temperatures, as seen Figures 4.10 and 4.11, where the difference in voltage between the average of the logical cells and the degraded logical cell increases as the temperature decreases. Due to this it is important that functions for detecting these kind of anomalies are implemented in the BMS as well, in order to find the faults so that they may be addressed as soon as possible. However, such functions does not fall within the test scope of this thesis. If functions that detect faults does not operate correctly, the safety functions will still work according to the results.

4.2.2 Current monitoring

The current is monitored in order to prevent extreme temperatures in the battery cells. Higher currents leads to an increased heat generation, which must be observed carefully to avoid a thermal runaway. The impedance of the battery cells will either increase or decrease the voltage over the cells when a current is applied or drawn from it. When a high power is requested from the battery the voltage over the battery pack will decrease. In order to meet the power demand the current then has to increase, which will in turn increase the voltage drop further. The current limit is tested during discharge of the battery only, as it is possible to draw much higher power during the driving of the vehicle compared to when charging or through regenerative breaking.

4.2.2.1 High power request

The current response when maximum specified power is requested from the battery at 80% SOC, and at different temperatures can be seen in Figure 4.13.

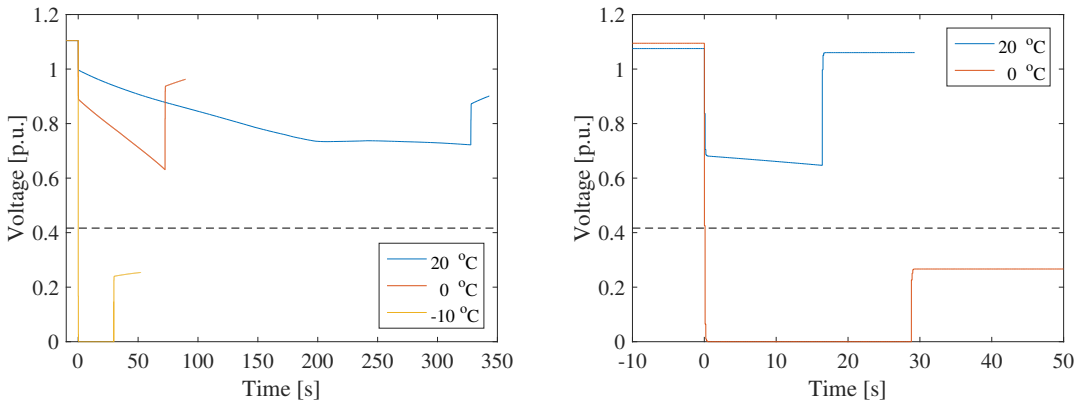


(a) New battery pack. **(b)** Aged battery pack.

Figure 4.13: Current measurement for a request of constant maximum specified power at 80% initial SOC.

The new battery is able to supply maximum specified power for 298 seconds at 20 °C before reaching the lower current limit. The contactors should open within a specified time if the current remains over the limit for a duration of 5 s shorter than the specified time. However for 0 °C the current reaches the lower limit after 45 s but continues to increase to the higher limit after 62 s. Once the current reaches the higher limit then the contactors should open within a specified time shorter than that of the lower current limit if the current is above the higher limit for a duration of 5 s shorter than the specified time. For the aged cells the higher current limit is reached instantly. In both these cases the BMS sends the request to open the contactors in time, as seen by the current dropping to 0C.

At -10 °C the resistance has increased so much that the voltage drops to 0 instantly when the current is applied. The contrasting behaviour of the current at -10 °C is due to the limitations within the model. The same is seen for the aged battery at 0 °C which is why the test was not performed at -10 °C, as this would yield the same results. Although an accurate current behaviour cannot be obtained it is reasonable to assume that requesting maximum power from the battery at such low temperatures would lead to severe degrading of the battery or even immediate failure within the time window before the contactors open.



(a) New battery pack. **(b)** Aged battery pack.

Figure 4.14: Voltage measurement for a request of constant maximum specified power at 80% initial SOC.

In Figure 4.14 the cell voltage drop is seen when maximum specified power is requested from the battery. The voltage drop is more significant at lower temperatures, which leads to an increased current to meet the power demand. When the test was performed for the aged battery pack at 0 °C voltage drops to 0 V instantly after the power request. The current is then set to a constant value of approximately 1.5C, which in reality would have peaked in magnitude and then decreased as the battery would not be able to deliver any power if the voltage is decreased to 0 V.

4.3 Automation of test

The test case that was chosen to be automated is when the battery is discharged from a low initial SOC to observe the low voltage behaviour. The automated test has the same test strategy like that performed manually in Section 4.2.1.1, which is described in Section 3.4.1.1. The outcome of the automated test shows results that are almost identical to the manually performed test, which indicates that the automated test was executed successfully. This verifies that the method used to reset the relaxation of the voltage by setting the capacitance in the RC-link close to zero works as intended.

In Figure 4.15 the automated test result can be seen in comparison to the manually performed test. The manual tests have been inserted into the graph of the automated test, and then adjusted on the time axis so that the initial voltage drop occurs at the same time. When the voltage drops down close to zero, the model becomes unstable and the voltage starts to flicker. This varies randomly between every test, thus it looks different between the manually and automated test. This flickering behaviour is not of interest as it depends on the unstable model at low voltages. The voltage response that is of interest is between the moment the SOC is set to 5% until the voltage reaches zero. The conclusion that can be made is that critical voltage levels are reached at the same time as for the manual tests.

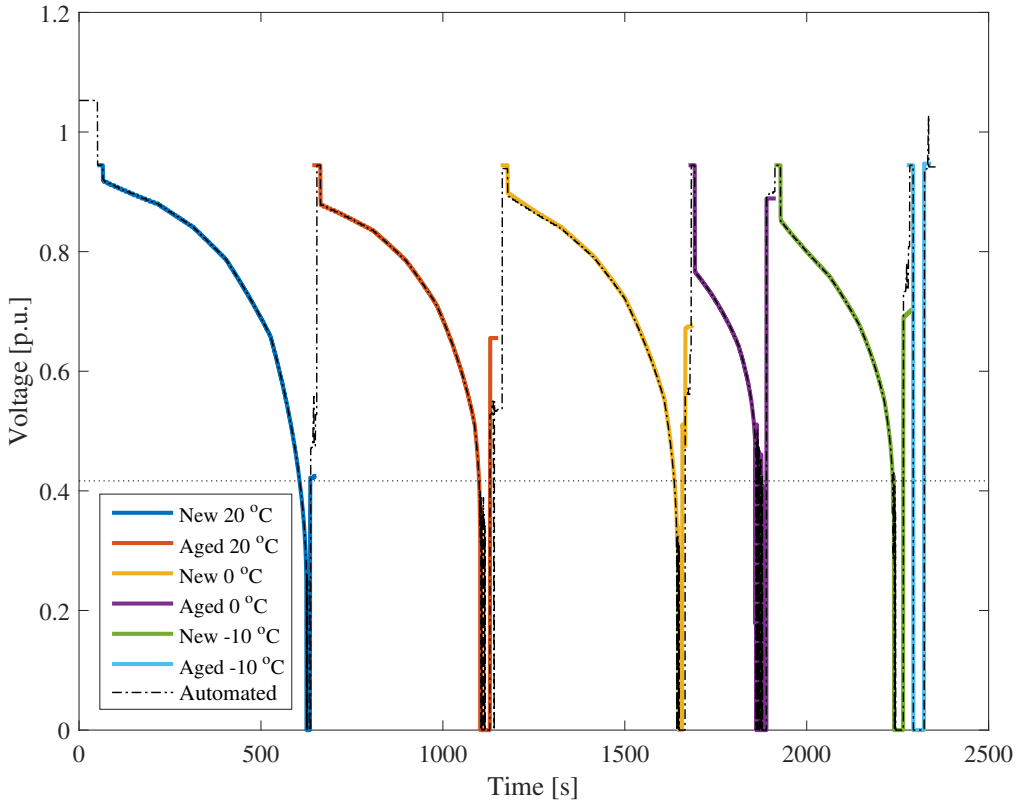


Figure 4.15: Comparison of the automated test against the manually performed tests.

5
Validation

In this chapter the outcome of the analysis will be examined, i.e. if it provides evidence that the safety is fulfilled. Are the safety goals achieved or are there safety precautions that must be taken in order to ensure safe operation? This will be discussed as well as suggestions for solutions.

5.1 Functional and technical safety validation

The safety goals states that the battery should be operated so that the risk for thermal event or outgassing is minimized as much as possible. The TSRs derived from the safety goals that have been the focus for this thesis, are related to voltage and current limits and can be seen in Appendix A.1. For the performed tests the focus has been to evaluate the functionality of the limits both for new cells but more specifically when the battery cells are degraded. The TSRs generally state that if one or more cells violate the limits, safety actions need to be taken, which for these cases means that the contactors should open. As shown in Section 4.2, these actions are performed for all voltage and current limits.

5.1.1 Test case

The tests show that there is a significant difference in the response of the battery when degraded, which is expected due to the large scaling factors. The scaling factor that has the most substantial impact is that of the initial resistance (R_0), as it is the instant voltage drop once a current is applied that causes the cells to decrease or increase in voltage or current beyond the safety limits. This is evident in both voltage and current monitoring tests for the aged battery at lower temperatures. As mentioned, the safety functions act consistently, however there are situations where the simulations indicates that the battery reaches limits that may cause significant damage.

The sensitive cases are mainly when the battery is at the ends of the SOC range and a discharging or charging current is applied to an aged battery. The voltage can in such cases, according to the simulation, reach extreme over or undervoltages instantly. It should be considered that at a discharge, the cells reaches and maintains 0 V until the contactors open, which is reasonable in simulations. However for a physical battery this would only be possible if the battery was short circuited, since it cannot provide any power if the battery connection has no voltage, meaning that

it cannot provide the current needed for the substantial voltage drop. Even though a physical cell may not maintain 0 V it is not unreasonable that it would operate below the limit in which case the safety function would open the contactors.

In the opposite case, when the cells are overcharged and the voltage reaches the upper limits, this could be seen as a more severe case since the current is supplied from an external source. In such cases the aged battery could reach voltages greater than shown in simulations. This is due to the measurements reaching a limit within the model that a physical cell would not have. The battery pack could therefore, in a real case, experience voltages that may cause immediate damage.

Looking at the case when a single logical cell is degraded, the simulations show that the system is less sensitive to discharging at low SOCs since the degraded cell only reaches voltages just below the safety limit. This can be put in comparison to the entire pack being aged where the cell voltages quickly reaches 0 V. The difference is explained by the voltage of the pack being much lower for a complete, aged pack which increases the current. If only one of the logical cells is degraded then the voltage across the pack will remain close to normal operations and the current will not increase rapidly, which would cause the voltage drop to increase. Since the BMS acknowledges the divergent voltage of the degraded logical cell and opens the contactors, the cell will not be exposed to such low voltages as for a complete pack that is aged.

As discussed in the analysis of Section 4.2.1.3 the charging of a pack with one degraded logical cell at lower temperatures may be associated with a higher risk. As the simulation hits the model limit for the degraded cell at -10 °C it is hard to confirm the exact behaviour of the voltage. However the test verifies that the safety function works since the contactors open within the same time as for the remainder of the tests.

As described in Section 3.4 there are requirements on safety functions that should restrict the operation of the battery if certain limits are reached. These limits are within the critical safety limits and should for overcharge communicate to other ECUs to stop charging. For overdischarge it should communicate a limitation in the amount of power that can be discharged, set to 15% of the maximum specified power. However, as tests have proven, this limit might be too high if the temperature is low for new batteries, and for degraded cells, this effect will be even greater.

Looking at the current measurement when the maximum specified power is requested from the battery it shows that the safety functions act according to the requirements for both cases at 20 °C and for the new battery at 0 °C. The system detects the current reaching both the lower and higher current limits and opens the contactors accordingly. There are however issues for the new cell at -10 °C and the degraded cell at 0 °C and below, as the model cannot simulate the battery behaviour correctly. In these cases the voltage in the model reaches 0 V leading to currents that are below the limit, hence the contactors are opened due to the low voltage.

5.2 Tests in relation to safety goals

Considering the voltage levels that are reached when the voltage is beyond the critical safety limit and when the contactors opens after approximately 30 seconds, the safety goals may be violated. It is unsure what the effects on the battery will be exactly when it is exposed to the critical voltages for this amount of time. The effects depend on the time duration as well as current rates.

For the overcharge test the voltage reaches beyond 123.6% of nominal voltage for a new battery pack at -10 °C and for the aged battery pack at the temperatures 0 and -10 °C, before the contactors opens. The duration above this limit is approximately 30 seconds for each of these tests with a current above 0.83C. For lithium cobolt oxide (LCO) LIBs a thermal runaway can occur if the voltage is above 4.5 V, which is above the limits, and the current rate is greater then 2C [16]. There is still a chance that a thermal runaway may occur even though a current rate of 2C is not reached. The functional safety requirement should avoid unreasonable risks for hazardous events according to ISO 26262-3:2018 6.4.4.1, which in this case might not be sufficient when allowing the overvoltage for this duration.

The degradation of the battery drastically increase above 4.2 V, which degrades both the capacity and thermal stability. This is also a safety issue as the degradation can eventually lead to an internal fault in the battery cell, due to lithium plating. A degradation mode will avoid the system to operate for too long at critical overvoltages by inhibiting the system from charging the battery. If the voltage still have not reached normal operation, the battery will be disconnected. This safety function also prevents the voltage from reaching the disconnection level. If the degradation safety function would be considered in the tests performed, the voltage would not be as critical for some of the tests. For some of the overcharge tests the disconnection overvoltage level is reached instantly when a current pulse is applied, then the degradation mode will not be of any help.

Deeply discharging the battery is not as critical from a safety point of view compared to overcharging. It will not lead to a dangerous event instantly, but the degradation of the battery cell can be severe and lead to an internal short circuit in the future. This is due to anodic dissolution of the copper current collector when the voltage of a battery cell is below 1.5 V, which in turn will build up dendrites [16]. The duration of operating below this voltage, as well as current rate, will impact the degradation. As the system requests a constant power, the current will increase as the voltage drops, leading to high currents at critically low voltages, which leads to even faster degradation.

Depending on the type of internal short circuit that occurs, it may lead to a thermal event. As this is a safety issue, it is important to avoid discharging the battery deeply. By setting appropriate limits and allowed time outside the normal operation window this can be prevented. The battery cells that are deeply discharged may also fail in operation immediately due to other reasons then copper current

collector dissolution. As the voltage in LIBs drop fast when they are close to fully discharged, it is hard to set a critical safety limit. If the discharge power is not restricted drastically, the lower voltage limit will be reached instantly if the battery is aged, in the same way as was seen for overcharging.

The overcharge and overdischarge tests performed for the battery pack with a highly degraded logical cell behave similarly as the tests performed for a new and aged battery pack. The highly degraded logical cell exceeds the voltage limits, meanwhile the rest of the battery cells in the pack are within the operational window. In order to prevent this it is important that the BMS consider all logical cell voltages. But as a voltage sensor might have a fault, it may show an incorrect value of the battery cell voltage. Therefore it might not be possible to consider each logical cell voltage as the BMS would see each sensor fault as an electrical fault. This is of course a safety issue which is difficult to handle where a compromised solution must be found.

5.3 Safety solution

To avoid exceeding the safety limits of the battery, the power can be limited at low temperatures and critical SOC levels. Limiting the power will prevent the system from reaching too high or too low voltages, as the voltage drop will decrease with the limited power. This function is already implemented in the software but was disabled in this work in order to reach the critical safety limits and be able to verify the functional safety mechanisms.

5.3.1 Variance in operation

It is preferred to adapt the control strategy in order to secure the batteries performance as it is aged [2], [11]. The ageing conditions of a LIB results in enhanced temperature development and also makes it more sensitive to overcharge and overdischarge. The items degraded functional behaviour should be stated in line with the safety goal, according to ISO 26262-3:2018 7.1.

In ISO 26262-4:2018 8.4.1.3, it is recommended to consider variance in operation as it can affect the technical characteristics. The results from the analysis supports this statement as it has been proven that it will affect the cell voltage in a great extent. It impacts both the voltage and current characteristics in a negative manner, as the limits are reached faster. This should be considered in the HARA as well.

If the ASIL for the cell voltage monitoring is classified to a high level it is considered to be appropriate to perform the tests when the battery pack is degraded. As it is unavoidable that the battery will age with time the probability of exposure is high. But the critical safety limits are simply controllable and the ASIL level that is already defined for the safety function is considered to be sufficient. When it comes to a highly degraded battery cell in the battery pack, the controllability is more difficult, but the probability is very low that a logical cell would degrade so that the impedance difference is as great as investigated.

5.3.2 Stress test

If requirement based tests where cell voltages are overridden are complemented with stress tests, it will increase the credibility that the software operates correctly. The test verifies correct operation during abusive conditions and is highly recommended to perform on the ASIL of the requirements, to verify the level of robustness at the system level, according to ISO 26262-4:2018 7.4.3.2.5. As the test scenarios presented in this thesis rarely occur in reality, the tests are probably not essential in order to ascertaining the most crucial functions of the system. Therefore the tests are considered to be suitable to be performed in an acceptance test, as the safety functions are important but not necessary to propel the vehicle. Before the product is delivered to the customer the ageing effects should be considered to see if the acceptance criteria is met. It is seen from the analysis that the ageing of the battery will have a significant impact on the voltage response and therefore it should be tested in the final stage before delivery.

As the functionality of the safety function can be tested simply by overriding signals, it can be seen as unnecessary to perform the stress test as it is much more time consuming. However, if the tests are implemented in automated testing scripts, the time of performing these tests will not be of any concern. It proves the functionality with a different test method, which ensures robustness of the system and provides an insight into how the system behaves in reality. The critical voltages and currents should be evaluated to check if they are acceptable. A protocol which determines the safety risk depending on which voltage levels that are reached could be of use for the evaluation.

The test is preferably verified in a representative context at vehicle level, according to ISO 26262-4:2018 8.4.1.1. Testing options are limited in this thesis work, as destructive tests cannot be performed. In order to verify it in a representative context, a stress test could be sufficient at the battery pack level instead of performing it in a vehicle. This would add coverage as an addition to existing tests.

5.3.3 Adaptive parameters in correlation with ageing

To secure the battery performance, dynamic parameters are preferable for the voltage and current limits. As aged cells become more sensitive to overcharge and overdischarge the safety limits should be restricted during its lifetime. Even though the power limit is changed over the batteries lifetime, which purpose is to limit the battery from operating outside the operational window, it might be a good idea to use dynamic voltage and current limits for redundancy.

5.3.4 Voltage difference between battery cells

Cell balancing mitigates the issue with voltage differences between battery cells. However, if the cell balancing is not working properly the voltage of a highly degraded cell and cells with less capacity or SOC will not be balanced. This issue could result in an overdischarge of one of the battery cells, which can be prevented if the voltage difference between the cells are considered. If the voltage difference between the cells are not within a set voltage range the system should command degradation mode. The voltage difference becomes more apparent at low SOC and the problem might be seen before the critical lower voltage limit is reached. Even if the cell balancing is working properly this requirement would also prevent any undesirable risk of a highly degraded logical cell reaching critical voltage levels due to the high voltage drop. The highly degraded logical cell will reach a low or high voltage faster then the healthy cells.

As mentioned in Section 5.2, due to a faulty voltage sensor this voltage difference can be hard to evaluate. But if it is possible to detect that the voltage sensor is not working properly, for example that it is set constant, this requirement could be of use.

6
Conclusion

The purpose of this thesis has been to evaluate the current safety goals and requirements using the ISO 26262 standard. From this evaluation new tests are derived that could provide a better test coverage or a new approach to testing. As batteries are a new area of technology for car manufacturers, and ageing of batteries is not fully investigated, this was selected as an operational use case which would be of interest to perform further testing on. As the standard recommends that safety goals are validated when taking variance in operation into consideration, the choice of an aged battery was supported by the standard.

The tests performed for this thesis show that the safety goals where compromised with the early version of the software that was available. The parameters of that software were temporary and with the correct parameters that was implemented in the subsequent software, the safety goals are considered to be fulfilled. It can however not be confirmed beyond reasonable doubt. This is because of the over and undervoltages that are reached in testing and the unknown effects that these will have on the battery.

In order to increase the safety and reduce the risk of damaging the battery cells it is suggested that the voltage and current limits, as well as safety related power limits, are adapted to the SOH of the cells. It is also proposed that stress tests like those performed in this thesis is implemented in the acceptance test. This is to verify that the battery is not subjected to any unnecessary risk and to expand the coverage of the testing.

6.1 Future work

During the tests and validation, questions or topics have been brought up that are beyond the scope of the thesis, but that could be of interest to investigate in future work. One question is how the cells would react to the exposure to high or low voltage for the duration of the different tests. The effects that could cause further degradation or damage have been presented in this thesis. It is however not clear if these would occur in the first incident of an over or undervoltage or if it would require the limits to be exceeded multiple times before the damage becomes hazardous. Tests on real battery cells to asses the damage that the over and undervoltages may have on the cell health is of interest in order to determine the risk.

Another topic is how the circulating currents would appear in a logical cell where one cell is more degraded than the others, which indirectly compromises the safety. A report was found which looked into this topic performing this analysis through simulations [19]. It could be of interest to perform this on physical batteries where the voltage is measured over each cell and the currents measured in each branch. A long term test could be performed to see how fast the healthy cells will degrade and a short term to see how the current is distributed in the parallel connection.

The power requested when testing the voltage window for the lower voltage limit, was the maximum discharge power when in degradation mode. Similarly, the power injected for the upper voltage limit, was the maximum regeneration power. For the analysis of the current limit, the power request was set to the maximum output power of the vehicle. To improve the test case the power input and output from a drive cycle could be used to analyze the impact on the voltage and current in a more realistic scenario.

Bibliography

[1] A. Emadi, Y. Gao and M. Ehsan, *Modern Electric, Hybrid Electric, and Fuel Cell Vehicles*, ser. Power Electronics and Applications Series. Boca Raton, FL, USA: Taylor & Francis, 2010, vol. 6. [Online]. Available: https://www.taylorfrancis.com/books/9781420054002 (visited on 24/01/2019).

[2] H. Berg, *Batteries for Electric Vehicles - Materials and Electrochemistry*. Cambridge, United Kingdom: Cambridge University Press, 2015.

[3] M. Broy, "Challenges in automotive software engineering", in *Proceeding of the 28th international conference on Software engineering - ICSE '06*, New York, USA: ACM Press, 2006, p. 33. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1134285.1134292 (visited on 24/01/2019).

[4] K. Grimm, "Software technology in an automotive company: major challenges", in *Proceedings of the 25th International Conference on Software Engineering*, Institute of Electrical and Electronics Engineers, 2003, p. 833. [Online]. Available: https://dl.acm.org/citation.cfm?id=776878 (visited on 24/01/2019).

[5] Volvo Car Group, "VOLVO CAR GROUP ANNUAL REPORT 2018", Volvo Car Group, Gothenburg, Tech. Rep., 2019, p. 167. [Online]. Available: https://investors.volvocars.com/annualreport2018/res/pdf/VCG_AR_2018_ENG_20190325_hi-res.pdf (visited on 02/05/2019).

[6] S. Bigouette, *Where does Volvo's reputation for safety come from?*, 2019. [Online]. Available: https://wyantgroup.com/where-does-volvos-reputation-for-safety-come-from/ (visited on 02/05/2019).

[7] M. Heusser and G. Kulkarni, *How to Reduce the Cost of Software Testing*, 1st. Boca Raton, FL, USA: CRC Press, 2012, p. 312. [Online]. Available: https://books.google.se/books?id=56t-DwAAQBAJ&printsec=frontcover&dq=How+to+Reduce+the+Cost+of+Software+Testing&hl=sv&sa=X&ved=0ahUKEwjR0bKp-ZriAhUh_SoKHfmpDtQQ6AEIKTAA#v=onepage&q=How%20to%20Reduce%20the%20Cost%20of%20Software%20Testing&f=false (visited on 03/05/2019).

[8] R. Faria, P. Moura, J. Delgado and A. T. de Almeida, "A sustainability assessment of electric vehicles as a personal mobility system", in *Energy Conversion and Management*, vol. 61, Pergamon, 2012, pp. 19–30. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0196890412000945 (visited on 02/05/2019).

[9] T. Lipman and M. Delucchi, "Expected Greenhouse Gas Emission Reductions by Battery, Fuel Cell, and Plug-In Hybrid Electric Vehicles", in *Electric and hybrid vehicles : power sources, models, sustainability, infrastructure and*

the market, P. Gianfranco, Ed., Berkeley: Elsevier, 2010, ch. 5, p. 652. [Online]. Available: https://www.researchgate.net/publication/278703543_Expected_Greenhouse_Gas_Emission_Reductions_by_Battery_Fuel_Cell_and_Plug-In_Hybrid_Electric_Vehicles (visited on 02/05/2019).

[10] J. Groot, "State-of-Health Estimation of Li-ion Batteries: Ageing Models", PhD thesis, Chalmers, 2014, p. 99. [Online]. Available: http://publications.lib.chalmers.se/records/fulltext/205605/205605.pdf (visited on 20/03/2019).

[11] W. Waag, S. Käbitz and D. U. Sauer, "Experimental investigation of the lithium-ion battery impedance characteristic at various conditions and aging states and its influence on the application", *Applied Energy*, vol. 102, pp. 885–897, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S030626191200671X (visited on 28/02/2019).

[12] S. Skoog and S. David, "Parameterization of linear equivalent circuit models over wide temperature and SOC spans for automotive lithium-ion cells using electrochemical impedance spectroscopy", *Journal of Energy Storage*, vol. 14, pp. 39–48, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352152X16301906?via\%3Dihub (visited on 09/04/2019).

[13] Klett Matilda, "Electrochemical Studies of Aging in Lithium-Ion Batteries", PhD thesis, Department of Chemical Engineering and Technology, KTH Royal Institute of Technology, Stockholm, Sweden, 2014. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:715990/FULLTEXT01.pdf (visited on 27/03/2019).

[14] Q. Liu et al., "Understanding undesirable anode lithium plating issues in lithium-ion batteries", *RSC Advances*, vol. 6, no. 91, pp. 88 683–88 700, 2016. [Online]. Available: http://dx.doi.org/10.1039/C6RA19482F (visited on 11/03/2019).

[15] V. Agubra and J. Fergus, "Lithium Ion Battery Anode Aging Mechanisms", *Materials*, vol. 6, no. 4, pp. 1310–1325, 2013. [Online]. Available: http://www.mdpi.com/1996-1944/6/4/1310 (visited on 28/03/2019).

[16] H. Maleki and J. N. Howard, "Effects of overdischarge on performance and thermal stability of a Li-ion cell", *Journal of Power Sources*, vol. 160, no. 2 SPEC. ISS. Pp. 1395–1402, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0378775306004277 (visited on 10/03/2019).

[17] J. Vetter et al, "Ageing mechanisms in lithium-ion batteries", *Journal of Power Sources*, vol. 147, no. 1-2, pp. 269–281, 2005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378775305000832 (visited on 27/03/2019).

[18] T. Volck et al., "Method for Determination of the Internal Short Resistance and Heat Evolution at Different Mechanical Loads of a Lithium Ion Battery Cell Based on Dummy Pouch Cells", *Batteries*, vol. 2, no. 2, p. 8, 2016. [Online]. Available: https://www.researchgate.net/publication/299998913_Method_for_Determination_of_the_Internal_Short_Resistance_and_Heat_Evolution_at_Different_Mechanical_Loads_of_a_Lithium_Ion_Battery_Cell_Based_on_Dummy_Pouch_Cells (visited on 10/03/2019).

[19] T. Bruen and J. Marco, "Modelling and experimental evaluation of parallel connected lithium ion cells for an electric vehicle battery system", *Journal of Power Sources*, vol. 310, pp. 91–101, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.jpowsour.2016.01.001 (visited on 03/04/2019).

[20] J. Jiang and C. C. Zhang, *Fundamentals and applications of lithium-ion batteries in electric drive vehicles*. Singapore: John Wiley & Sons, Incorporated, 2015, p. 299. [Online]. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118414798 (visited on 12/03/2019).

[21] GAMRY, *Basics of EIS: Electrochemical Research-Impedance*, 2018. [Online]. Available: https://www.gamry.com/application-notes/EIS/basics-of-electrochemical-impedance-spectroscopy/ (visited on 11/03/2019).

[22] S. Skoog, "Parameterization of equivalent circuit models for high power lithium-ion batteries in HEV applications", in *2016 18th European Conference on Power Electronics and Applications (EPE'16 ECCE Europe)*, IEEE, 2016, pp. 1–10. [Online]. Available: http://ieeexplore.ieee.org/document/7695340/ (visited on 10/12/2018).

[23] B. Pattipati, B. Balasingam, G. V. Avvari, K. R. Pattipati and Y. Bar-Shalom, "Open circuit voltage characterization of lithium-ion batteries", *Journal of Power Sources*, vol. 269, pp. 317–333, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.jpowsour.2014.06.152 (visited on 11/03/2019).

[24] D. Sturk and L. Hoffmann, "e-fordons Potentiella Riskfaktorer vid Trafikskadehändelse", Tech. Rep., 2013. [Online]. Available: https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/e-fordons-potentiella-riskfaktorer-vid-trafikskadehandelse-/ (visited on 09/04/2019).

[25] *Road vehicle - Functional safety - Part 3: Concept phase*. ISO 26262:2018, International Organization For Standardization, Geneva, Switzerland, 2018.

[26] IEC, *Functional safety - Essential to overall safety*. Geneva, Switzerland: International Electroctechnical Commision, 2015. [Online]. Available: www.iec.ch.

[27] *Road vehicles - Functional safety - Part 1: Vocabulary*. ISO 26262:2018, International Organization For Standardization, Geneva, Switzerland, 2018.

[28] Scaled Agile INC, *Nonfunctional Requirements*, 2018. [Online]. Available: https://www.scaledagileframework.com/nonfunctional-requirements/ (visited on 22/02/2019).

[29] *Road vehicle - Functional safety - Part 4: Product development at the system level*. ISO 26262:2018, International Organization For Standardization, Geneva, Switzerland, 2018.

[30] *Road vehicle - Functional safety - Part 8: Supporting processes*. ISO 26262:2018, International Organization For Standardization, Geneva, Switzerland, 2018.

[31] R. Bender, *Requirements Based Testing Process Overview*, Queensbury, NY, 2009. [Online]. Available: http://benderrbt.com/Bender-Requirements%20Based%20Testing%20Process%20Overview.pdf (visited on 18/02/2019).

[32] E. van Veenendaal, "Standard glossary of terms used in Software Testing", ISTQB, Tech. Rep., 2010. [Online]. Available: http://glossary.istqb.org/search/ (visited on 27/03/2019).

[33] G. Duggal and M. B. Suri, "UNDERSTANDING REGRESSION TESTING TECHNIQUES", Tech. Rep. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.5875&rep=rep1&type=pdf (visited on 23/04/2019).

[34] Software Testing Fundamentals, *Acceptance Testing*, 2019. [Online]. Available: http://softwaretestingfundamentals.com/acceptance-testing/ (visited on 23/04/2019).

[35] *Road vehicle - Functional safety - Part 6: Product development at the software level*. ISO 26262:2018, International Organization For Standardization, Geneva, Switzerland, 2018.

[36] DSPACE, "SCALEXIO", 2019. [Online]. Available: https://www.dspace.com/shared/data/pdf/2019/dSPACE_SCALEXIO_Product-information_01-2019_English1.pdf (visited on 19/03/2019).

[37] A. Himmler, K. Lamberg and M. Beine, "Hardware-in-the-Loop Testing in the Context of ISO 26262", 2012. [Online]. Available: http://papers.sae.org/2012-01-0035/ (visited on 18/02/2019).

[38] dSpace, *ControlDesk*. [Online]. Available: https://www.dspace.com/shared/data/pdf/2019/dSPACE_ControlDesk-Brochure_03_2019_English.pdf (visited on 19/03/2019).

[39] DSPACE, "Test Automation Software", 2019. [Online]. Available: https://www.dspace.com/shared/data/pdf/2019/dSPACE_TestAutomation_SW_Product-information_01_2019_English.pdf (visited on 18/02/2019).

[40] B. Barnett, D. Ofer, S. Sriramulu and R. Stringfellow, "Lithium-Ion Batteries, Safety", in *Batteries for Sustainability*, New York, NY: Springer, 2013, pp. 285–318. [Online]. Available: http://link.springer.com/10.1007/978-1-4614-5791-6_9 (visited on 16/04/2019).

[41] F. Lambert, *Tear down of 85 kWh Tesla battery pack shows it could actually only be a 81 kWh pack*, electrek. [Online]. Available: https://electrek.co/2016/02/03/tesla-battery-tear-down-85-kwh/ (visited on 16/04/2019).

Appendices

A

Hazard and risk analysis flow chart

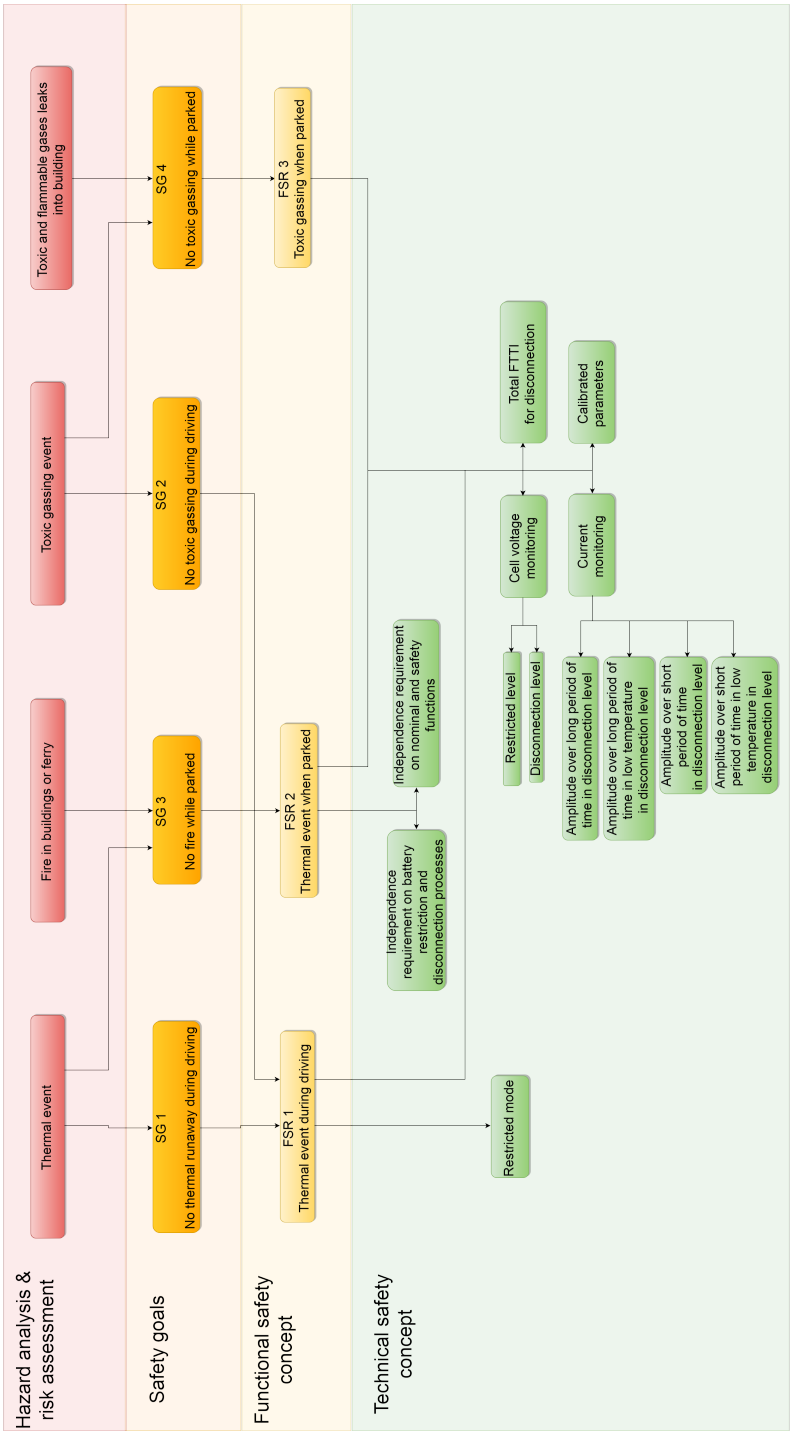


Figure A.1: Part of the requirement model with dependencies for the BMS.