POLITECNICO DI TORINO

The Department of Control and Computer Engineering (DAUIN)

Master's degree in Mechatronic Engineering

Master's degree thesis

Functional Safety Verification of the SIRIH₂ Hybrid Hydrogen Fuel Cell and Battery System. Applying IEC 61508 and ISO 13849 Standards with Focus On BMS

Supervisors:
Prof. Massimo Violante, Ing. Ph.D.
Lorenzo Sisca, Ing. Ph.D.

Candidate:
Irfan Ribic

Academic year 2025/2026

Contents

List of Figures

Acronyms and abbreviations

AC – Alternating Current

ADC – Analog-to-Digital Converter

AI – Artificial Intelligence

BESS – Battery Energy Storage System

BMS – Battery Management System

CAN – Controller Area Network

CC – Constant Current

CV – Constant Voltage

DC – Direct Current

DoD – Depth of Discharge

DSP – Digital Signal Processor

ECU – Electronic Control Unit

EKF – Extended Kalman Filter

EMS – Energy Management System

EOL – End of Life

ESS – Energy Storage System

EV – Electric Vehicle

H2 – Hydrogen

HIL – Hardware-in-the-Loop

HV – High Voltage

HVAC – Heating, Ventilation, and Air Conditioning

IC – Integrated Circuit

IEC – International Electrotechnical Commission

IEC 61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

IEC 61508-3 – Software Requirements of IEC 61508

ISO – International Organization for Standardization

ISO 13849-1 – Safety of Machinery – Safety-Related Parts of Control Systems

LFP – Lithium Iron Phosphate

Li-ion – Lithium-Ion

LV – Low Voltage

MATLAB – Matrix Laboratory (Technical Computing Environment)

MiL – Model-in-the-Loop

MTTFd – Mean Time To Dangerous Failure

OCV – Open Circuit Voltage

PFH – Probability of Dangerous Failure per Hour

PFDavg – Average Probability of Failure on Demand

PL – Performance Level

PLr – Performance Level Required

SCU – Shelter Control Unit

SiL – Software-in-the-Loop

SIL – Safety Integrity Level

SIRIH$_2$ – Hybrid Hydrogen Fuel Cell and Battery System (System Identifier Used in Thesis)

SOC – State of Charge

SOH – State of Health

SOP – State of Power

SRP/CS – Safety-Related Parts of Control Systems

UKF – Unscented Kalman Filter

Abstract

An increase in use of hybrid hydrogen fuel cell and battery energy storage systems in modern energy applications brings significant safety challenges. The example of SIRIH$_2$ hybrid system combines hydrogen-based energy conversion with battery storage, creates a complex interaction between high-voltage components, control electronics, and management systems. Ensuring safe and reliable operation under both normal and fault conditions requires detail and structured approach to functional safety.

This thesis field of research is a functional safety of the SIRIH$_2$ hybrid hydrogen fuel cell and battery system, with Battery Management System (BMS) as a main subsystem responsible for functional safety. Work applies the safety standards IEC 61508 and ISO 13849 to identify hazards, assess risks, define safety goals, and assign suitable Safety Integrity Level (SIL) and Performance Level targets.

Model based approaches are performed to support early verification. MATLAB/Simulink model of the battery subsystem and BMS logic is created to simulate simplified real environment, allowing Model-in-the-Loop (MIL) testing of safety-related functions. Different fault scenarios, as overvoltage, overcurrent, thermal overload, and sensor failures, are introduced to the simulation using structured fault injection techniques. The performance of subsystems responsible for functional safety including the BMS as main system is evaluated. Main indicators of evaluation are fault detection time, transition to safe state, and diagnostic coverage, and the results are compared with defined integrity targets and standards.

The goal is to demonstrate that model-based functional safety verification provides an effective and systematic way to evaluate safety performance before phase of hardware implementation. The research shows the importance and relationship between safety requirements and verification results. As well as role of simulation-based validation in supporting compliance with international safety standards. End goal is contribution to the development and methodology of a practical safety verification framework for hybrid hydrogen battery energy systems.

1. Introduction

In last decade energy systems have been passing through significant transformation. Increased demand for decrease in emissions and increased a share of green energy led to development of BESS systems. Lithium-ion battery takes significant place because of its high energy density, long life and good efficiency. Thanks to these characteristics BESS systems are present in wide spectra of applications.

However, managing battery systems is regarded as engineering challenge. Any deviation from strictly bound working conditions in terms of voltage current and temperature leads to accelerated degradation. Consequently, causing loss of capacity and in extreme cases danger for humans and environment. This is a reason why safety represents a key field of exploration in modern energy technology.

Central role in ensuring safety of these system has a Battery Management System. BMS is a specialized managing system whose basic task is to continuously monitor state of battery and that all working parameters stay inside allowed limits while delivering optimum performance. System acquires information about voltage of single cells, temperature of battery module, currents while charging and discharging as well as total state of battery. These information uses BMS to make decisions about allowed working conditions and activates safety function in case of abnormal conditions. Modern BMS can be seen as subsystem whose task is to monitor and predict potentially dangerous working situations and prevent their escalation. For that reason, development and verification of BMS is conducted with functional safety principles and well-defined safety standards as IEC 61508.

In this thesis the focus is put on analysis of safety functions of BMS inside SIRIH2 system, which is transportable energy system based on combination on battery storage and hydrogen fuel cell. This hybrid system ensures flexible production and storage of electrical energy, where battery subsystem has important role in stabilization of energy flows. Integration of multiple energy technologies increases complexity and importance of safety mechanisms.

In this framework simplified model of battery system and BMS logic is developed using MATLAB/Simulink environment. Model provides safety functions evaluation of BMS under different working scenarios. Special focus is put on monitoring voltage current and temperature.

Implemented logic detects abnormalities as overvoltage undervoltage extreme values of current and suitably reacts to these states.

To verify the correctness of safety function Model-in-the-Loop (MIL) simulated environment gives us possibility to execute different working scenarios and controlled introductions to faults.

Goal of this work is to show that with simulation modeling it is possible to verify functional safety functions of BMS. Besides that the thesis identify limitations and developed model and suggestions for further improvements.

2. Introduction Of Functional Safety

2.1 Fundamentals of Functional Safety

In modern electrical and industrial systems, the application of ISO and IEC standards represent a international framework for verification and implementation of safety standards, reliability and quality of products and systems. This is highly important in area of ESS (energy storage systems) where many risks are present due to high energy concentration involved in operations in form of electrical, thermal or chemical. Standards like ISO and IEC provide a safety framework for the lifecycle of systems. Their application does not only decrease probability of faults and dangerous situations for humans and environment but also provide compliances with legal requirements, product certification and acceptance on international market which has direct effect on confidence of consumer and regulatory entities.

Functional safety deals with the question: Will the system in the present of faults and errors react in the way where it prevents the occurrence of unacceptable risks. Unlike general technical or mechanical safety, functional safety focuses on the behavior of system as the consequence of what electrical electronic and programable subsystems do to prevent risk and ensure acceptable behavior.

IEC 61508 is an international standard applied to electric and electronical and programmable systems where the safety functions depend on control electronics. Standard defines whole life cycle starting from development of hardware and software until verification validation and maintenance of the system. IEC 61508 is not related to any specific industry. Instead of that it gives generic framework which can be applicable to many sectors of industry, energy, and transport. This is reason why IEC 61508 is particularly relevant for stationary BESS systems which often do not belong directly to automotive or other sectorial standards.

2.2 Safety Lifecycle According to IEC 61508

Standard is structured as multi-part pack where the goal is to cover all the aspects of functional safety. This modular structure allows for systematic separation between requirements based on level of abstraction as well as clear distribution of responsibilities between system engineering, hardware design and software development. In total IEC 610508 has 7 interconnected parts where every part has a clearly defined role inside safety lifecycle.

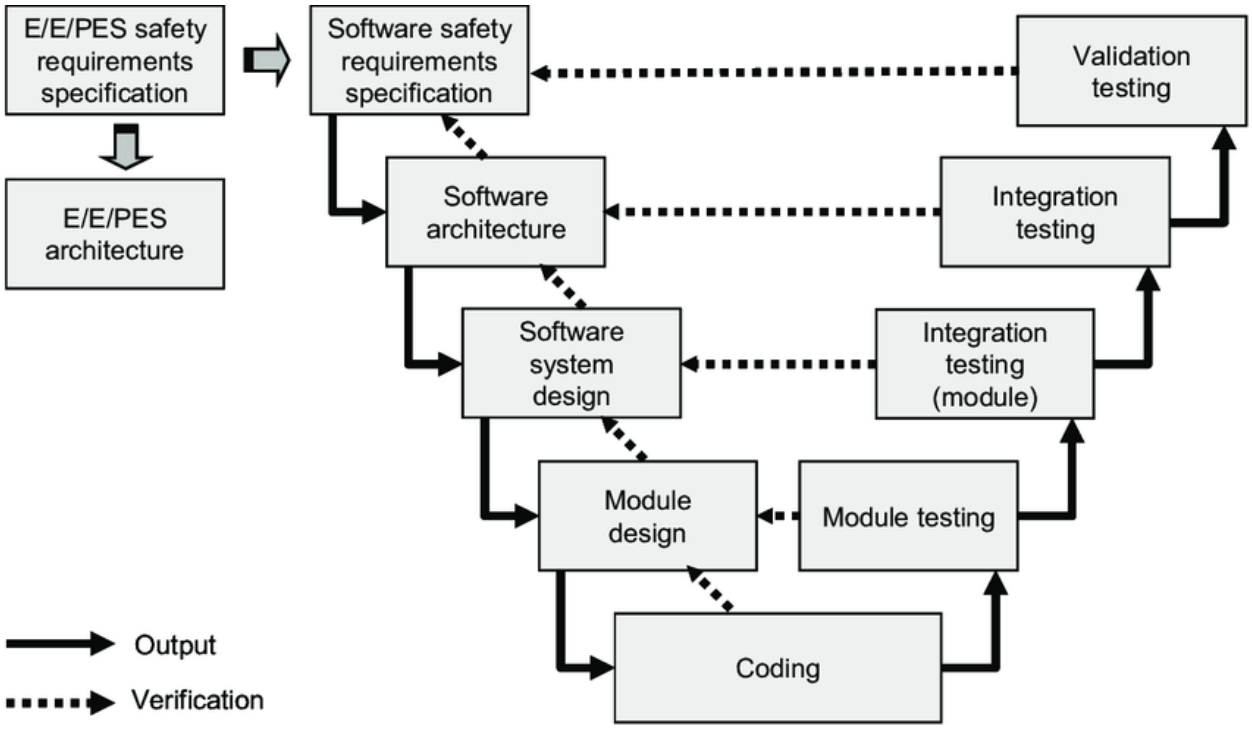

Figure 1. Software safety lifecycle model of IEC 61508

First part of standard represents introduction to key terminology and principles of functional safety. Concepts as safety-related-systems, safety function, safety goals, safety life cycles and safety integrity level are one of focus of interest.

In context of BESS systems these concepts formally define role of BMS as a relevant functional safety system. BMS in this environment does not only represent a control unit for the optimization of battery but a key safety mechanism which needs to detect potentially dangerous conditions and prevent their escalation. Application of principles from this part of standard identifies safety

functions which BMS implements as protection of overvoltage, high current, overheating etc. Afterwards these functions are related to safety goals on the level of whole battery system.

Second part is related to hardware architecture and system design of safety connected E/E/PE systems. In this part quantitative metrics are introduced such as Safe Failure Fraction (SFF), Hardware Fault Tolerance (HFT) and probability of dangerous failure. These parameters give us insight into ability of system to detect and control dangerous situations and provide objective measure for that.
In the context of BESS this is related to architecture of BMS, including redundant channels for measurement of battery working parameters and independent hardware and software protection mechanisms which handle react to different situations accordingly and in extreme case disconnect battery or part of it completely from the system. Central concept is Safety Integrity Level (SIL) which defines required safety requirements.
Third part of standard is dedicated to software development in safety critical systems which is very important in this application because modern BMS heavily depends on software and algorithms. Standards define principles of software development with lifecycle approach, verification and validation of software function, configuration management and control of changes. The goal is to prevent systematic errors which can possibly occur in development phase of software. In practice for BMS the safety functions need to be clearly identified and implemented with suitable mechanisms for error detection. One of these features is parameters operating limit, monitoring of software execution and credibility verification of measuring data.

Besides basic requirements described in first three parts of standard IEC 61508 contain additional part in interpretation and application principles in realistic industrial systems. In that context forth part of standard is dedicated to terminology and definitions. Even if it does not introduce new technical requirements the role of this part is to ensure consistent interpretation of key terminology. Using standardized terminology ensures precise development of technical documentation and prevents potential miss interpretation of safety requirements. Fifth part of standard provides methodologies which can be used for required level of integrity. Standard does not impose certain methodology but provides different approaches which include qualitative and quantitative methods of risk assessment. Example of these methods includes risk matrix, analysis based on failure

probability. These methods are used to determine SIL based on factors such as severity of consequences, exposure to risk and possibility of evading dangerous event. Sixth part of standard provides guidelines for hardware and software. Its role is to connect theoretical principles with their implementation in real systems. Guidelines from this part are useful for evaluation of existing systems by comparing implemented technical solutions with recommended practices and identification of potential gaps. Last part of standard shows techniques and best engineering practices to achieve functional safety. These techniques cover hardware protection software methods for detection and organization standards.

These parts of IEC 61508 standard in context of SIRIH2 provide important methodological framework for implementation of safety goals.

2.3 SIL and PL – Conceptual and Quantitative Framework

SIL has discrete levels form SIL 1 to SIL 4 where it is described as a level of integrity of safety function. SIL quantifies probability that the safety function fails when it is needed to act. Higher SIL level means strict demand in terms of design verification and certification which results in higher level of risk reduction. It is important to outline that SIL level is assigned to safety function and not to a system or device because different functions of same system can have different level of importance thus different integrity goals.

Safety Integrity Level	Probability of Failure on Demand	Reduction Factor
SIL 4	>= 10^5 to < 10^4	10^5 to 10^4
SIL 3	>= 10^4 to < 10^3	10^4 to 10^3
SIL 2	>= 10^3 to < 100	10^3 to 100
SIL 1	>= 100 to < 10	100 to 10

Table 1. of Safety Integrity level

In framework of IEC 61508 the key idea is to reduce the risk to very low probability of catastrophic failure. IEC 61508 differentiates two working regimes of safety function using 2 key metrics:

PFDavg (average Probability of Failure on Demand) – average probability that safety function will not perform as expected when needed. This metric is typical on low demand where demand for safety functions is low. In that regime the system can operate for extended period without need

for safety function activation but when dangerous event occurs needs to respond reliably. PFDavg describes average risk of failure on demand during some timeframe.

PFH (Probability of dangerous Failure per Hour) this metrics describe probability of dangerous failure on high demand or continuous regime of dependance on safety function. Integrity is described as frequency of dangerous failures per unit of time.

Performance Level is concept from ISO 13849-1 which is primary used in machine safety and safety related parts of controlling systems. PL describes ability of safety function to perform in predictable working condition and failure, where levels are assigned from PL a,b,c,d,e, where e is highest level of performance, a is lowest. As in case of SIL is PL is related to safety function not a system.

2.4 Managing risk methodology

Managing risk represents central element of functional safety. In complex energy systems as it is SIRIH2 which combines hydrogen fuel cells, batteries and complex control logic can potentially create dangerous situations when faults occur or under wrong working conditions. Main goal managing risk is not only identification risk but establishment of clear relationship between identified risks and technical measures for protection in the system. Only with this well structured approach is it possible to determine suitable safety functions and required level of reliability. In framework of IEC 61508 the risk methodology includes three phases: Hazard indentification, risk assessment and determining suitable level of integrity.

2.4.1. Hazard identification

Hazard identification is the first step in functional safety. A hazard can be define as potential source of harm for humans, equipment or environment. In context of SIRIH2 system the hazard identification is done by analyzing functional architecture of the system, energy flows and subsystems interaction. Special attention is given to interaction between different subsystems because in these interfaces often complex failure can occur. System analysis identified certain groups of hazard sources.

Hazards related to hydrogen includes possible leakage, accumulation in closed environment and possible explosion or combustion. Second group involves electrical hazards which are due to high current and voltages in battery system and converters. Third group is related to thermal processes with risk of overheating of battery modules and electronic components. At the end some risk can occur as the consequence of errors in control logics and incorrect sensor readings. Result of this stage is hazard register which makes a baseline for further assessment which will be discussed in chapter 4.

2.4.2. Risk assessment

After identification next step is to evaluate a risk level related to every hazard scenario. Risk assessment has a goal to determine a occurrence probability of event and its consequences. Methodology is in line with standard IEC 61508-5 where qualitative engineering assessment and simplified methods of risk analysis are combined.

Risk is evaluated based on 3 parameters. First is severity which represents the consequences of event and its impact on human safety, equipment and environment. Second parameter is likelihood of event occurring during operation of system.

Based on the risk assessments, hazard scenarios are categorized according to the severity of their potential consequences:

- Catastrophic consequences
- Major consequences
- Localized consequences

The goal of this phase is to ranking hazards events based on level of risk which allows determining the priorities in implementation of safety measures.

2.4.3. Defining safety functions and assigning SIL level

After risk assessment it is possible to identify safety function according to its definition as specific technical function whose goal is detection of dangerous state and activation of safety measure which brings system back to safety. In SIRIH2 safety function is described through input parameters which are for example voltage current and temperature of batteries. Second part is decision logics which analyses measured parameters and determines whether system operates

inside safe limits. Final part is output action which goal is to bring system back to safe operating conditions.

After defining safety function, it is necessary to determine suitable SIL level for every one of them. In SIRIH2 highest integrity level is assigned on functions which are related to uncontrolled leakage of hydrogen considering potential catastrophic consequences of such event. Functions related to overvoltage and short circuit protection have a high level of SIL because it directly affects the safety of battery system. Function of temperature control of battery modules have lower required integrity level because they control degradation of system.

3. Description of the SIRIH₂ Hybrid Hydrogen–Battery System

3.1 System Architecture Overview

SIRIH2 is the prototype of transportable charging system, multifunctional and adaptable to different areas of use with hydrogen as its main energy source. On macroscopic level SIRIH2 can be understood as coupled fuel cell and battery system that provides electrical energy to end user. The fuel cell produces electricity through electro chemical reaction of hydrogen stored in special cylinders and oxygen in air.

Figure 2. SIRIH2 shell

In context of whole architecture of system energy flows are very important for understanding SIRIH2 functioning. Electrical energy produced in fuel cells is not used to supply end user but to charge BESS subsystem. Battery's function has a function of buffer which enables to cover sudden spikes in power demand. Configurations like this are very common because fuel cells have slower dynamical responses in comparison to batteries systems. Besides internal energy production

SIRIH2 is designed to be able to work with interaction with power grid. System enables connection with three phase AC power grid of 400V which is used as alternative source of power supply for energy pack. This approach enables higher operational flexibility in different environments. This means that control systems can decide which energy source to use fuel cell, battery system or directly from grid where end goal are lower operating costs and more stable supply for end user. Main advantage of SIRIH2 is the ability to be deployed fast and to work in autonomous and off grid environments using only hydrogen power.

Figure 3 SIRIH2 charging station(left) and hydrogen power cell(right)

Important aspect of architecture is controlling and monitoring units. In framework of SIRIH2 these functions is performed by Shelter Control Unit (SCU) which represents brain of the system. SCU takes data from different subsystems including BMS, fuel cell controller, cooling system, energy converter and based on this information makes decisions related to operating mode. In this way there is coordinating control of production of energy, charging of battery, supplying of end user and interaction with power grid.

The Battery Management System (BMS) plays a central role in ensuring the safe operation of a battery storage system. The BMS continuously controls the operating parameters of the battery included. Within the SIRIH2 system, the BMS measures the voltage of individual cells and modules, the battery temperature, the charging and discharging current, as well as the assessment of the state of charge (SoC) and the state of health (SoH).

The functionality of the BMS of the SIRIH2 system is indicated in its ability to detect dangerous states in time and manage it back to safe conditions. Example of these is overvoltage, undervoltage, excessive temperature, excessive current, cell imbalance, as well as sensor or communication link failures. If it detects any abnormality the BMS will automatically readjust. Where its functions have a direct impact on reducing the risk of thermal runaway, fire or permanent damage to the batteries.

The functions of the BMS on the SIRIH2 system are controllable by the program, so it is possible to choose limits on parameters. It is noted that the verification based on the BMS must be performed according to the basic standards of correct functionality, according to IEC 61508, as defined by correct cycles, which can be hard and soft, so that the verification can be performed on the safety functions. The application of these principles allows for the systematic identification of hazards and the demonstration that the BMS meets the requirements without safety integrity.

It is noted that the SIRIH2 system can be accessed from the BMS and other subsystems, such as the Shelter Control Unit (SCU), the fuel cell and the user interface. A reliable and deterministic community is crucial for functional safety, as delays or errors in data exchange can lead to incorrect management decisions. For this reason, critical safety information is transmitted via CAN communications, while supervisory and information data are used for display and remote monitoring systems.

3.3 Energy Flow and Control Interfaces

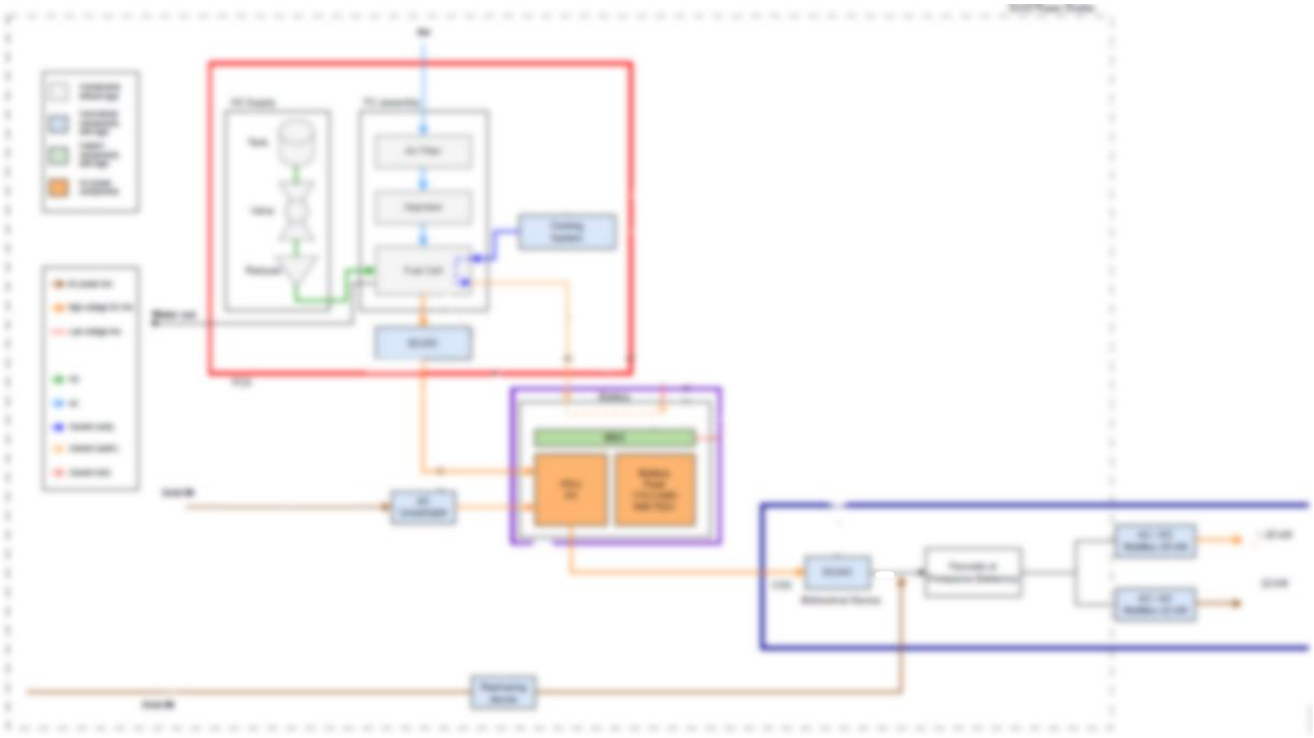

Figure 4. SIRIH2 system architecture

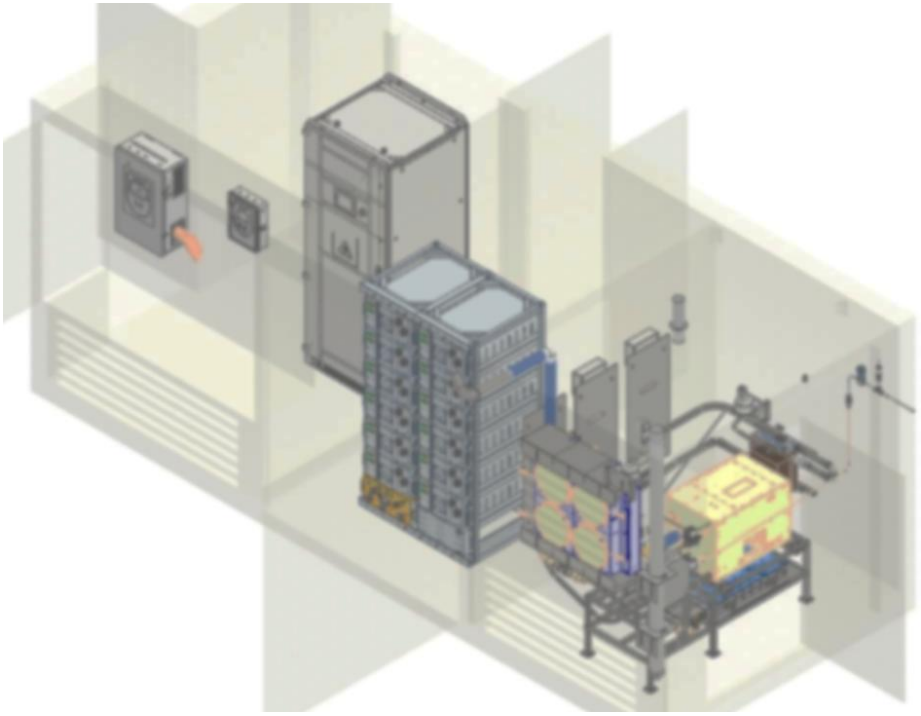

Figure 5. SIRIH2 system CAD model

4. Hazard Analysis and Risk Assessment of SIRIH$_2$

Combining different energy technologies in one system complexity of managing and requires additional safety evaluation significantly increases. Systematic analysis is required to map all safety risks. Based on analyzed architecture of system and interaction of subsystems and their energy flows there are few main categories of source of hazards identified where suitable safety functions are required. Analysis is made in line with principle of functional safety standard IEC 61508. Every identified hazard has initiating event, estimation of consequences and suitable Safety Integrity Level. This process allows systematic connection of hazards with functions which must detect and control it.

4.1 Hazard Identification and Classification

4.1.1 Hydrogen-Related Hazards

Hydrogen is flammable gas where any leak could lead to serious consequences. In SIRIH2 hydrogen is stored in pressurized tanks and it is used in fuel cells for electrical energy production. Possible scenario includes leakage due to damage on pressurized cables, valve and pressure regulation. Risk of explosion and fire requires high level of integrity for safety function.

Hazard	Initiating Event ID	Consequence	SIL
Uncontrolled hydrogen release (cables)	SIRIH2_IE_001	Catastrophic	SIL 4
Uncontrolled hydrogen release (fuel cell)	SIRIH2_IE_002	Catastrophic	SIL 4
Uncontrolled hydrogen release (pressure regulator)	SIRIH2_IE_003	Catastrophic	SIL 4

4.1.2 Battery Overcharge Hazards

Overvoltage of battery cells represent one of the most critical scenarios in battery systems. Overcharging leads to accelerated degradation, increase of temperature which can potentially lead to thermal runaway process. In SIRIH2 system overcharging can happen due to different causes where some of them is faulty behavior of DC/DC converter, continuous charging from fuel cell and wrong estimation of SOC of battery.

Hazard	Initiating Event ID	Consequence	SIL
DC/DC continues charging	SIRIH2_IE_004	Major	SIL 3
Fuel cell continues charging	SIRIH2_IE_005	Major	SIL 3
SOC underestimation	SIRIH2_IE_006	Major	SIL 3
Cell imbalance leading to overvoltage	SIRIH2_IE_007	Major	SIL 3

4.1.3 Battery Short Circuit Hazards

Short circuit scenario causes high currents in battery system. These high currents leads to heating of components, battery cells and in event of escalation even fire.

Hazard	Initiating Event ID	Consequence	SIL
DC load short circuit	SIRIH2_IE_008	Major	SIL 3

4.1.4 High Voltage Exposure During Maintenance

During maintenance of SIRIH2 due to different sources of electrical energy there is increased possibility that some part of system remains under voltage tension. These situations can cause safety risk for personnel performing maintenance.

Hazard	Initiating Event ID	Consequence	SIL
DC rail powered during maintenance	SIRIH2_IE_010	Hazardous	SIL 2
AC/DC grid powering DC rail	SIRIH2_IE_011	Hazardous	SIL 2
Fuel cell powering DC rail	SIRIH2_IE_012	Hazardous	SIL 2

4.1.5 Thermal Hazards

Increased temperature is a important indicator that certain components in energy systems are not working properly. Thermal events can happened under increased load, insufficient cooling and faults on component.

Hazard	Consequence	SIL
Fuel cell overheating	Major	SIL 1
Battery overheating	Major	SIL 1
DC/DC overheating	Major	SIL 1
AC/DC overheating	Major	SIL 1
DC/AC overheating	Major	SIL 1

4.2 Allocation of Safety Functions to BMS

From the Hazard Register, the following hazards fall directly under BMS responsibility:

Hazard Category	Target SIL	BMS Responsible
Battery Overcharge	SIL 3	YES
Battery Short Circuit	SIL 3	YES
Battery Overheating	SIL 1	YES
Cell Imbalance	SIL 3	YES

This analysis shows that BMS must implement safety functions with different levels of integrity. Continuous functions of protection of overvoltage and short circuit require SIL 3 level where other functions lower. This classification directly defines requirements for design and verification of BMS. Higer level of SIL includes higher standards in architecture, implementation, verification and documentation in order to prove safety of the system.

5. Role of the BMS as a Safety-Related System

5.1. BMS roadmap

To secure a safe and effective performance of battery systems it is necessary to use battery management systems BMS. BMS is a complex system where it main function is to monitor the state of battery, protection from undesirable working conditions and optimization of battery usage. It behaves as interface between battery and remaining energy system. BMS ensures that battery works inside defined voltage, current and temperature limit which results has increase life spam. Development of BMS can be flowed through 4 generations based on functionalities and technological maturity of the system. Every generation made a step forward in terms of technological development.

5.1.1. First generation (1990-2000)

Represents the beginning of BMS with basic function of monitoring and protection. First generation BMS was primarily monitoring basic variables as voltage and current on cells and in some cases temperature. This early system did not have complex algorithms and the acted extension in form of switched which would disconnect a battery from the circuit. Communication capabilities were very limited or nonexistent. Application was present is small portable electronics and tools which was enough. Early electric vehicles of low performance were built for experimental purposes such as GM EV1. In this period lithium-ion battery was entering a wide consumer market in forms of phones and portable PCs where demand for more advanced protective systems increased.

5.1.2. Second generation (2000 - early 2010)

This generation is followed by digitalization and algorithm application. As lithium batteries started to be used in first hybrid vehicles, the necessity for precise and smart management of batteries. BMS of second generation integrated microcontroller or DSP processors which process data in real time. This opened path for implementation of first algorithms for estimation of SOC and SOH, instead on dependance on voltage values. Typically, simple algorithms were implemented as Kalman filter and Colomb counting. This represented significant improvement in comparison to first generation. BMS also got to communicate with other parts of system using CAN and LIN as with that batteries becomes integrated parts in vehicle. Passive cell balancing with resistive circuit was standard function of BMS. Use of better ADC converter enabled precise measurements where decision making processes were made using software and not only on hardware thresholds.

5.1.3. Third generation (late 2000 early 2020)

Third phase of development is connected to integration and integration of BMS. It was driven by expansion of high voltage electric vehicles and energy storage systems, BMS becomes more sophisticated in terms of precision in measuring and algorithms. From hardware point of view high precision sensors and ADC convectors which permit monitoring of a big number of battery cells with multichannel temperature measuring. Kalman filters are upgraded with nonlinear models of batteries based on equivalent circuits as first implementation of neural networks for pattern

recognition of cell degradation. Batteries become more efficient with active balancing where loss of energy in passive balancing with resistor is replaced with capacitive and inductive converters.

5.1.4. Fourth generation (mid 2020 - present)

Modern BMS enters an era of global network and artificial intelligence with a goal of complete control over lifecycle of battery. This generation develops at the same time with electrification of transport internet of things and big data analytics. BMS of fourth generation spread influence beyond single unit where data is collected for multiple different units and data is collected in centralized cloud and processed to perform better analysis of data. Information about batteries cycles and habits of users and environmental influence can be processed in remote and enhance the prediction of state of batteries and optimize strategies of charging and discharging. Thanks to machine learning BMS can make predictions instead of having a status of current state in terms of failure predictions and potential risks. This approach in practice predicts thermal runaway few minutes faster than traditional systems where the goal is to monitor battery through whole life cycle and prevent the problems before they occur with integration to wide energy infrastructure. Application of this generation includes most advanced electric vehicles and big BESS systems.

5.2 Monitoring Functions

Nowadays electrical systems and machines rely more on batteries as reliable and flexible source of electrical energy. Their application has widespread fields of application from portable electronic devices, electrical vehicles, systems for energy storage from renewable sources. Among the available technologies lithium-ion batteries have dominant place thanks to high energy density, large life cycles and desirable electrochemical characteristics. These advantages come with great sensitivity for undesirable working conditions, which can result in degradation of battery cells, decrease of reliability of system and possible risky and hazardous behavior.

Functionalities of BMS is usually grouped into 4 main categories: Battery protection, monitoring of working parameters, balancing of cells, controlling the battery systems. Every of these categories has well defined function where their interaction enables stable and predictable performance under various working conditions.

5.2.1. Battery protection

Lithium-ion batteries require operation inside well specified conditions. Operation outside voltage current and temperature limit can cause irreversible electrochemical degradation increase of internal resistance, loss of capacity and most dangerous condition of thermal runaway. Functional safety of BMS must be implemented as multilayered protection mechanism which combines constant monitoring and fast protective actions.

Overcharge protection is realized by comparing every cell inside battery pack with maximum allowed value defined by battery specification. Overcharging starts oxidation of electrolyte and destabilization of cathode material. BMS in these cases breaks the circuit using mosfet switch relay or by sending the controlling signal to charger.

In advanced system multilayer protection in overcharging is present. First layer is warring threshold where the limit is just under maximum allowed value. When battery reaches this value, it does not stop charging but gradually decreases current of charging. Second layer is soft cutoff where current is additionally lowered or decreased to minimal value. Third layer is hard cutoff where it breaks the circuit completely using switches. In practical applications multilayered protection is combined with temperature dependent current limitation where BMS adjust allowed charging or discharging current in dependence of measured cell temperature. This adaptive approach is commonly used in BMS systems for electric vehicle and stationary systems for energy storage ESS. Multilayered protection is an example of intelligent management of functional safety of BMS where BMS is not only having reactive but also predicting and optimizing role.

5.2.2. Working parameters

Precise and reliable measuring of voltage current and temperature ensures realistic state of battery and its behavior under different working conditions. Quality of monitoring is directly influenced by accuracy of estimation of state of charge and state of health.

Measuring voltage of single cells is crucial in serial connected battery packs. Small differences in voltage can indicate uneven degradation or need for balancing. For that reason, BMS uses multichannel analog digital converters of high resolution to ensure precise measurement of voltage with minimal noise in signal.

Monitoring of current tracks the energy movement inside battery system. With integration of current over time the method of coulomb counting is preformed, which is basic technique to estimate SOC. This methos is prone to errors like sensor drift.

Temperature is third key parameter which is monitored. Because of nonhemogenic distribution of heat inside battery packs often multiple sensors are used to monitor the temperature at critical location, for result having decrease of thermal load.

Estimation of SOC and SOH is a complex problem requiring specific mathematical methods, equivalent circuits and algorithms as Kalman filter. This estimation gives us insight into degree of degradation and remaining battery life.

5.2.3. Balancing

Balancing of battery cells represent key mechanisms for ensuring equal distribution of voltage capacity and state of charge in battery packs. Although cells in battery packs are nominally identical in realistic condition they show a deviation due to manufacturing tolerances in internal resistance, temperature gradients and unequal rate of aging. These differences cause asymmetrical performance of battery cells during charging or discharging which has a direct negative effect on total performance and security.

Without balancing total capacity of battery packs is determined by cells with lowest capacity. During the process of charging cells with lower total capacity or higher internal resistance reach voltage limit sooner than other cells which force BMS to stop charging. In contrast to that during discharging the same cell reach lower limiting voltage level sooner which limits the usability of whole battery pack. Without balancing, not only that we lose useful capacity in battery pack, but we increase the risk of overcharging or deep discharging of single cells.

The simplest and most frequent type of balancing is passive balancing. This method is based on dispersion of excess energy from cells with higher voltage with balancing resistors, which are activated with the help of transistor switches. Passive balancing is usually performed in final phase of change when the voltage differences are more evident. Advantages of this method are cheap implementation, low cost and high reliability. Disadvantage of passive balancing is low efficiency due to excess of energy is transformed into heat which can lead to additional heating stress which requires correct thermal handling.

Active balancing enables redistribution of energy between cells with significantly higher efficiency. Active balancing systems use different topologies for transport of energy capacitive balancing, inductive balancing, DC–DC converter-based balancing.

Besides hardware topology significant role has the strategy of balancing. Balancing can be based only on voltage of cell or on estimation of SOC, where different models and algorithms are used to estimate a state. Advanced BMS implement adaptable strategies which consider temperature, internal resistance and SOH for the result of having more optimal distribution of stress and reducing aging of individual cells. Balancing can be activated during charging or discharging or when battery is in a state of rest. The choice depends on available energy for balancing. Continuous balancing allows maintaining of more uniform state of cells inside battery, but it increases in complexity. Limiting balancing only on charging phase makes compromise between complexity and efficiency. Balancing represents one of the key functions in modern BMS systems essentially in application with high energy demand and long lifecycle.

5.2.4. Controlling the battery systems

Controlling the operation in battery represents the highest functional level of BMS in which protective, balancing and monitoring functions are implemented into single controlling framework. One of the key aspects is the control of charging. In practice the most common is combined Constan Voltage CV and Constant Current CC profiles. During CC BMS defines maximum allowed value of current in dependence of temperature SOC SOH. In CV phase voltage is on limiting value while current is gradually decreasing. This approach ensures charging with minimal electrochemical stress on cells.

BMS also implements adaptive strategies of charging where charging parameters are adjusted to working conditions and level of degradation. For example, under higher temperatures or increased internal resistance allowed current is decreased to prevent additional heating and accelerated degradation of battery.

During a process of discharging BMS controls the delivery of energy to users considering limits on tension current and power. BMS are often integrated into bigger systems where it communicates with other control units using standardized protocols like CAN LIN or ethernet. This enables exchange of data about battery life, fault diagnostic.

5.2.5. SOP

In modern BMS solutions the State of Power (SOP) introduced a new dimension how battery pack can be used monitored and limited due to safety. It enables improvement from statical and conservative operation boundaries to dynamic and contextual dependent decision-making framework. With new techniques it increases the usability of the system and increases complexity of safety management.

One of the key concepts of SOP is the formalization of time dimension of power. SOP is always defined for a certain time horizon of 1 ,10 30s where there is an explicit difference between short term and long-term power output. This approach gives BMS possibility to use high power in short intervals where it at same time limits the energy and temperature stress over longer periods. For stationary BESS system, this is very important when power grids require fast and short intervention. SOP precisely demarcates between technically allowed and long term sustainable working conditions.

SOP ability to handle battery degradation through safety function not only optimization where there is no need to explicit change of boundary conditions or manual calibration. In this way degradation becomes integrated into safe working framework which is very important for longevity and reliability of BESS installation.

SOP transforms the relationship between BMS and higher-level management systems by introducing a continuous, quantitative signal of available power, instead of binary permissions or prohibitions. This allows for better coordination between the technical limitations of the battery and the operational goals of the system. It is in this transition from passive protection to active, model-driven limitation that the essential novelty that SOP brings to modern BMS.

6. Model-Based Approach for Functional Safety Verification

6.1 Motivation for Model-Based Verification

Model based approach represents modern engineering methodology which is applied in the design process analysis and verification of complex systems, especially where safety has important role. This method uses formalized models of systems and subsystems as a main tool for understanding analysis and proving the behavior of the system during its whole lifecycle. In the context of functional safety this approach allows us to observe safety not as set of protective measurements but as systematic behavior which arises from dynamical behavior of the system. This is especially effective with the system which includes the combination of hardware software and decision algorithm as modern BESS systems.

This approach describes a system using relevant mathematical logical and hybrid models which describes relations between inputs outputs and internal states of system. These models do not represent exact copy of reality but controlled abstraction. Beside statical analysis model-based approaches observe how system behaves in time where reaction of systems depends on previous states.

In context of functional safety model-based approaches have multiple roles. The most important role is that it provides behavior of the system and based on that it is possible to identify deviations which can indicate undesirable and possible dangerous states. Using models, it is possible to test the behavior in a condition which surpasses nominal working condition of machine. These are boundary conditions and extreme points of working conditions, degenerative working conditions and combination of undesirable conditions which are hard to reach in real system without consequences. Other dynamic benefits:

- detection delays
- inertness of physical processes
- interdependence of variables
- feedback loops between subsystems

6.2 Abstraction of the BMS and Battery Plant

Model of BMS and Battery Plant is developed through controlled abstraction of the system. Idea is not to reproduce complete physical reality but to include critical dynamic characteristics which are relevant for validation safety functions and detection of hazard scenarios rather than to reproduce electrochemical processes.

Battery plants are modeled on the level of energy flow and dominant dynamic variables. In this model there are voltage responses, current flow and basic thermal dynamics, where complex processes of degradation, diffusion and microscopic change inside cells are not covered. This level of abstraction enables realistic simulation of overvoltage, overcurrent and overtemperature which are directly connected to already defined hazards in risk register.

BMS is abstracted as controlling- safety layer which takes inputs from battery plant and based on predefined thresholds and logics decides about safety function activation. There is clear separation between monitoring fault detection and safe state activation. This abstraction provides direct link to hazard analysis, predefined safety goals, assigned SIL levels

6.3 Simplified model of battery system

In real BESS battery packs usually contain high number of single cells connected to serial and parallel configurations. For industrial system these numbers are order of hundreds of cells to obtain necessary working voltage and capacities. Direct modeling of whole battery system with high number of cells in MATLAB/Simulink environment would significantly increase complexity of model and time of simulation. Besides that full model approach would not necessarily add additional value to verification of functions of BMS. Due to this in following evaluation the simplified model of battery pack connected in series with 6 cells. This model represents reduced version of real system, but it maintains basic electrical and thermal characteristics which are relevant for analysis and verification.

Goal of this representation is not complete reproduction of BESS but observing dominant physical processes which influence safety of BMS. Reduced model successfully tracks voltage changes during charging and discharging, current trough battery pack, changes in temp, unbalanced voltage between cells, reaction logic for abnormal conditions. Safety functions are based on tracking limiting values of current voltage and temperature. That is a reason why algorithms can be

analyzed in simplified model with lower number of cells. Another important reason to use simplified models is more effective variety scenario execution and testing of different faults as overvoltage, undervoltage, overcurrent, over temperature.

7. Development of the MATLAB/Simulink Model

7.1 Battery Plant Modeling

Battery plant is modeled in Simulink environment as simplified plant but with key dynamic parameters. Instead of detailed electrochemical model the equivalent circuit model is used which describes good enough the relationship between current voltage and temperature. Model enables simulation transient states extreme condition overvoltage overcurrent and temperature deviations which is necessary for functional safety.

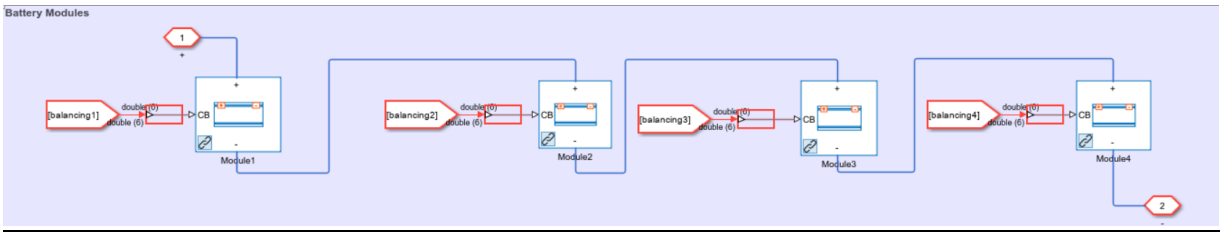

Figure 6. Battery model plant

7.2 BMS & Battery MATLAB model

Models of battery plant and BMS are organized to be modular, in that way BMS control/protection logic and battery plant is divided into clear subsystems. This structure is favorable for repeating tests, injecting faults, monitoring parameters without direct modification of base BMS model. Simulink is central platform for Model in Loop testing where with simulation input signals are generated (sensor measurements, state of battery) then follows the response of BMS (fault detection, activation of protection, safe state transition). With that it is possible to work in controlled environment for verification of safety functions before performing hardware tests.

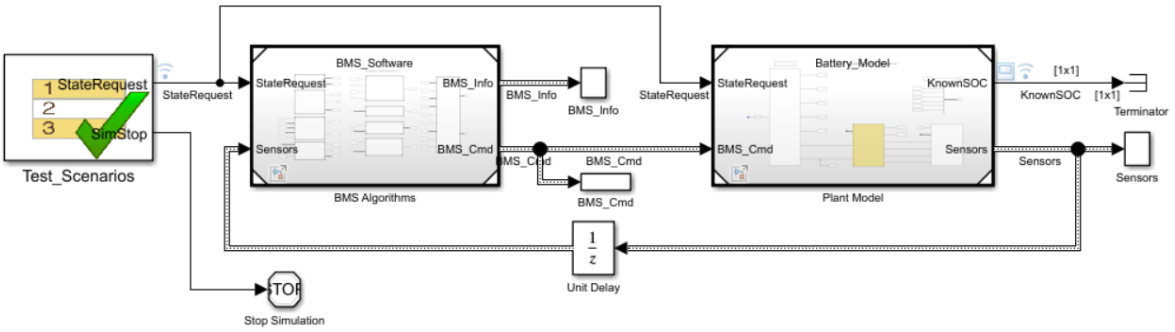

Figure 7. Plant of the BMS and Battery plant system integrated

7.3 BMS logic

Logic of BMS is implemented as a set of functions for monitoring diagnostic and protection which are continuously monitoring basic parameters about battery and makes decisions if certain conditions are detected which are not in standard operation boundaries. In this model overvoltage, undervoltage, overcurrent for charging and discharging, overheating and sensor correctness are present. When conditions are met for fault BMS logic imposes flag signals which execute predefined safe state.

Separate subsystems determine charge and discharge limits, and the most restrictive value is selected to ensure safe operation under all conditions. The measured pack current is continuously compared with the calculated current limits. If the current exceeds these limits a fault condition is triggered. In addition to current monitoring, the model includes protection mechanisms for cell overvoltage, undervoltage, high temperature and low temperature conditions. When any fault condition is detected the BMS generates fault flags that activate predefined protective actions. In the simplified model these actions are represented by forcing the allowable current limits to zero, effectively transitioning the battery system into a safe operating state.

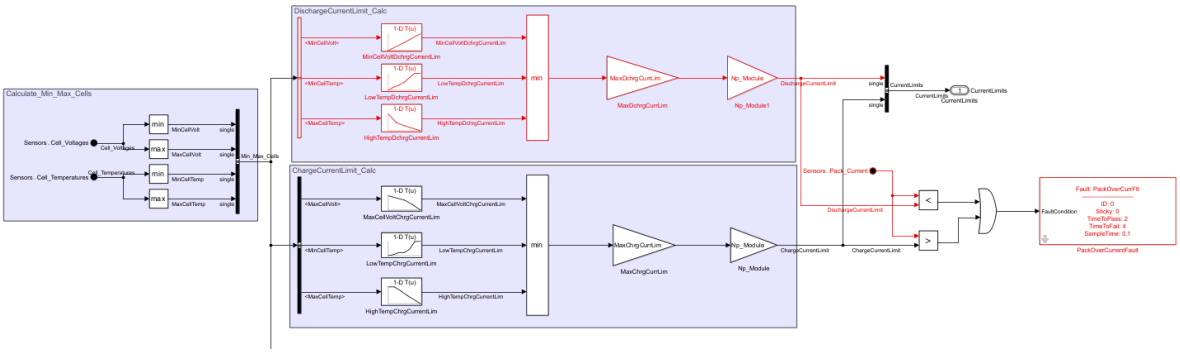

Figure 7. BMS battery pack over-under current logic

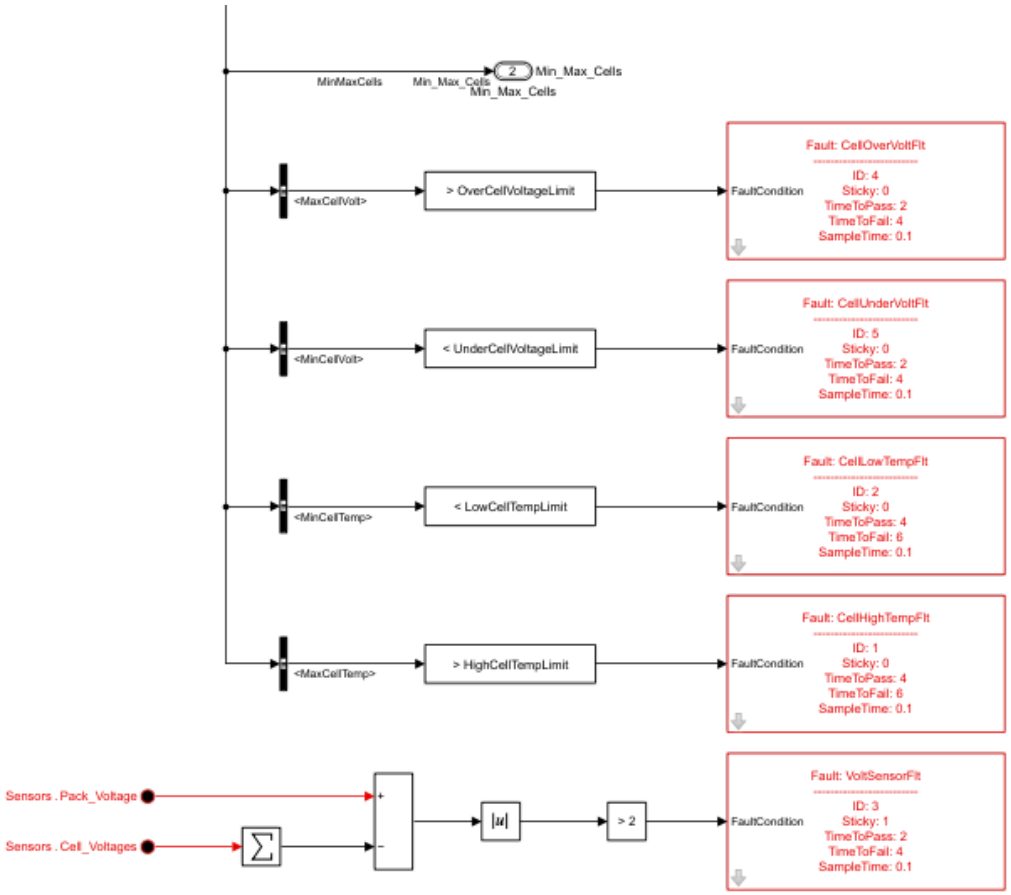

Figure 7. BMS battery cell overvoltage under voltage logic

8. Results and Safety Evaluation

This chapter represents verification of safety function of simplified BMS using approach of MIL simulation. The goal of verification is to evaluate does BMS detects dangerous states which were identified in analysis process and can it activate suitable action to get to safety state. Under evaluation is one battery pack containing 6 cells.

Safety functions are directly developed and supported by MATLAB/Simulink model:

- battery voltage monitoring
- battery current monitoring
- battery temperature monitoring

Evaluation is based on different simulation scenarios where in controlled way fault injection is performed to simulate different hazard scenarios. Results are analyzed based on measurable indicators of performance:

- Proper activation of safety function
- Time of detection
- Time for system transit to safe behavior

8.1 Reference model

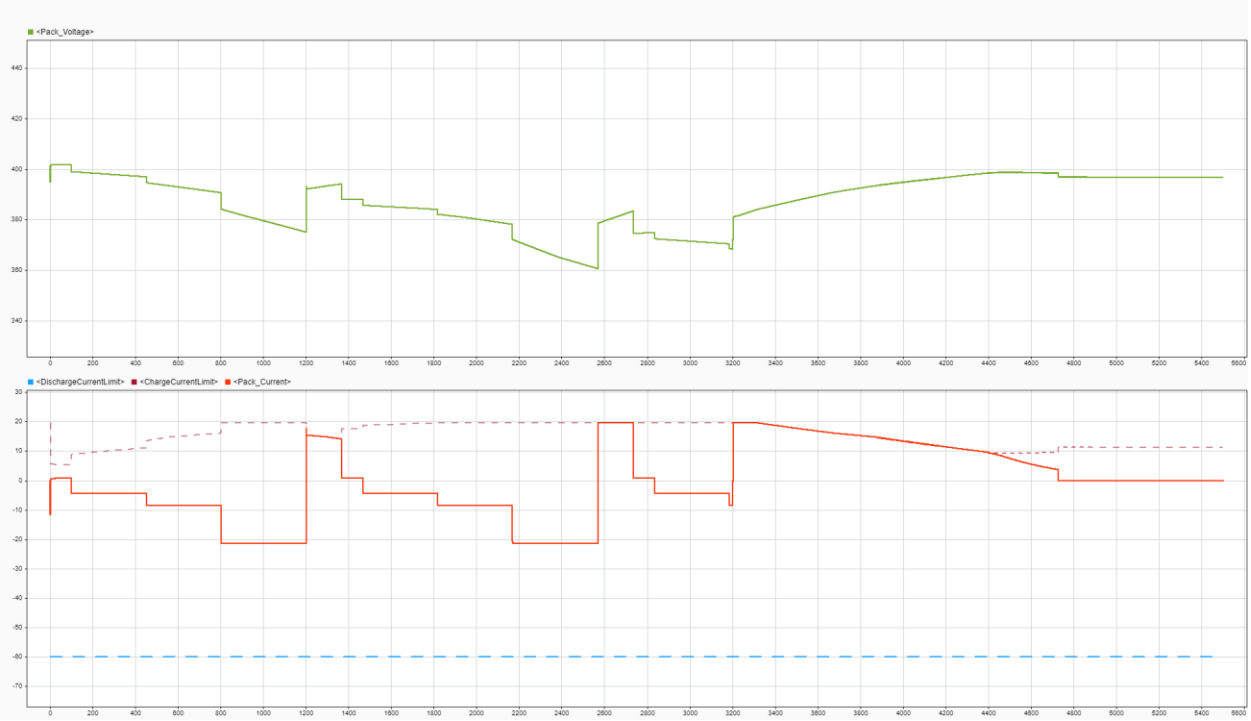

Figure 8 Performance under normal condition

The system's behavior is analyzed under normal operating conditions, without the presence of faults or hazardous events. In this scenario the Battery Management System (BMS) monitors the battery pack while it operates within the predefined safe limits of voltage and temperature. As shown in the corresponding graphs, all monitored variables remain within their allowable operating thresholds and no-fault conditions are triggered.

During this operation the BMS continuously calculates the allowable charge and discharge current limits based on the measured state of the battery pack. These limits depend on the instantaneous values of voltage and temperature and ensure that the battery operates within safe electrical and thermal boundaries.

This scenario represents the reference operating condition of the system. The results obtained under these normal conditions serve as a baseline for comparison with subsequent simulations, where specific fault conditions and abnormal operating requests are intentionally introduced in order to evaluate the response of the protection logic implemented in the BMS.

8.2 Overtemperature

Following graph shows behavior under detection of abnormal temperature. On graph allowed values are shown of ChargeCurrentLimit, DischargeCurrentLimit, Pack_Current. Fault is intentionally introduced at time t=250 s to simulate overheating of battery system. Fault was introduced trough modification of input signal of temp sensor on BMS to an abnormal value. At t = 250.1 s detection occurred and the BMS goes to safe state. Upper and lower limit are set to 0A in that way any circulation of energy through system is stopped and potential escalation and damage to battery is stopped. Observed current goes to 0A in fast way where it is confirmed efficient protection logic.

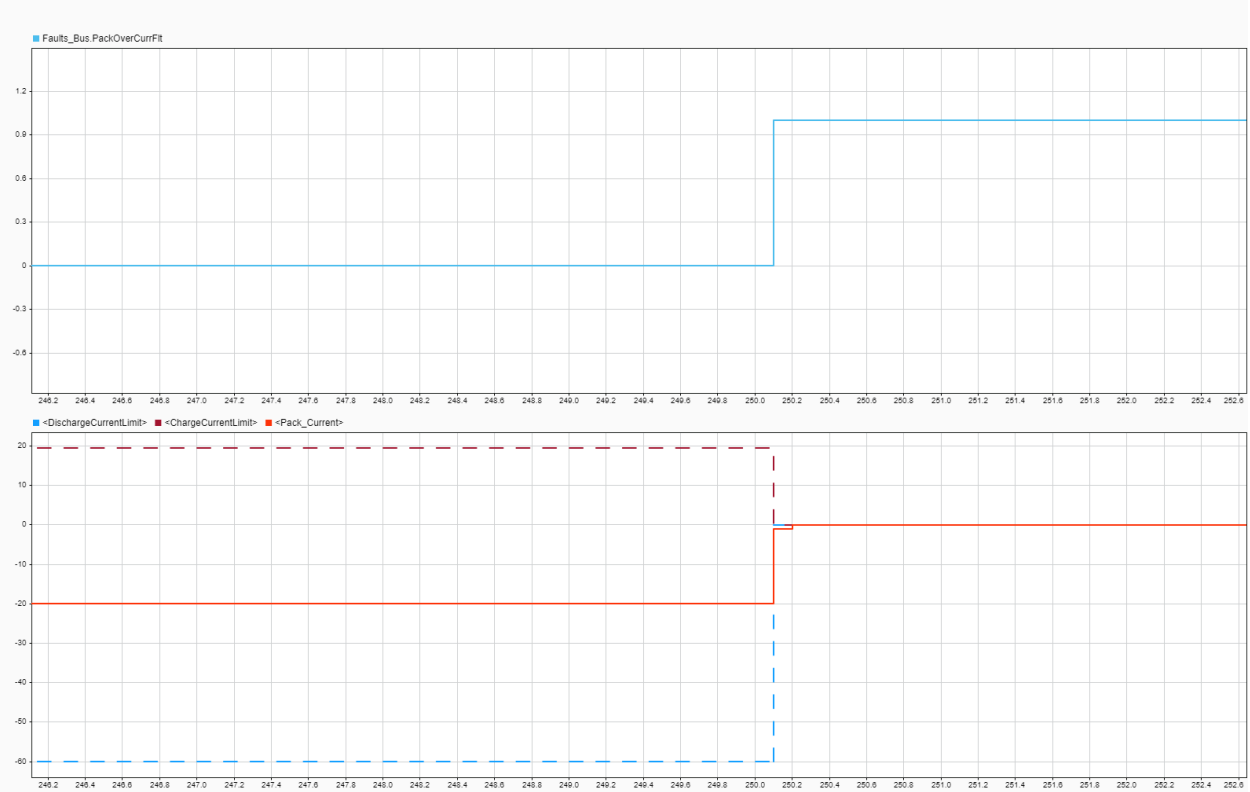

Figure 9. Overtemperature fault injection and BMS response showing detection delay and transition to safe state (current limits set to 0 A)

8.2 Overcurrent with short circuit trigger

The following simulation scenario shows what happens when a short circuit causes too much current to flow in an electrical circuit. In this situation, the current from the battery pack suddenly spikes, which can be dangerous for the battery system. The BMS (Battery Management System)

always keeps an eye on the current and checks it against the safe charging and discharging limits it has calculated.

If the measured current goes above the set maximum limit, the system activates an overcurrent protection feature. Once this fault is detected, the BMS sends a fault signal and triggers the right safety response. As a result, the system switches to a safe state where both charging and discharging current limits are set to 0 A. This stops any more current from flowing through the battery pack.

This way, the BMS responds quickly to short circuit conditions and helps prevent damage to the battery, power converters, and other parts of the system.

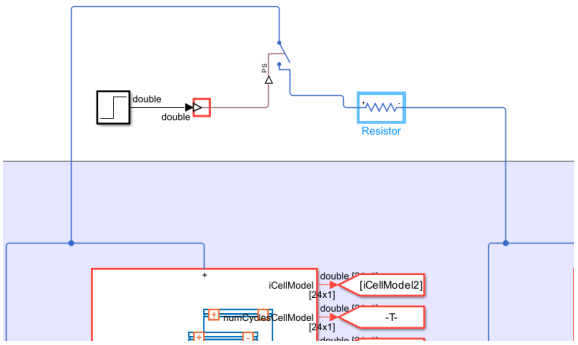

Figure 10 Short circuti falut introduction

Figure 11. Short circuit fault injection and BMS response showing rapid overcurrent detection and transition to safe state (charge and discharge current limits set to 0 A).

8.3 System fault handling logic

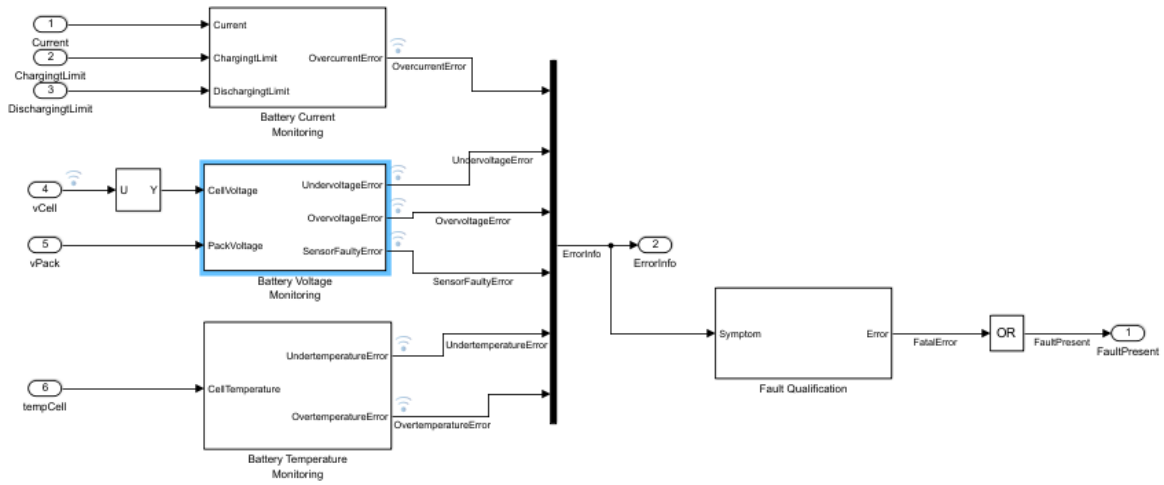

Figure 12 Fault logic of BMS

9. Identified Weaknesses and Gaps

Model in Loop testing environment developed in this project shows successful verification of basic safety function of BMS. Even though results show that implemented approach is working during the analysis it is possible to identify limitations. These limitations do not represent leak of concept, but they indicate possible direction of further improvement of system of verification. The goal of this chapter is to identify key technical and methodological improvements for this safety function.

9.1 Improvement of MIL simulation environment

The MIL model that has been developed allows us to simulate how the battery system and the BMS safety logic work together. This is an important step in checking and verifying functional safety. However, the current simulation model only covers a limited number of operating states and a relatively small set of controlled fault scenarios.

In future work MIL environment can be improved by adding more operating scenarios to the simulation. This includes different battery operating modes, changing system loads, and the effects of varying surrounding temperatures on how the battery system behaves. By introducing more real-world operating scenarios, we can better analyze how the system's safety functions perform under a wider range of actual working conditions.

Another possible improvement would be to use more detailed battery cell models. These models could consider how the battery degrades over time, changes in internal resistance, and the thermal processes happening inside the battery pack. This approach would make the simulations more realistic and help us more accurately assess how the system behaves during long-term use.

9.2 Hardware in the Loop (HIL) testing

After checking how everything works in the MIL environment, the next natural step in the development process is to move on to Hardware-in-the-Loop (HIL) testing. In a HIL setup, the BMS algorithms actually run on the real control hardware, while the battery system and other parts are simulated in real time.

This approach helps uncover issues that are not visible during MIL simulations. In real systems, control units have limited processing power and memory, which can affect how fast algorithms run and how well the system performs. HIL testing lets us look at real timing constraints and see how communication delays between different system components impact things.

On top of that, HIL testing also allows us to analyze real sensor behavior. In MIL simulations, signals are modeled as perfect, but in real systems sensors have noise, limited resolution, and measurement errors. All these factors can affect how the safety functions behave so taking them into account is key to getting a realistic picture of system reliability.

9.3 Automated tests & Advanced fault injection framework

In complex energy systems like Battery Energy Storage Systems (BESS), there can be a huge number of possible operating states and potential faults. That's why it's essential to use automated testing methods when verifying safety functions.

An automated test framework makes it possible to generate and run many simulation scenarios without needing someone to manually step in between each test. This way, you can analyze how the system behaves across many different working conditions and input settings.

Advanced fault injection systems take verification even further by simulating complex and rare scenarios which would be hard to recreate in real-world experiments. These scenarios can include things like sensor failures, communication errors between subsystems, individual cell degradation, or noise and delays in the system. Combination of automated testing with advanced fault

injections, it is possible to get a much deeper understanding of potential weaknesses of the system and detect possible design flaws that can occur early on.

9.4 Improvements on SIRIH$_2$

Besides improving how we verify the system, there are also some clear directions for developing the system itself to make it even more reliable and safer. One important area is upgrading the diagnostic features of the sensor system. By adding advanced algorithms that can detect when a sensor is failing, and maybe even using backup sensors for critical measurements, we can make the system much more dependable. This helps reduce the chance of incorrect readings affecting the safety functions. Another improvement could be building smarter diagnostic functions right into the BMS. These could spot early signs of battery cell degradation or other abnormal conditions before they become bigger problems. Having these kinds of monitoring tools can improve operational safety and help extend the overall life of the battery system. We could also look at adding extra independent safety layers at the hardware level. These would act as a backup safeguard if the software or control logic ever fails.

Another idea worth exploring could potentially increase performance of the system by doing a diversification of electrical power sources as for example with solar panels. If we assume that adding solar panels only to the roof of SIRIH2 it is possible to increase output of 30kW for additional 10% in power output with direct consequence of lower consumption of hydrogen.

References

[1] IEC, IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Geneva, 2010.

[2] ISO, ISO 13849-1: Safety of Machinery — Safety-Related Parts of Control Systems — Part 1: General Principles for Design, International Organization for Standardization, Geneva, 2015.

[3] G. L. Plett, Battery Management Systems, Volume I: Battery Modeling, Artech House, Boston, 2015.

[4] G. L. Plett, Battery Management Systems, Volume II: Equivalent-Circuit Methods, Artech House, Boston, 2015.

[5] G. L. Plett, Battery Management Systems, Volume III: Battery State Estimation, Artech House, Boston, 2016

[6] D. Andrea, Battery Management Systems for Large Lithium-Ion Battery Packs, Artech House, Boston, 2010.

[7] H. Chen, T. N. Cong, W. Yang, C. Tan, Y. Li and Y. Ding, “Progress in electrical energy storage system: A critical review,” Progress in Natural Science, vol. 19, no. 3, pp. 291–312, 2009.

[8] Y. Wang *et al.*, “Advances in safety of lithium-ion batteries for energy storage,” *Energy Storage and Saving*, 2025, doi: 10.1016/j.enss.2024.100506.

[9] X. Hu, S. Li and H. Peng,“A comparative study of equivalent circuit models for Li-ion batteries,” Journal of Power Sources, vol. 198, pp. 359–367, 2012.

[10] A. Barré, B. Deguilhem, S. Grolleau, M. Gérard, F. Suard and D. Riu, “A review on lithium-ion battery ageing mechanisms and estimations for automotive and stationary applications,” Journal of Power Sources, vol. 241, pp. 680–689, 2013.

[11] M. Berecibar, I. Gandiaga, I. Villarreal, N. Omar, J. Van Mierlo and P. Van den Bossche, “Critical review of state of health estimation methods of Li-ion batteries,” Renewable and Sustainable Energy Reviews, vol. 56, pp. 572–587, 2016.

[12] M. A. Hannan, M. M. Hoque, A. Mohamed and A. Ayob, “Review of energy storage systems for electric vehicle applications and renewable energy integration,” Renewable and Sustainable Energy Reviews, vol. 69, pp. 771–789, 2017.

[13] A. Emadi, K. Rajashekara, S. Williamson and S. Lukic, “Topological overview of hybrid electric and fuel cell systems,” IEEE Transactions on Power Electronics, vol. 23, no. 6, pp. 2809–2829, 2008.

[14] J. Larminie and A. Dicks, Fuel Cell Systems Explained, 2nd ed., Wiley, Chichester, 2003.

[15] B. Sørensen, Hydrogen and Fuel Cells: Emerging Technologies and Applications, Academic Press, Oxford, 2012.

[17] NFPA, NFPA 855: Standard for the Installation of Stationary Energy Storage Systems, National Fire Protection Association, Quincy, MA, 2023.

[18] UL, UL 9540A: Test Method for Evaluating Thermal Runaway Fire Propagation in Battery Energy Storage Systems,Underwriters Laboratories, Northbrook, IL.

[19] R. Isermann, Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance, Springer, 2006.

[20] M. Blanke, M. Kinnaert, J. Lunze and M. Staroswiecki, Diagnosis and Fault-Tolerant Control, 3rd ed., Springer, 2016.

[21] MathWorks, Model-Based Design with MATLAB and Simulink, MathWorks Documentation, 2024.