LFP Lithium Battery Safety in Hazardous Areas

Paper No. PCIC energy EUR25_17

Kim Fumagalli, Antonio Pacetti
Excen S.r.l.
Via Marcora 61/69, 20097 San Donato Milanese (MI)
Italy

Santiago Alongi, Roberto Sebastiano Faranda
Politecnico di Milano- Dip. Energia
Via La Masa 34, 20156 Milano
Italy

Abstract – In recent years, lithium batteries have revolutionized energy storage and power supply across various fields, from consumer electronics to large-scale energy grids and electric vehicles. The demand for this technology is steadily growing, even in explosive atmospheres. Their high energy density, lightweight design, and long cycle life have positioned lithium batteries as a cornerstone in advancing modern technology and meeting growing energy demands. However, the increase in lithium battery applications brings forth critical safety concerns, primarily due to the risks of over-heating, gas emissions, and potential thermal runaway under specific conditions. Specifically for hazardous areas, these failures can become a source of ignition for explosive atmosphere. These risks underscore the necessity for in-depth analyses of failure rates, modes, and robust safety mechanisms within Battery Management Systems (BMS).
Recognizing the growing role of lithium batteries in diverse industries, the study addresses critical safety concerns, including thermal runaway, gas emissions, and the conditions leading to system instability.
The work further integrates Safety Integrity Level (SIL) considerations, assessing how SIL-rated components can ensure functional safety and compliance in explosive atmospheres. This research contributes valuable insights into the safe deployment of lithium batteries, providing a foundation for future advancements in battery safety standards and management technologies across high-risk applications such as explosive atmospheres, where there is still no well-defined standard. This paper is a continuation of the previous research work presented in 2019 at PCIC (Paris) [1].

Index Terms — Lithium Iron Phosphate (LFP) Battery, Battery Management System (BMS), Safety Integrity Level (SIL), Thermal Runaway, Hazardous Environments, ATEX, IECEx, Battery Safety, Functional Safety, Failure Rate Analysis, Energy Storage.

I. INTRODUCTION

Nowadays, Lithium-ion batteries have dramatically altered energy storage across a wide range of applications, from consumer electronics to industrial power systems. Their high energy density, lightweight construction, and long cycle life have made them mandatory in different sectors, including large-scale renewable energy storage, electric vehicles and critical infrastructure. As their deployment continues to expand, industries are increasingly integrating lithium-ion batteries into demanding environments, including industrial sites and hazardous areas (Ex environments), where safety and reliability are paramount.

In industrial environments, lithium-ion batteries are essential for ensuring continuous operation of critical systems such as Uninterruptible Power Supplies (UPS), automation networks, and backup power solutions. Their efficiency and long lifespan contribute to reducing maintenance costs and enhancing overall system performance. However, these advantages come with significant safety challenges, particularly in environments with high electrical loads, extreme temperatures, and potential exposure to corrosive or flammable substances.

The risks associated with lithium-ion batteries become even more pronounced in hazardous environments where the presence of explosive gases, vapours, or dust requires stringent safety considerations. Failure scenarios such as over-heating, gas emissions, and thermal runaway can transform a malfunctioning battery into an ignition source, posing severe threats to people and infrastructure. Therefore, the safe integration of lithium batteries in Ex environments requires a comprehensive understanding of failure mechanisms, failure rate analysis, and the implementation of robust safety measures, including Battery Management Systems (BMS) and compliance with Safety Integrity Level (SIL) standards.

This paper aims to address the critical safety concerns associated with lithium-ion batteries in both industrial and hazardous environments. By analysing key failure modes [1], risk mitigation strategies, and safety compliance frameworks, this study provides valuable insights into the safe and effective deployment of lithium-ion battery technologies. Special emphasis is placed on thermal runaway, gas emissions, and the role of SIL-rated components in ensuring functional safety. Ultimately, this research contributes to the development of enhanced battery safety standards, fostering reliability and security in high-risk applications where well-defined guidelines are still evolving.

II. BATTERIES: GENERAL OVERVIEW

A foundational overview of battery technologies was provided, examining the characteristics and applications of Lead-Acid, Nickel-Cadmium (NiCd), and Lithium-Ion batteries. It highlights the strengths and limitations of each type:

1) Lead-Acid Batteries: known for robustness and affordability, widely used in automotive and backup power applications despite limitations in weight and cycle life;
2) Nickel-Cadmium (NiCd) Batteries: appreciated for their durability and high discharge rates, though limited by lower energy density and environmental concerns;
3) Lithium-Ion Batteries: offering high energy density and long cycle life, these are critical in consumer electronics, electric vehicles, and renewable energy storage, though their safety concerns require sophisticated BMS.

These battery types are compared, in Fig 1, in terms of energy density, self-discharge, maintenance needs, and environmental impact.

Considering the big advantages of leading Lithium-Ion Batteries in subsequent paragraphs, the discussion is focused on them and into the analysis of Lithium Iron

Phosphate (LFP) batteries that seem to be very interesting for the Ex environmental.

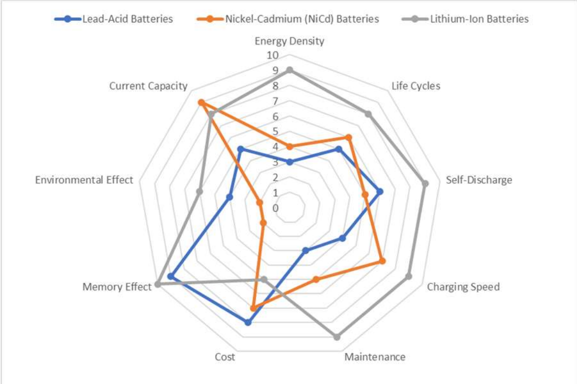

Fig 1: Radar Diagram of Battery Types

III. LITHIUM-ION BATTERY TECHNOLOGIES

Departing from the results reported in the paper [1], the different Lithium-Ion battery technologies were explored, delving into the unique characteristics, compositions, and applications of various chemistries within this category [9].

The main characteristics of each battery technology are summarized in Table I.

TABLE I
LITHIUM-ION BATTERY TECHNOLOGIES NUMERICAL COMPARISON

Characteristic	LiCoO2	LiMn2O4	NMC	NCA	LTO	LiFePO4
Energy Density (Wh/kg)	150-190	100-140	150-220	200-250	60-80	90-140
Life Cycles	500-1000	1000-1500	1000–2000	1000-1500	3000-20000+	2000-5000
Self-Discharge Rate (%/month)	2-5	2-5	2-5	2-5	<1	2-3
Safety (*)	5-6	6-7	7-8	6-7	9-10	9-10
Charging time (hours)	1-3	1-4	1-2	1-5	<1	1-10
Working Temperature (°C)	-20°C - +60°C	-20°C - +60°C	-20°C - +60°C	-20°C - +60°C	-30°C - +60°C	-25°C - +60°C
Nominal voltage [V]	3.8	4.1	3.7	3.6	2.4	3.2
Specific Capacity [mAh/g]	145	120	170	200	175	150
Onset temperature for irreversible thermal instability [°C]	140	200	180	150	>260	230
Cost [$/kWh]	200	100-150	120-200	350	500-1000	200-300

From this Table, it is possible to summarize the main key elements of each technology:

1) Lithium Cobalt Oxide ($LiCoO_2$): known for high energy density, commonly used in consumer electronics, though limited by safety concerns and a shorter lifespan;
2) Lithium Manganese Oxide ($LiMn_2O_4$): recognized for its thermal stability and safety, making it suitable for electric vehicles and energy storage, though it has a moderate energy density;
3) Nickel Manganese Cobalt (NMC): balances energy density, safety, and lifespan, widely used in electric vehicles and power tools;
4) Nickel Cobalt Aluminum (NCA): high energy density and long life make it suitable for high-performance electric vehicles, though it is relatively costly;
5) Lithium Titanate (LTO): known for extremely high cycle life and fast charging, though it has lower energy density, making it ideal for applications requiring rapid charging and longevity, like electric uses;
6) Lithium Iron Phosphate ($LiFePO_4$): valued for its excellent safety profile, long cycle life, and thermal stability, commonly used in high-risk applications and energy storage systems.

By examining attributes such as energy density, life cycles, charging speed, safety, cost, and thermal stability, it is possible to highlight the strengths and weaknesses of each type.

A practical comparison of measurable Lithium-Ion batteries characteristics is performed and highlighted by the radar diagram in Fig 2.

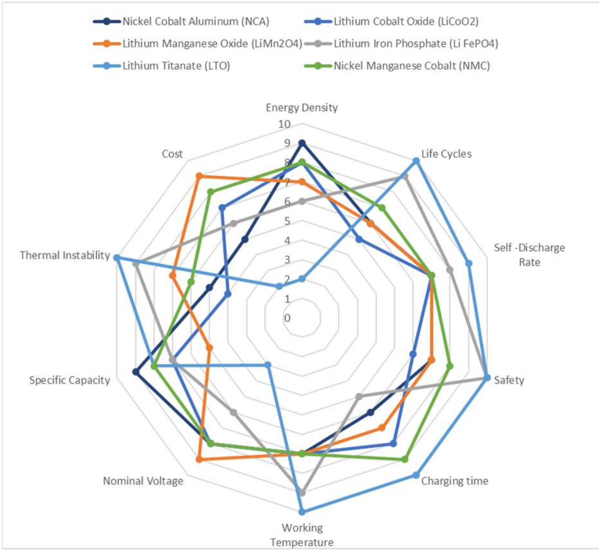

Fig 2: Characteristics of Lithium-Ion technologies Radar Diagram

This comparison facilitates the analysis of how these technologies perform, offering insights into their optimal uses and potential trade-offs. Moreover, this diagram assesses each technology across ten critical characteristics: Energy Density (Wh/kg), Life Cycles, Self-Discharge Rate (%/month), Safety, Charging Time (hours), Working Temperature (°C), Nominal Voltage (V), Specific Capacity (mAh/g), Onset Temperature for Irreversible Thermal Instability (°C), and Cost ($/kWh). Each characteristic is rated on a scale from 0 to 10, with 10 representing the best performance and 0 the worst. The radar diagram provides a visual representation of the strengths and weaknesses of each battery technology, offering a clear and intuitive comparison that highlights how each type excels or falls short in various performance and safety parameters [8]. This visual tool is essential for identifying the most suitable battery technology for specific applications, based on a balanced consideration of efficiency, longevity, safety, and cost.

The Safety characteristic attribute has an assigned qualitative value in a scale of 1 to 10, where 10 is the safest case and 0 is the worst possible case. These assigned values for every Lithium-Ion technology come from an in-depth safety analysis.

To provide a detailed understanding of the safety aspects associated with the various Lithium-Ion battery technologies, the focus was set on the advantages and disadvantages in terms of safety for the Lithium-Ion technologies studied in this research. The specific safety benefits and potential risks of each battery chemistry were highlighted, offering insights into their thermal stability, resistance to over-charging and short-circuiting, susceptibility to thermal runaway, and overall reliability under various operating conditions. By systematically comparing these safety-related characteristics, a clear framework is provided for understanding the inherent safety trade-offs of each technology, as shown in Table II, which is crucial for making informed decisions in applications where safety is a primary concern.

TABLE II
SAFETY IN LITHIUM-ION TECHNOLOGIES

Battery Technology	Advantages in Safety	Disadvantages in Safety
LiCoO2 (LCO)	Established technology with mature safety protocols Protective circuits are widely available. High energy density enables more compact battery designs.	Prone to thermal runaway at high temperatures. Requires stringent charging/discharging control to prevent over-heating. Cobalt is toxic and environmentally hazardous if not properly recycled.
LiMn2O4 (LMO)	More thermally stable compared to LCO. Less prone to thermal runaway. Lower internal resistance reduces heat generation.	Moderate energy density means larger battery sizes for the same capacity. Requires additional safety mechanisms for large-scale applications. It can experience capacity fading at high temperatures.
NMC	Balanced performance and safety. Less toxic than cobalt-only chemistry. Good thermal stability.	Moderate risk of thermal runaway. Requires careful management of charge/discharge cycles. Potential safety concerns in high power applications.
NCA	High energy density with reasonable safety measures. Higher power output is suitable for high-performance applications. Good cycle life with proper management.	More prone to thermal runaway compared to LFP and LMO. Requires advanced battery management systems to ensure safety. Nickel and cobalt pose environmental and health hazards if not properly managed.
LTO	Exceptional thermal stability with a very high tolerance to temperature variations (operating range -30°C to 55°C). Very low risk of thermal runaway and high safety margins. Very low self-discharge rate enhances safety during storage.	Lower energy density leads to larger battery sizes for the same capacity. Higher cost due to advanced materials and production processes. Lower nominal voltage requires more cells to achieve desired voltage levels.
LiFePO4 (LFP)	Extremely stable chemistry with a high tolerance to abuse (over-charging, short circuits). Less prone to thermal runaway and does not combust as easily. Wide operating temperature range (-25°C to 60°C).	Lower energy density compared to other lithium-ion chemistries. Higher initial cost compared to some other chemistries. Requires larger physical space for the same energy capacity compared to high-density chemistries.

This analysis aims to highlight the strengths and weaknesses of each type, and to highlight the advantages of $LiFePO_4$ (LFP) batteries for safe, reliable performance, setting the stage for the in-depth examination of their behavior in high-risk environments. Indeed, LFP batteries are preferred for applications requiring higher energy density, cost-efficiency, good cycle life and safety; they are ideal for electric vehicles, renewable energy storage, and cost-sensitive projects.

A. *Battery Safety*

It is important to focus on the safety challenges and failure causes in Lithium-Ion batteries, detailing the main factors that can lead to battery degradation or failure. As shown in [1] there are critical issues regarding lithium batteries, mainly the failure causes such as:

1) over-heating: a significant risk that can lead to thermal runaway, where the battery's internal temperature rapidly increases, causing potential fire or explosion;
2) over-charge and over-discharge: charging or discharging beyond recommended levels can damage internal components and reduce battery lifespan, increasing the risk of failure;
3) short circuits: internal or external short circuits can cause dangerous heat build-up, posing severe safety risks;
4) physical damage: external impacts or deformations can compromise battery integrity, leading to internal damage or short circuits;
5) aging and improper use: natural wear over time, as well as poor maintenance and handling, can lead to reduced capacity, instability, and heightened risk of failure.

The basis for understanding the conditions that contribute to Lithium-Ion battery failures was established and it underscored the need for robust protective mechanisms within BMS. These insights are essential to analyse specific failure modes and prevention strategies, particularly in LFP batteries.

B. *Thermal Runaway*

Thermal runaway is delved into, and it is a critical safety concern in Lithium-Ion batteries. Thermal runaway is described as a rapid, uncontrollable increase in temperature within the battery, potentially leading to fire or explosion [13]. The key factors contributing to thermal runaway, include:

1) fire triangle components: the presence of fuel, oxygen, and a heat source within the battery creates conditions for combustion, making control essential;
2) gas emissions: during thermal runaway, various flammable and harmful gases can be released, which can escalate risks if containment measures fail;
3) causes of gas generation: these include over-charging, mechanical damage, and internal short circuits, all of which increase pressure within the battery cell.

The three critical components of the fire triangle are an ignition source, fuel and oxygen, and they relate to the onset and progression of thermal runaway in lithium-ion batteries; given that this lithium-ion battery contains all three of the components of the triangle. Table III was developed to show the presence of each of these elements in the topic of lithium-ion batteries and thermal runaway.

TABLE III
FIRE TRIANGLE FOR LITHIUM-ION BATTERIES

Fuel	Oxygen	Heat
Combustible Materials: The organic electrolyte The polymeric separator Cathode and anode materials. **Flammable gases:** during thermal breakdown or decomposition, flammable gases such as hydrogen, methane, ethane and ethylene can be generated.	**Oxygen Source:** the cathode can release oxygen when over-heated or over-loaded. **Surrounding Atmosphere:** oxygen in the surrounding air can contribute to combustion if the battery ruptures and releases its contents	**Heat sources:** heat can be generated by various factors such as over-charging, over-discharging, internal short circuits, and thermal abuse. **Thermal failures:** A chain reaction of failures can increase the internal temperature of the battery, leading to the decomposition of the electrolyte and the generation of flammable gases, thus creating ideal conditions for a fire or an explosion.

The mitigation strategies were discussed, such as temperature monitoring, proper ventilation, and the use of safety valves. Identifying common gases emitted by different Lithium-Ion chemistries, it is possible to provide a foundation for understanding how specific safety mechanisms and design choices can help prevent or control thermal runaway in high-risk applications, particularly in Lithium Iron Phosphate (LFP) batteries.

Gas generation [12] in lithium-ion batteries can be the result of various chemical reactions that occur during abnormal operating conditions such as over-charging, over-discharging, over-heating, or thermal decomposition of internal materials. The most common gases that can be released and emitted from Lithium-Ion batteries were recapitulated in Table IV and Table V respectively [10, 11]].

TABLE IV
GASES RELEASED BY LITHIUM-ION BATTERIES

Gas	Source	Dangers
Oxygen (O_2)	Cathode decomposition especially in metal oxide-based materials	Serves as fuel for fires Accelerates the burning of flammable materials
Carbon dioxide (CO_2)	Reaction between the electrolyte carbonate and the cathode or anode materials	Not inflammable Increases the internal pressure of the cell
Carbon Monoxide (CO)	Partial oxidation of the organic electrolyte	Toxic Flammable Risk to health and safety
Hydrogen (H_2)	Electrolyte decomposition reaction or reaction of residual water with lithium	Highly Flammable Explosive when mixed with air
Methane (CH_4)	Decomposition of the organic electrolyte	Flammable Contributes to fire risks
Ethane (C_2H_6) and Ethyl (C_2H_4)	Decomposition of the organic electrolyte	Flammable They can contribute to fire risks
Hydrogen Fluoride (HF)	Decomposition of fluorine salts in the electrolyte	Extremely corrosive Extremely toxic It can cause serious irritation and damage to the respiratory tract and tissues Is not explosive under normal conditions

TABLE V
MAIN GASSES EMITTED BY EACH BATTERY TECHNOLOGY

Battery Technology	CO2	CO	H2	CH4	C2H4	C2H6	O2	HF
LiCoO2 (LCO)								
LiMn2O4 (LMO)								
LiFePO4 (LFP)								
NMC								
NCA								
LTO								

In Table V, green represents the gases commonly liberated by the different technology types after over-charging, over-heating, or physical damage, blue represents that these gases are also liberated but in a much lesser extent compared with the other technologies and yellow represents gases that are liberated only after a certain stress condition, that can vary according to the chemistry, SOC and the operating conditions of the battery.

C. *Battery Management Systems (BMS)*

It was provided an in-depth overview of Battery Management Systems (BMS), essential for ensuring the safety, reliability, and performance of Lithium-Ion batteries. The primary functions of a BMS include:

1) monitoring: constantly tracking critical battery parameters, such as voltage, current, and temperature, to prevent unsafe conditions;
2) balancing: ensuring uniform charge across all battery cells to avoid imbalances that can lead to over-charging or over-heating in individual cells;
3) protection: safeguarding against potential hazards like over-voltage, undervoltage, over-current, and over-heating;
4) communication: transmitting real-time data to other system components, allowing for proactive responses to any detected issues;
5) state estimation: calculating metrics such as the State of Charge (SoC) and State of Health (SoH), which are crucial for understanding the battery's remaining capacity and lifespan.

The BMS has the critical role in preventing failures and maximizing battery life, particularly in high-stakes applications where safety and functional integrity are paramount. It sets the stage for later steps that delve into specific protection methods and failure analysis, demonstrating how an effective BMS design can reduce risks in Lithium Iron Phosphate (LFP) battery systems.

D. *Protection Methods*

The protection methods implemented within Battery Management Systems (BMS) and other safety mechanisms are examined to prevent failures in Lithium-Ion batteries. Key protection methods covered include:

1) BMS protections: essential safeguards managed by the BMS, such as:
   - over-voltage and undervoltage protection: preventing cells from operating outside safe voltage ranges;
   - over-current and short circuit protection: limiting current to prevent dangerous over-heating or damage during high demand or fault conditions;
   - thermal protection: monitoring and controlling temperature to prevent thermal runaway;
   - balancing Protection: Ensuring even charge distribution among cells to maintain stability and prolong battery life;
   - reverse polarity and insulation monitoring: preventing accidental polarity reversal and ensuring system insulation integrity;
2) additional protections: other critical safety features not handled directly by the BMS, including:
   - thermal management systems: Using cooling methods and design features to control heat dissipation;
   - physical design and robust packaging: ensuring battery durability to resist external impacts;
   - maintenance and emergency preparedness: implementing protocols for safe operation and rapid response to potential failures.

The importance of comprehensive safety measures in managing the complex risks associated with Lithium-Ion batteries, especially in high-risk applications using Lithium Iron Phosphate (LFP) technology is highlighted. These protections are essential to the battery's overall reliability and form the backbone of effective failure prevention strategies.

IV. HAZARDOUS LOCATIONS

Considering what has been discussed in the previous paragraph, the situation is even more critical when there is a need to use lithium batteries in a hazardous area.

A hazardous area is an environment where there is a potential for fire or explosion due to the presence of flammable gases [7], vapors, dust, or fibers mixed with air. These areas require special safety considerations and equipment to prevent ignition and protect both people and property. The classification of hazardous areas is based on the frequency and duration of the presence of explosive atmospheres, as well as the type of materials involved.

A. Categories of Hazardous Area

In hazardous areas different from mines, categories are used to define the level of protection required for equipment operating in environments where there is a risk of explosion due to the presence of flammable gases, vapors, dust, or fibers. These categories are established primarily under the ATEX Directive (for Europe) and correspond to different risk levels in potentially explosive atmospheres.

The ATEX Directive 2014/34/EU defines three categories of equipment, which determines where the equipment can be used based on the risk of an explosive atmosphere occurring.

1) Category 1 (Very High Protection): It is intended for use in Zone 0 (gases) or Zone 20 (dusts) environments, where an explosive atmosphere is present continuously or for long periods. The equipment must ensure a very high level of protection, remaining safe even in the event of two independent faults; it must be designed to handle continuous exposure to explosive atmospheres; and it must be fault-tolerant, meaning if one protection method fails, another will still prevent ignition;
2) Category 2 (High Protection): Intended for use in Zone 1 (gases) or Zone 21 (dusts) environments, where an explosive atmosphere is likely to occur occasionally during normal operation. Equipment must provide a high level of protection and must remain safe even in the event of expected faults; it also must prevent ignition in normal operation and remain safe in the event of a fault that is reasonably expected to occur during its operational life;
3) Category 3 (Normal Protection): Intended for use in Zone 2 (gases) or Zone 22 (dusts) environments, where an explosive atmosphere is unlikely to occur during normal operation, or if it does, will occur only infrequently and for short periods. The equipment must ensure a normal level of protection, functioning safely in normal operating conditions but not required to handle faults. This category of equipment is designed for environments where the likelihood of an explosive atmosphere is minimal and typically short-lived.

B. Equipment Protection Levels (EPLs)

Equipment Protection Levels (EPLs) are used to classify equipment intended for use in hazardous areas based on the risk of ignition and the required level of protection against explosive atmospheres. EPLs are defined in the standards and provide a risk-based method to ensure equipment is suitable for use in specific zones were explosive gases, vapors, or dust may be present.

There are three EPL levels, each one corresponding to the equipment's protection level and its suitability for different hazardous zones, as here described:

1) EPL "Ga" (Very High Protection): the equipment is suitable for Zone 0 (gases) or Zone 20 (dusts). it assures very high protection given its risk level and it must not become a source of ignition under normal operation, during expected faults, or even under rare fault conditions. So, it is used in areas where explosive atmospheres are continuously present or present for long periods.
2) EPL "Gb" (High Protection): suitable for Zone 1 (gases) or Zone 21 (dusts). Equipment with high protection that must not become a source of ignition in normal operation and must remain safe under expected faults. Used in areas where explosive atmospheres are likely to occur occasionally during normal operation.
3) EPL "Gc" (Enhanced Protection): suitable for Zone 2 (gases) or Zone 22 (dusts). Equipment with enhanced protection that must not become a source of ignition under normal operating conditions but is not required to handle severe faults. Used in areas where explosive atmospheres are unlikely to occur during normal operation, or only for short periods.

V. SAFETY INTEGRITY LEVEL

Safety Integrity Level (SIL) is a critical standard used to quantify the safety performance of systems, particularly those operating in high-risk environments [2].

A. SIL in Hazardous Areas

As presented in [2], in hazardous areas, Safety Integrity Level (SIL) is a key concept used to assess and ensure the safety of systems that prevent or mitigate risks associated with explosive atmospheres, as shown in Table VI [5].

TABLE VI
MINIMUM REQUIREMENTS FOR SAFETY INTEGRITY LEVEL (SIL) AND FAULT TOLERANCE OF A SAFETY DEVICE

EUC Hardware Fault Tolerance	2	1	0	1	0	0
Safety device						
Hardware Fault Tolerance	-	0	1	-	0	-
Safety Integrity Level	-	SIL 1	SIL 2	-	SIL 1	-
Combined Equipment						
Group I Category	M1 1			M2 2		-
Group II, III Category						3

NOTE 1 Fault tolerance:
"0" indicates that the EUC is safe in normal operation. One single fault may cause the apparatus to fail.
"1" indicates that the apparatus is safe with one single fault. Two independent faults may cause the apparatus to fail.
"2" indicates that the apparatus is safe with two independent faults. Three faults may cause the apparatus to fail.
NOTE 2 SIL1 or SIL2 indicates the Safety Integrity Level of the Safety device according to EN 61508 series.
NOTE 3 Category 1 or 2 or 3: the appropriate categories are defined in EN 13237.
NOTE 4 "-" means, that no safety device is required
NOTE 5 Equipment which contains a potential ignition source under normal operation is not included in Table 1, because this equipment is already covered under the types of protection.

SIL is defined in functional safety standards like IEC 61508 [3] and IEC 61511 [4], which outline the framework for the reliability and performance of safety systems designed to reduce the risk of catastrophic events, such as fires or explosions, to an acceptable level.

However, it is important to note that IEC 61508 and IEC 61511 are not directly harmonized with the ATEX Directive 2014/34/EU, which regulates equipment and protective systems intended for use in potentially explosive atmospheres within the European Union. Despite this, these standards are referred to in EN 50495 [5], that is harmonized with the ATEX Directive, giving it the presumption of being the state of the art in explosion-risk safety.

EN 50495 allows the Equipment Protection Level (EPL) of equipment used in hazardous areas to be adjusted based on the integration of safety systems with an appropriate SIL level. This adjustment enables the use of SIL-rated systems to enhance the overall safety of equipment when used in dangerous atmospheres where explosive gases, vapors, or dust could be present.

The SIL system is divided into four levels (SIL 1 to SIL 4), each representing a different degree of safety, with SIL 4 being the highest and most stringent. These levels are determined based on the Probability of Failure on Demand (PFD), which refers to the likelihood that the system will fail when needed, and the required risk reduction for a given safety function. Table VII illustrates the SIL levels and their corresponding risk reduction values.

TABLE VII
SIL LEVELS AND THEIR RISK REDUCTION

SIL Level	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD)
SIL 1	10 to 100	10^{-1} to 10^{-2}
SIL 2	100 to 1000	10^{-2} to 10^{-3}
SIL 3	1000 to 10000	10^{-3} to 10^{-4}
SIL 4	10000 to 1000000	10^{-4} to 10^{-5}

In particular the meaning of each SIL level is:

1) SIL 1: offers a basic level of risk reduction, where failure might occur but is less likely to result in a catastrophic event;
2) SIL 2: provides moderate risk reduction for systems where higher reliability is needed;
3) SIL 3: used in high-risk systems where failure could result in serious consequences, such as industrial explosions;
4) SIL 4: the highest level of safety, suitable for critical applications where any failure could lead to catastrophic events (e.g., oil refineries, chemical plants).

B. *The SIL Approach as a Method to define the EPL*

The Safety Integrity Level (SIL) approach can be used as a method to help define the Equipment Protection Level (EPL) in hazardous areas by linking the reliability and performance of safety systems with the level of protection required to prevent ignition in explosive atmospheres.

This method involves assessing the likelihood of system failure and determining whether the equipment can reliably prevent dangerous events like ignition, even under faulty conditions. The table VIII shows the correlation between the EPL and SIL.

TABLE VIII
EPL AND SIL CORRELATION

Zone	EPL	SIL	Risk Reduction Required	Description
Zone 0/20	Ga/Da	SIL 3-4	Continuous exposure to explosive atmospheres	Equipment must be able to tolerate rare faults (highest level of protection).
Zone 1/21	Gb/Db	SIL 2-3	Occasional presence of explosive atmospheres	Equipment must handle normal operation and expected faults.
Zone 2/22	Gc/Dc	SIL 1-2	Infrequent or short-lived explosive atmospheres	Equipment must be safe under normal operation only (lower fault tolerance).

C. *Methods for determining SIL*

SIL determination follows a structured approach, typically based on the hazard and risk assessment of the process or system.

The methods involved in determining the required SIL level include:

1) hazard and risk analysis: the process starts with an analysis of the potential hazards and the consequences of system failure. Several methods can be used to assess the risk, like Hazard and Operability Study (HAZOP), Failure Modes and Effects Analysis (FMEA) [3] and Layer of Protection Analysis (LOPA);
   The objective of risk analysis is to estimate the likelihood of a hazardous event and its severity, which will then help define the SIL required for safety.
2) safety lifecycle (IEC 61508): it is a systematic framework described in IEC 61508 that covers all phases of designing, implementing, and maintaining safety systems. It consists of several key steps:
   - hazard identification and risk assessment;
   - SIL determination;
   - safety function design;
   - implementation and validation;
   - operation and maintenance;
   - periodic review and audits;
3) failure probability and reliability analysis: SIL is closely tied to the Probability of Failure on Demand (PFD), which measures the likelihood that the system will fail when required. The lower the PFD, the higher the SIL level;
4) FMECA and FMEDA: Failure Modes, Effects, and Criticality Analysis (FMECA) [6]: FMECA is used to identify failure modes, evaluate their effects on system operation, and prioritize them based on their criticality. This helps to identify which failure modes must be addressed to achieve the desired SIL level.
   Failure Modes, Effects, and Diagnostic Analysis (FMEDA): FMEDA is an advanced analysis that considers the system's diagnostic capabilities to detect and respond to failures. This analysis ensures that all failure modes are adequately managed to meet the required SIL;
5) architectural constraints: SIL levels are also determined by the architecture of the safety system. IEC 61508 defines specific architectural

requirements for each SIL level, which include:

- Safe Failure Fraction (SFF): the ratio of safe failures to total failures. A higher SFF is required for higher SIL levels.
- hardware redundancy: higher SIL levels (such as SIL 3 or SIL 4) require more redundant components and subsystems to ensure that the system can continue operating even if parts of it fail.

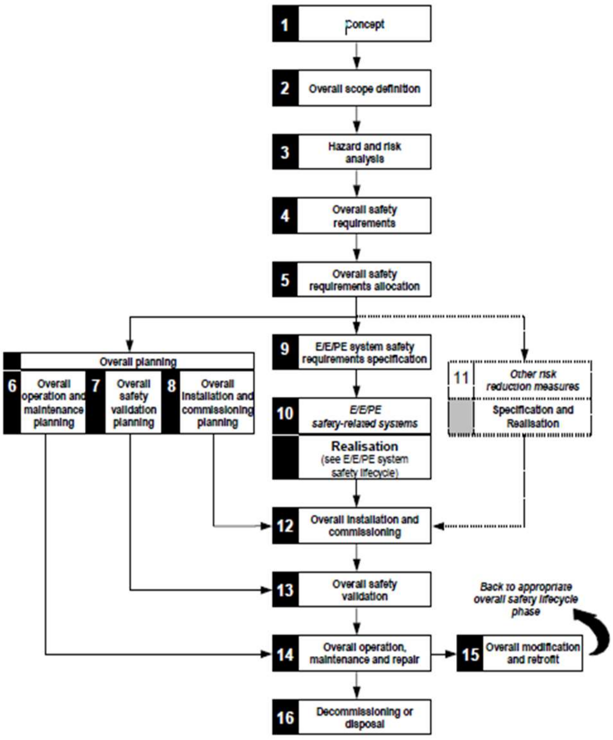

Figure 3: Safety Lifecycle according to IEC/EN61508-1

D. Determination of the SIL Target

Determining the SIL target is a critical process in functional safety that involves selecting the appropriate Safety Integrity Level (SIL) for a safety-related system based on the risk reduction needed to mitigate hazardous events. The SIL target ensures that the system provides an adequate level of protection against failure, preventing dangerous outcomes like explosions, fires, or equipment malfunctions.

The goal is to assign a SIL level that reflects the necessary risk reduction factor (RRF) for each safety function. The RRF is the factor by which the risk must be reduced to reach the tolerable risk level, it is computed through the next formula:

$$RRF = \frac{Initial\ Risk}{Tolerable\ Risk}$$

The higher the RRF, the greater the risk reduction required, which corresponds to a higher SIL level

E. SIL Relevant Figures

SIL relevant figures and the selection of failure modes through functional analysis are critical steps in ensuring that a safety-related system meets the required Safety Integrity Level (SIL) [2]. These processes help quantify system reliability and assess how well it can handle failures, ensuring that the system achieves the risk reduction required for safe operation. The key figures used in SIL determination are:

1) Probability of Failure on Demand (PFD): Represents the likelihood that a system will fail to perform its safety function when required. PFD is the most important figure in assessing the SIL level. Lower PFD values correspond to higher SIL levels. It is calculated based on system architecture, reliability, and fault tolerance.
2) Risk Reduction Factor (RRF): Inverse of the PFD, RRF quantifies how much the safety function reduces the overall risk of a hazardous event.
3) Safe Failure Fraction (SFF): The percentage of failures that lead to a safe state rather than a dangerous failure. SFF helps in determining how much fault tolerance a system has. Systems with higher SFF are generally safer and can achieve higher SIL levels. It is calculated as:

$$SFF = \frac{Safe\ Failures}{Total\ Failures} * 100$$

   A higher SFF means fewer dangerous failures and a better chance of meeting higher SIL levels.
4) Hardware Fault Tolerance (HFT): The system's ability to continue functioning safely despite hardware failures. For high SIL levels, systems need redundant architecture that allow them to handle multiple hardware faults without causing dangerous conditions.
   - HFT 0: No redundancy (1 out of 1)
   - HFT 1: One redundant channel (1 out of 2)
5) Diagnostic Coverage (DC): it refers to the proportion of dangerous failures that the system can detect and mitigate. It directly affects the ability to meet higher SIL levels. High DC means the system can detect most dangerous failures and take corrective actions to prevent hazardous events.
6) Average Probability of Failure on Demand (PFDavg): it is used to calculate the system's overall reliability during its operational period. It reflects how often the safety function will fail to respond correctly when a hazardous condition arises.
7) Device Type: In functional safety standards, particularly in the IEC 61508 framework, devices are categorized into two main types based on their complexity: Type A and Type B. This classification is crucial for assessing and managing the reliability of devices, especially in safety-related applications.
   - Type A Devices (Low Complexity): Type A devices are considered low-complexity components, generally with well-known failure modes and behavior. Their key characteristics include simple design and known failure modes.
   - Type B Devices (High Complexity): Type B devices are higher-complexity components that may contain microprocessors, programmable logic, or software. Their key characteristics include complex design and diverse failure modes.

VI. ANALYSIS RESULTS

It should be noted that the analysis performed, and the results obtained are specifically related to a particular LFP battery. In fact, BMS, cells, connection and the construction/assembly of the battery itself play a key role in the SIL analysis. Moreover, it is important to underline that the LFP battery under evaluation is a traction battery type with the following electrical parameters: 24V – 110 Ah.

Failure Modes, Effects, and Criticality Analysis (FMECA) and Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [14, 15] are methodologies used to systematically evaluate potential failure modes in a system, analyze their effects, and assess the system's reliability in terms of safety. These analyses are critical in industries where safety is a priority, such as chemical plants, oil and gas refineries, and hazardous environments, as they help ensure compliance with Safety Integrity Levels (SIL).

For this analysis, it is assumed that the BMS software meets Safety Integrity Level 1 (SIL1) requirements. This assumption suggests that the BMS software incorporates design measures and fault detection capabilities that align with SIL1 criteria.

An FMEA analysis of a Lithium-Ion battery was used as a base and adapted to fulfill the requirements of the FMECA, so, every hazard and failure mode analyzed was evaluated through their criticality and their possible detection by the control system. After evaluating the consequences of each failure mode on the overall system, the failure modes were classified as Safe (S) or Dangerous (D) and Detected (D) or Undetected (U).

FMEDA is an advanced version of FMECA that considers diagnostic coverage; it is used to support SIL certification and is crucial for determining the Probability of Failure on Demand (PFD) and Safe Failure Fraction (SFF), that is detailed data required for calculating SIL.

To obtain the data required for calculating SIL, the failure rates for every hazard were to be assigned. So, using the probability of failure of each hazard it was assigned a failure rate.

The next step was to categorize each failure rate and obtain the cumulative failure numbers described in the table below:

TABLE IX
CUMULATIVE FAILURE NUMBERS

λ_D	Dangerous Failure Rate	λ_{DD}	Dangerous Detected Failure Rate
		λ_{DU}	Dangerous Undetected Failure Rate
λ_S	Safe Failure Rate	λ_{SD}	Safe Detected Failure Rate
		λ_{SU}	Safe Undetected Failure Rate

After obtaining the above cumulative failure numbers it is possible to evaluate the Diagnostic Coverage (DC) that is the percentage of dangerous failures that the system can detect and respond to, and it is calculated as:

$$DC = \frac{\lambda_{DD}}{\lambda_{DU} + \lambda_{DD}} * 100$$

Higher DC increases system reliability and helps achieve higher SIL levels.

Then, the Safe Failure Fraction (SFF) is computed, which represents the fraction of total failures that are either safe or detected with the next formula:

$$SFF = 1 - \left(\frac{\lambda_{DU}}{\lambda_{TOT}}\right) = 1 - \left(\frac{\lambda_{DU}}{\lambda_{DD} + \lambda_{DU} + \lambda_{SU} + \lambda_{SD}}\right) = \frac{\lambda_{DD} + \lambda_{SU} + \lambda_{SD}}{\lambda_{DD} + \lambda_{DU} + \lambda_{SU} + \lambda_{SD}}$$

The SFF number is independent of the absolute value of the failure rate but sensitive to the number of safe failures against the total amount of failures only. The reason is that there is the necessity to verify that the architecture suffers mainly safe failures or detects a possible menace instead of unsafe failures that cannot be detected.

A lithium battery is typically classified as a Type B device under the IEC 61508 standard. Given that it is a device that has complex components, and whose failure modes and behaviours are not fully predictable. These elements often include components like microprocessors, programmable electronics, sensors, and complex electrochemical systems such as lithium batteries. Since their failure mechanisms are harder to analyse and predict, Type B elements require more stringent design, testing, and fault tolerance measures compared to Type A elements.

A Lithium battery, as the studied one, is of type B since it matches the next characteristics:

1) It is complex in design, often involving programmable or microelectronic components;
2) The failure modes of are not always fully understood or easily identifiable;
3) The elements of the battery under failure conditions can be less predictable, leading to more uncertainty in their failure modes.

The IEC/EN61508-2 lists the SFF architecture requirements for element TYPE B, as the Lithium Battery studied; these requirements are shown in the table below:

TABLE X
ARCHITECTURE REQUIREMENT FOR ELEMENT TYPE B (LITHIUM BATTERY)

Safe Failure Fraction of an Element	**Hardware Fault Tolerance**		
	0	**1**	**2**
<60%	N/A	SIL1	SIL2
60% to <90%	SIL1	SIL2	SIL3
90% to <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

Using the failure rates of each hazard and considering failure modes, every Cumulative Failure Number was computed.

Once these values were obtained it was possible to compute the Diagnostic Coverage (DC) and the Safe Failure Fraction (SFF) with the formulas shown above.

The Lithium Battery studied is a Type B element and the diagnostic coverage and the Safe Failure Fraction (SFF) obtained with the calculation were between 60% and 90%. The achievable Safety Integrity Level (SIL) will depend on the element's Hardware Fault Tolerance (HFT), based on the architecture constraints demonstrated above by IEC 61508. The achievable SIL for this Type B element is constrained by its Hardware Fault Tolerance (HFT) as follows:

1) For HFT 0 (no redundancy): SIL 1 can be achieved, as the SFF between 60% and 90% is within the allowable range for SIL 1. SIL 2 cannot be achieved with HFT 0, as a higher SFF (> 90%) would be required.
2) For HFT 1 (with redundancy): SIL 2 can be achieved, as the combination of a SFF between 60% and 90% and HFT 1 meets the requirements for SIL 2. Even though, for this to be achieved, every battery component must have a redundant pair, meaning a higher safety but a much higher cost.

VII. CONCLUSIONS

Not all lithium batteries are the same. From “safety” point of view, as seen in the previous paragraphs due to extremely stable chemistry with a high tolerance to abuse (over-charging, short circuits, …) and less prone to thermal runaway and does not combust as easily, it is believed that LFP batteries are the least problematic from this point of view. This fact is a very important aspect, especially for the use of such batteries in an explosion hazard environment.

The research highlights the essential role of an effective BMS in monitoring, balancing, and protecting LFP batteries, with features like redundancy and diagnostic coverage emerging as critical for mitigating risks.

As stated in EN50495, SIL 1 is mandatory for the safety device (BMS) to be able to utilize the battery (cells, modules, etc...) in Category 2 when their Fault Tolerance is 0. From the FMEA/FMEDA analysis performed on this LFP traction battery system and because of their characteristics (failure modes and failure rate), SIL 1 is also considered necessary for Category 3, although the failure case should not be considered in Category 3.

Incorporating Safety Integrity Level (SIL) requirements ensures that LFP battery systems meet necessary safety standards, particularly in hazardous environments where functional safety is paramount. Obviously, it is not enough; in fact, SIL is only the part of the analysis done. In order to install such batteries in hazardous area, it is necessary to define what may be the suitable Ex type of protection for these electrical devices.

This investigation suggests avenues for future research, such as improving diagnostic capabilities within BMS and developing advanced materials for even greater safety. It also encourages the ongoing refinement of battery safety standards as LFP technology continues to advance.

These results will be discussed during the international committees for the use of lithium batteries in hazardous environments (IEC WG37) of which we are active members.

VIII. REFERENCES

[1] R. S. Faranda, K. Fumagalli, M. Bielli, "Lithium-Ion Batteries for explosive atmosphere", PCIC Europe EUR 19_32, 2019.

[2] K. Fumagalli, M. Martina and P. Corbo, "Light Emitting Diodes (LED) for installation in Zone 1: A feasible procedure to determine the equilvalent protection level", PCIC London LO-141, 2015.

[3] IEC 61508-1, "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements".

[4] IEC 61511-1, "Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements".

[5] EN 50495:2010 Safety devices required for the safe functioning of equipment with respect to explosion risks.

[6] L. Cristaldi, "Lesson of FMEA," Politecnico di Milano, Milano, 2023.

[7] IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements

[8] F. &. S. M. Mohammadi, "A comprehensive overview of electric vehicle batteries market," Department of Electrical and Computer Engineering (ECE), University of Windsor, Windsor, 2023.

[9] G. Bhutada, "The Six Major Types of Lithium-ion Batteries: A Visual Comparison," Elements. Available: https://elements.visualcapitalist.com/the-six-major-types-of-lithium-ion-batteries/.

[10] V. Svoboda, "BATTERIES | Fast Charging,," in Encyclopedia of Electrochemical Power Sources, Elsevier, 2009, pp. 424-442

[11] "Gas-related risks: flammability, toxicity and asphyxiation," BE ATEX. Available: https://www.be-atex.com/en/gas-related-risks-flammability-toxicity-and-asphyxiation.

[12] N. G.-A. Ben Rowden, "A review of gas evolution in lithium-ion batteries," Energy Reports, pp. 10-18, 2020.

[13] M. A.-C. Seham Shahid, "A review of thermal runaway prevention and mitigation strategies for lithium-ion batteries," Energy Conversion and Management, vol. XVI, 2022.

[14] Z. W. X. Z. Lizhi Wang. Yusheng Sun. Xiaohong Wang, "Reliability Modeling Method for Lithium-ion Battery Packs Considering the Dependency of Cell Degradations Based on a Regression Model and Copulas," Materials, 2019.

[15] L. L. B. D. Y. K. C. Z. Hanxiao Liu, "Multi-fault detection and diagnosis method for battery packs based on statistical analysis," Energy, vol. 293, 2024.

IX. VITA

Kim Fumagalli graduated in Electrical Engineering from the University of Politecnico di Milano in 2005. He obtained the Ph.D. degree in Electrical Engineering at Politecnico di Milano, Milan, Italy, in 2009. His research areas include LED Source and LED Lighting System, Electrical and Lighting systems for Ex environment, Batteries and Cells, PV panels, Industrial Trucks and Internal Combustion Engines for Explosive Atmosphere, Ex Products Certification and Testing. He is an ATEX/IECEx Consultant and a collaborator of the Department of Energy, Politecnico di Milano. He is a member of several IEC Work Group and Italian Standards Committee (CEI). He has received IECEx Certificate Personnel Competence. He is a member of the PCIC Europe committee and holds the position as Assistant Technical Secretary. He has authored several papers.
kim.fumagalli@kfex.it

Antonio Pacetti is the Chairman of EXCEN Srl and involved in design, certification and production of equipment for explosive atmosphere from 40 years as chairman and owner of various enterprises. Member of CEN/TC 150/WG 13: Industrial Trucks for Explosive Atmosphere and of IEC SC 31M PT 80079-41: Internal Combustion Engines for Explosive Atmosphere. Member of UNI (Italy) SC 1 Internal Transports. He participates as member to the working committee for the publication of EN 1834-1/-2/-3:2000.

Santiago Alongi graduated in Electrical Engineering from the University of Politecnico di Milano in 2024. His reasearch areas include Lithium Batteries, Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), Safety Integrity Level (SIL), Hazardous Environments, Failure Rate Analysis and Energy Storage. He works as Service Sales Support for Hitachi Energy.
Alongi.santiago@gmail.com

Roberto Sebastiano Faranda received the Ph.D. degree in electrical engineering from the Politecnico di Milano, Milano, Italy, in 1998. He is currently Full Professor with the Department of Energy, Politecnico di Milano. His research areas include power electronics, power system harmonics, power quality, power system analysis, smart grids, Ex environment and distributed generation. Dr. Faranda is a member of the Italian Standard Authority; the Italian Electrical, Electronic, Automation, Information, and Telecommunications Federation; and the Italian National Research Council group of Electrical Power Systems. He has authored more than 150 papers.
roberto.faranda@polimi.it