Agenzia nazionale per le nuove tecnologie,
l'energia e lo sviluppo economico sostenibile

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Analisi di rischio di sistemi di accumulo di interesse automotive con tecniche HAZOP e LOPA: studio preliminare sulla gestione delle deviazioni dal normale funzionamento da parte del BMS

M. Schiavetti, T. Pini, M. Carcassi

UNIVERSITÀ DI PISA

Report RdS/PAR2017/248

ANALISI DI RISCHIO DI SISTEMI DI ACCUMULO DI INTERESSE AUTOMOTIVE CON TECNICHE HAZOP E LOPA: STUDIO PRELIMINARE SULLA GESTIONE DELLE DEVIAZIONI DAL NORMALE FUNZIONAMENTO DA PARTE DEL BSM

M. Schiavetti, T. Pini, M. Carcassi (Università di Pisa – DICI)

Settembre 2018

Report Ricerca di Sistema Elettrico

Accordo di Programma 2015-2017 MiSE – ENEA stipulato in data 21 Dicembre 2016 per le attività di ricerca e sviluppo di interesse generale per il Sistema Elettrico Nazionale
Piano Annuale di Realizzazione 2017
Progetto: D7 – Mobilità elettrica sostenibile
Obiettivo: Sicurezza accumulo al litio
Responsabile del Progetto: Maria Pia Valentini

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione "Analisi di rischio di sistemi di accumulo di interesse automotive con tecniche HAZOP e LOPA: studio preliminare sulla gestione delle deviazioni dal normale funzionamento da parte del BSM"
Responsabile scientifico ENEA: Cinzia Di Bari
Responsabile scientifico: Marco Carcassi

Indice

Sommario

Il presente documento esplicita in dettaglio l'intervento del Battery Management System (BMS) in risposta alle deviazioni dal normale funzionamento identificate durante l'analisi di sicurezza applicato a livello della cella. I risultati di tale studio sono contenuti nel Report Studio sulla caratterizzazione dei vari livelli di protezione di sistemi di accumulo litio-ione per uso automotive, mediante "Layer Of Protection Analysis (LOPA)" [8].
Il presente studio contiene inoltre un'appendice che riassume la metodologia ed i risultati di un analisi di pericoli effettuata attraverso applicazione di un'analisi HAZOP al sistema elettronico di gestione e controllo della batteria, il Battery Management System (BMS). Lo scopo dell'analisi HAZOP è quello di individuare le fenomenologie di base che possono produrre sequenze incidentali potenzialmente pericolose (incendio, esplosione e rilascio tossico).

1 Introduzione

Il Ministero dello Sviluppo Economico ed ENEA hanno stipulato in data 21 dicembre 2016 un Accordo di Programma 2015-2017 in base al quale è concesso il contributo finanziario per l'esecuzione delle linee di attività del Piano Triennale 2015-2017 della Ricerca e Sviluppo di Interesse Generale per il Sistema Elettrico Nazionale.

ENEA ha stipulato un accordo di collaborazione con l'Università di Pisa per quanto attiene al Progetto D.7 "MOBILITÀ ELETTRICA SOSTENIBILE".

Pertanto, sulla base delle attività previste dal Progetto D.7, i temi da sviluppare nell'ambito del presente accordo di collaborazione tra ENEA e " Università di Pisa", riguardano l'applicazione delle tecniche di analisi di rischio (HAZOP) per la tecnologia Litio-ione nelle applicazioni auto motive. Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione "Analisi di rischio di sistemi di accumulo di interesse automotive con tecniche HAZOP e LOPA: studio preliminare sulla gestione delle deviazioni dal normale funzionamento da parte del BSM".

Prendendo a riferimento i risultati dell'analisi HAZOP applicata ad una cella Litio-ione commerciale [8], sono state isolate le deviazioni dal normale funzionamento dei parametri significativi del processo nelle varie fasi di utilizzo (carica, stoccaggio e scarica), i cui effetti possono essere prevenuti o mitigati dall'intervento del BMS. Partendo dalle sequenze incidentali descritte e prendendo a riferimento un BMS presente sul mercato è stata verificata l'effettiva capacità di intervento del BMS nelle varie situazioni previste.

Inoltre, sempre prendendo a riferimento uno specifico BMS, sono state ricercate, tramite analisi HAZOP, le deviazioni dal normale funzionamento e le fenomenologie di base che hanno la potenzialità di produrre sequenze incidentali potenzialmente pericolose (incendio, esplosione e rilascio tossico).

2 Descrizione generale dei BMS

Il termine Battery Management System (BMS) non ha una definizione universale o formale, né esiste un unico elenco dei compiti che dovrebbe svolgere [1,2]. La ragione principale risiede nella forte dipendenza delle sue caratteristiche dal campo di applicazione. Non esiste infatti una soluzione ideale per tutte le esigenze di gestione della batteria, infatti le soluzioni derivano dalle diverse scelte in termini di chimica o geometria delle celle [3].

In generale il BMS è un sistema responsabile della supervisione, controllo e protezione delle celle di una batteria, sia a livello individuale che nella loro configurazione all'interno di un pacco batteria.

Il compito più importante del BMS è quello di adempiere alle funzioni di sicurezza in modo tale che le celle di un sistema di batterie non vengano utilizzate oltre i limiti specificati in termini di tensione, temperatura e corrente. Questo insieme di limiti di specifiche per le celle viene spesso definito come Area Operativa Sicura (SOA). Il BMS deve quindi monitorare continuamente le condizioni delle celle e mettere in atto le procedure di correzione quando rileva un comportamento anomalo. Il BMS è un dispositivo elettronico analogico e/o digitale che soddisfa i seguenti requisiti essenziali:

- Acquisizione dei dati.
- Elaborazione ed archiviazione dati.
- Gestione elettrica.
- Gestione della temperatura.
- Gestione della sicurezza.
- Comunicazione.

Per un BMS utilizzato per gestire la batteria di veicoli elettrici gli obiettivi ed i requisiti essenziali sono i seguenti:

- Aumentare la sicurezza e l'affidabilità dei sistemi di batterie.
- Proteggere le singole celle e i sistemi di batterie da eventuali danni.
- Migliorare l'efficienza di utilizzo dell'energia della batteria (per aumentare l'autonomia del veicolo).
- Prolungare la durata della batteria

Le singole funzioni di un BMS possono quindi essere derivate da questi requisiti. Queste funzioni possono essere suddivise in cinque aree:

1. Misura e controllo dei parametri di batteria: il BMS deve misurare le tensioni delle celle, le temperature dei moduli e la corrente del pacco batteria. Deve inoltre rilevare guasti di isolamento e controllare i contattori e il sistema di gestione termica.
2. Protezione: il BMS deve includere l'elettronica e la logica per proteggere l'operatore del sistema alimentato a batteria ed il pacco batteria stesso da sovraccarica, sovra scarica, sovracorrente, cortocircuiti della cella e temperature estreme.
3. Interfacciamento: il BMS deve comunicare regolarmente con l'applicazione che il pacco batteria alimenta, riportando energia e potenza disponibili e altri indicatori dello stato del pacco batteria. Inoltre, deve registrare errori insoliti o eventi di abuso nella memoria permanente, questo per la diagnostica dei tecnici tramite download occasionale su richiesta.
4. Gestione delle prestazioni: il BMS deve essere in grado di stimare lo stato di carica (SOC) per tutte le celle del pacco batteria, calcolare i limiti di energia e potenza disponibili e di bilanciare (equalizzare) le batterie nel pacco batteria.
5. Diagnostica: infine, il BMS deve essere in grado di stimare lo stato di salute (SOH), compreso il rilevamento dell'abuso, e può essere richiesto di stimare la vita utile residua delle celle e del pacco batterie.

L'elenco sopraindicato comprende funzioni rilevanti per la sicurezza, come ad esempio il rilevamento delle tensioni delle celle, ma anche funzioni di stato, come ad esempio la stima dello stato di carica (SOC). Indipendentemente dai suddetti requisiti e funzioni, il sistema deve essere testato per la sicurezza elettrica secondo la ISO 26262 [9].

2.1 Topologie e sotto-componenti di un BMS

Sulla base dei principi discussi sopra, le diverse possibilità di connettere più celle individuali portano a diverse possibili configurazioni e progetti architettonici di un BMS. Inoltre, le diverse attività soddisfatte da un BMS possono essere distribuite tra diversi sotto-componenti, costituiti in genere da schede a circuito stampato (PCB). I sotto componenti di un BMS si possono racchiudere in 3 livelli:

1. Unità di monitoraggio delle celle (CMU): è livello più basso, un'unità collegata a ciascuna cella. La CMU misura la tensione della cella, la temperatura e i parametri aggiuntivi a livello di cella e gestisce il bilanciamento a livello di cella.
2. Unità di gestione modulo (MMU): livello intermedio, gestisce e controlla un gruppo di CMU e quindi celle (in genere tra 8 e 12 celle). La MMU li raggruppa in un modulo e fornisce funzioni di bilanciamento inter-cellulare.
3. Pack Management Unit (PMU): il livello più alto, gestisce e controlla MMU. La PMU comunica con sistemi esterni, misura parametri a livello di pacco batteria come la corrente e la tensione del pacco e controlla i dispositivi di sicurezza del pacco.

I termini CMU, MMU e PMU non sono standardizzati, e talvolta ci sono altri termini usati nella letteratura e nell'industria automobilistica. Ad esempio, "unità di gestione centrale" (CMU) è anche usata come termine per la PMU, o "unità di acquisizione dati" per la CMU, o "circuito di supervisione cellulare" per la MMU con CMU integrata

Utilizzando questa classificazione dei livelli, è possibile distinguere le seguenti tre varianti principali delle topologie BMS.

2.1.1 BMS centralizzato

In un BMS centralizzato, tutti e tre i livelli (CMU, MMU, PMU) sono combinati in un'unica entità (circuito stampato, PCB), che gestisce tutte le attività richieste dal BMS ed è direttamente collegata alle celle della batteria. Questa topologia è rappresentata schematicamente in Figura 1.

I BMS centralizzati sono semplici e compatti, ma difficili da scalare. Una ragione è che, per un numero crescente di celle, il cablaggio delle stesse al BMS diventa complesso. Inoltre, i requisiti di isolamento diventano difficili da soddisfare quando sono coinvolte alte tensioni, in quanto, in questa disposizione, la differenza di potenziale sugli ingressi BMS è uguale alla tensione totale del pacco batteria.

La topologia BMS centralizzata è quindi generalmente utilizzabile solo per gli accumulatori con un numero limitato di celle e non è comunemente utilizzata per veicoli elettrici con batterie più grandi. Un'eccezione notevole è il BMS della Nissan Leaf. Tuttavia, i BMS centralizzati sono spesso utilizzati, ad esempio, in piccole biciclette elettriche a bassa capacità con un numero limitato di celle.

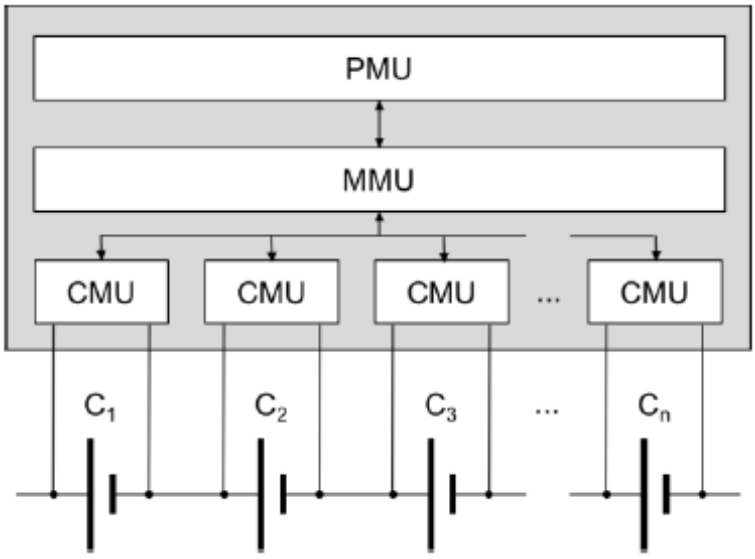

Figura 1. Topologia di un BMS centralizzato [4]

2.1.2 BMS Master-Slave modulare

In una topologia BMS modulare, la MMU è divisa in più istanze separate. Questi possono essere posizionati vicino ai moduli della batteria, riducendo così la complessità del cablaggio. Le MMU trasferiscono quindi le misurazioni dei parametri della cella alla PMU tramite un'interfaccia di comunicazione. Questa comunicazione interna può essere realizzata, ad esempio, tramite CAN bus o isoSPI. Pertanto, in contrasto con la topologia BMS centralizzata, in una disposizione modulare la PMU è collegata solo indirettamente con le singole celle.
Un'ulteriore variante avanzata della topologia modulare è la topologia master-slave. Qui, le funzioni e gli elementi degli slave, detti anche circuiti di supervisione delle celle (CSC), sono ridotti al minimo e le funzioni relative al sistema di batteria completo sono implementate solo sul master. Pertanto, con questa topologia il costo dei moduli slave viene ulteriormente ridotto.

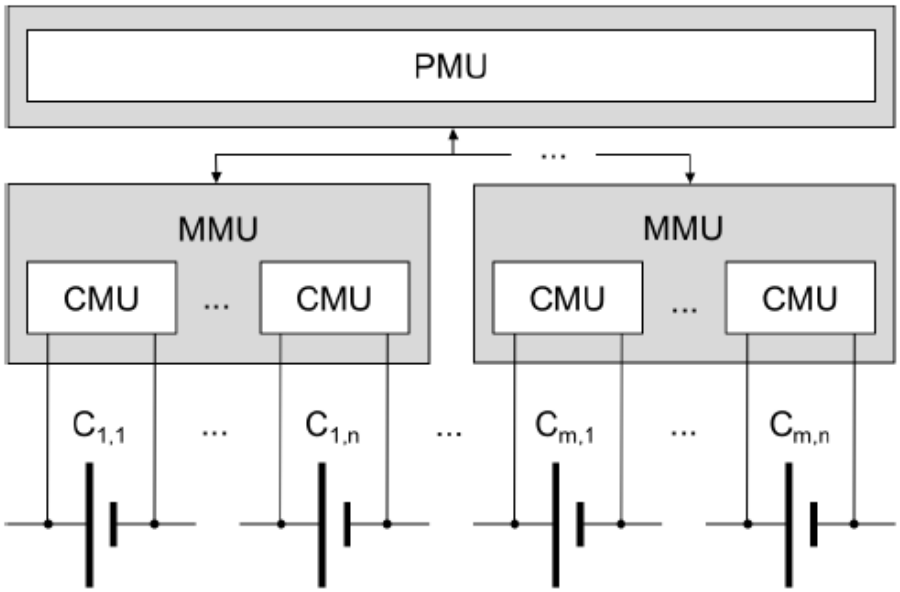

Figura 2. Topologia di un BMS modulare [4]

Le possibili configurazioni utilizzabili con questa topologia sono due: "*Master and Slave*" e "*Daisy Chain*". Nella prima, *Master and Slave*, le celle sono suddivise in blocchi, ognuno dei quali è gestito da un modulo S (Slave). Ogni cella è dotata di un sensore di tensione e di uno di temperatura. I sensori sono collegati al modulo Slave che monitora le condizioni della cella e attua le funzioni di bilanciamento. I moduli Slave sono connessi al Master che monitora la corrente e, conoscendo anche i valori di tensione e temperatura delle celle, calcola il SOC. Il Master gestisce inoltre i contattori di isolamento per la protezione della batteria e il sistema di comunicazione.
I vantaggi di questa configurazione sono la possibilità di gestire batterie ad alta tensione aggiungendo moduli. Inoltre non si ha la necessità di avere un circuito stampato dedicato a ogni singola cella. Gli svantaggi sono che la comunicazione analogica tra sensori e slave è suscettibile al rumore, e prevede un numero elevato numero di cavi necessari. La seconda configurazione, *Daisy Chain*, prevede l'utilizzo di un piccolo circuito stampato per ogni cella (o gruppo di celle) che ospita i sensori di tensione e temperatura, il bypass di corrente per il bilanciamento e il sistema di comunicazione. Il modulo Slave si alimenta direttamente dalla cella che sta monitorando; un unico cavo dati connette i nodi di tutti gli Slave al Master. L'elaborazione dei dati è interamente eseguita dal Master, insieme alle funzioni di monitoraggio, protezione e comunicazione.
I principali vantaggi della connessione Daisy Chain sono semplice design e realizzazione e la potenzialità di un'elevata affidabilità in ambito automotive. Gli svantaggi sono l'elevato numero di circuiti stampati, uno slave per ogni cella (o gruppo di celle), e un lavoro di elaborazione più pesante per il master.

2.1.3 BMS distribuito

In una tipologia BMS distribuita, esistono numerose PMU indipendenti che supervisionano il proprio insieme di celle o supercelle. Le diverse PMU possono comunicare tra loro e, a seconda dei requisiti, funzionare autonomamente o ricevere ed emettere comandi di controllo da altre PMU. La variante più ampia è il cosiddetto concetto di cella batteria intelligente, in cui ogni cella batteria è dotata del proprio microcontrollore dedicato. Questa topologia offre la massima flessibilità e scalabilità, ma ha anche la più alta complessità e costi, dal momento che è necessaria una disposizione completa di CMU, MMU e PMU per ogni set di celle o supercelle.
I BMS centralizzati sono economici, ma meno flessibili e scalabili. Le topologie BMS distribuite sono le più costose e versatili e le più semplici da installare. Le topologie BMS modulari e master-slave offrono un buon compromesso dei vantaggi e degli svantaggi delle altre due topologie.

2.2 Componenti di un sistema batterie ad alta tensione

Oltre alle funzioni del BMS, un confronto ed un'analisi del BMS richiede anche una conoscenza di base della struttura di un pacco batterie ad alta tensione (HV). Pertanto, in questa sezione, vengono presentati brevemente i componenti tipici di un pacco batterie le cui relazioni sono mostrate schematicamente in Figura 3.
Nel caso di un veicolo elettrico (BEV) i componenti presenti sono i moduli batteria, il BMS, un sistema di raffreddamento/condizionamento, un'unità di disconnessione batteria (BDU – battery disconnection unit). Sono infine presenti l'alloggiamento e le interfacce per HV e connessioni dati. Questi componenti sono mostrati schematicamente nella Figura 3, dove la BDU è chiamata switch box o "scatola di commutazione" (a volte la BDU o switch box viene anche chiamata "scatola di giunzione della batteria").

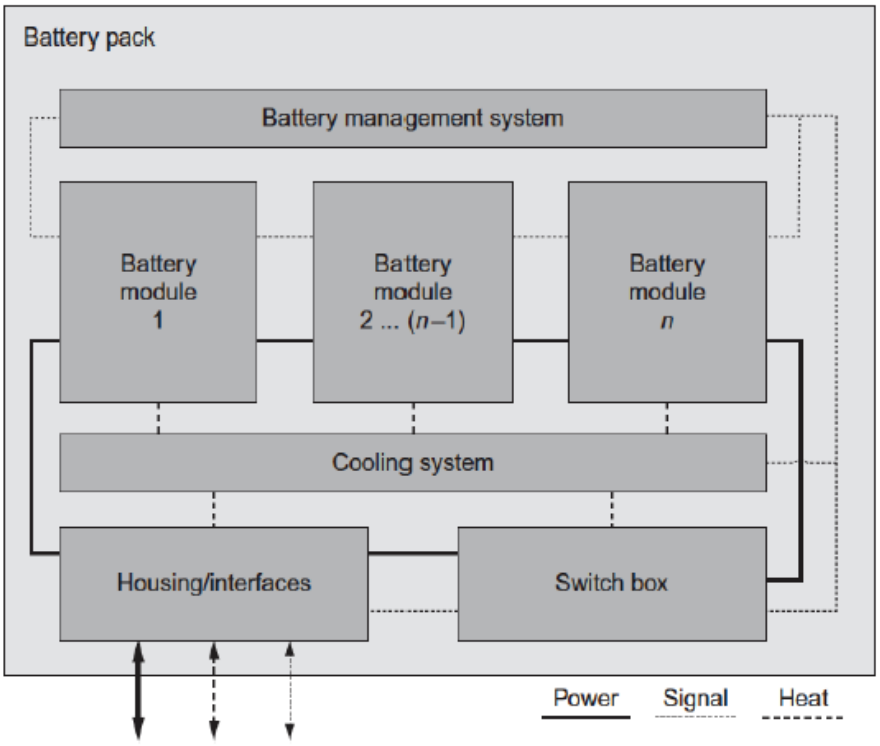

Figura 3. Descrizione schematica dei componenti di un sistema batterie ad alta tensione [4]

Su ciascun modulo batteria, in questo caso, si trova uno slave BMS, che esegue il monitoraggio diretto delle celle ed è collegato al master BMS. Il BDU contiene - oltre ai contattori HV, che commutano la tensione del pacco batteria all'esterno - un fusibile, un sensore di tensione e corrente erogate dall'intero pacco, un resistore di precarica e un controllore dell'isolamento. La resistenza di precarica limita la corrente di spunto e il controllore dell'isolamento verifica costantemente se l'alloggiamento o la massa del veicolo sono sufficientemente isolati dalle parti ad alta tensione. Il BMS può anche gestire attivamente la temperatura del

pacco controllando un riscaldatore per mantenere la sua temperatura operativa minima, o un ventilatore o un sistema di raffreddamento a liquido per mantenerlo al di sotto della sua temperatura massima di funzionamento.

2.3 Circuiti integrati del BMS

Il BMS utilizza circuiti integrati (IC, anche indicati come microchip) per implementarne le funzioni. I circuiti integrati utilizzati nel BMS possono essere suddivisi in circuiti integrati che forniscono misurazioni delle tensioni e delle temperature delle celle e circuiti integrati (microcontrollori) che utilizzano i valori forniti per determinare lo stato del pacco batteria e proteggere le celle dal funzionamento al di fuori delle aree di funzionamento sicuro.
Inoltre, i circuiti integrati per la gestione della batteria possono essere distinti in circuiti integrati generici e ASIC progettati appositamente (circuiti integrati specifici dell'applicazione). In alcuni progetti BMS più orientati alla ricerca e sperimentali - ad esempio, il FoxBMS di Fraunhofer – sono stati incorporati i cosiddetti FPGA (array di gate programmabili sul campo). Gli FPGA sono circuiti integrati che possono essere configurati da un cliente o uno sviluppatore dopo la produzione. Possono essere utilizzati per accelerare compiti computazionalmente intensi nel BMS, come il filtro di Kalman per l'identificazione dei parametri delle celle della batteria e il supporto del microcontrollore principale.
Invece di monitorare tutte le celle collegate in serie, i circuiti integrati dei sensori di cella spesso incorporano una cosiddetta architettura di multiplexing che commuta la tensione da ciascuna cella (coppie di ingressi di fili) a sua volta a una singola linea di uscita analogica o digitale. Questo approccio riduce i costi, ma incorre nello svantaggio che è possibile monitorare solo una tensione di cella alla volta, potenzialmente perdendo informazioni importanti a causa del campionamento. È quindi necessario un meccanismo di commutazione ad alta velocità per commutare la linea di uscita su ciascuna cella in modo che tutte le celle possano essere monitorate sequenzialmente in una frequenza sufficiente.

2.4 Architettura software

La decisione di distribuire le funzioni BMS in diverse unità o di concentrarla in una singola unità, si applica non solo per le parti hardware. Il software e la potenza di elaborazione associate alle funzioni BMS possono anche essere strutturate in modi diversi.
Nella topologia BMS centralizzata, che utilizza solo un singolo microprocessore, questa unità è responsabile di implementare tutte le funzioni software.
In un'architettura modulare o master-slave, tuttavia, ciascun dispositivo slave avrà in genere un microprocessore responsabile, almeno, della misurazione della tensione e della temperatura e del bilanciamento delle celle. Anche se è possibile implementare funzionalità aggiuntive in questi microcontrollori, ci sono alcune limitazioni, poiché ad esempio i moduli slave potrebbero non avere sempre accesso a tutti gli ingressi del sistema.
Simile ad altri sistemi di controllo di tipo “embedded”, le implementazioni BMS spesso seguono un'architettura multilivello. Ciò significa che le funzioni del software BMS possono essere suddivise in diversi livelli:

- basso livello per i driver di dispositivo e le routine di interfaccia hardware
- medio livello che fornisce le implementazioni di protocolli di comunicazione e interpretazioni di misurazioni fisiche.
- alto livello per calcoli di batteria come quelli relativi allo stato di carica e al limite di potenza
- livello top per i processi decisionali basati sulle informazioni fornite dai livelli inferiori

L'uso rigoroso dell’approccio a più livelli permette a qualsiasi livello di essere modificato con conseguenze limitate sui livelli adiacenti. Ad esempio, un'applicazione che decide di connettere o disconnettere la batteria in base al proprio SOC non ha bisogno di informazioni su come viene calcolato il SOC, ed infatti potrebbe essere vantaggioso utilizzare diversi metodi di SOC in diverse applicazioni.
La maggior parte delle architetture software BMS implementano un ambiente multi-tasking per le diverse funzioni. Poiché il BMS è un sistema critico per la sicurezza, è necessario garantire che i compiti responsabili

delle funzioni di sicurezza, come la misurazione della tensione e la protezione da sovraccarica associata, la misurazione della temperatura e della corrente e l'attuazione del contattore, siano eseguiti in modo tempestivo per garantire risposte tempestive a potenziali rischi. In un ambiente multi-tasking in cui è possibile che le attività vengano temporaneamente interrotte per eseguire altre attività e quindi riprese in un secondo momento, è di vitale importanza che le attività BMS critiche per la sicurezza non vengano ritardate in modo significativo ed eseguite troppo tardi. Al fine di garantire questa funzionalità in tempo reale, numerose implementazioni BMS si basano su sistemi operativi in tempo reale (RTOS) come FreeRTOS o µC / OS-II, che commutano le attività in base alla priorità e possono fornire garanzie sul tempo necessario per accettare e completare un compito specifico.

3 Descrizione del BMS oggetto di analisi

Il sistema preso in considerazione per l'analisi è il "foxBMS" [5, 6], sviluppato da Fraunhofer [7], integrato in un sistema batteria per applicazione automotive, composto da 96 celle, suddivise in 8 moduli da 12. Il foxBMS è un ambiente libero di progettazione e programmazione di un BMS che può essere utilizzato in diversi settori: ricerca, automotive, accumulo stazionario etc. Il foxBMS è composto da una parte hardware e una software che possono essere gestite e impostate a seconda dell'utilizzo finale.

L'architettura del foxBMS è del tipo Daisy Chain. La Master Unit è composta da tre schede: BMS-Master Board, BMS-Interface Board e BMS-Extension Board. Nella BMS-Master Board sono installati due microprocessori: MCU0 e MCU1. Il software del BMS lavora sul MCU0 mentre il MCU1 è utilizzato per la ridondanza di sicurezza: MCU1 monitora le Slave su una apposita daisy chain separata. Il MCU0 comunica con l'esterno attraverso un bus CAN.

Le Slave Unit vengono usate per misurare tensione e temperatura delle celle e per il bilanciamento passivo delle stesse; comunicano con la Master Unit attraverso la BMS-Interface Board. Ogni Slave Unit può lavorare con un massimo di 12 celle connesse in serie.

La batteria viene connessa o disconnessa dal carico attraverso due contattori principali (polo positivo e negativo) e un contattore di pre-charge. I contattori sono comandati dal MCU0: attraverso le richieste provenienti dal canale di comunicazione CAN il sistema apre o chiude i contattori, basandosi sulle misure e sugli algoritmi implementati nel software. Inoltre è presente una linea interlock che, se aperta, disconnette immediatamente tutti i contattori. Interviene in casi di emergenza e può essere aperta sia da MCU0 che da MCU1.

In Figura 4 viene riportato uno schema generale del sistema foxBMS connesso ad una generica batteria. Le Slave Board rilevano i dati di tensione e temperatura dalle celle, li comunicano attraverso la daisy chain alla Master Unit che elabora i dati e decide la strategia di controllo e/o intervento. Contemporaneamente comunica lo stato del sistema al mondo esterno utilizzando il bus CAN. Il sensore di corrente monitora la corrente del pacco batteria e segnala eventi indesiderati al processore tramite l'invio di messaggi di errore. Ripetuti e prolungati messaggi di errore provocano l'apertura della catena di interlock e quindi la disconnessione della batteria.

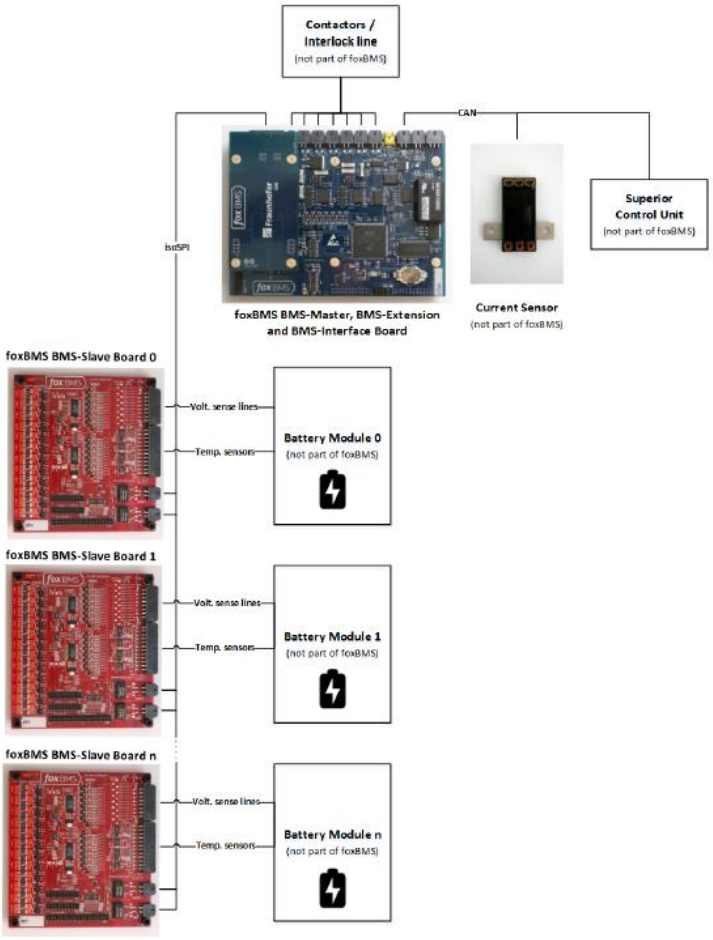

Figura 4 - Layout del sistema integrato foxBMS- batteria

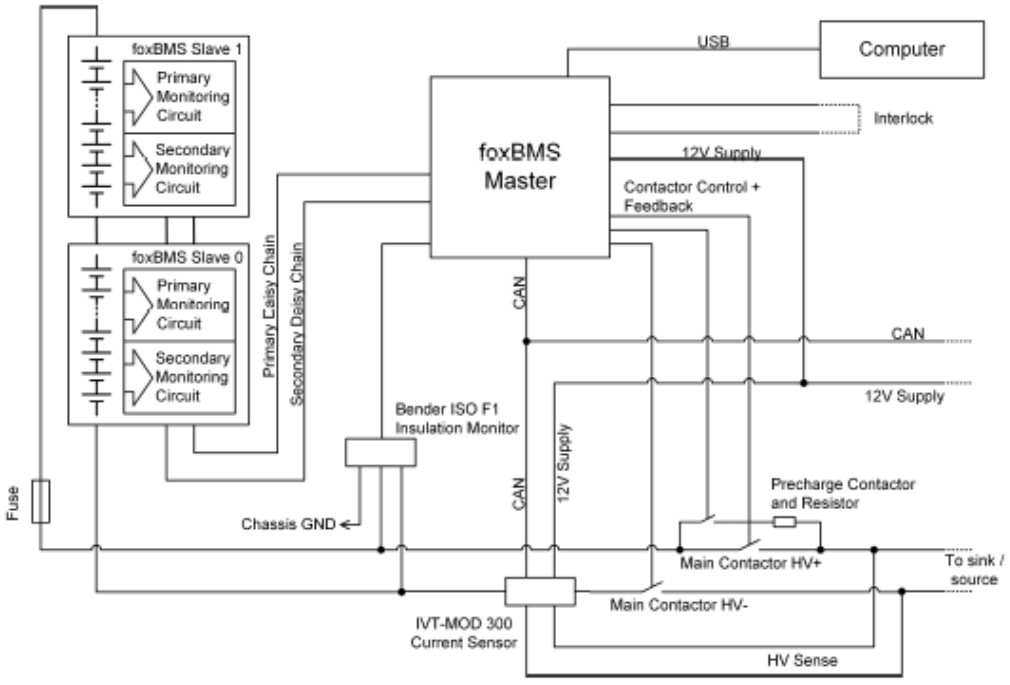

Figura 5 - Schema a blocchi del sistema foxBMS-batteria

3.1 Master Unit

La Master Board, Figura 6 , è l'unità di controllo principale del BMS, sulla quale sono installati I due microprocessori MCU0 e MCU1. Come già anticipato, MCU0 è la sede del software di gestione della batteria, mentre MCU1 è presente come ridondanza di sicurezza.

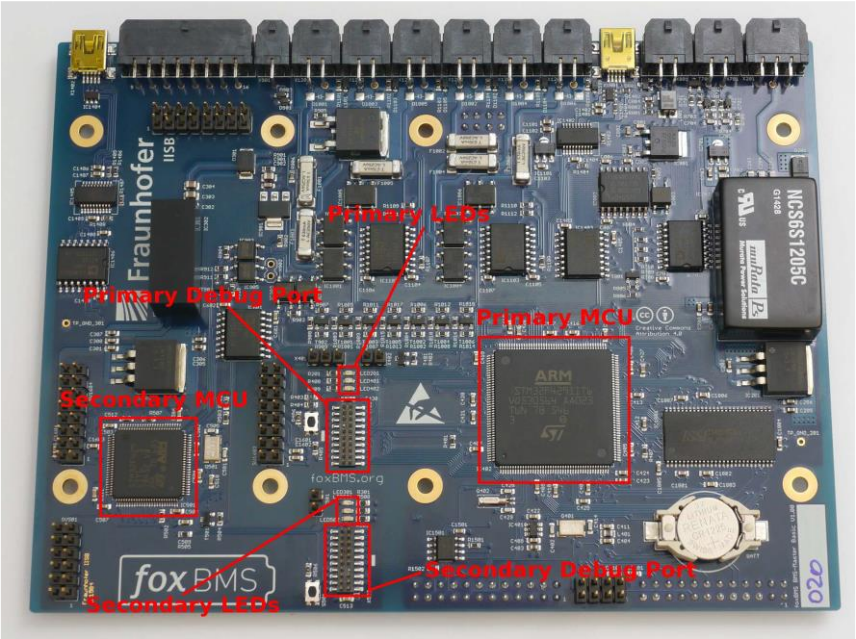

Figura 6 - FoxBMS BMS-Master Board

3.2 Slave board

La Slave Board, Figura 7 , è la sede dei sensori per il monitoraggio dello stato delle celle. Si basa sul chip monitor TC6804-1/LTC6811-1. Supervisiona 12 celle connesse in serie, misurando tensione e temperatura. La tensione viene rilevata per ciascuna cella, mentre i sensori di temperatura sono 8 per 12 celle. La Figura 8 consente di visualizzare le zone in cui sono posizionati i diversi dispositivi di misura e di gestione delle celle. La Slave Board opera anche il bilanciamento passivo delle celle. Il bilanciamento viene realizzato con l'utilizzo di due resistori da 68 Ω posti in parallelo a ciascuna cella. Gli switch MOSFET che controllano la connessione delle celle sono comandati dal processore primario. Il secondario non esegue il bilanciamento. La corrente di bilanciamento è di circa 100 mA.

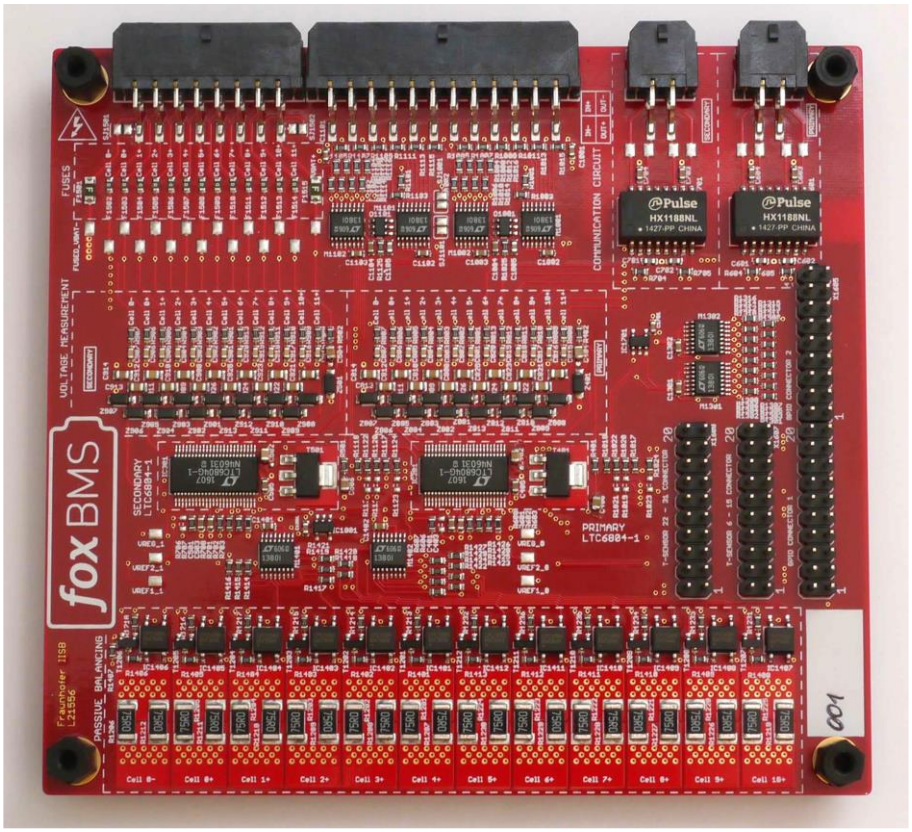

Figura 7 - FoxBMS BMS-Slave Board

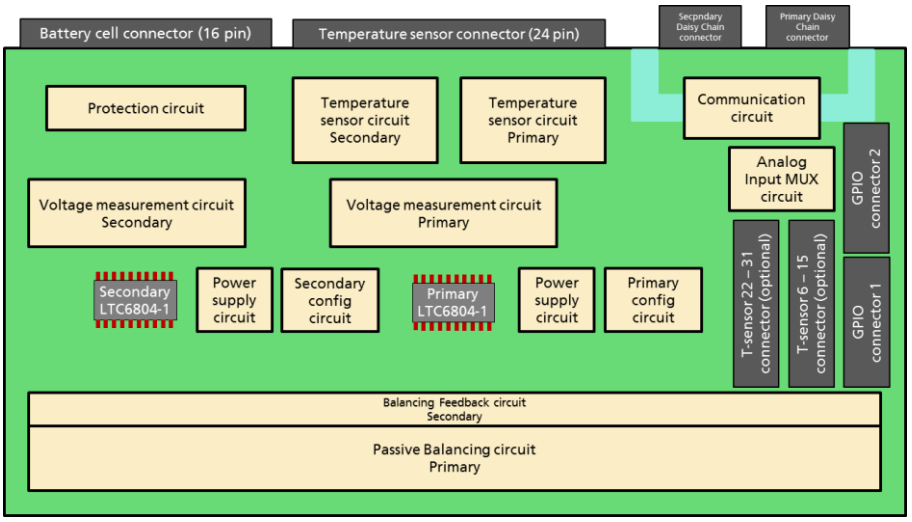

Figura 8 - Schema a blocchi di una Slave Board

4 Intervento del BMS in risposta a deviazioni dal normale funzionamento individuate dall'applicazione dell'HAZOP a livello cella

Per ognuna delle sequenze incidentali identificate attraverso l'analisi HAZOP applicata ad una cella litio-ione di tipo NMC [8], e per le quali era stato identificato l'intervento del BMS come sistema di sicurezza, è stato dettagliato l'intervento del BMS prendendo a riferimento il Fox-BMS.

Il dettaglio dell'intervento del Fox-BMS in risposta alle deviazioni dal normale funzionamento delle celle è stato determinato con l'aiuto del gruppo di lavoro del Dipartimento di Ingegneria dell'Informazione dell'Università di Pisa costituito dai proff. Roberto Roncella, Roberto Saletti e Federico Baronti, nonché dai dottorandi di ricerca Andrea Carloni e Roberto Di Rienzo.

La seguente tabella riporta le deviazioni dal normale funzionamento delle celle, e l'intervento previsto del Fox-BMS.

Causa	**Ipotesi intervento BMS**	**Commenti gruppo di lavoro DII**
Sovra scarica della cella	Il BMS è progettato per interrompere l'utilizzo della batteria al raggiungimento di un potenziale minimo sulla cella a potenziale minore.	Il BMS interviene non appena una cella all'interno del pacco batteria raggiunge il livello di tensione minimo consentito. L'intervento del BMS consiste nell'apertura di tutti i contattori e della linea di interlock (questo avviene se il BMS è attivo). Anche l'autoscarica e l'assorbimento di corrente delle schede in stand-by possono provocare la sotto scarica della cella. La capacità di rilevare allarmi dipende dall'architettura e dall'assorbimento di corrente delle schede spente. Il fox-BMS in caso di sosta prolungata non rileva l'autoscarica se non quando si prova a riaccendere il veicolo.
Corto circuito esterno al pacco batteria	Il BMS è progettato per interrompere l'utilizzo del pacco batteria nel caso di un aumento non controllato di corrente dovuto a un cortocircuito esterno al pacco	Il pacco batteria è protetto da un fusibile che scollega la batteria dal carico in caso di cortocircuito esterno. Il BMS è impostato per diverse soglie in funzione dell'intensità della corrente e della durata.
Corto circuito esterno provocato da impatto del veicolo	Il BMS è progettato per interrompere l'utilizzo del pacco batteria nel caso di un aumento non controllato di corrente dovuto a un cortocircuito esterno al pacco	Il pacco batteria è protetto da un fusibile che scollega la batteria dal carico in caso di cortocircuito esterno. Il BMS è impostato per diverse soglie in funzione dell'intensità della corrente e della durata.
Stoccaggio ad elevata temperatura (con celle cariche o scariche)	All'avvio, le celle vengono controllate per determinare se il loro stato è all'interno della Safe Operating Area (SOA) (in termini di tensione corrente e temperatura).	Il BMS in STANDBY MODE assorbe 150mA di corrente. Quindi, ipotizzando di utilizzare un pacco batteria da 90Ah, durante la fase di (STANDBY MODE) che si verifica quando la macchina non è né in funzione né in ricarica, molto probabilmente il BMS verrebbe spento perché se non lo fosse scaricherebbe il pacco batteria nel giro di un mese.

Causa	Ipotesi intervento BMS	Commenti gruppo di lavoro DII
Sovra tensione durante la carica (anche rigenerativa)	Il BMS è progettato per inibire la ricarica del modulo se la tensione del caricatore è troppo elevata	Se ipotizziamo di impostare nel caricatore una tensione più elevata della tensione massima prevista per il pacco batteria in questione e immaginiamo il pacco batteria come un grosso condensatore (che ha un comportamento inerziale in tensione), non appena colleghiamo il caricatore al pacco, la tensione della linea rimane fissata alla tensione del pacco. Successivamente, Il generatore cercherà di aumentare la corrente di ricarica per aumentarne la tensione del pacco fino al raggiungimento della soglia impostata nel caricatore. Ma: • Se l'aumento di corrente è tale da superare la massima consentita dal BMS, il BMS stacca il pacco. Se la corrente massima che eroga il caricatore viene limitata a un valore inferiore al massimo consentito dal BMS, il BMS stacca il pacco non appena una cella raggiunge il limite di tensione massimo consentito (il pacco quindi non viene esposto a un pericolo di sovratensione prodotto dal caricatore). Ma dipende dalla fase di utilizzo che implica un protocollo di intervento diverso (NORMAL o CHARGE)
Sovra corrente durante la carica	Il BMS è progettato per inibire la ricarica del modulo se la corrente del caricatore è troppo elevata.	Si il BMS interviene aprendo i contattori.

Causa	Ipotesi intervento BMS	Commenti gruppo di lavoro DII
Malfunzionamento del BMS (perdita di equalizzazione)	Nella versione base del SW non è previsto alcun tipo di intervento nel caso in cui il feedback e lo stato di controllo del bilanciamento sono discordanti	Il FoxBMS opera con sistema passivo che prevede 2 resistenze da 68Ω in parallelo per ogni cella. La corrente di equalizzazione è 100 mA. La tipologia di bilanciamento utilizzata è di tipo passivo. Ogni cella può essere temporaneamente scaricata su due resistori da 68Ω in parallelo ad essa. L'equalizzazione viene attivata tramite il controllo di un MOSFET che collega i resistori alla cella. Il controllo del MOSFET viene gestito dalla BMS Salve Board che attiva l'equalizzazione su comando del BMS Master. In particolare, solo il chip monitor primario presente nel BMS slave controlla lo stato del MOSFET. Mentre il chip monitor secondario, assieme al primario, può leggere un segnale di feedback che rimane attivo fintanto che almeno una cella all'interno di quel modulo è in fase di bilanciamento. C'è un opto-isolatore che vede se scorre corrente nella singola resistenza di equalizzazione. (Nella versione base del SW non è previsto alcun tipo di intervento nel caso in cui il feedback e lo stato di controllo del bilanciamento sono discordanti).
Sovraccarica della cella	Il BMS è progettato per mantenere l'equalizzazione di tutte le celle e interrompere la ricarica del modulo al raggiungimento della tensione massima di progetto sulla singola cella	Il BMS è progettato per equalizzare le celle. Se, nonostante l'equalizzazione, viene raggiunto da una cella all'interno del pacco il limite superiore di tensione consentita, il BMS interviene aprendo tutti i contattori e la linea di interlock.
Elevata temperatura di funzionamento della cella (o malfunzionamento del sistema di raffreddamento)	IL BMS per ogni modulo da 12 celle acquisisce 8 punti di temperatura	Il BMS interviene non appena un sensore di temperatura posizionato sul pacco batteria supera: • La *massima* temperatura consentita in fase di carica o in fase di scarica (generalmente sono diverse); • La *minima* temperatura consentita in fase di carica o in fase di scarica (generalmente sono diverse). L'intervento del BMS consiste nell'apertura di tutti i contattori e della linea di interlock.

Causa	Ipotesi intervento BMS	Commenti gruppo di lavoro DII
Corto circuito interno (provocato da impatto del veicolo)	Il BMS interviene interrompendo l'utilizzo del modulo nel caso di superamento di una soglia prestabilita di corrente	Se il cortocircuito interno riguarda una o più celle, il BMS rileva che la tensione delle celle è scesa sotto il cut-off inferiore e apre i contattori del pacco, ma non risolve il cortocircuito interno. E' più pericoloso perché dipende quale zona della batteria interessa, cioè se colpisce il fusibile o no

Lo studio ha evidenziato gli interventi del BMS in risposta alle deviazioni dal normale funzionamento della batteria individuate nel corso dell'analisi applicata alla cella [8]. Nella maggior parte dei casi il sistema è programmato per rilevare un funzionamento non corretto e disconnettere il pacco batteria dal carico prima del verificarsi di situazioni ancora più gravose.

Una criticità rilevata è relativa al corto circuito interno, che potrebbe essere non rilevato in funzione della zona in cui questo si verifica. Il rilevamento in questo caso è importante per avvertire gli occupanti del veicolo, non ci sono comunque azioni possibili da parte del BMS per influire sul decorso dell'incidente.

Il BMS a veicolo fermo può essere funzionante o meno. In questo caso la batteria è comunque disconnessa e non eroga potenza, ma il funzionamento del BMS potrebbe innescare degli allarmi in caso verificasse delle condizioni anomale.

E da segnalare inoltre come nella presente versione del BMS non sia attivo a livello software un controllo nel caso in cui il feedback e lo stato di controllo del bilanciamento sono discordanti. Questo potrebbe comportare il mancato bilanciamento di una delle celle provocando effetti immediati sull'efficienza e la vita del pacco ed un peggioramento delle condizioni di sicurezza dello stesso.

5 Sicurezza funzionale dei componenti elettrici ed elettronici utilizzati in ambito automotive (ISO 26262:2011 Functional safety in vehicles)

L'ambito di applicazione della "ISO 26262 - Veicoli stradali - Sicurezza funzionale" si riferisce a sistemi rilevanti per la sicurezza che contengono almeno un sistema elettrico o elettronico (E/E) che si trovano in una normale autovettura, con una massa del veicolo fino a 3500 kg [9].

Pertanto e in senso stretto, lo standard non è applicabile ai prototipi in quanto sono sistemi E/E unici. Inoltre, i componenti o i sistemi e i loro componenti, che sono stati rilasciati per la produzione prima della data di pubblicazione dello standard nel 2011, o che in quella data erano già stati sviluppati, sono esenti dallo standard.

Il campo di applicazione della norma esclude pericoli quali scosse elettriche, incendio, fumo, calore, radiazioni, avvelenamento, infiammazione, reazione chimica, corrosione, emissione di energia e rischi comparabili, purché non siano stati causati da un malfunzionamento di un sistema E/E rilevante per la sicurezza (BMS) [9]. Inoltre, non è tra gli obiettivi della ISO 26262, trattare il malfunzionamento provocato intenzionalmente.

5.1 Sicurezza funzionale (Functional safety)

La sicurezza funzionale è generalmente descritta come una reazione corretta di un sistema, in un ambiente definito, per una determinata stimolazione definita all'ingresso di tale sistema. Dalle definizioni della ISO 26262 La functional safety è definita come "assenza di un rischio irragionevole a causa di pericoli causati dal comportamento scorretto dei sistemi E/E" [9]. La norma rende obbligatorio che un componente o un sistema fallisca in uno stato sicuro in caso di guasto (Fail Safe).

Al fine di garantire e certificare l'assenza da rischi inaccettabili, la procedura di sviluppo della sicurezza funzionale è applicata come stabilito nella norma ISO 26262. Il veicolo e i suoi componenti sono analizzati nei loro ambienti. Il veicolo e i suoi sistemi devono soddisfare i requisiti degli obiettivi di sicurezza. Al livello successivo, più dettagliato, gli specifici sistemi E/E, vengono soggetti ai requisiti tecnici di sicurezza, dovendo ancora soddisfare i requisiti generali di sicurezza funzionale. L'ultimo passaggio consiste nel creare requisiti di sicurezza per hardware e software intesi a garantire l'assenza di rischi inaccettabili a livello di componenti e di parti. Una rappresentazione semplificata del percorso critico da seguire sull'applicazione della norma ISO 26262 [9, 10, 11, 12, 13,14, 15, 16, 17], che mira a ottenere l'assenza da rischi inaccettabili durante il ciclo di vita dei sistemi E/E automobilistici, vedi schema a blocchi, in Figura 9.

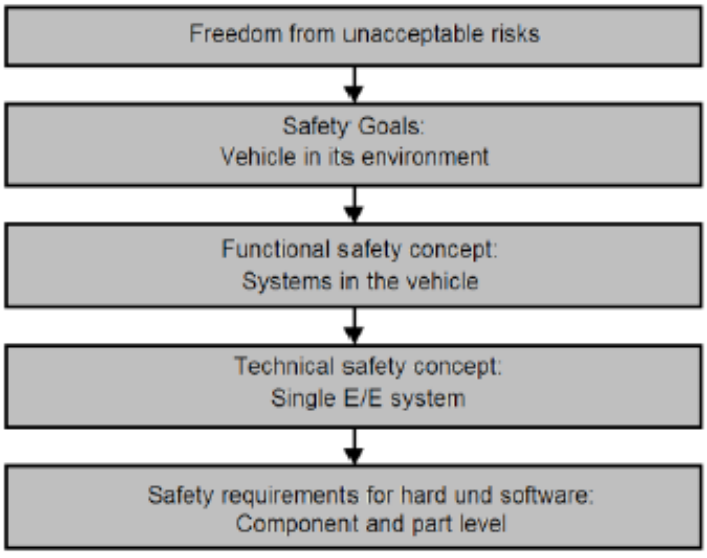

Figura 9. Procedura di sviluppo della sicurezza funzionale per la certificazione di assenza da rischi inaccettabili

5.2 Definizione di guasto (fault) errore (error) e failure (fallimento)

Nell'applicazione della norma ISO 26262 sono da tenere in considerazione le seguenti definizioni:

- Guasto (fault): Condizione anomala che può causare il fallimento di un elemento, un'unità funzionale o un sistema del veicolo
- Errore (error): Discrepanza tra un valore o una condizione calcolata, osservata o misurata e il valore o la condizione corretta, specificata o teoricamente prevista
- Failure (fallimento): Termine della capacità di un elemento di eseguire una funzione come richiesto

Su questi concetti è possibile definire una relazione causa-effetto implicita che li collega. Come si può vedere nella Figura 10, un guasto (fault) può causare un errore (error), che può portare al fallimento di un'unità funzionale o di un sistema.

Figura 10. Relazione tra guasto, errore e fallimento

Quando si considera la sicurezza funzionale secondo la norma ISO 26262, si possono distinguere fondamentalmente due tipi di guasti, errori e fallimenti: casuali e sistematici.
Quelli sistematici possono essere evitati con metodi appropriati nel processo di progettazione, mentre quelli casuali possono essere ridotti solo in misura tollerabile. Errori hardware possono essere sistematici o casuali, i guasti software, d'altra parte, sono rigorosamente sistematici.

In definitiva il rispetto della normativa ISO da parte del costruttore del BMS assicura di per se che ogni guasto del BMS non possa ripercuotersi sul sistema in modo pericoloso. Il produttore del BMS deve assicurare il rispetto della normativa, il produttore dell'autoveicolo deve estendere l'applicazione al sistema integrato sul pacco batterie.
Di seguito viene descritta l'applicazione di un'analisi di sicurezza HAZOP al fox- BMS integrato su un'applicazione automotive. L'analisi in questione non è da considerarsi una verifica dell'applicazione della normativa o dell'analisi effettuata dai produttori per l'adesione alla normativa stessa. Infatti da una parte l'oggetto di studio non è il BMS fornito prodotto e sviluppato da Fraunhofer in se ma il sistema BMS connesso ad un'applicazione automotive, dall'altra i rischi ed i pericoli che andiamo a ricercare nell'analisi di sicurezza sono più ampi rispetto a quelli identificati dalla norma.

6 Metodologia HAZOP

Originariamente questa metodologia fu sviluppata per processi e tecnologie nuove, ove si aveva disponibile una limitata esperienza di funzionamento; successivamente è stata applicata in maniera efficace in tutte le fasi di vita di un impianto: dal progetto esecutivo in poi. I risultati di un'analisi HAZOP includono l'identificazione dei rischi e/o dei problemi operativi connessi con l'esercizio di un impianto/sistema e possono aiutare nell'identificazione di raccomandazioni circa modifiche progettuali od operative (procedurali), così come possono essere utili per l'identificazione di tutti quegli aspetti che necessitano di uno studio più approfondito.

La metodologia HAZOP si basa su un'analisi sistematica dello schema di processo o di un P&Id di impianto, con l'intento di identificare ogni possibile deviazione dal funzionamento ordinario, definito in termini tecnici "intenzione", ossia il funzionamento settato sulla base di tutti i parametri di progetto/regolazione dell'impianto.

L'analisi viene condotta da specialisti e procede tramite un brainstorming finalizzato ad un'indagine rigorosa degli schemi progettuali. Per poter fare ciò occorre conoscere bene a livello funzionale l'impianto/sistema da analizzare, ed occorre poi applicare in maniera sistematica ad ogni parametro caratteristico della parte interessata (pressione, temperatura, portata, ecc.) tutte le "parole chiave" indicanti una condizione di deviazione dalle caratteristiche di progetto (es. parte 1, parola chiave "more" applicata al parametro "pressione" indica la condizione di deviazione che porta ad avere "alta pressure nella parte 1").

Nello specifico del presente studio l'analisi HAZOP è stata utilizzata per l'identificazione dei pericoli.

Un pericolo ("Hazard") è definito come un evento, scatenato da una causa esterna o interna, che può generare condizioni dannose per l'uomo o per il sistema nel suo complesso. I pericoli, nel caso di un sistema di stoccaggio di energia ricaricabile, ricadono in una delle seguenti quattro categorie:

- Pericolo elettrico: esempi concreti di questo pericolo sono il corto circuito o la sovraccarica del sistema.
- Pericolo termico: elevate temperature, incendio etc.
- Pericolo meccanico: derivante da situazioni quali urti, penetrazioni del sistema batteria, cadute etc.
- Pericoli di sistema: risultante da eventi originati nel sistema del quale la batteria fa parte.

L'analisi è stata condotta secondo l'applicazione descritta dalla Norma CEI IEC 61882.

Per facilitare l'esame, il sistema preso a riferimento è suddiviso in elementi in modo che l'intento di progettazione per ciascun elemento possa essere adeguatamente definito. La dimensione degli elementi scelto dipende dalla complessità del sistema e dalla gravità del pericolo.

L'intento di progettazione per una data parte di un sistema è espresso in termini di elementi che ne rappresentano le caratteristiche essenziali.

Il team che conduce l'analisi HAZOP esamina ogni elemento (e/o caratteristica) per la deviazione dall'intento di progetto che può portare a conseguenze indesiderabili. La confidenza dell'identificazione di tutte le deviazioni dall'intento di progettazione viene raggiunta mediante un processo sistematico guidato dall'applicazione di "parole guida".

Il diagramma di flusso riportato nella figura seguente rappresenta le fasi di analisi.

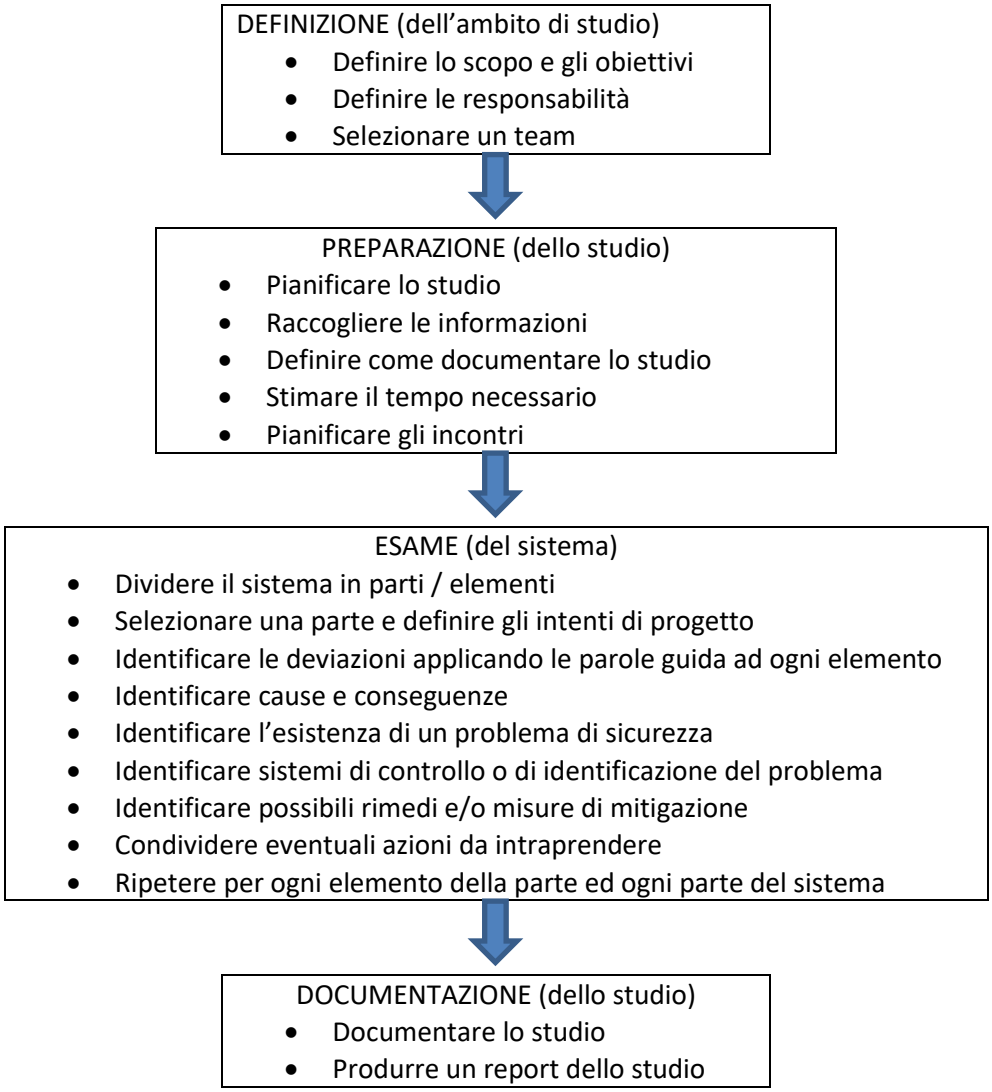

Figura 11. Schema a blocchi della metodologia HAZOP

6.1 Scopo della presente analisi HAZOP

Dal momento che un'analisi HAZOP, per una sua corretta applicazione, necessita di uno scopo ben definito, è importante precisare che la finalità dell'analisi di sicurezza HAZOP condotta per il sistema in esame è stata incentrata sull'**individuazione delle sequenze incidentali che possano avere ripercussioni sulla sicurezza interna ed esterna al sistema di accumulo**. Ove nell'analisi HAZOP si fosse identificata una conseguenza "non rilevante" (si riporta la dicitura "Nessuna" nella colonna "Conseguenze") ed è intesa "non rilevante" unicamente ai fini della sicurezza. Ripercussioni legate all'esercizio ed operatività del sistema non sono state valutate.

6.2 Identificazione degli elementi e delle caratteristiche

Al fine di applicare la tecnica di analisi HAZOP al BMS, questo è stata suddiviso in elementi, per ciascuno dei quali vengono identificate le caratteristiche che hanno influenza sul funzionamento del sistema. La suddivisione del BMS in elementi è riportata in Tabella 1, con una breve descrizione degli stessi. In Tabella 2 vengono riportate le caratteristiche di riferimento associate agli elementi, applicando alle quali le parole guida si intende ricercare in modo sistematico le deviazioni dal normale funzionamento del BMS.

Tabella 1. Suddivisione in elementi del BMS e loro descrizione

ELEMENTO / BLOCCO	*DESCRIZIONE*
1 Master BMS MCU primario	Microprocessore primario installato sulla scheda principale del BMS, dove è memorizzato e viene eseguito il software (lista delle istruzioni) del BMS
2 Master BMS MCU secondario	Microprocessore secondario, presente per ridondanza di sicurezza. Il software è memorizzato su diverso supporto rispetto a quello elaborato dal microprocessore primario (ridondanza hardware e software)
3 Catena di controllo e feedback interlock	L'interlock è un circuito l'apertura del quale apre tutti i contattori de-energizzandoli. L'apertura dei contattori isola la batteria dal mondo esterno. La catena di feedback controlla costantemente lo stato dell'interlock loop.
4 Alimentazione di servizio	E' un sistema di accumulo energetico addizionale che alimenta il BMS.
5 Contattore di potenza	E' il contatto che connette la batteria con il sistema elettrico del veicolo (motore elettrico etc.).
6 Catena di controllo e di feedback dei contattori di Potenza	La catena di feedback controlla costantemente lo stato dei contattori di potenza.
7 Linea di comunicazione CAN	E' una linea condivisa (multiutente) utilizzata per scambiare i dati (comunicazione tra il sensore di corrente, MCU0 e il controllore del veicolo). Il BUS condiviso è "message oriented" (rileva e risolve le collisioni di più operatori che contemporaneamente mandano messaggi sul BUS). Viene completamente gestito da un circuito dedicato posizionato sulla scheda di MCU0 ma indipendente, tutta la complessità di gestione del protocollo è gestito da questa periferica (velocità 500kbit/sec). Normalmente, in caso di rilevazione di errori è prevista la ritrasmissione del messaggio. Esiste inoltre un contatore di errori che, dopo un certo numero di errori consecutivi rilevati, provoca la disconnessione della batteria.
8 Sensore di corrente	Esegue la misura di corrente ed è in grado di capire se la misura è affidabile o no. Ha internamente 2 ADC (Analog Digital Converter), se dal confronto delle due misure la differenza supera un valore prefissato la misura viene ritenuta non affidabile e la notifica dell'errore viene inserita nel pacchetto trasmesso sul CAN.
9 Linea di comunicazione SPI isolata tra MCU primario e secondario [(1)]	La linea è predisposta in termini di collegamenti e software ma non viene utilizzata dal Fox BMS nella sua versione base.
10 Monitor per la verifica della resistenza di isolamento tra il case e le due linee che collegano la batteria	Verifica che il modulo o la batteria alimentata sia isolata dal telaio del veicolo. Prevede la presenza di un generatore di segnale caratterizzato da una determinata forma d'onda. La ricezione di un segnale modificato è ritenuta indice di perdita di isolamento e provoca il distacco della batteria.
11 Fusibile di batteria.	Il fusibile è un dispositivo in grado di proteggere un circuito dalle sovracorrenti, la corrente infatti attraversa un sottile filo conduttore che fonde se la corrente che lo attraversa supera un determinato limite per un certo periodo di tempo.
12 Daisy chain percorso primario	Connessione che provvede al trasferimento dati fra Slave e MCU0. Per ogni dato inviato c'è un'analisi CRC che riconosce i dati errati (in questo caso il dato non viene ritrasmesso, perché la trasmissione è periodica). Il numero dei dati consecutivi che devono risultare errati prima di aprire il contattore è pari a 500, in caso di dati errati consecutivi corrisponde a 0.5 s
13 Daisy chain percorso secondario	Connessione che provvede al trasferimento dati fra Slave e MCU1. Per ogni dato inviato c'è un'analisi CRC che riconosce i dati errati (in questo caso il dato non viene ritrasmesso, perché la trasmissione è periodica). Il numero dei dati consecutivi che devono risultare errati prima di aprire il contattore è pari a 500, in caso di dati errati consecutivi corrisponde a 0.5 s
14 Slave BMS chip monitor primario	E' il microprocessore primario di una Slave board. Il sistema prevede un numero di Slave board ognuna delle quali gestisce 12 celle. Il processore della Slave board elabora i dati di tensione e temperatura prelevati dal modulo e li trasmette alla MCU0. La catena di misura MCU0 e MCU1 è indipendente e completamente ridondante.

15 Slave BMS chip monitor secondario	E' il microprocessore secondario di una Slave board. Il sistema prevede un numero di Slave board ognuna delle quali gestisce 12 celle. Il processore della Slave board elabora i dati di tensione e temperatura prelevati dal modulo e li trasmette alla MCU1. La catena di misura MCU0 e MCU1 è indipendente e completamente ridondante.
16 Connettore unico per prelievo delle tensioni di cella e di modulo	E' il collegamento elettrico di tipo meccanico tra i cavi provenienti dai sensori e i piedini del circuito stampato della Slave board.
17 Connettore unico per il prelievo di 8 punti di temperatura all'interno del modulo.	E' il collegamento elettrico di tipo meccanico tra i cavi provenienti dai sensori e i piedini del circuito stampato della Slave board.
NOTE: (1) La linea di comunicazione SPI isolata tra MCU primario e secondario, seppur fisicamente presente sul Fox-BMS non è utilizzata nella versione base e la sua gestione non è implementata neanche a livello software. Per questo motivo questo elemento per quanto inserito nella descrizione non verrà analizzato in fase di analisi.	

Tabella 2. Suddivisione in elementi del BMS

ELEMENTO / BLOCCO	*CARATTERISTICA*
1 Master BMS MCU primario	Elaborazione dati
2 Master BMS MCU secondario	Elaborazione dati
3 Catena di controllo e feedback interlock	Dati
4 Alimentazione di servizio	Tensione
5 Contattore di potenza	Connessione
6 Catena di controllo e di feedback dei contattori di Potenza	Confronto
7 Linea di comunicazione CAN	Trasferimento dati
8 Sensore di corrente	Corrente
10 Monitor per la verifica della resistenza di isolamento tra il case e le due linee che collegano la batteria	Trasferimento dati
11 Fusibile di batteria.	Corrente di apertura
12 Daisy chain percorso primario	Trasferimento dati
13 Daisy chain percorso secondario	Trasferimento dati
14 Slave BMS chip monitor primario	Elaborazione dati
15 Slave BMS chip monitor secondario	Elaborazione dati
16 Connettore unico per prelievo delle tensioni di cella e di modulo	Corrente
17 Connettore unico per il prelievo di 8 punti di temperatura all'interno del modulo.	Corrente

6.3 Applicazione delle parola guida per l'identificazione delle deviazioni

Come precedentemente introdotto, ad ogni caratteristica dell'elemento considerato sono state applicate le parole guida, per l'ottenimento delle deviazioni dal funzionamento ordinario.

L'applicazione di tutte le parole guida ai vari parametri operativi caratteristici dell'elemento costituente la parte oggetto dello studio, ha consentito l'individuazione delle potenziali deviazioni, l'identificazione delle possibili cause ed infine delle potenziali conseguenze associate a tali eventi al fine di evidenziare i punti critici del sistema. La Tabella 3 riporta le parole guida e le conseguenti deviazioni associate alle caratteristiche di ogni elemento in cui è stato suddiviso il BMS.

Tabella 3. Parole guida e deviazioni associate alle caratteristiche di ogni elemento

ELEMENTO / BLOCCO	*CARATTERISTICA*	*PAROLA GUIDA*	*DEVIAZIONE*
1 Master BMS MCU primario	Elaborazione dati	NO	Elaborazione dati assente
		OTHER THAN	Elaborazione dati errata
2 Master BMS MCU secondario	Elaborazione dati	NO	Elaborazione dati assente
		OTHER THAN	Elaborazione dati errata
3 Catena di controllo e feedback interlock	Dati	NO	Interruzione della comunicazione hardware tra catena di interlock e MCU0 e/o MCU1
4 Alimentazione di servizio	Tensione	NO	Alimentazione assente
		MORE	Alta tensione
		LESS	Bassa tensione
5 Contattore di potenza	Connessione	MORE	Contattore sempre chiuso
		NO	Contattore sempre aperto
6 Catena di controllo e di feedback dei contattori di Potenza	Confronto	OTHER THAN	Confronto errato per parametri uguali
7 Linea di comunicazione CAN	Trasferimento dati	NO	Nessun trasferimento dati
		PART OF	Dati incompleti
		OTHER THAN	Dati completi ma errati
8 Sensore di corrente	Corrente	NO	Nessuna corrente rilevata
		LESS	Corrente rilevata più bassa di quella effettiva
		MORE	Corrente rilevata più alta di quella effettiva
10 Monitor per la verifica della resistenza di isolamento tra il case e le due linee che collegano la batteria	Trasferimento dati	NO	Nessun trasferimento dati
		PART OF	Dati incompleti
11 Fusibile di batteria.	Corrente di apertura	MORE	Corrente di apertura maggiore rispetto a quella di progetto
		LESS	Corrente di apertura minore rispetto a quella di progetto
12 Daisy chain percorso primario	Trasferimento dati	NO	Nessun trasferimento dati
		PART OF	Dati incompleti
13 Daisy chain percorso secondario	Trasferimento dati	NO	Nessun trasferimento dati
		PART OF	Dati incompleti
14 Slave BMS chip monitor primario	Elaborazione dati	NO	Elaborazione dati assente
		OTHER THAN	Elaborazione dati errata
15 Slave BMS chip monitor secondario	Elaborazione dati	NO	Elaborazione dati assente
		OTHER THAN	Elaborazione dati errata
16 Connettore unico per prelievo delle tensioni di cella e di modulo	Corrente	NO	Assenza di collegamento
		LESS	Bassa corrente
		MORE	Alta corrente
17 Connettore unico per il prelievo di 8 punti di temperatura all'interno del modulo.	Corrente	NO	Assenza di collegamento
		MORE	Corrente superiore al valore corrispondente alla temperatura effettiva

6.4 Severità del danno

Nel presente studio viene presa a riferimento la classificazione della severità suggerita all'interno dello studio EUCAR che originariamente era stata introdotta per valutare la severità di un evento pericoloso a livello della cella.

In questa classificazione ad ogni pericolo rilevato viene assegnata una categoria, da 0 a 7, che rappresenta, in ordine crescente, la severità del pericolo considerato. Dato lo scopo del presente studio partendo da tale classificazione si è semplificato limitando l'assegnazione della severità a due sole categorie, la prima definita "BASSA" e comprendente tutti quegli eventi che non possono avere ricadute al di fuori della cella o del modulo e quindi per il pubblico, la seconda categoria definita "ALTA" comprende tutte quelle sequenze incidentali che hanno il potenziale di mettere a rischio le persone.

Tabella 4. Severità del danno secondo EUCAR e correlazione con quella adottata nel presente studio

Severità secondo EUCAR	***Severità adottata nel presente studio***	***Descrizione***	***Criteri per l'assegnazione del grado di severità***
0	**BASSA**	Nessun effetto	Nessun effetto. Nessuna perdita funzionale.
1		Perdita di funzionamento reversibile	Nessun difetto, nessuna perdita, nessuna espulsione di gas, no fiamme o incendi. Temporanea perdita funzionale della batteria. Necessità di ri-settare il dispositivo di protezione intervenuto.
2		Difetto/Danneggiamento irreversibile	Nessuna perdita, nessuna espulsione di gas, no fiamme o incendi, nessuna reazione esotermica o "thermal runaway" Batteria irreversibilmente danneggiata, necessità di riparazione.
3		Perdita di massa (<50%)	No venting, nessuna fiamma, nessuna rottura, nessuna esplosione. Perdita di massa <50% rispetto al peso dell'elettrolita. Fumo leggero prodotto dall'evaporazione dell'elettrolita (solvente e sale).
4	**ALTA**	Venting (>50% della massa)	Nessuna fiamma, nessuna rottura, nessuna esplosione. Perdita in peso dell'elettrolita >=50%. Fumo pesante prodotto dall'espulsione dell'elettrolita (solvente e sale) dal vent.
5		Fiamma o incendio	Nessuna rottura, nessuna esplosione. (no produzione di proiettili)
6		Rottura	Nessuna esplosione. La batteria può pure disintegrarsi ma lentamente, senza produzione di missili o rilasci istantanei di energia termica o cinetica.
7		Esplosione	Esplosione (disintegrazione della batteria con potenziale produzione di missili e liberazione di energia termica). Esposizione a sostanze tossiche in concentrazioni superiore ai limiti OSHA.

6.5 Gruppo di lavoro e partecipanti all'analisi HAZOP

Il gruppo di lavoro che ha effettuato, tramite brainstorming, l'analisi di sicurezza del Fox BMS è composto dai gruppi di lavoro del Dipartimento di Ingegneria Civile e Industriale (DICI) e del Dipartimento di Ingegneria dell'Informazione (DII) dell'Università di Pisa. Il gruppo di lavoro del DICI ha competenze in applicazione delle tecniche di analisi del rischio mentre il gruppo di lavoro del DII ha fornito il know-how in ambito di elettronica e conoscenze specifiche di diversi tipi di BMS per diverse applicazioni.

Di seguito si riportano i nominativi dei partecipanti alle riunioni durante le quali è stata svolta l'analisi HAZOP:

- per il DICI:
    - Ing. Martino Schiavetti
    - Ing. Tommaso Pini
    - Prof. Marco Carcassi
- Per il DII:
    - Prof. Roberto Roncella
    - Prof. Roberto Saletti
    - Prof. Federico Baronti
    - Ing. Andrea Carloni
    - Ing. Roberto di Rienzo

6.6 Schede analisi HAZOP

A livello pratico tutte le informazioni sono state raccolte in una tabella che prevede le colonne identificate di seguito:

- **Id#**: Identificativo della sequenza incidentale analizzata
- **Elemento**: Costituente della parte del quale si identificano una o più caratteristiche importanti per l'esercizio del sistema
- **Caratteristica**: Proprietà qualitativa o quantitativa di un elemento alla quale viene applicata la parola guida per ricercare deviazioni dal normale funzionamento, cause e conseguenze
- **Parola guida**: parola chiave utilizzata in riferimento al parametro sotto studio (Tensione, Corrente, Elaborazione dati, etc.) per determinare la deviazione;
- **Deviazione**: Deviazione dal normale esercizio del sistema;
- **Possibile causa**: Riporta le cause che possono concorrere al verificarsi della deviazione precedentemente identificata;
- **Conseguenza**: Descrive la conseguenza della sequenza incidentale considerata;
- **Severità del danno**: Indice qualitativo che indica il grado di severità dell'evento considerato;
- **Sistemi di sicurezza**: elenco di tutte le misure di protezione e sicurezza implementate sul sistema ed in grado di evitare o limitare i danni derivanti da una determinata deviazione dal normale funzionamento;
- **Commenti**: riporta eventuali commenti riguardanti incertezze o aspetti particolari inerenti la sequenza incidentale considerata;
- **REF#**: riferimento bibliografico ed assunzioni per la valutazione della sequenza incidentale;

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
1	Master BMS MCU primario	Elaborazione dati	No	Elaborazione dati assente	Errore nel codice BMS in memoria	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	In fase di boot dello MCU0 viene controllata l'integrità in memoria del programma	In caso di errore riscontrato il BMS e quindi il sistema non si attiva.
2					Una subroutine del programma in esecuzione si blocca	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	Wathcdog software BMS master apre i contattori e la catena di interlock se rileva un blocco dell'esecuzione	
3					Tutto il programma in esecuzione si blocca	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	Watchdog hardware resetta lo MCU0 e apre i contattori e la catena di interlock se rileva un blocco nell'esecuzione	
4			Other than	Elaborazione dati errata	BUG nell'esecuzione del programma	Non corretta interpretazione delle informazioni	ALTA	Confronto con MCU1 (gestito da software indipendente)	A livello hardware la comunicazione tra le due MCU è prevista, ma non è stata implementata a livello software. Per questo motivo lo MCU0 e lo MCU1 nella versione base del software del foxBMS non comunicano tra di loro, quindi non viene eseguito alcun confronto. Conseguentemente se è presente un bug nel software dello MCU0 tale per cui dei dati vengono intrepretati male, il BMS potrebbe entrare nello stato di sicurezza dove vengono aperte la catena di interlock e i contattori anche se lo MCU1 continua a funzionare correttamente.
5	Master BMS MCU secondario	Elaborazione dati	No	Elaborazione dati assente	Errore nel codice BMS in memoria	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	In fase di boot dello MCU0 viene controllata l'integrità in memoria del programma	In caso di errore riscontrato il BMS e quindi il sistema non si attiva.

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
6	Master BMS MCU secondario	Elaborazione dati	No	Elaborazione dati assente	Una subroutine del programma in esecuzione si blocca	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	Wathcdog software BMS master apre i contattori e la catena di interlock se rileva un blocco dell'esecuzione	
7					Tutto il programma in esecuzione si blocca	Impossibilità di utilizzare o conoscere lo stato del sistema	ALTA	Watchdog hardware resetta lo MCU0 e apre i contattori e la catena di interlock se rileva un blocco nell'esecuzione	
8			Other than	Elaborazione dati errata	BUG nell'esecuzione del programma	Non corretta interpretazione delle informazioni	ALTA	Confronto con MCU0 (gestito da software indipendente)	A livello hardware la comunicazione tra le due MCU è prevista, ma non è stata implementata a livello software. Per questo motivo lo MCU0 e lo MCU1 nella versione base del software non comunicano tra di loro, quindi non viene eseguito alcun confronto. Conseguentemente se è presente un bug nel software dello MCU1 tale per cui dei dati vengono intrepretati male, il BMS potrebbe entrare nello stato di sicurezza dove vengono aperte la catena di interlock e i contattori, anche se lo MCU0 continua a funzionare correttamente.
9	Catena di controllo e feedback interlock	Dati	No	Interruzione della comunicazione hardware tra catena inrterlock e MCU0 e/o MCU1	Danneggiamento del MOS che connette la linea di attuazione	Blocco del sistema	BASSA	Ogni linea di comunicazione ha una linea di feedback (più watchdog) che provvede a comunicare l'errore	I contattori sono 2 ed è sufficiente l'apertura di uno dei due per interrompere il circuito
10	Alimentazione di servizio	Tensione	No	Assenza di tensione	Interruzione dei contatti o batteria ausiliaria scarica	Impossibilità di utilizzare il sistema / blocco del sistema	BASSA		

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
11	Alimentazione di servizio	Tensione	No	Assenza di tensione	Salto del fusibile	Impossibilità di utilizzare il sistema / blocco del sistema	BASSA		
12	Alimentazione di servizio	Tensione	Less	Bassa tensione	Malfunzionamento del regolatore (sotto i 9 volt)	Impossibilità di utilizzare il sistema / blocco del sistema	BASSA	Provoca a catena un malfunzionamento sugli alimentatori a basse tensioni provocando un errore che viene rilevato e stacca il modulo	
13					Malfunzionamento del regolatore (sotto i 10 ma sopra i 9 volt)	Malfunzionamento dell'isolatore (isometer IR155) e la comunicazione CAN	BASSA	MCU0 e/o MCU1 si accorgono degli errori di comunicazione CAN e staccano il modulo al raggiungimento della soglia di errore	
14			More	Alta tensione	Rottura del regolatore sull'alimentazione del servizio	Possibile causa di un guasto multiplo sui Master del BMS (perdita di controllo del modulo)	ALTA	C'è un meccanismo che fa saltare il fusibile (Crossbar)	
15	Contattore di potenza	Connessione	More	Contattore sempre chiuso	Incollaggio (meccanico) del relais a causa di extracorrente di chiusura	Batteria non completamente isolata (per avere corrente si dovrebbero incollare entrambe)	ALTA	Presenza di due contattori sul circuito di alimentazione. Il sistema rileva il problema attraverso una linea di feedback	
16			No	Contattore sempre aperto	Danneggiamento della bobina o limitazione della corrente nella bobina	Impossibile avviare il sistema non viene avviato il motore	BASSA		
17	Catena di controllo e di feedback dei contattori di Potenza	Confronto	Other than	Confronto errato per parametri uguali	Rottura foto-accoppiatore o resistenza di pullup	Il confronto tra stato del contattore e quello di feedback provoca l'apertura del contattore e l'interruzione dell'alimentazione	BASSA	MCU0 confronta costantemente il valore impostato con il valore di feedback	

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
18	Linea di comunicazione CAN	Trasferimento dati	No	Nessun trasferimento dati	Interruzione fisica della linea (distacco di un connettore o corto circuito tra due conduttori)	Il BMS perde lo stato del sistema	ALTA	La periferica CAN si accorge di errori consecutivi ed apre i contattori e l'interlock	Se il controllore del veicolo "muore" (i.e. impatto del veicolo etc.), dopo un numero prefissato di operazioni il BMS entra nello stato di errore, apre i contattori e la catena di interlock. Solo MCU0 comunica con il controllore dell'auto ed è quindi l'unico che può gestire questa tipologia di errore.
19			Part of	Dati incompleti	Presenza di rumore elettromagnetico o di altro tipo sulla linea	Informazioni erronee verso il BMS	ALTA	C'è un controllo di CRC che comunica errore in caso che i dati trasmessi siano corrotti. In prima istanza ignora il messaggio (trasmettendo un error frame) e ritrasmette il messaggio aggiornando il contatore degli errori. Se il contatore degli errori supera una soglia lo comunica al software MCU0 che stacca (Apre contattori e interlock).	il CRC (Cyclic Redundancy Check) è un metodo che permette di verificare la presenza di errori sui dati trasmessi sulla linea CAN.

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
20	Linea di comunicazione CAN	Trasferimento dati	Other than	Dati completi ma errati	Software del veicolo invia un dato errato	Informazioni erronee verso il BMS	ALTA	C'è un controllo di CRC che comunica errore in caso che i dati trasmessi siano corrotti. In prima istanza ignora il messaggio (trasmettendo un error frame) e ritrasmette il messaggio aggiornando il contatore degli errori. Se il contatore degli errori supera una soglia lo comunica al software MCU che stacca.	il CRC (Cyclic Redundancy Check) è un metodo che permette di verificare la presenza di errori sui dati trasmessi sulla linea CAN.
21					Sensore di corrente invia un dato errato (variazioni di accuratezza della resistenza - per uscita dalle condizioni operative per un determinato tempo)	Mancato rilevamento di una sovracorrente	ALTA	Il sensore di corrente è in grado di capire se la misura è affidabile o no. Ha internamente 2 ADC, se dal confronto delle due misure la differenza supera un valore prefissato la misura viene ritenuta non affidabile e la notifica dell'errore viene inserita nel pacchetto. I fusibili proteggono contro il cortocircuito. Le temperature vengono sempre monitorate ma agiscono con ritardo	Dei due ADC uno campiona sempre e solo la corrente e l'altro intervalla misure di corrente e tensione. Quando il secondo sensore campiona la corrente viene effettuato il confronto. Il sensore di corrente è in grado di notificare un fault sulla misura di corrente al BMS, ma attualmente nella versione base del software del foxBMS questa tipologia di errore non viene trattata. Nella linea di comunicazione CAN non sono presenti fusibili.
22	Sensore di corrente	Corrente	No	Nessuna corrente	Rottura del sensore di corrente	Nessuna. Sistema fermo come per apertura dell'interlock.	BASSA		

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
23	Sensore di corrente	Corrente	Less	Corrente rilevata più bassa di quella effettiva	Abuso subito dal misuratore di corrente	Sottostima di una sovracorrente. Rischio di accettare un valore sovrasoglia per un tempo indefinito	ALTA	Il sensore di corrente è in grado di capire se la misura è affidabile o no. Ha internamente 2 ADC, se dal confronto delle due misure la differenza supera un valore prefissato la misura viene ritenuta non affidabile e la notifica dell'errore viene inserita nel pacchetto.	Dei due ADC uno campiona sempre e solo la corrente e l'altro intervalla misure di corrente e tensione. Quando il secondo sensore campiona la corrente viene effettuato il confronto.
24			More	Corrente rilevata più bassa di quella effettiva	Abuso subito dal misuratore di corrente	Possibile intervento per sovracorrente quando non ce n'è bisogno.	BASSA	Il sensore di corrente è in grado di capire se la misura è affidabile o no. Ha internamente 2 ADC, se dal confronto delle due misure la differenza supera un valore prefissato la misura viene ritenuta non affidabile e la notifica dell'errore viene inserita nel pacchetto.	Dei due ADC uno campiona sempre e solo la corrente e l'altro intervalla misure di corrente e tensione. Quando il secondo sensore campiona la corrente viene effettuato il confronto.
25	Monitor per la verifica della resistenza di isolamento tra il case e le due linee che collegano la batteria (IR155)	Trasferimento dati	No	Nessun trasferimento dati	Linea interrotta	Nessuna. Sistema fermo per apertura dell'interlock e contattori.	BASSA	In assenza di segnale di ritorno il BMS provoca l'apertura dei contatti e l'interlock	Il rilevamento del segnale avviene ogni millisecondo

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
26	Monitor per la verifica della resistenza di isolamento tra il case e le due linee che collegano la batteria (IR155)	Trasferimento dati	Part of	Dati incompleti	Ricevimento di una forma di segnale (per frequenza o distanza tra salita e discesa) fuori specifica rispetto al funzionamento del generatore di forma d'onda	Nessuna. Isolamento comunque presente	BASSA	La ricezione di una forma d'onda non corretta porta al distacco del modulo (il controllo è ciclico e continuo)	Misura la distanza tra due fronti in salita (tra 50 e 100 ms) e la distanza tra salita e discesa.
27	Fusibile di batteria	Corrente di apertura	More	Corrente di apertura maggiore rispetto al progetto	Errore di montaggio del tipo di fusibile	Rischio di corrente di corto circuito su elementi attivi del sistema (brucerà un elemento diverso dal fusibile e provocherà un principio di incendio)	ALTA		Il fusibile deve essere ben dimensionato. La sostituzione del fusibile deve essere effettuata da personale autorizzato. Normalmente il fusibile interviene solo per un corto circuito esterno importante (a seguito di un incidente o di operazioni non corrette di manutenzione)
28			Less	Corrente di apertura minore rispetto al progetto	Errore di montaggio del tipo di fusibile	Mancanza di operatività per salto del fusibile in condizioni operative corrette	BASSA		
29	Daisy chain percorso primario	Trasferimento dati	No	Nessun trasferimento dati	Interruzione cavi o disconnessione del connettore	Il BMS perde lo stato del sistema	ALTA	L'MCU0 o 1 attiva l'interlock ed apre i contattori.	

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
30	Daisy chain percorso primario	Trasferimento dati	Part of	Dati incompleti	Rumore elettrico o rumore elettromagnetico generato da interferenze col motore	Il BMS perde parzialmente lo stato del sistema	ALTA	Per ogni dato inviato c'è un'analisi CRC che riconosce i dati errati (in questo caso il dato non viene ritrasmesso, perché la trasmissione è periodica). Il numero dei dati consecutivi che devono risultare errati è 500 prima di aprire il contattore, in caso di dati errati in fila corrisponde a 0.5 s)	
31	Daisy chain percorso secondario	Trasferimento dati	No	Nessun trasferimento dati	Interruzione cavi o disconnessione del connettore	Il BMS perde lo stato del sistema	ALTA	L'MCU0 o 1 attiva l'interlock ed apre i contattori.	
32			Part of	Dati incompleti	Rumore elettrico o rumore elettromagnetico generato da interferenze col motore	Il BMS perde parzialmente lo stato del sistema	ALTA	Per ogni dato inviato c'è un'analisi CRC che riconosce i dati errati (in questo caso il dato non viene ritrasmesso, perché la trasmissione è periodica). Il numero dei dati consecutivi che devono risultare errati è 500 prima di aprire il contattore, in caso di dati errati in fila corrisponde a 0.5 s)	
33	Slave BMS chip monitor primario	Elaborazione dati	No	Elaborazione dati assente	Malfunzionamento del chip monitor dedicato	Il BMS master perde comunicazione col chip monitor in lettura (anche se si riavvia il chip monitor si avvia in stato reset)	ALTA	Il watchdog sul chip monitor lo resetta Il BMS master rileva il problema dal momento che anche se si riavvia il chip monitor lo fa in stato reset	

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
34	Slave BMS chip monitor primario	Elaborazione dati	Other than	Elaborazione dati errata	Malfunzionamento del convertitore	Misure inconsistenti delle celle	ALTA	La catena di misura MCU0 e MCU1 è indipendente e completamente ridondante. In caso di malfunzionamento del convertitore sulla catena di una cella l'altra se ne accorge al momento che il parametro esce dalle condizioni operative	
35	Slave BMS chip monitor secondario	Elaborazione dati	No	Elaborazione dati assente	Malfunzionamento del chip monitor dedicato	Il BMS master perde comunicazione col chip monitor in lettura (anche se si riavvia il chip monitor si avvia in stato reset)	ALTA	Il watchdog sul chip monitor lo resetta Il BMS master rileva il problema dal momento che anche se si riavvia il chip monitor lo fa in stato reset	
36			Other than	Elaborazione dati errata	Malfunzionamento del convertitore	Misure inconsistenti delle celle	ALTA	La catena di misura MCU0 e MCU1 è indipendente e completamente ridondante. In caso di malfunzionamento del convertitore sulla catena di una cella l'altra se ne accorge al momento che il parametro esce dalle condizioni operative	

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
37	Connettore unico per prelievo delle tensioni di cella e di modulo	Corrente	No	Assenza di collegamento	Rottura del collegamento	Perdita di comunicazione con 2 celle, e perdita di bilanciamento delle celle stesse	ALTA	In teoria il chip monitor può rilevare l'interruzione di un collegamento attraverso un'istruzione chiamata ADOW. Il BMS nella versione base non ha alcuna funzione/algoritmo che possa attivare questo comando.	Se un collegamento tra le celle di un modulo e il BMS slave dovesse saltare, la tensione ai capi del condensatore collegato alla linea rimarrebbe pari all'ultima rilevata. Successivamente, quando il condensatore inizia a scaricarsi per la presenza di correnti parassite, agisce sui diodi in due modi potenzialmente diversi ma che portano entrambe alla rilevazione dell'errore da parte del BMS con apertura dei contattori e dell'interlock. Le tempistiche relative al blocco del sistema a seguito della disconnessione ipotizzata sono difficili da calcolare e dipendenti dalle correnti parassite che si instaurano.
38			Less	Bassa corrente	Percorso resistivo	Il bilanciamento non avviene nei tempi usuali o non avviene	BASSA		La misura di tensione è un'altissima impedenza (la misura è corretta anche in caso di filo resistivo)
39			More	Alta corrente	Corto della resistenza di bilanciamento	Cella in corto in fase di bilanciamento	ALTA	Presenza di un fusibile sul filo che collega la cella al chip monitor	
40					Apertura del circuito di potenza	Nessuna.	BASSA	Presenza di un fusibile sul filo che collega la cella al chip monitor	
41	Connettore unico per il prelievo di 8 punti di temperatura all'interno del modulo.	Corrente	No	Assenza di collegamento	Rottura del collegamento	Nessuna.	BASSA	Viene rilevato come una temperatura bassissima (sotto soglia). Interviene il BMS per parametro fuori dalla operating area.	Le misure di temperatura sono 8 a fronte di 12 celle controllate da ogni slave. La disposizione degli 8 punti di misura risulta quindi fondamentale per anticipare correttamente ogni deviazione.
42	Connettore unico per il prelievo di 8 punti di temperatura all'interno del modulo.	Corrente	More	Corrente superiore al valore corrispondente allo stato di temperatura	Corto circuito del sensore di temperatura	Nessuna.	BASSA	Viene rilevato come una temperatura altissima (sopra soglia). Interviene il BMS per parametro fuori dalla operating area.	Le misure di temperatura sono 8 a fronte di 12 celle controllate da ogni slave. La disposizione degli 8 punti di misura risulta quindi fondamentale per anticipare correttamente ogni deviazione.

7 Risultati HAZOP

I risultati ottenuti dall'applicazione della metodologia HAZOP al foxBMS hanno evidenziato come, anche grazie alla progettazione in accordo alla ISO 26262, in caso di malfunzionamenti del BMS, questo è in grado di rilevare situazioni indesiderate e di intervenire per evitare o limitarne gli effetti negativi. Risulta fondamentale l'architettura hardware del BMS che, oltre ai sensori di misura e ai sistemi di elaborazione dati, prevede elementi di ridondanza di sicurezza e di rilevazione degli errori. Inoltre è indispensabile la corretta comunicazione tra il sistema BMS/batteria e il carico, in modo che la gestione sia ottimizzata, soprattutto in relazione all'utilizzo finale.

Tuttavia elemento di fondamentale importanza è la corretta programmazione del software. L'analisi ha evidenziato la mancanza di comunicazione software tra MCU0 e MCU1 nella versione base del foxBMS. Anche se la corretta esecuzione di uno dei due microprocessori risulta sufficiente a rilevare un eventuale problema ed interrompere l'erogazione di potenza della batteria, la comunicazione tra le due MCU potrebbe segnalare la non corretta esecuzione di uno dei due processi ed anticipare malfunzionamenti prima di portare all'interruzione dell'erogazione di potenza.

Inoltre non è prevista l'elaborazione degli errori provenienti del sensore di corrente. La rilevazione di un simile guasto avviene comunque, ma con tempistiche difficili da prevedere; in particolare è impossibile valutare se tali tempistiche sono sufficienti ad anticipare una potenziale situazione di pericolo effettivamente presente sulla cella che non viene più monitorata.

Questi due aspetti rappresentato due criticità, e possono essere migliorati per incrementare la sicurezza del sistema.

Un altro punto di criticità è rappresentato dalla misura di 8 temperature per ogni modulo di 12 celle. I sensori cioè non prelevano il dato per ogni singola cella, ma in 8 punti tra le 12 celle. E' fondamentale che i punti di prelievo siano significativi al fine di monitorare correttamente lo stato delle celle e permettere al BMS di intervenire in caso di malfunzionamento. In questo caso è opportuno sottolineare come il foxBMS sia stato progettato e realizzato per un'ampia gamma di utilizzi, tra cui l'automotive. L'utilizzo del BMS in un applicazione automotive commerciale e non di ricerca comporterebbe l'assoggettamento dell'intero sistema alla ISO 26262. Tale applicazione dovrebbe verificare se gli aspetti sottolineati sono gestiti dalla configurazione attuale o se un miglioramento della strategia di misura risulti necessario.

8 Conclusioni

Il presente studio ha dettagliato l'intervento di uno specifico BMS, fox-BMS, in riposta alle deviazioni dal normale funzionamento di una cella litio-ione tipo NMC determinate in una precedente analisi di sicurezza. Infatti la citata analisi ha messo in evidenza come sia il BMS che il sistema di condizionamento (raffreddamento e/o riscaldamento) dei moduli batteria rappresentino sistemi critici sia per la gestione che per la sicurezza del sistema nel suo complesso.

Rispetto alle deviazioni messe in evidenza dall'analisi e per le quali l'intervento del BMS era stato preso in considerazione come safeguard, è stato descritto ed analizzato in dettaglio l'intervento del fox-BMS.

Lo studio ha evidenziato gli interventi del BMS in risposta alle deviazioni dal normale funzionamento della batteria individuate nel corso dell'analisi applicata alla cella [8]. Nella maggior parte dei casi il sistema è programmato per rilevare un funzionamento non corretto e disconnettere il pacco batteria dal carico prima del verificarsi di situazioni ancora più gravose.

Una criticità rilevata è relativa al corto circuito interno, che potrebbe essere non rilevato in funzione della zona in cui questo si verifica. Il rilevamento in questo caso è importante per avvertire gli occupanti del veicolo, non ci sono comunque azioni possibili da parte del BMS per influire sul decorso dell'incidente.

Il BMS a veicolo fermo può essere funzionante o meno. In questo caso la batteria è comunque disconnessa e non eroga potenza, ma il BMS attivo potrebbe innescare degli allarmi in caso verificasse delle condizioni anomale.

E' da segnalare inoltre come nella presente versione del BMS non sia attivo a livello software un controllo nel caso in cui il feedback e lo stato di controllo del bilanciamento sono discordanti. Questo potrebbe comportare il mancato bilanciamento di una delle celle provocando effetti immediati sull'efficienza e la vita del pacco ed un peggioramento delle condizioni di sicurezza dello stesso.

Inoltre nel presente studio la tecnica HAZOP è stata applicata per determinare le deviazioni dal normale funzionamento, che possono provocare sequenze incidentali pericolose per il sistema autoveicolo ed i suoi utilizzatori, dello stesso BMS collegato ad un sistema di accumulo di un veicolo elettrico.

I risultati ottenuti dall'applicazione della metodologia HAZOP al foxBMS hanno evidenziato come, anche grazie alla progettazione in accordo alla ISO 26262, in caso di malfunzionamenti del BMS, questo è in grado di rilevare situazioni indesiderate e di intervenire per evitare o limitarne gli effetti negativi. Risulta fondamentale l'architettura hardware del BMS che, oltre ai sensori di misura e ai sistemi di elaborazione dati, prevede elementi di ridondanza di sicurezza e di rilevazione degli errori. Inoltre è indispensabile la corretta comunicazione tra il sistema BMS/batteria e il carico, in modo che la gestione sia ottimizzata, soprattutto in relazione all'utilizzo finale.

Tuttavia elemento di fondamentale importanza è la corretta programmazione del software. L'analisi ha evidenziato la mancanza di comunicazione software tra MCU0 e MCU1 nella versione base del foxBMS. Anche se la corretta esecuzione di uno dei due microprocessori risulta sufficiente a rilevare un eventuale problema ed interrompere l'erogazione di potenza della batteria, la comunicazione tra le due MCU potrebbe segnalare la non corretta esecuzione di uno dei due processi ed anticipare malfunzionamenti prima di portare all'interruzione dell'erogazione di potenza.

Inoltre non è prevista l'elaborazione degli errori provenienti del sensore di corrente. La rilevazione di un simile guasto avviene comunque, ma con tempistiche difficili da prevedere; in particolare è impossibile valutare se tali tempistiche sono sufficienti ad anticipare una potenziale situazione di pericolo effettivamente presente sulla cella che non viene più monitorata.

Questi due aspetti rappresentato due criticità, e possono essere migliorati per incrementare la sicurezza del sistema.

Un altro punto di criticità è rappresentato dalla misura di 8 temperature per ogni modulo di 12 celle. I sensori cioè non prelevano il dato per ogni singola cella, ma in 8 punti tra le 12 celle. E' fondamentale che i punti di

prelievo siano significativi al fine di monitorare correttamente lo stato delle celle e permettere al BMS di intervenire in caso di malfunzionamento. In questo caso è opportuno sottolineare come il foxBMS sia stato progettato e realizzato per un'ampia gamma di utilizzi, tra cui l'automotive. L'utilizzo del BMS in un applicazione automotive commerciale e non di ricerca comporterebbe l'assoggettamento dell'intero sistema alla ISO 26262. Tale applicazione dovrebbe verificare se gli aspetti sottolineati sono gestiti dalla configurazione attuale o se un miglioramento della strategia di misura risulti necessario.

8.1 Criticità

Le criticità insite nel presente studio risiedono nella mancanza di informazioni dettagliate sulla relazione esistente tra il foxBMS ed il sistema di accumulo. Tali relazioni nel presente studio sono state definite a livello teorico e non si riferiscono ad un'applicazione realmente esistente. L'esempio più chiaro di questo aspetto è la gestione delle 8 temperature acquisite sulle 12 celle. Il posizionamento degli strumenti che rilevano la temperatura è infatti critico per valutare se queste siano sufficienti ad identificare aumenti di temperatura nella cella con posizione più sfavorevole. Una valutazione in tal senso non può essere condotta in assenza di un layout specifico dei moduli e dei sensori posizionati al loro interno.

L'analisi è inoltre stata condotta esclusivamente in modo qualitativo. Per eseguire un'analisi di rischio quantitativa dovrebbero essere introdotti dati affidabilistici dei vari componenti e costituenti del sistema specifici per l'applicazione automotive.

L'assenza di dati riguardanti l'affidabilità dei componenti, in particolare eserciti nell'applicazione specifica, rende impossibile ed impropria l'estensione del presente studio ad una più accurata analisi del rischio quantitativa. Il presente studio si è limitato infatti nell'identificare delle possibili sequenze incidentali senza esprimersi sulla effettiva probabilità che tali sequenze incidentali possano effettivamente verificarsi.

Le suddette criticità sono quindi riassumibili nelle seguenti categorie:

- Mancanza di informazioni sui layout dei sistemi implementati
- Mancanza di dati di affidabilità per i sistemi ed i componenti (derivanti da applicazioni specificatamente automotive).

9 Abbreviazioni, acronimi e definizioni

ADC	Analog Digital Converter
ASIC	Application Specific Integrated Circuit
BDU	Battery Disconnect Unit
BEV	Battery Electric Vehicle
BMS	Battery Management System (Sistema elettronico associate ad un pacco di batterie che controlla e gestisce in modo sicuro lo stato elettrico e termico controllando l'ambiente e che comunica lo stato della batteria al controllore del Sistema nel suo complesso (es: Vehicle Management System (VMS) e/o Energy Management System (EMS)).
BPCS	Basic Process Control System
BUS	Binary Unit System
CAN	Controller Area Network
Caratteristica	Proprietà qualitativa o quantitativa di un elemento alla quale viene applicata la parola guida per ricercare deviazioni dal normale funzionamento, cause e conseguenze
CID	Current Interrupt Device
CMU	Cell Monitoring/Management Unit
Conseguenza	Effetto di un evento incidentale, valutato ai fini della presente analisi HAZOP esclusivamente in termini di rilascio (ubicazione, tipologia e portata/massa rilasciata).
CRC	Controller Redundancy Check
CSC	Cell Supervision/Sensor Unit
Danno	Entità della conseguenza negativa a seguito del verificarsi di un evento incidentale. La sua valutazione può essere fatta tramite funzioni matematiche o in termini qualitativi tramite parere di esperti; può quindi essere espressa sia in termini quantitativi (giorni di infortunio, perdite economiche, vite perdute), sia in termini qualitativi
EC	Ethylene Carbonate (Carbonato di etilene)
EMC	Ethymethyl Carbonate (Etilmetilcarbonato)
Elemento	Costituente della parte del quale si identificano una o più caratteristiche importanti per l'esercizio del sistema

EV	Electric vehicle (Veicolo elettrico)
Eventi Iniziatori	Evento (guasto, rottura, errore) che provoca una deviazione dal funzionamento ordinario del sistema, e che potrebbe dare origine ad una sequenza incidentale.
EVSE	Electric Vehicle Supply Equipment
Funzionamento ordinario	Funzionamento dell'impianto/sistema secondo le specifiche del costruttore.
HAZOP	Hazard and Operability Analysis.
HEV	Hybrid Electric Vehicle (Veicolo elettrico ibrido)
HV	High Voltage
IC	Integrated Circuit
IPL	Livello di Protezione Indipendente
LOPA	Layer of Protection Analysis
MCU	Monitor Control Unit
MMU	Module Management Unit
NMC	Nickel, Manganese, Cobalto
Parola guida	Parola che aiuta il processo sistematico di ricerca di deviazioni dal normale funzionamento della caratteristica dell'elemento considerato
Parte	Sezione del sistema presa a riferimento per lo sviluppo dell'analisi
Pericolo	Qualunque condizione di un sistema, dovuta a proprietà o qualità intrinseche delle sostanze in esso contenute, o derivante dalle condizione di funzionamento degli attrezzi, macchine, dispositivi ecc., potenzialmente in grado di causare danni ad un determinato target di riferimento (ambiente, popolazione etc.).
PMU	Pack Monitoring Unit
PVDF	Polivinildenfloruro
RTOS	Real Time Operating System
SEI	Solid Electrolyte Interphase
SIL	Safety Integrity Level
SOA	Safe Operation Area

SOC	State of Charge
SOH	State Of Health
SPI	Serial Peripheral Interface
SW	Software

10 Riferimenti bibliografici

1 D. Andrea, Battery management systems for large lithium-ion battery packs. Boston: Artech House, 2010.
2 B. Scrosati, J. Garche, and W. Tillmetz, Eds., Advances in battery technologies for electric vehicles. Amsterdam: WP, Woodhead Publishing/Elsevier, 2015.
3 P. Weicker, A systems approach to lithium-ion battery management. Boston: Artech House, 2014.
4 J. Muñoz Alvarez, M. Sachenbacher, D. Ostermeier, H. J. Stadlbauer, U. Hummitzsch, A. Alexeev (LION SMART), EVERLASTING (Electric Vehicle Enhanced Range, Lifetime And Safety Through INGenious battery management), D6.1 – Analysis of the state of the art on BMS, February 2017.
5 https://foxbms.org
6 https://media.readthedocs.org/pdf/foxbms/latest/foxbms.pdf
7 https://www.iisb.fraunhofer.de
8 M. Schiavetti, T. Pini, F. D'Errico, M. Carcassi, Studio sulla caratterizzazione dei vari livelli di protezione di sistemi di accumulo litio-ione per uso automotive, mediante "Layer Of Protection Analysis (LOPA)", (2017) Report RdS/PAR2016/242.
9 "ISO 26262-1: Road vehicles — Functional safety — Part 1 Vocabulary." International Organization for Standardization (ISO), 2011.
10 "ISO 26262-2: Road vehicles — Functional safety — Part 2 Management of functional safety." International Organization for Standardization (ISO), 2011.
11 "ISO 26262-3: Road vehicles — Functional safety — Part 3 Concept phase." International Organization for Standardization (ISO), 2011
12 "ISO 26262-4: Road vehicles — Functional safety — Part 4 Product development at the system level." International Organization for Standardization (ISO), 2011
13 "ISO 26262-5: Road vehicles — Functional safety — Part 5 Product development at the hardware level." International Organization for Standardization (ISO), 2011.
14 "ISO 26262-6: Road vehicles — Functional safety — Part 6 Product development at the software level." International Organization for Standardization (ISO), 2011.
15 "ISO 26262-7: Road vehicles — Functional safety — Part 7 Production and operation." International Organization for Standardization (ISO), 2011.
16 "ISO 26262-8: Road vehicles — Functional safety — Part 8 Supporting processes." International Organization for Standardization (ISO), 2011.
17 "ISO 26262-9: Road vehicles — Functional safety — Part 9 Automotive Safety Integrity Level (ASIL) oriented and safety-oriented analyses." International Organization for Standardization (ISO), 2011.

11 Curricula

Prof. Ing. Marco Nicola CARCASSI

Il Prof. Marco Carcassi tiene attualmente i corsi, presso la Scuola di Ingegneria dell'Università di Pisa, di: Sicurezza ed Analisi del Rischio, nel corso di laurea in Ingegneria Ingegneria Meccanica ed Ingegneria Gestionale, di Sicurezza Nucleare, nel corso di laurea Magistrale di Ingegneria Nucleare ed di Scienza e Tecnica della Prevenzione Incendi, nei corsi di laurea Magistrale in Ingegneria Nucleare e Ingegneria Civile.
Oltre ad essere stato responsabile scientifico di numerosi contratti di ricerca sia nazionali che internazionali, è stato Coordinatore Europeo di due progetti sul Rischio Idrogeno negli Impianti Nucleari condotto entro il IV FWP della UE e ha partecipato negli ultimi anni, a numerosi progetti europei (NoE HYSAFE -Hydrogen Safety- HYPER , H2FC , HYSEA) sull'uso dell'idrogeno e del metano. Ultimamente si è interessato alla tecnologia riguardante l'utilizzazione del GNL e la sicurezza nell'uso delle Batterie elettriche
Presidente del Comitato Organizzatore della serie dei convegni VGR (il più importante appuntamento biennale degli esperti di rischio), Presidente del Comitato Organizzatore della serie dei convegni ICHS (il più importante appuntamento internazionale biennale degli esperti di sulla sicurezza del Vettore Idrogeno), Past-President del Forum Italiano dell'Idrogeno (la più antica Associazione italiana nel settore del vettore energetico Idrogeno).
Membro del gruppo di lavoro del Comitato Centrale Tecnico Scientifico per la Prevenzione Incendi del Ministero dell'Interno. Comitato che ha predisposto la normativa per quanto riguarda il vettore idrogeno, le Stazioni di rifornimento di Metano e Metano liquido e l'uso del GNL negli impianti satelliti.
Fa parte di numerosi Comitati Scientifici di Enti, ed Associazioni attivi nel campo della ricerca.
Membro dell'ISO TC 197 (Hydrogen Technologies – Refueling stations)
Membro dell'EHSP (European Hydrogen Safety Panel)
Rappresentante Italiano in seno al IEA Task 37 Hydrogen Safety
Membro del Board della International Association for Hydrogen Safety, la maggiore associazione internazionale per l'uso del media Idrogeno che annovera più di 36 membri fra Istituti di ricerca pubblici internazionali, Autorità Nazionali, Università ed Industrie.
E' autore di circa 200 pubblicazioni principalmente relative alla sicurezza ed analisi del Rischio nel campo industriale e nucleare.

Ing. Martino Schiavetti – Curriculum.

L'Ing. Martino Schiavetti si è laureato in Ingegneria Nucleare nel 2006 presso l'Università di Pisa discutendo una tesi sperimentale sulle deflagrazioni ventate di idrogeno. Dal 2012 svolge la libera professione essendo iscritto all'Albo degli Ingegneri della Provincia di Pisa.
Dal 2006 collabora con l'Università di Pisa su progetti di ricerca inerenti la sicurezza industriale e dell'idrogeno comprendenti analisi di rischio di installazioni stoccaggio idrogeno e stazioni di servizio eroganti idrogeno. Ha eseguito per conto dell'Università di Pisa campagne di prove sperimentali di deflagrazioni ventate di idrogeno comprendenti la progettazione meccanica delle apparecchiature e l'acquisizione dati di tali prove. Ha partecipato a progetti europei quali HYSAFE, HYSEA e italiani, quali H2FC e HYDROSTORE.
Nel corso della vita professionale ha applicato tecniche di analisi del rischio, tra le quali What-if e Hazop, per processi autorizzativi, tra gli altri, di impianti stoccaggio GNL a servizio di distributori stradali, di impianti di stoccaggio GNL ricadenti in Seveso; per la verifica di procedure operative su campi di colata di altoforni e per validare operazioni non standard di riavviamenti dopo fermate di emergenza di altoforni. Ha effettuato analisi di rischio in applicazione della Norma ISO21001 per marcatura CE di reattori per produzione preparati chimici per conceria ed altri macchinari.
Ha inoltre esperienza nell'applicazione della direttiva ATEX ed utilizzato codici di calcolo CFD per la determinazione delle conseguenze di scenari incidentali.
E' autore o coautore di 13 pubblicazioni principalmente relative all'analisi di rischio e prove sperimentali di deflagrazioni ventate di idrogeno pubblicate sull'International Journal of Hydrogen Energy.