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

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Analisi HazOp specifica di BMS per applicazioni automotive (con riferimento a realizzazione qualificata automotive in ambito open hardware disponibile presso il Fraunhofer Institute)

F. Baronti, A. Carloni, R. Di Rienzo,
R. Roncella, R. Saletti

UNIVERSITÀ DI PISA

Report RdS/PAR2017/250

ANALISI HAZOP SPECIFICA DI BMS PER APPLICAZIONI AUTOMOTIVE (CON RIFERIMENTO A REALIZZAZIONE QUALIFICATA AUTOMOTIVE IN AMBITO OPEN HARDWARE DISPONIBILE PRESSO IL FRAUNHOFER INSTITUTE)

F. Baronti, A. Carloni, R. Di Rienzo, R. Roncella, R. Saletti (Università degli Studi di Pisa)

Settembre 2018

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico - ENEA
Piano Annuale di Realizzazione 2017
Area: Efficienza Energetica e risparmio di energia negli usi finali elettrici e interazione con altri vettori energetici
Progetto: D7 – Mobilità elettrica sostenibile
Obiettivo: Tecnologie e infrastrutture di ricarica di veicoli elettrici – Sicurezza dei sistemi di 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 HazOp specifica di BMS per applicazioni automotive (con riferimento a realizzazione qualificata automotive in ambito open hardware disponibile presso il fraunhofer institute"*
Responsabile scientifico ENEA: Cinzia Di Bari
Responsabile scientifico: Roberto Roncella

Indice

Sommario

Il presente rapporto inizialmente descrivere, in maniera dettagliata, tutti gli elementi che compongono l'architettura hardware e software di un BMS completamente open-source, il fox-BMS. Nella parte centrale del documento viene eseguita un'analisi sistematica, di tipo HazOp, sul sistema circuitale del fox-BMS. L'obbiettivo è quello di identificare tutte le possibili deviazioni dal normale funzionamento del sistema, associate ad ogni elemento circuitale del fox-BMS, che possono produrre sequenze incidentali potenzialmente pericolose (incendio, esplosione e rilascio di sostanze tossiche), sia per il sistema che per l'utilizzatore. Inoltre, il report si basa sulla determinazione delle cause responsabili della deviazione di sistema a livello circuitale e sulla descrizione degli elementi di prevenzione e di sicurezza previsti dal fox-BMS. La descrizione continua, con l'assegnazione della classificazione di rischio associata ad ogni deviazione di sistema individuata. In fine, facendo riferimento, a un'analisi HazOp condotta a livello di cella [1], vengono descritti gli elementi di sicurezza previsti dal fox-BMS che agiscono in risposta a una o più deviazioni inusuali del pacco batteria, causate da un evento scaturito a livello di cella.

1 Introduzione

Oggigiorno, i sistemi di accumulo dell'energia basati sulla tecnologia Litio-ione, sono sempre più utilizzati come sistema di alimentazione portatile partendo dai dispositivi elettronici di piccola taglia, come per esempio Smart-phone e tablet, fino ad arrivare a sistemi di propulsione per autoveicoli, navi e aeromobili. A supporto di questo, soprattutto nel settore della mobilità elettrica, in Italia il numero di veicoli elettrici venduti sino ad oggi rappresenta lo 0,1% del mercato totale. Percentuale, che in previsione, è destinata a crescere del 26% entro il 2020 [2].

Tuttavia, la tecnologia Litio-ione possiede un limite dal punto di vista della sicurezza del sistema di accumulo. Per esempio, il surriscaldamento del sistema, la sovraccarica, la sovra scarica possono condurre alla fuga termica del sistema. Ovvero, si possono innescare delle reazioni chimiche non desiderate caratterizzate da un'elevata velocità di reazione e di produzione di calore che sottopongono, potenzialmente, il sistema al rischio di esplosione e di incendio. Conseguenze che vanno, verosimilmente, a incidere sulla salute e sull'incolumità dell'utilizzatore. Per questo motivo, ENEA e i suoi partner, hanno deciso di intraprendere un progetto di ricerca triennale allo scopo di quantificare e gestire il rischio dovuto all'introduzione dei nuovi sistemi di accumulo elettrochimico basati sulla tecnologia Litio-ione in ambito automotive. I rapporti pubblicati, fino ad ora, mostrano i risultati derivanti dallo studio di valutazione del rischio a livello di cella di un sistema di questo tipo [1], ma allo stesso tempo evidenziano, come criticità, la mancata conoscenza delle specifiche funzioni di sicurezza e degli algoritmi implementati dal BMS.

Per quanto detto, il presente rapporto ha lo scopo di descrivere, in maniera dettagliata, tutti gli elementi che compongono l'architettura hardware e software di un BMS completamente open-source, il fox-BMS (free.open.flexible-BMS). Nella parte centrale del documento viene eseguita un'analisi sistematica, di tipo HazOp, sul sistema circuitale del fox-BMS. L'obbiettivo è quello di identificare tutte le possibili deviazioni dal normale funzionamento del sistema, associate ad ogni elemento circuitale del fox-BMS, che possono produrre sequenze incidentali potenzialmente pericolose (incendio, esplosione e rilascio di sostanze tossico), sia per il sistema che per l'utilizzatore. Inoltre, il rapporto si basa sulla determinazione delle cause responsabili della deviazione di sistema a livello circuitale e sulla descrizione degli elementi di prevenzione e di sicurezza previsti dal fox-BMS. La descrizione continua, con l'assegnazione della classificazione di rischio associata ad ogni deviazione di sistema individuata. In fine, facendo riferimento, a un'analisi HazOp condotta a livello di cella [1], vengono descritti gli elementi di sicurezza previsti dal fox-BMS che agiscono in risposta a una o più deviazioni inusuali del pacco batteria, causate da un evento scaturito a livello di cella.

La scelta del fox-BMS, piuttosto che: un BMS commerciale sviluppato direttamente da una ditta produttrice di autoveicoli elettrici; o di uno "CUSTOM" sviluppato a livello prototipale in laboratorio; risponde a due motivazioni.

Il primo motivo è dovuto al fatto che il fox-BMS è un sistema completamente open-source, sia a livello software che a livello hardware, ovvero, tutta la documentazione e i file sorgenti del sistema elettronico sono direttamente scaricabili e consultabili in [3]. La presenza di una documentazione libera ed aperta è di fondamentale importanza per portare a termine l'analisi HazOp che richiede l'individuazione di tutti gli elementi che compongono il sistema e la conoscenza delle loro funzionalità. Informazioni che sarebbero state di difficile estrazione se avessimo preso come riferimento un BMS commerciale.

Il secondo, può essere spiegato dal fatto che, se avessimo progettato un BMS a livello "CUSTOM" in laboratorio, molto probabilmente non avremmo potuto replicare esattamente tutti i sistemi di sicurezza a livello hardware e software previsti da un normale BMS commerciale per applicazioni di tipo automotive. Tuttavia, la versione attuale del fox-BMS è frutto di un esperienza quindicennale del Fraunhofer IISB nello sviluppo di BMS prototipali per applicazioni anche avanzate che richiedono alti livelli di affidabilità e sicurezza, come il settore automotive che fa riferimento allo standard di sicurezza ISO-26262 [4]. Pur non essendo un dispositivo direttamente utilizzabile per applicazioni commerciali, si adatta per la ricerca, lo sviluppo e il test di un BMS, a livello prototipale, per sistemi elettrochimici al Litio-ione con la stessa complessità e dimensioni dei sistemi tipicamente utilizzati in commercio e/o presenti nella letteratura scientifica del settore.

1 Architettura hardware

Come mostrato in Figura 1, il fox-BMS adotta un'architettura distribuita di tipo gerarchico su due livelli.

Il primo livello, quello più basso nella gerarchia, è composto da una o più schede BMS-slave. Ogni scheda BMS-Slave viene posizionata direttamente su un modulo della batteria e il numero di BMS-Slave è pari al numero di moduli che compongono il pacco batteria. Lo scopo di un BMS-Slave è quello di acquisire periodicamente tutte le tensioni di cella e le temperature di più punti distribuiti all'interno del modulo. Le singole informazioni acquisite non vengono processate dal BMS-slave; ma vengono inviate periodicamente al livello superiore. Inoltre, i BMS-Salve sono in grado di attivare il bilanciamento del modulo su comando del livello superiore.

Il secondo livello è composto da tre schede: il BMS-Master, il BMS-Extension e il BMS-Interface. IL BMS-Master è la scheda principale, che si occupa della gestione dell'intero pacco batteria. In particolar modo, processa i dati di tensione e temperatura acquisiti al livello inferiore, quelli ottenuti dal sensore di corrente e comunica i risultati dell'elaborazione all'unità di controllo superiore, che può essere ad esempio, il controllore dell'autoveicolo. Nella fase di analisi dei dati, il BMS-Master svolge tutte le funzioni descritte nel documento (Report rRd/PAR2017/249), tra cui la verifica del rispetto della SOA (Safe Operating Area) di ogni cella, controlla l'interruttore principale, gestisce l'equalizzazione e determina lo stato interno del pacco batteria. Inoltre, nel caso in cui, viene rilevata una potenziale situazione di rischio dovuta a un'anomalia hardware e/o software del sistema o scaturita da un malfunzionamento di una o più celle del pacco, il BMS-master è in grado di valutare la situazione di rischio e se necessario isolare il pacco batteria dal veicolo aprendo gli interruttori di potenza. In fine, il BMS-Interface e il BMS-Extension sono schede ausiliarie che permettono, rispettivamente, la comunicazione tra i BMS-Slave e il BMS-Master e forniscono un'interfaccia secondaria verso l'esterno.

In Figura 2, viene mostrata una possibile configurazione di sistema del fox-BMS. Il BMS-Master rappresenta l'unità centrale del sistema ed è l'unica dotata di "intelligenza". Grazie all'ausilio di due microcontrollori, quello primario e quello secondario (vedi paragrafo 1.11.1), il BMS-Master ha capacità di elaborazione dei dati, ma anche di tipo attuativo. Infatti, è in grado di produrre delle azioni sui dispositivi ad esso collegato con lo scopo di preservare il corretto funzionamento dell'intero pacco batteria.

I dispositivi ausiliari che il BMS-Master è in grado di controllare sono vari. In particolar modo il Bender ISO F1 è un dispositivo elettronico in grado di misurare la resistenza di isolamento tra le line di potenza HV+ e HV-, che collegano il pacco batteria al motore dell'autoveicolo, e la struttura di contenimento del pacco. La comunicazione con il BMS-Master avviene attraverso un'interfaccia galvanicamente isolata costituita da due segnali: uno digitale su due livelli logici e uno PWM. Il primo indica lo stato del misuratore, se sta funzionando correttamente o meno. Il secondo, invece, oltre che fornire informazioni sulla misura della resistenza di isolamento, fornisce informazioni di tipo diagnostico. Infatti, il misuratore è in grado di discriminare una tipologia di errore da un'altra, attraverso un encoder in frequenza. Per quanto riguarda la misura di corrente, il BMS-Master si affida al sensore di corrente IVT-300 appartenente alla famiglia degli shunt resistivi. Il sensore oltre che misurare correnti fino ±300 A è anche in grado di prelevare tre misure di tensione con una dinamica d'ingresso di ±600 V. Le misure di tensione vengono prelevate in corrispondenza dei terminali, positivo e negativo, di batteria e ai capi del resistore presente nella linea di precharge. Inoltre, il sensore è dotato di un microcontrollore dedicato, che attraverso l'algoritmo del coulomb counting, riesce a fornire al BMS-Master anche l'informazione sullo stato di carica del pacco batteria. Lo scambio di informazioni tra i due dispositivi avviene attraverso il protocollo CAN (Controller Area Network). Questo protocollo di comunicazione, nato per applicazioni automotive, è in grado di funzionare anche in ambienti fortemente disturbati da campi elettromagnetici. Attraverso lo stesso protocollo di comunicazione, il BMS-Master comunica periodicamente con il controllore di sistema a livello superiore, inviando tutte le acquisizioni delle tensioni di cella, delle temperature, della corrente e tutte le informazioni sullo stato interno del pacco batteria tra cui lo stato di carica, lo stato di potenza e lo stato di energia.

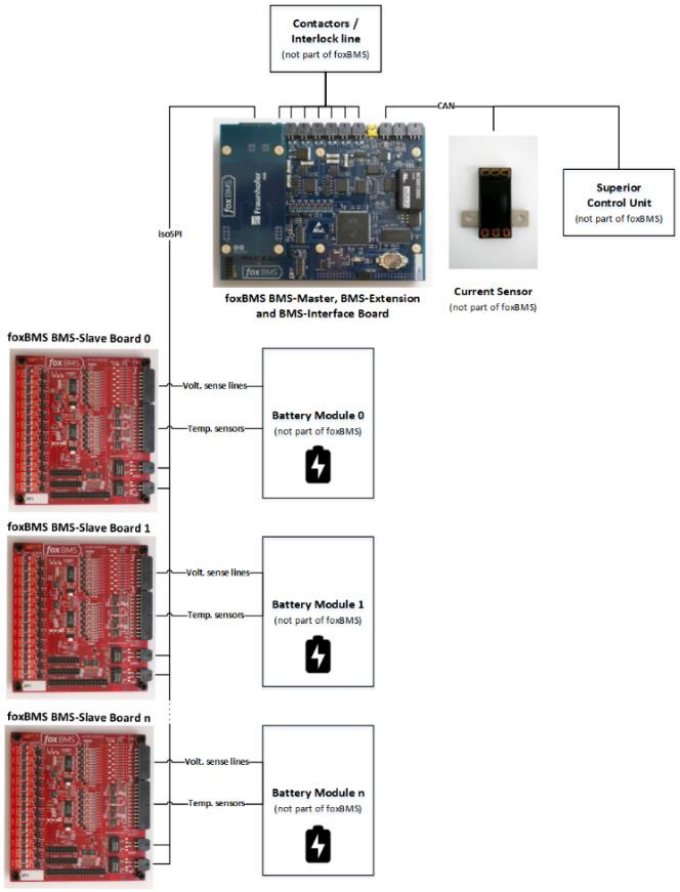

Figura 1 Architettura gerarchica del fox-BMS.

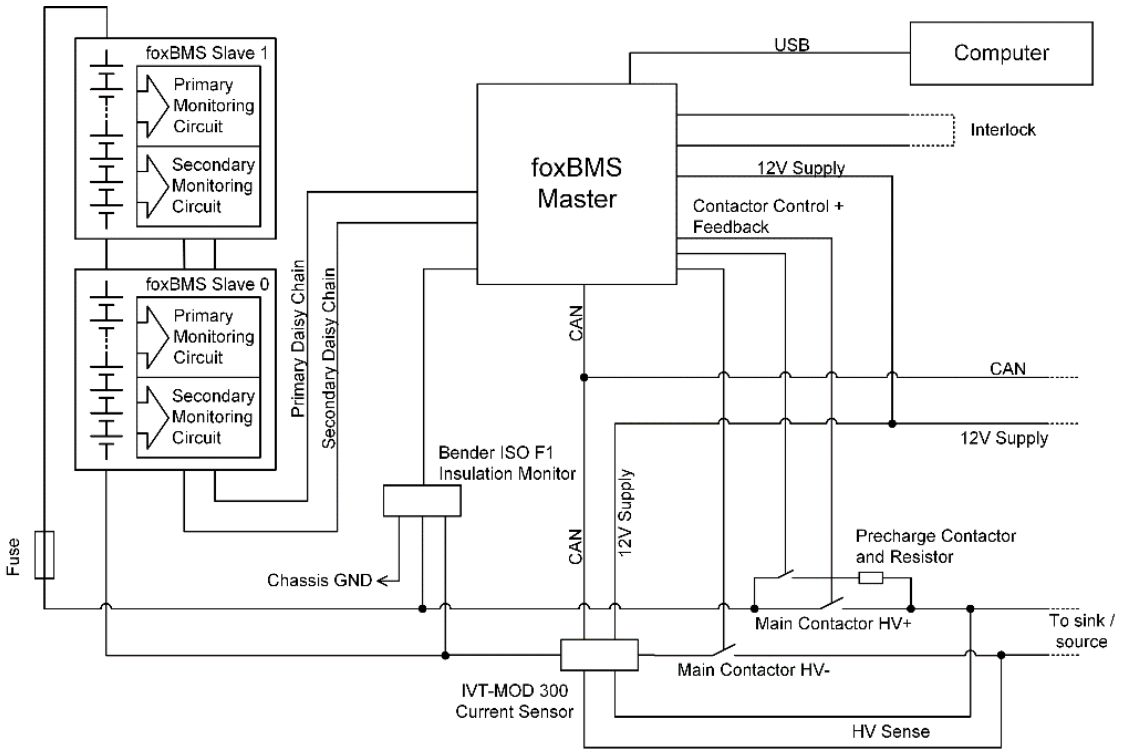

Figura 2 Configurazione del sistema fox-BMS

Inoltre, il BMS-Master controlla lo stato di tre interruttori meccanici di potenza normalmente aperti: il Main Conctactor HV+, il Main Conctactor HV- per connettere e/o isolare il pacco batteria al carico; il Precharge Contactor per collegare la linea di precharge al pacco batteria. Gli interruttori sono dei Gigavac GX14 in grado di sopportare correnti continue fino a 350 A. Gli interruttori, per ragioni di sicurezza, prevedono anche dei contatti ausiliari che permettono al BMS-Master di verificare se lo stato dell'interruttore corrisponde a quello effettivamente impostato. In questo modo il BMS-Master è in grado di discriminare una possibile criticità dovuta alla rottura di uno o più interruttori meccanici.

La comunicazione tra il BMS-Master e i BMS-Slave avviene attraverso il protocollo isoSPI (proprietario di Linear Technology); mentre a livello hardware, la linea di comunicazione tra i due dispositivi è galvanicamente isolata e assume una configurazione di tipo Daisy-Chain. All'interno della Daisy-Chain ogni BMS-Slave è collegato in serie l'uno rispetto all'altro. Quando il BMS-Master deve comunicare un comando agli slave, lo invierà al primo che lo eseguirà e lo propagherà al BMS-Slave successivo e così via, fino all'ultimo modulo. A sua volta la risposta al comando, precedentemente inviato dal BMS-Master, verrà inserita in un pacchetto dati. Il riempimento del pacchetto dati inizierà dall'ultimo BMS-Slave della Daisy-Chain, che riempirà l'area a sua disposizione con i dati raccolti, e a ritroso, propagherà il pacchetto al BMS-Slave successivo, fintanto che il pacchetto completo raggiungerà il BMS-Master per l'elaborazione dei dati. Questo meccanismo permette al fox-BMS di essere un sistema completamente modulare. Infatti, una volta definito il numero di celle all'interno di un modulo e il numero dei moduli che compongo il pacco batteria, basterà aggiungere un numero di BMS-Slave, in serie, pari al numero di moduli del pacco batteria, senza dover modificare l'hardware del BMS-Master. La modularità del sistema rende il fox-BMS un sistema molto flessibile (non a caso la lettera "x" dell'acronimo fox-BMS sta per "flexibility" che tradotto in italiano significa flessibilità).

In fine, ogni qualvolta si voglia usare il fox-BMS come sistema di gestione di un pacco batteria Litio-Ione, l'inserimento di un fusibile nel percorso di corrente del pacco batteria è obbligatorio. Infatti, il fusibile risulta estremamente utile in caso di cortocircuito esterno al pacco, ad esempio provocato da un incidente oppure da un malfunzionamento del motore dell'autoveicolo. In questo caso il fusibile, rompendosi, è in grado di fermare l'aumento incontrollato di corrente che potrebbe provocare seri danni sia al fox-BMS sia al pacco batteria, mettendo a serio rischio anche l'incolumità dell'utilizzatore.

1.1 il BMS-Master

Il BMS-Master, in Figura 3, come affermato precedentemente, è il sottosistema principale del fox-BMS. In Figura 4 viene rappresentato lo schema a blocchi, che identifica, l'architettura hardware del BMS-Master.

Partendo dall'alimentazione, il BMS-Master può essere alimentato con una tensione tra 12 V e 24 V. Generalmente, la sorgente di alimentazione è una batteria ausiliaria rispetto a quella Litio-ione. Entrando nel particolare, il sistema BMS-Master è suddiviso in due sottosistemi indipendenti e ridondanti, ognuno con un microcontrollore della famiglia ARM-Cortex M4 dedicato. Per come è stata progettata l'architettura di questo sottosistema, lo MCU_0 è in grado di: controllare lo stato degli interruttori meccanici; controllare le resistenza di isolamento tra il pacco batteria e la struttura di contenimento di quest'ultimo attraverso il Bender Isometer; comunicare con il controllore di sistema a livello superiore e con il sensore di corrente attraverso la linea di comunicazione CAN; salvare nella memoria EEPROM informazioni di tipo diagnostico sull'utilizzo del pacco batteria tra cui la temperatura e la corrente massima registrata; comunicare con un FPGA esterna che utilizza algoritmi dello stato interno del pacco più complessi del coulomb counting; comunicare con l'interfaccia RS485 con altri dispositivi.

Lo MCU_1 è il microcontrollore secondario utilizzato esclusivamente per scopi di ridondanza funzionale. Le funzioni che svolge sono ridotte rispetto a quelle che può svolgere lo MCU_0, ma assieme a quest'ultimo, controlla: l'acquisizione delle tensioni e le temperature di modulo; verifica che ogni cella del pacco lavori all'interno della sua SOA e agisce sulla linea di interlock. La linea di interlock è una linea condivisa dai due microcontrollori presenti nel BMS-Master: quello primario e quello secondario; entrambi sono in grado di leggere lo stato della linea e di interromperla attraverso degli opto-isolatori.

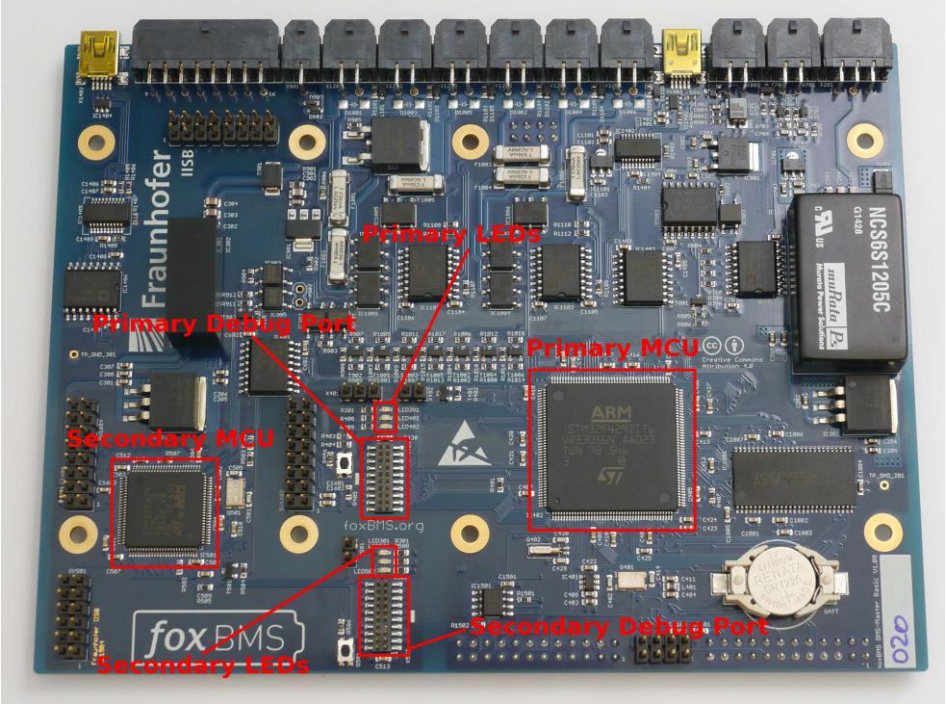

Figura 3 Circuito stampato BMS-Master

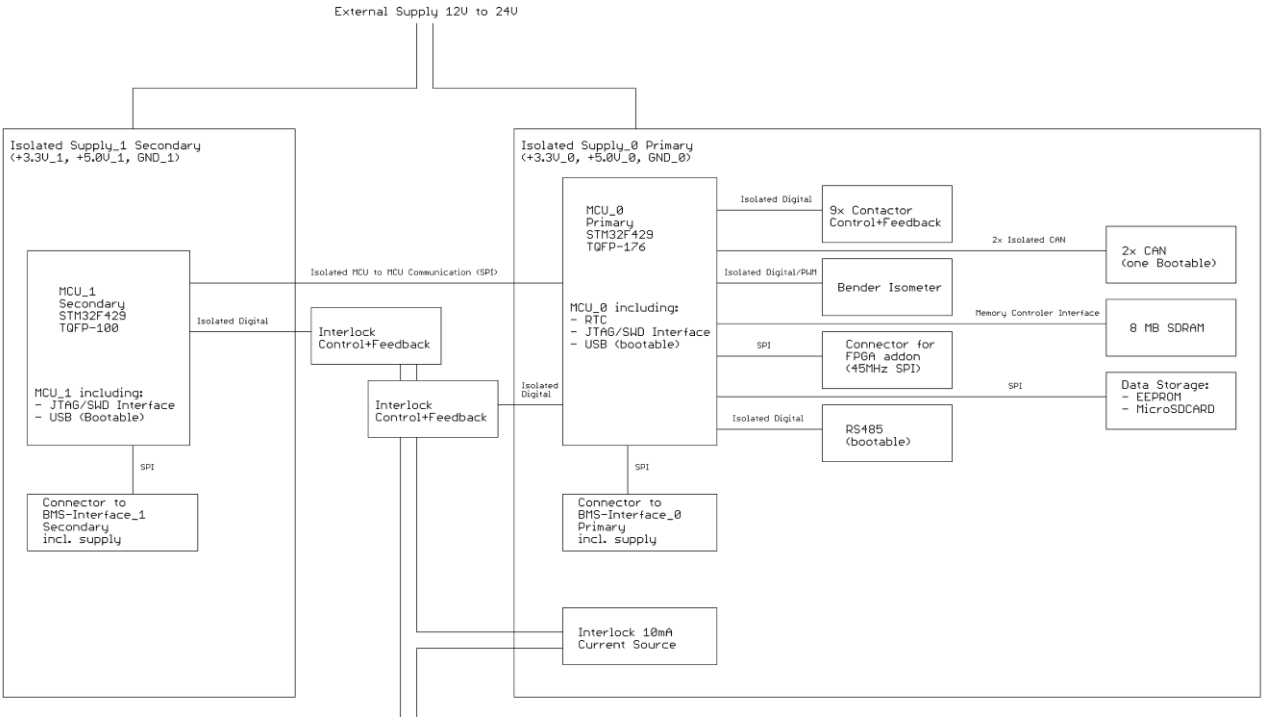

Figura 4 Architettura hardware BMS-Master.

Quando la linea di interlock viene interrotta, viene aperto il percorso di corrente verso massa, di tutte le bobine, di tutti gli interruttori meccanici che automaticamente si disattivano indipendentemente dallo stato in cui si trovavano. Come per gli interruttori meccanici anche la linea di interlock prevede dei segnali di feedback che permetto al BMS-Master di discriminare un possibile malfunzionamento degli optoisolatori che controllano la linea. Questa linea è un ulteriore dispositivo di sicurezza pensato, principalmente, per dare la possibilità anche al microcontrollore secondario di disattivare gli interruttori meccanici anche se non può controllare direttamente il loro stato. Grazie a questo meccanismo, se il sottosistema ridondante a cui appartiene lo MCU_1 individua un malfunzionamento può comunque isolare il pacco batteria dall'esterno, mettendo tutto il sistema in sicurezza.

In conclusione, a livello hardware, i due microcontrollori MCU_0 e MCU_1 possono scambiare informazioni tra di loro. La comunicazione tra i due è isolata galvanicamente e avviene attraverso il protocollo SPI (Serial Peripheral Interface). Seppur a livello hardware, lo scambio di informazioni tra i due sottosistemi del BMS-Master è possibile, nella versione base del software questa funzionalità non è stata implementata. Questo significa che al momento i due sottosistemi agiscono in maniera completamente separata senza influenzarsi l'uno con l'altro.

1.2 I BMS-Slave

L'unità BMS-Slave, Figura 5, è usata per acquisire direttamente, su un modulo del pacco batteria, le tensioni e le temperature di ogni cella. La struttura di un BMS-Slave, come per il BMS-Master, è completamente ridondante. Come mostrato in Figura 6, l'architettura è suddivisa in due sottosistemi completamenti simmetrici e indipendenti: quello primario e quello secondario. Il blocco principale di ogni sottosistema è il circuito integrato LTC6804-1 prodotto dall'azienda Linear-Technology (anche lo LTC6811-1 è compatibile con l'architettura del BMS-Slave). Lo LTC6804-1 e lo LTC6811-1 sono dei chip-monitor di batteria.

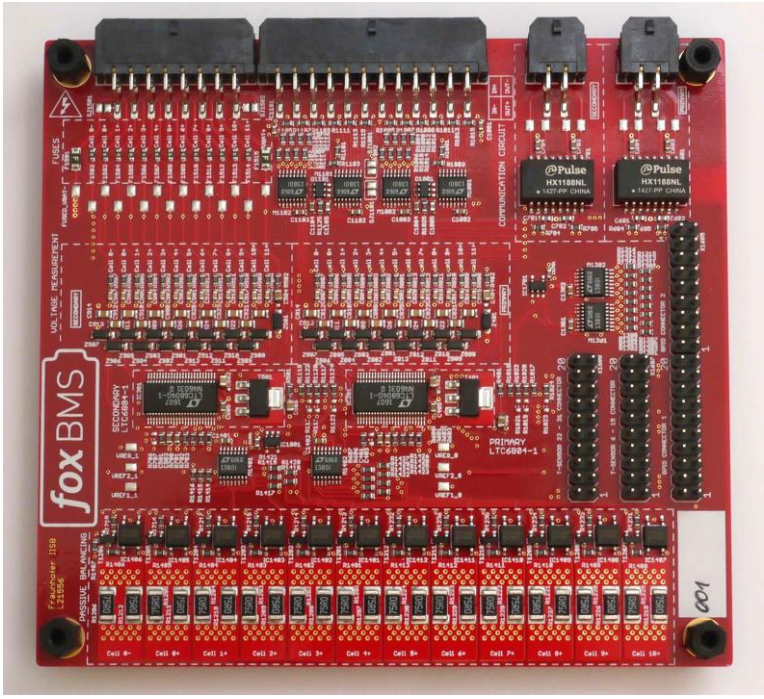

Figura 5 Circuito stampato BMS-Slave

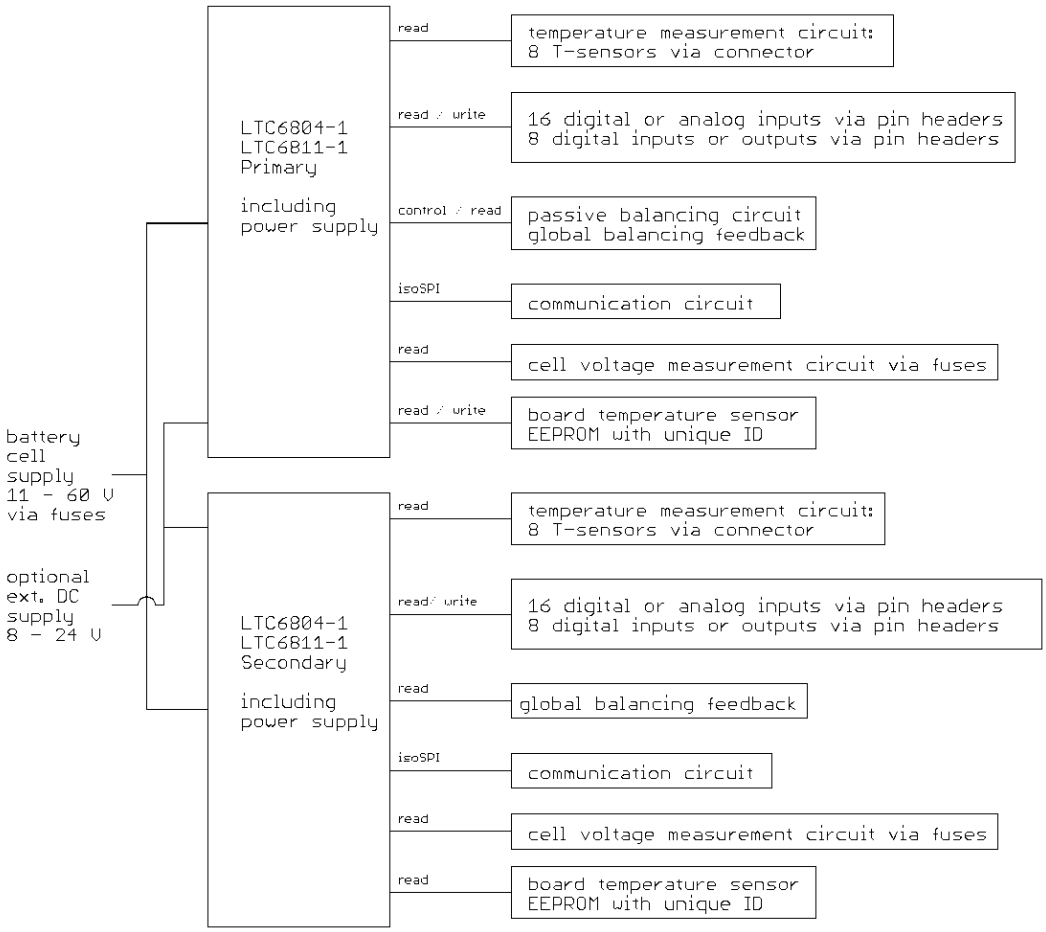

Figura 6: Architettura BMS-Slave

Ogni LTC6804/LTC6811 è in grado, oltre che prelevare le tensioni di ogni cella, anche: di prelevare la misura di temperatura di più punti all'interno del modulo di batteria; di comunicare con il BMS-Master attraverso le linee Daisy-Chain indicate al paragrafo 1; di gestire il bilanciamento del modulo su richiesta del BMS-Master; di gestire una memoria EEPROM.

Partendo dalla misura delle tensioni di cella, è di fondamentale importanza notare che, i due sottosistemi del BMS-Slave adottano un connettore unico e condiviso. Ogni chip-monitor è in grado di gestire un massimo di 12 celle connesse in serie. Ogni linea utilizzata per il prelievo delle tensioni di cella è protetta da un fusibile, montato su scheda, da 250 mA; inoltre, è presente un filtro capacitivo, a massa. Dallo stesso connettore vengono prelevati anche due ulteriori terminali per l'alimentazione del BMS-Slave. IL BMS-Slave può essere alimentato sia dal modulo del pacco batteria a cui fa riferimento, sia da una sorgente di alimentazione ausiliaria. In entrambi i casi la tensione di alimentazione può andare da 11 V fino a 60 V. Le line di alimentazione, come quelle inerenti al prelievo delle tensioni di cella, sono protette da un fusibile, montato direttamente sulla scheda, da 500 mA.

Per quanto riguarda la misura delle temperature di modulo, il BMS-Slave utilizza due connettori separati: uno per il chip-monitor primario e uno per il secondario; entrambi con la possibilità di prelevare fino ad 8 punti di temperatura. I sensori utilizzati per il prelievo delle temperature appartengono alla famiglia dei resistori NTC (Negative Temperature Coefficient). Questi sensori si basano sulla variazione della resistenza interna che corrisponde a una variazione della temperatura, ovvero, se si registra un aumento della temperatura si avrà come effetto un abbassamento della resistenza del sensore. Gli NTC, raccomandati per l'utilizzo dei BMS-Slave, sono degli NTC standard da 10 KΩ (es. Farnell-Nr. 1299926). Tutti gli 8 sensori che fanno riferimento a uno dei due chip-monitor sono connessi a un multiplexer analogico che ne seleziona, uno alla volta. La

selezione dell'ingresso analogico del multiplexer viene gestita dal chip-monitor corrispondente tramite il protocollo di comunicazione I^2C (Inter Integrated Circuit).

In fine, il bilanciamento adottato per equalizzare lo stato di carica delle celle di un modulo è di tipo passivo. Il sistema prevedere che ogni cella del modulo possa, selettivamente, essere collegata in parallelo a due resistori da 68 Ω in parallelo. In questo modo la cella selezionata viene scaricata attraverso le resistenze finché non raggiunge lo stato di carica desiderato. Ogni coppia di resistori può essere collegata alla cella corrispondente, in maniera selettiva, grazie all'ausilio di MOSFET controllati dal chip-monitor primario su comando del BMS-Master. Il chip-monitor secondario, invece, non supporta il sistema di bilanciamento sopracitato. Al fine di controllare il corretto funzionamento del processo di bilanciamento, o la presenza di eventuali malfunzionamenti, è stato previsto un segnale di feedback globale connesso sia al chip-monito primario che a quello secondario. Il segnale, nel particolare, rimane nello stato logico basso fintanto che nessuna cella è in fase di bilanciamento.

In conclusione, si può affermare che i due sottosistemi ridondanti del BMS-Slave sono del tutto simmetrici, tranne per quanto riguarda l'azionamento del processo di bilanciamento su comando del BMS-Master. Questa funzione è permessa solo al chip-monitor primario mentre il secondario può solo interpretare il segnale globale di feedback.

2 Architettura software

In questa sezione, verrà descritta l'architettura del software che verrà eseguito dai due microcontrollori, quello primario e quello secondario, presenti nel BMS-Master. Come vedremo in seguito i moduli del software che struttureranno l'architettura del programma non saranno identici per lo MCU_0 e lo MCU_1, ma saranno leggermente differenti, in linea con le funzionalità hardware pensate per i due microcontrollori.

2.1 l'Avvio del programma.

Ogni qualvolta il fox-BMS viene accesso, parte una procedura di inizializzazione del programma che si suddivide in tre fasi

In primo luogo, vengono inizializzati i registri del microcontrollore, il clock di sistema, la memoria dati (es. lo chip, il program counter, il vettore delle interruzioni, ecc…).

Successivamente viene avviata la funzione main(). Durante l'esecuzione di questa funzione vengono inizializzate le periferiche e i moduli software (es. il DMA, le priorità delle interruzioni, moduli software che gestiscono la comunicazione SPI, ecc…). Alla fine della funzione main(), anche le risorse del sistema operativo FreeRTOS vengono attivate, come per esempio: i thread, gli eventi, i semafori mutex, le code. A questo punto anche lo scheduler di sistema viene avviato. Lo scheduler di sistema è quel componente del sistema operativo che si occupa di gestire l'assegnazione dei thread, al microcontrollore per essere eseguiti secondo le priorità assegnate. All'avvio, lo scheduler esegue per primo il thread *void OS_TSK_Engine(void)*. Questo thread è quello a priorità più alta. Durante la sua esecuzione, tutti gli altri rimangono nello stato di attesa fintanto che lo *OS_TSK_Engine()* termina la terza fase dell'inizializzazione per entrare nell'esecuzione periodica del programma.

La terza fase dell'inizializzazione consiste, nell'attivazione delle interruzioni del sistema operativo tramite l'esecuzione della funzione *OS_PostOSInit().* Dopo di che, lo *OS_TASK_Engine()* gestisce periodicamente tutte le informazioni raccolte dall'esecuzione del programma dentro un database di sistema, ogni 1 ms. Un momento prima di entrare nell'esecuzione periodica lo *OS_TSK_ Engine()* esegue la funzione *void ENG_init(void)*. Questa funzione, inizializza tutti gli altri thread periodici, con priorità più bassa rispetto allo *OS_TSK_Engine(),* previsti per il corretto funzionamento del fox-BMS.

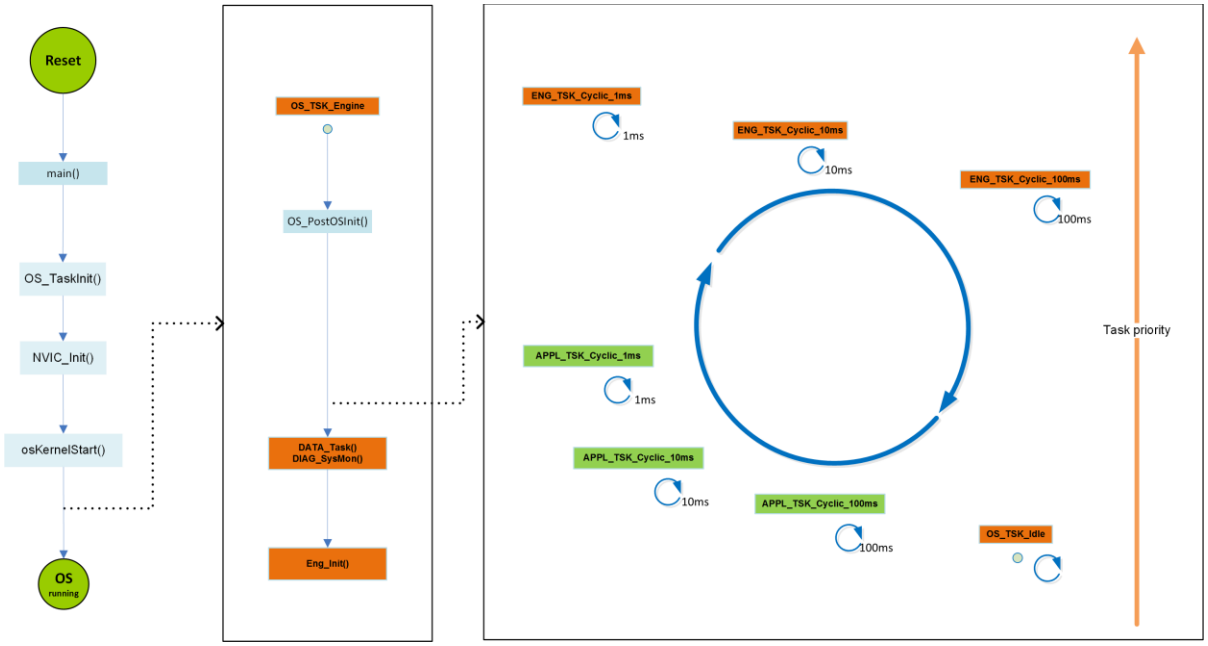

Figura 7 Thread di sistema

Come mostrato in Figura 7, i thread periodici si suddividono in due famiglie con due livelli di priorità differenti. La prima famiglia, con priorità più alte, è composta da:

- *void ENG_TSK_Cyclic_1ms(void);*
- *void ENG_TSK_Cyclic_10ms(void);*
- *void ENG_TSK_Cyclic_100ms(void).*

Queste tre funzioni, oltre che *la OS_TSK_ Engine(),* costituiscono il nucleo del sistema ed è fortemente sconsigliato apportare modifiche software a questo livello. La seconda famiglia agisce a livello applicativo, ha priorità più basse rispetto a quella precedente ed è composta dalle funzioni:

- *void APP_TSK_Cyclic_1ms(void);*
- *void APP_TSK_Cyclic_10ms(void);*
- *void APP_TSK_Cyclic_100ms(void).*

Proprio a questo livello l'utente può, se vuole, implementare nuovi algoritmi per adattare l'architettura software alle sue esigenze specifiche.

Ogni thread, al suo interno, racchiude dei moduli software specifici, ognuno pensato per svolgere delle azioni ben determinate. Sebbene, l'architettura software descritta, sin qui, è identica sia per lo MCU_0 che per lo MCU_1 per i moduli questa simmetria non è prettamente rispettata (vedi paragrafo 2.4).

In fine, prima di ogni avvio, sia per il microcontrollore primario che per quello secondario, viene eseguita una verifica dell'integrità del software presente nella loro memoria flash; tramite la funzione *CHK_crc32()*. La funzione si basa sul ricalcolo del CRC (Cyclic Redundancy Check) su ogni istruzione memorizzata. Se il risultato del ricalcolo è identico al valore "hardcode" presente in memoria il software del sistema è integro. Se non lo fosse verrebbe prodotto un errore e la procedura di avvio si bloccherebbe.

2.2 I moduli del programma.

In Figura 8 viene descritta l'architettura software del fox-BMS dal punto di vista dei moduli software eseguiti dai thread descritti nel paragrafo precedente.

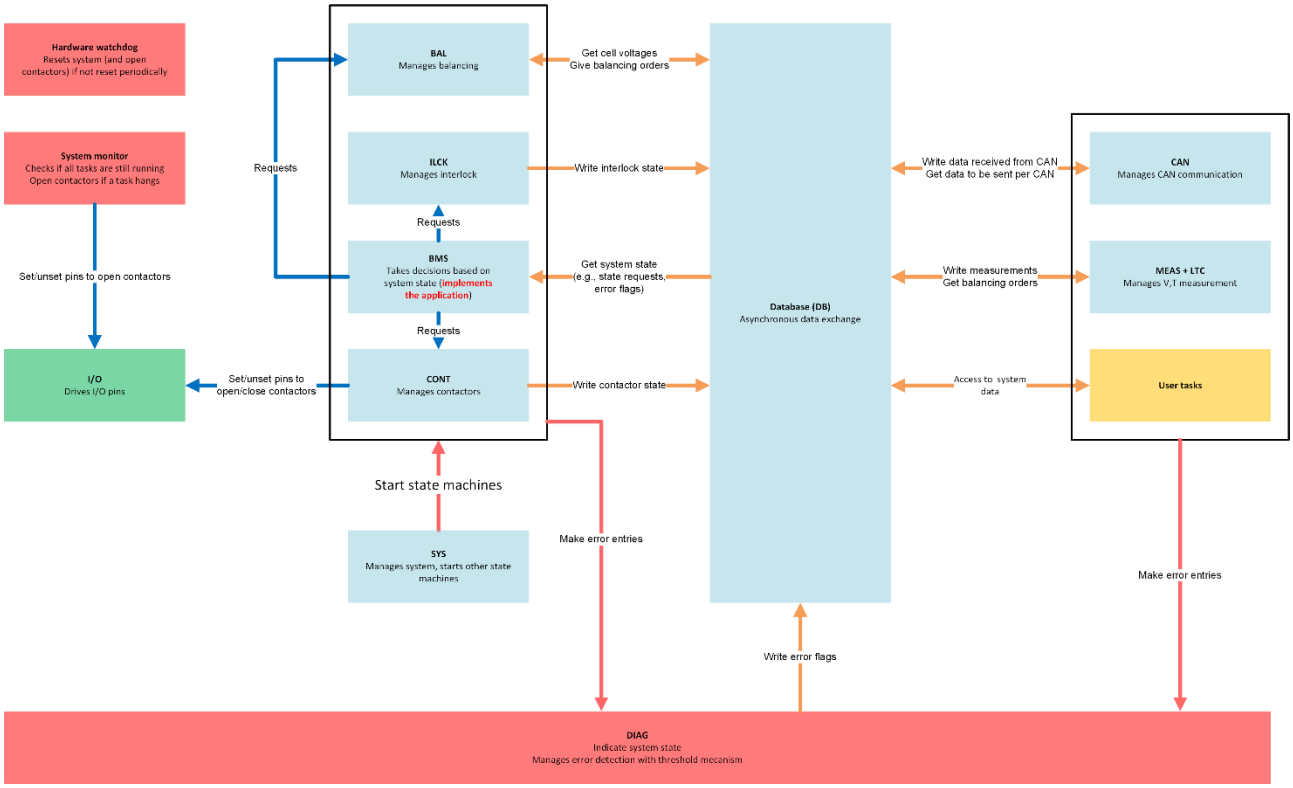

Figura 8 I moduli dell'architettura software

Partendo dal modulo "Database", si può affermare che è il modulo centrale dell'architettura. Viene eseguito dal thread *void OS_TSK_Engine()*,a più alta priorità. Il modulo "Database" non è altro che un'area di memoria condivisa che racchiude una struttura dati contente tutte le informazioni che vengono scambiate dai vari moduli durante l'esecuzione del programma. Insomma, tutto quello che succede all'interno del fox-BMS, viene registrato in questa struttura.

Altri due moduli di particolare interesse sono il modulo "SYS" e quello "BMS". Il modulo "SYS" viene eseguito generalmente da un thread a priorità più bassa di quello che gestisce il "Database" ma a priorità più alta rispetto a quello che gestisce il "BMS". Entrambi i moduli, "SYS" e "BMS", sono implementati attraverso una macchina a stati sincrona. In particolar modo, "SYS" si occupa di controllare lo stato operativo del sistema e avvia l'esecuzione degli altri moduli: "CONT","ILCK","BMS"; mentre il modulo "BMS" rappresenta il modulo principale che agisce a livello applicativo. Le funzionalità software che derivano da questo modulo sono le stesse domandante a un BMS generico per la gestione in sicurezza del pacco batteria. Infatti, il modulo preleva le informazioni di interesse dal "Database", le elabora e prende delle decisioni che possono essere anche di tipo attuativo sul sistema. Come vedremo nel paragrafo successivo, la macchina a stati del "BMS" prevede cinque stati; "STANDY", "NORMAL", "CHARGE", "PRECHARGE" e "ERROR"; ogni stato corrisponde a una configurazione degli interruttori meccanici diversa. L'entrata in uno stato, piuttosto che un altro, viene decisa dal controllore dell'autoveicolo a livello superiore che comunica con il fox-BMS attraverso il protocollo CAN. Le richieste di cambio di stato vengono inviate periodicamente al fox-BMS ogni 100ms e vengono salvate in prima istanza all'interno del "Database". L'invio periodico delle informazioni da parte del controllore dell'autoveicolo al fox-BMS è un meccanismo che aumenta la sicurezza del sistema. Infatti, se il controllore per qualche motivo smette di inviare periodicamente le informazioni al fox-BMS, o lo fa in maniera intermittente, il modulo "BMS" entra nello stato di protezione e fa richiesta al modulo "CONT" di

aprire tutti gli interruttori meccanici per isolare il pacco batteria. Oltre che attuare le richieste provenienti dal controllore di sistema, il modulo "BMS" controlla costantemente le tensioni e le temperature di cella assieme alla corrente di batteria. Se una di queste tre grandezze fisiche assume un valore al difuori della SOA di una o più celle, il modulo provvede a comunicare a "CONT" la richiesta di apertura di tutti gli interruttori meccanici.

In fine il "BMS" interagisce costantemente con i moduli "ICLK" e "CONT" anch'essi implementati da una macchina a stati sincrona. "CONT" controlla lo stato degli interruttori meccanici "ICLK", la linea di interlock.

Oltre alla gestione del pacco batteria, l'architettura software del fox-BMS prevede dei moduli dedicati per il monitoraggio del corretto funzionamento del software di sistema e per la gestione in sicurezza di eventuali errori e/o malfunzionamenti che potrebbero mettere seriamente a rischio l'incolumità dell'utilizzatore e del pacco batteria. Il monitoraggio del sistema viene eseguito dal modulo "System Monitor". Ad ogni thread che gestisce periodicamente una o più macchine a stati viene associato ad un watchdog software. Un watchdog software non è altro che un contatore opportunamente dimensionato, che se non viene periodicamente resettato, dopo il raggiungimento di un numero di conteggi prestabilito, attiva un segnale (software) di errore. Se il segnale di errore viene attivato significa che il thread associato a quel watchdog non lo ha resettato. Questo significa che, molto probabilmente, si è bloccato. Il "System Monitor", quindi, verifica periodicamente lo stato dei watchdog di ogni thread e se recepisce una segnalazione di errore provvede ad aprire tutti gli interruttori meccanici isolando il pacco batteria dal motore dell'autoveicolo. L'interruzione dei relè, però, non avviene attraverso il modulo "CONT", perché il thread che lo gestisce potrebbe essersi bloccato, ma attraverso un modulo a basso livello, quello "IO" che gestisce direttamente lo stato dei pin di controllo, del microcontrollore, associati ai singoli interruttori meccanici.

La gestione in sicurezza, al presentarsi di errori software o malfunzionamenti di sistema, del pacco batteria viene prevista dal modulo "DIAG". Il modulo "DIAG" è stato pensato per registrare e gestire tutte le problematiche di sistema (hardware e software) che potrebbero insorgere durante l'esecuzione del programma. Gli eventi che attivano questo modulo, devono essere definiti dall'utente all'interno di una struttura dati prestabilita. Ogni volta che viene rilevato, a livello software, un evento registrato all'interno della struttura dati viene chiamato il *DIAG_Handler(),* ovvero il gestore degli errori di sistema. Il modo con il quale il fox-BMS reagisce al presentarsi dell'errore dipende dalla funzione di "callback" associata a quella tipologia di errore. La velocità di reazione al presentarsi di una tipologia di errore dipende dal grado di rischio associato a quell'errore. Più il rischio associato a un determinato evento è elevato, più basso sarà il numero di eventi consecutivi che serviranno ad attivare la messa in sicurezza del sistema.

Nel caso in cui tutte le misure precedenti per la messa in sicurezza del sistema fallissero è presente un'ultima barriera di sicurezza rappresentata da un watchdog hardware. Se quest'ultimo non viene periodicamente resettato dal software, provocherà l'apertura di tutti gli interruttori meccanici.

2.3 Le macchine a stati.

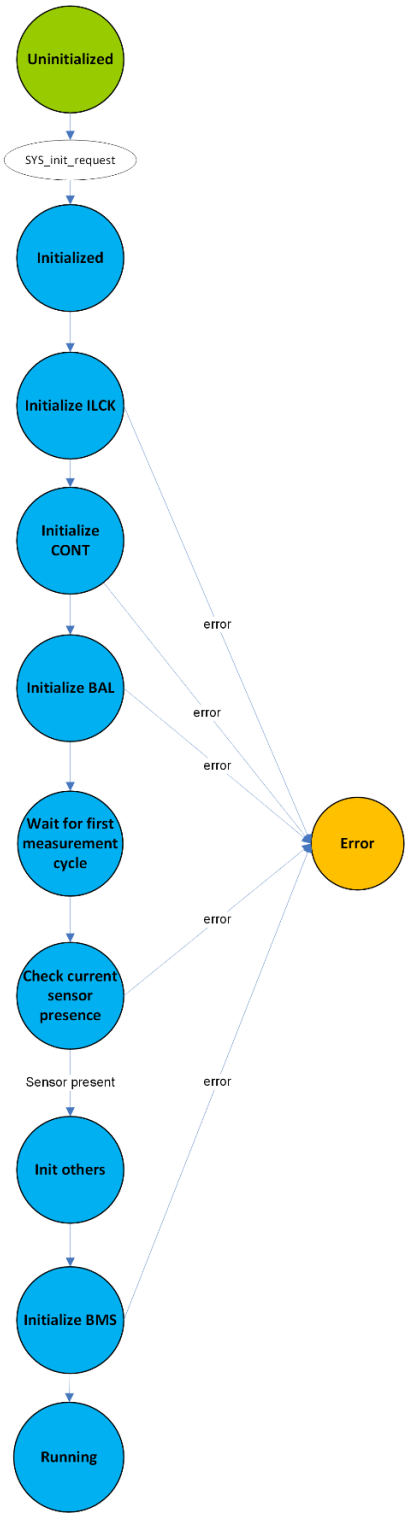

Figura 9 Stati del modulo "SYS"

Nel paragrafo precedente sono stati descritti i principali moduli che compongo l'architettura software del sistema. Come accennato, parte di questi, vengono implementati attraverso delle macchine a stati sincrone. In questo paragrafo verranno descritte le principali macchine a stati che compongono il software del fox-BMS, associate ai moduli: "SYS", "BMS", "LTC", "CONT", "ILCK".

Partendo dal modulo “SYS”, la macchina a stati corrispondente viene mostrata in Figura 9.

Una volta terminata la prima fase e la seconda fase di avvio del sistema, descritte al paragrafo 122.1, che si conclude con l’entrata in esecuzione periodica del thread *OS_TSK_Engine(void),* viene fatta una richiesta di inizializzazione del modulo “SYS”. In primo luogo, la macchina a stati, invia delle richieste di inizializzazione ad altre tre macchine a stati, quelle relative ai moduli: “ILCK”,”CONT” e “BAL”. Lo stato di queste macchine a stati viene continuamente controllato da “SYS”, attraverso un meccanismo di timeout, in modo da assicurare la corretta inizializzazione. Se una di queste procedure di inizializzazione non avviene correttamente entro il termine temporale stabilito dal meccanismo di timeout, la macchina a stati “SYS” entra nello stato di errore. In secondo luogo, “SYS” attende il completamento del primo ciclo di misure delle tensioni e delle temperature di cella, prima di abilitare l’invio periodico delle informazioni al controllore dell’autoveicolo tramite il protocollo CAN. Questo, serve ad evitare una trasmissione di dati erronei all’avvio del sistema. Successivamente, si verifica la presenza del sensore di corrente. In fine viene fatta la richiesta di inizializzazione della macchina a stati “BMS”.

Il modulo “BMS”, gestisce le richieste che provengono, via CAN, dal controllore dell’autoveicolo a livello superiore. Nella versione base del software, le richieste del controllore dell’autoveicolo e i flag di errore vengono salvati e/o letti nel “Database”.

In Figura 10 viene mostrata la struttura della macchina a stati “BMS”. La struttura è costituita dalla presenza di cinque stati principali: “STANDY”, “NORMAL”, ”CHARGE”, “PRECHARGE” e “ERROR” Ad ogni stato corrisponde una configurazione degli interruttori meccanici differente. Lo stato “STANDBY” equivale ad avere tutti gli interruttori meccanici aperti. Questa situazione potrebbe presentarsi quando l’autoveicolo viene parcheggiato senza essere ricaricato. Lo stato “NORMAL” o “CHARGE” corrisponde ad avere i due interruttori meccanici, collegati ai terminali di potenza della batteria, chiusi. Situazione che si verifica, durante il normale utilizzo o durante la fase di ricarica dell’autoveicolo. Tuttavia, lo stato “CHARGE” è disponibile solo se viene prevista una linea di potenza separata, per la gestione della ricarica del pacco, rispetto a quella utilizzata per lo stato “NORMAL”. Se viene prevista la linea secondaria devono essere utilizzati, e gestiti, altri tre interruttori meccanici, speculari, a quelli presenti sulla linea primaria. Le uniche transizioni consentite dal modulo “BMS”, sono quelle dallo stato “STANDBY” a quello “NORMAL” o “CHARGE” e viceversa. Mentre non sono previste, transizioni dirette tra gli stati “NORMAL” e “CHARGE”. Inoltre, la transizione dallo stato “STANBY” a quello “NORMAL” o “CHARGE” passa per uno stato intermedio, quello di “PRECHARGE”. Questo stato, corrisponde alla configurazione in cui gli interruttori meccanici, collegati al terminale negativo del pacco batteria e a quello della linea di precharge, sono chiusi. In fine, il modulo “BMS”, ad ogni iterazione controlla, sia che le misure di tensione, temperatura e corrente rientrino nella SOA di ogni cella, sia la presenza di errori di sistema segnalati attraverso dei flag di errore nel “Database”. Nel caso in cui viene attivata una segnalazione di errore di sistema o di sforamento della SOA da parte di uno o più celle, la macchina a stati “BMS” entra nello stato “ERROR”. All’interno di questo stato, viene inviata la richiesta, alle macchine a stati “CONT” e “ILCK”, di aprire tutti gli interruttori meccanici. A questo punto, il “BMS” rimanere in attesa di un’eventuale richiesta di entrata nello stato di “STANDBY” da parte del controllore dell’autoveicolo. Per quanto detto sopra, il modulo “BMS” interagisce con i moduli “CONT” e “ILCK” per controllare lo stato degli interruttori meccanici durante tutte le fasi di utilizzo dell’autoveicolo. Lo scopo della macchina “CONT” è quello di fissare lo stato degli interruttori meccanici, che regolano il passaggio di corrente nel pacco batteria, su richiesta del modulo “BMS”. Il modulo “BMS” gestisce la transizione da uno stato all’altro del modulo “CONT” attraverso delle richieste specifiche, che vengono slavate nel “Database”. Come mostrato in Figura 11, gli stati disponibili sono: “STANDBY”, ”NORMAL”, ”CHARGE”, ”PRECHARGE” e “ERROR”. Ad ogni stato corrisponde una configurazione degli interruttori specifica, questa volta attuativa, che corrisponde a quella descritta durante l’illustrazione del modulo “BMS”.

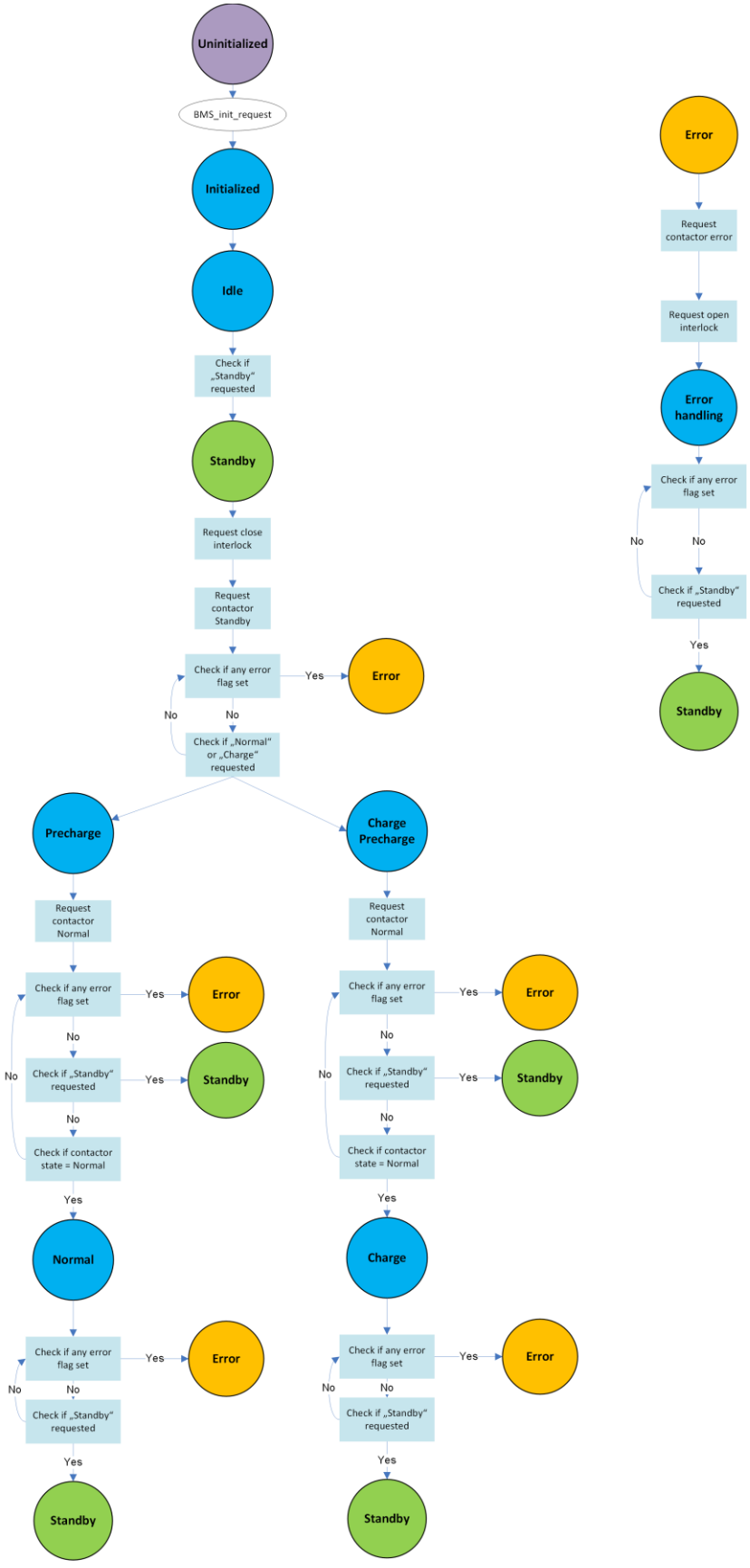

Figura 10 Stati del modulo "BMS"

In particolare, nello stato di “PRECHARGE” vengono chiusi gli interruttori collegati al terminale negativo di batteria e al resistore di precharge. Lo scopo di questa fase è quello di limitare le correnti di spunto che potrebbero interessare il pacco batteria quando lo si collega ad un carico o un alimentatore con una grande capacità, rispettivamente, in ingresso o in uscita. Grazie a questa configurazione e al resistore di precharge, la corrente di spunto viene limitata notevolmente. Durante questa fase viene continuamente monitorata la caduta di tensione sulla resistenza attraverso due canali dedicati del sensore di corrente IVT-300. Fin tanto che, la caduta di tensione rimane al disopra di una soglia prestabilita la macchina a stati rimane nello stato di “PRECHARGE”. Una volta terminata la fase impulsiva di corrente, “CONT” passa allo stato successivo (“NORMAL” o “CHARGE”). Le transizioni dirette tra gli stati “NORMAL” e “CHARGE” non sono permesse. Inoltre, lo stato “CHARGE” è disponibile solo se viene prevista una linea di potenza dedicata esclusivamente per la ricarica del pacco. Inoltre, “COUNT” ad ogni iterazione controlla se lo stato impostato degli interruttori è coerente con il segnale di feedback associato ad ognuno di essi. Nel caso in cui non lo fosse viene attivata una segnalazione di errore. Ogni segnalazione di errore porta “COUNT” ad entrare nello stato “ERROR” che ha come effetto quello di aprire tutti gli interruttori meccanici attraverso il modulo “io”.

Un ulteriore modulo che può determinare lo stato degli interruttori meccanici è “ILCK”. Questa macchina a stati è composta semplicemente, oltre che dallo stato di inizializzazione, dagli stati: “OPEN” e “CLOSE”. Il primo corrisponde all’interruzione della linea; il secondo la ristabilisce. Le richieste di passaggio da uno stato all’altro vengono gestite dal modulo “BMS” attraverso il “Database”. Quando il “BMS” entra nello stato di “STANDBY” invia la richiesta di chiusura della linea, mentre, quando entra nello stato “ERROR” ne richiede l’interruzione. Inoltre, ad ogni iterazione viene controllato se lo stato della linea è coerente con la lettura dei segnali di feedback dedicati. Qualora non lo fosse, verrebbe attivata una segnalazione di errore che verrebbe gestita dal modulo “BMS”.

In fine, il modulo software che gestisce i chip-monitor LTC6804-1/LTC6811-1, nei BMS-Save tramite la linea di comunicazione daisy-chain, è lo “LTC”. In Figura 12, vengono mostrati tutti gli stati di questo modulo. Dopo una prima fase di inizializzazione, la macchina a stati entra in un loop di misura che ciclicamente:

1. Misura le tensioni di cella;
2. Legge le tensioni di cella;
3. Seleziona un ingresso del multiplexer;
4. Legge l’ingresso del multiplexer;
5. Verifica se ci sono richieste di stato pendenti;
6. Se necessario avvia il bilanciamento di uno o più moduli.

Nel caso in cui non ci sono richieste pendenti da eseguire e per un’architettura composta da 8 moduli BMS-Slave connessi in serie, un ciclo di misura impiega non più di 20ms. Questo significa che la massima frequenza di campionamento, per un sistema di questo tipo, è pari a 50Hz.

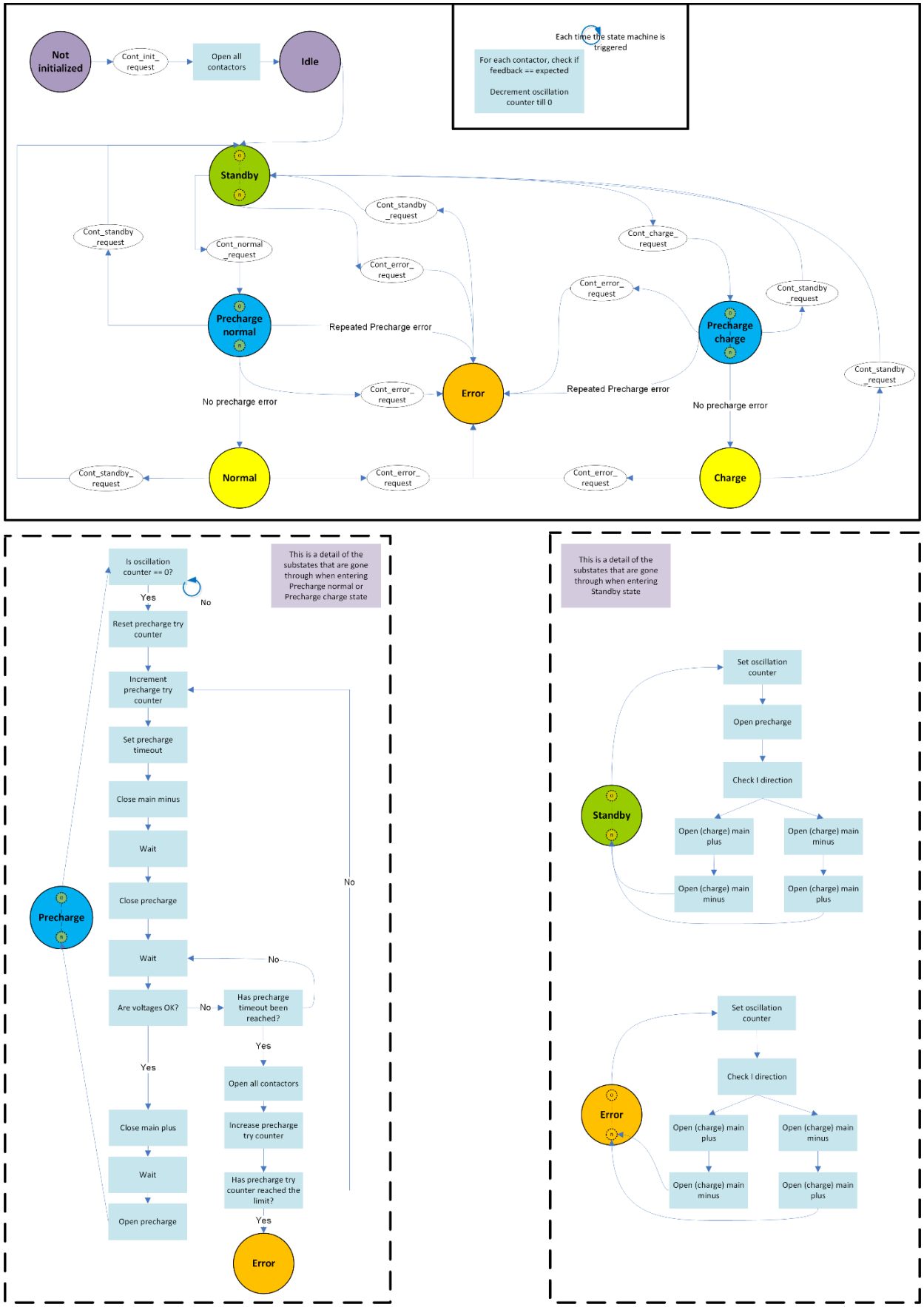

Figura 11 Stati del modulo "COUNT"

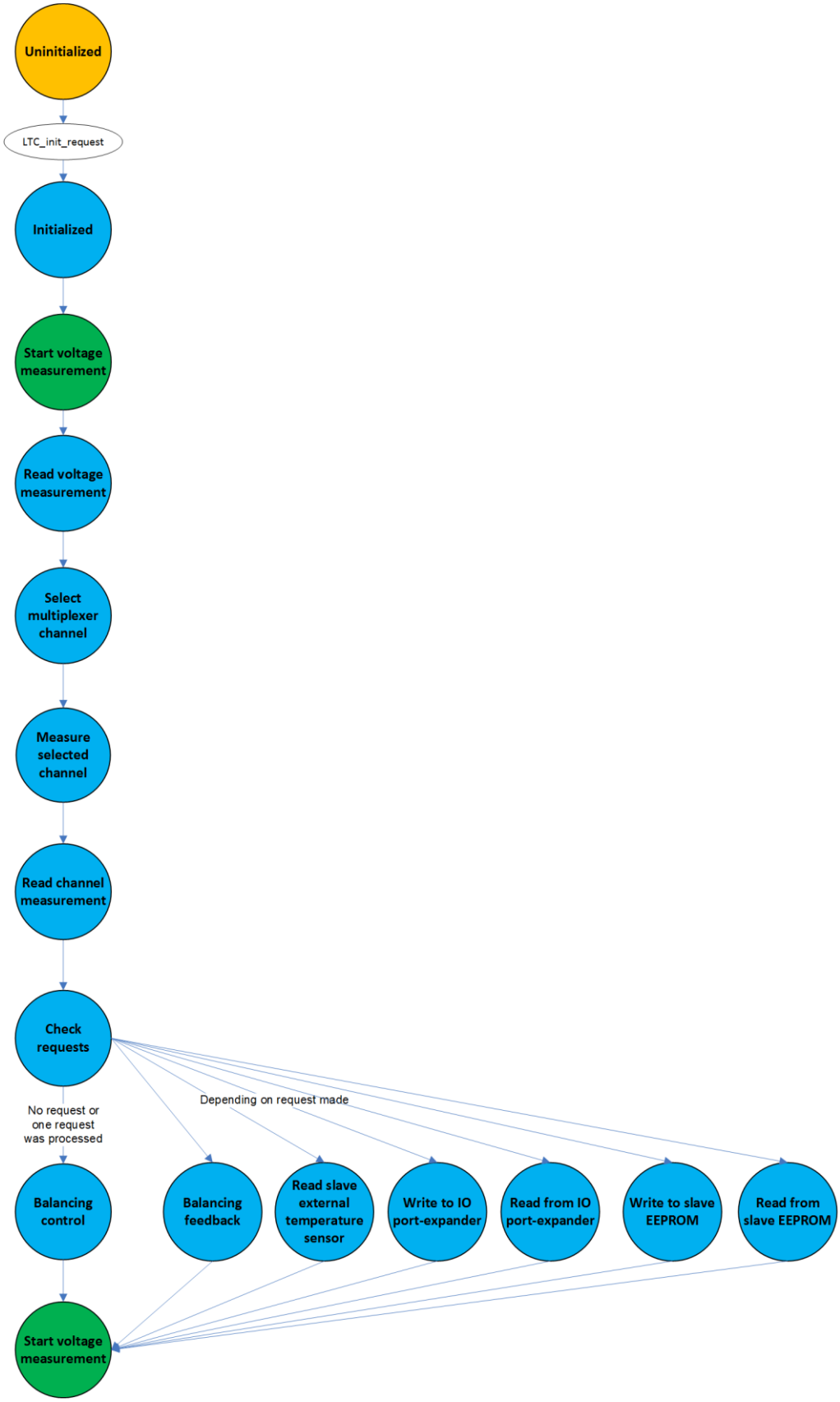

Figura 12 Stati del modulo "LTC"

2.4 Le differenze software tra MCU_0 e MCU_1

Sebbene, la struttura gerarchica e la tipologia dei thread in esecuzione sui due microcontrollori del BMS-Master è la stessa, i singoli moduli software eseguiti dai thread dipendono fortemente dalle funzionalità hardware previste per i due microcontrollori. In Tabella 1 viene riportata una descrizione dettagliata delle differenze software tra MCU_0 e MCU_1. Per esempio, lo MCU_1 non eseguirà le funzioni *COUNT_Trigger()* o *CAN_MainFUnction()* perché a livello hardware non è stato previsto, né il controllo diretto degli interruttori meccanici, né la comunicazione CAN con il sensore di corrente o con il controllore dell'autoveicolo. Inoltre, lo MCU_1, non gestisce: le misure sulla resistenza di isolamento prelevate dal bender isometer; la memoria EEPROM esterna ai due microcontrollori; le stime dello stato interno del pacco batteria. Funzioni che sono prettamente riservate allo MUC_0 che, quindi, rappresenta il microcontrollore primario del sistema. Detto questo lo MCU_1, viene adibito, esclusivamente, per scopi di ridondanza funzionale sul sistema, nell'acquisizione dei dati provenienti dai BMS-SLAVE. Anche l'associazione modulo-thread cambia in base alla tipologia di microcontrollore. Per esempio lo MCU secondario gestisce le macchine a stati "LTC","SYS","ILCK" attraverso un unico thread (lo *void ENG_TSK_Cyclic_1ms(void)),* mentre, quello primario utilizza due thread: *void ENG_TSK_Cyclic_1ms(void)* e *void ENG_TSK_Cyclic_10ms(void)*.

Tabella 1 Dipendenza tra i moduli software eseguiti dai thread di sistema in funzione dello MCU_0 e dello MCU_1

Thread	MCU_0	MCU_1
void ENG_TSK_Cyclic_1ms(void)	Meas_Ctrl() LTC_Trigger() EEP_Trigger()	LTC_Trigger() SYS_Trigger() ILCK_Trigger()
void ENG_TSK_Cyclic_10ms(void)	SYS_Trigger() COUNT_trigger() ILCK_Trigger()	LED_Ctrl()
void ENG_TSK_Cyclic_100ms(void)	ADC_Ctrl() Bender_isometer()	ADC_Ctrl()
void APP_TSK_Cyclic_1ms(void)	BMS_Trigger()	BMS_Trigger()
void APP_TSK_Cyclic_10ms(void)	CAN_MainFunction() SOC_Ctrl() SOF_Ctrl();	Empty
void APP_TSK_Cyclic_100ms(void)	LED_Ctrl()	Empty

3 Le stime dello stato interno.

In questa sezione vengono descritti, gli algoritmi di stima dello stato interno del pacco batteria adottati dal fox-BMS. In particolar modo, questa funzione è demandata esclusivamente al microcontrollore primario (lo MCU_0) del BMS-Master attraverso il modulo software "SOX". Il modulo "SOX" viene eseguito dal thread *void APP_TSK_Cyclic_10ms(void),* a livello applicativo, che ha un grado di priorità più basso rispetto a quello che gestisce il modulo "BMS". Le stime previste dal modulo sono: quella dello SoC (State of Charge), e quella dello SoF (State of Function).

3.1 Stima dello SoC.

Il parametro SoC rappresenta, in percentuale, la carica residua del pacco batteria normalizzata sulla sua capacità nominale [5]. L'algoritmo adottato dal fox-BMS per la stima dello SoC è quello del Coulomb Counting espresso in (1)

$$SoC(t) = SoC(0) + \frac{\int_0^t I(\tau)d\tau}{C} \cdot 100 \quad (1)$$

Dove: “SoC(0)” è lo stato iniziale, “I(τ)” è la corrente che scorre nel pacco batteria durante una fase di carica o scarica e “C” la capacità nominale del pacco.

Nella versione base del software, lo stato iniziale per t = 0, dello SoC viene letto dalla memoria non volatile EEPROM presente sulla scheda BMS-Master. Durante la carica o la scarica del pacco, il valore iniziale viene aggiornato ad ogni iterazione. Questa tecnica di determinazione dello stato iniziale, a lungo termine potrebbe portare ad un errore sistematico sulla stima dello stato di carica. Per esempio, supponiamo di parcheggiare l’autoveicolo quando il suo SoC ha raggiunto il 50%. Il BMS, quindi salverà in memoria questo valore e lo utilizzerà come stato iniziale, per stimare il SoC al prossimo avvio. Supponiamo, inoltre, che il veicolo sia rimasto fermo per un lungo periodo e che le correnti di auto-scarica, intrinseche al pacco, lo abbiamo scaricato leggermente. E’ quindi ovvio che al prossimo avvio lo SoC(0) salvato in memoria differirà da quello reale. Questa discrepanza produrrà, inevitabilmente, un errore sistematico sulla stima dello stato di carica. Per ovviare, al problema della determinazione dello stato iniziale, esistono delle tecniche che permettono di associare lo SoC(0) in funzione della tensione del pacco batteria, grazie ad una look-up table. Attualmente questa tecnica non è implementata nella versione base del software. Tuttavia, all’interno del modulo “SOX”, è stata prevista la struttura per poter gestire questo meccanismo.

3.2 Stima dello SoF

Il parametro SoF, da un’indicazione percentuale sulle performance del pacco batteria. Entrando più nello specifico, il SoF si riferisce alla capacità del pacco di far fronte alla richiesta di potenza del carico. Se il parametro assume il valore 1 significa che il pacco batteria è in grado di erogare tutta la potenza richiesta dal carico, viceversa, se assume il valore 0 significa che il pacco non riesce più a far fronte alla richiesta di potenza dal carico. Generalmente, nella letteratura scientifica del settore [6], il SoF viene definito come in (2)

$$SoF = \frac{P - P_{demands}}{P_{max} - P_{demands}} \tag{2}$$

Dove P è la potenza, attuale, erogabile dalla batteria; $P_{demands}$ è la richiesta di potenza da parte del carico (motore dell’autoveicolo); P_{max} è la potenza massima erogabile dalla batteria.

Nella versione base del software del fox-BMS, la stima del SoF non viene eseguita in maniera completa. Detto questo, il modulo “SOX”, attraverso l’esecuzione della funzione *SOF_Crtl()* si limita al calcolo della corrente massima erogabile dal pacco batteria in funzione del punto di lavoro in cui si trovano le celle che lo compongono. Ovviamente, la massima corrente erogabile dal pacco dipende dalle specifiche tecniche riportate sul manuale delle celle ed è strettamente correlato a valori di:

- Tensione;
- Temperatura;
- SoC.

Una volta estratta la corrente massima erogabile dal pacco, il BMS master provvederà ad inviala al controllore di sistema. A questo punto, il controllore, dispone di tutte le informazioni per ricavarsi la stima dello SoF in quanto conosce: la massima corrente erogabile dal pacco batteria; la tensione delle celle della batteria; la potenza richiesta dall’autoveicolo e la potenza erogata dal pacco. Nel caso in cui la stima del SoF si avvicini allo zero, sia per un aumento eccessivo della potenza richiesta dal motore, sia per un degrado delle prestazioni della batteria, il controllore dell’autoveicolo può decidere di ridurre la potenza richiesta, rispettivamente, in maniera momentanea o permanente.

In Figura 13, Figura 14 e Figura 15 vengono rappresentati gli andamenti della corrente massima erogabile da una cella generica relazionati, rispettivamente, alla sua temperatura, tensione e SoC [7]. L’utente, una volta scelta la tecnologia delle celle e consultato il manuale tecnico di queste, dovrà configurare correttamente il modulo “SOX”. La configurazione avviene attraverso l’utilizzo di definizioni specifiche in linguaggio C. Ad

esempio, per l'andamento della corrente massima in funzione della temperatura riportata in Figura 13, come per quelle in funzione della tensione e dello SoC, si dovranno impostare:

- I limiti di temperatura inferiore e superiore, oltrepassato i quali, si ha una corrente massima nulla;
- I punti di cut-off superiore e inferiore, oltrepassato i quali, si avrà una diminuzione della corrente massima erogabile;
- La pendenza delle zone comprese tra i punti di cut-off e le zone a corrente massima nulla.
- La massima corrente erogabile nella zona "piatta".

Una volta configurato tutto il modulo "SOX", il BMS è in grado di ricostruire le funzioni matematiche rappresentate in Figura 13, Figura 14 e Figura 15 ma questa volta adattate alla tecnologia delle celle utilizzate nel pacco batteria. Partendo dalle tre funzioni matematiche, il fox-BMS ricava le tre correnti massime erogabili dal pacco, in funzione al punto di lavoro in cui si trova, e invia al controllore del sistema il valore minimo delle tre;

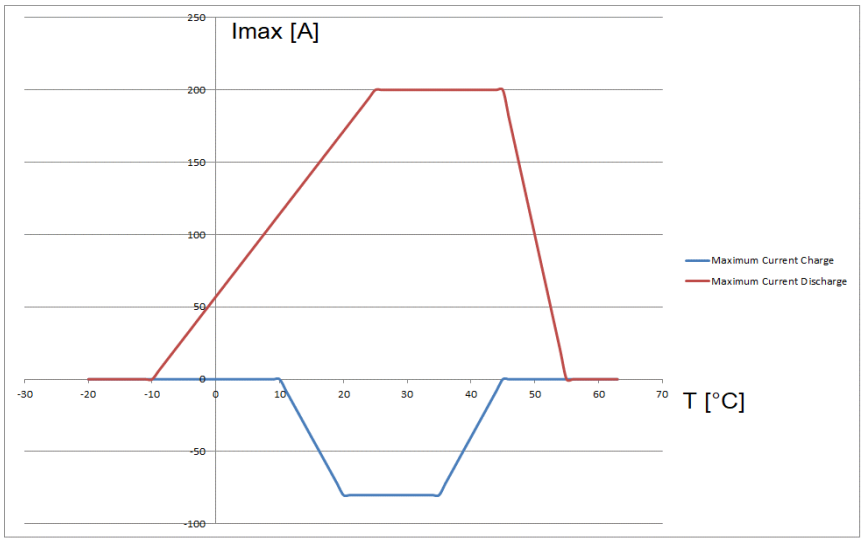

Figura 13 Curva di deterioramento della corrente massima di cella in funzione della temperatura

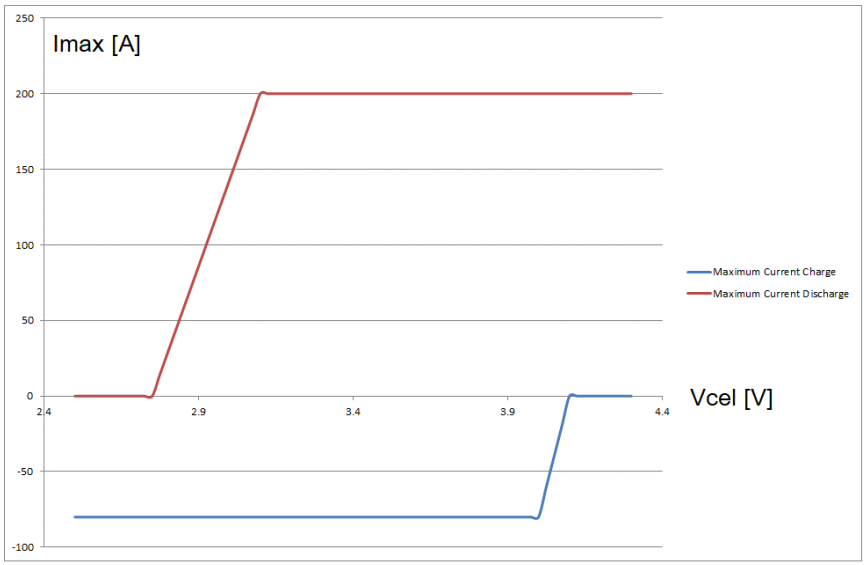

Figura 14 Curva di deterioramento della corrente massima di cella in funzione della tensione

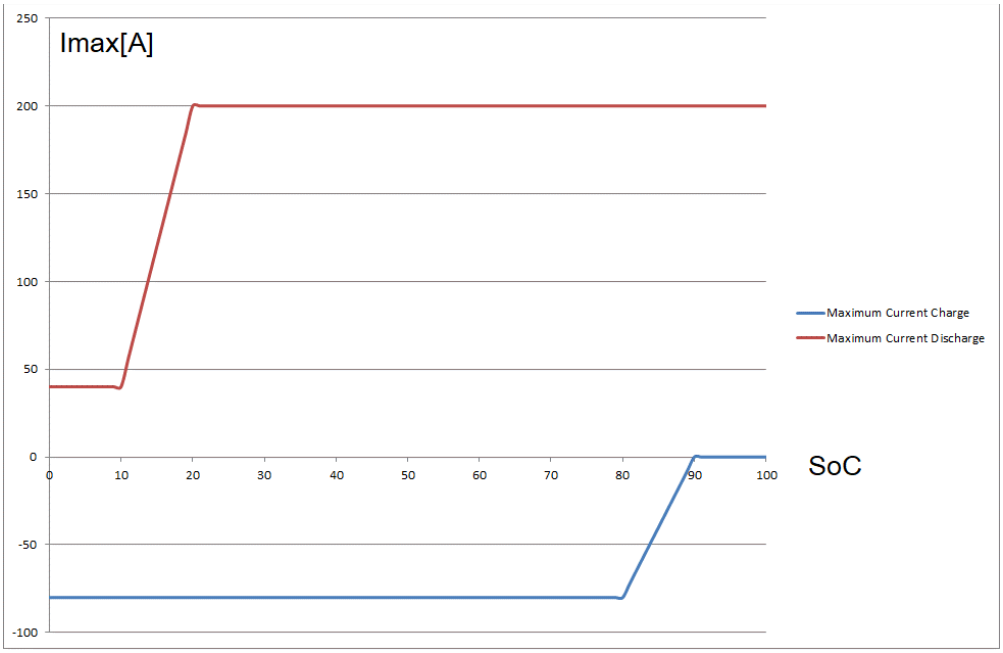

Figura 15 Curva di deterioramento massima della corrente cella in funzione dello SoC

4 Metodologia HazOp

Generalmente, la metodologia HazOp viene applicata su un impianto e/o su un sistema con lo scopo di identificare i rischi e/o le problematiche operative connesse al suo utilizzo. L'analisi HazOp si basa su un'analisi sistematica dello schema di processo o di un P&Id (Piping and Instrumentation Diagram) di impianto, con l'intento di identificare ogni possibile deviazione dal funzionamento ordinario, definito in termini tecnici "intenzione". L'intenzione può essere specificata come il funzionamento impostato dell'impianto sulla base di tutti i parametri di progetto e/o regolazione

L'analisi viene condotta da specialisti e procede tramite un'indagine rigorosa degli schemi progettuali. La conduzione dell'analisi richiede, quindi, un'ottima conoscenza a livello funzionale dell'impianto/sistema da analizzare. In primo luogo, il sistema viene suddiviso in elementi, scelti in funzione della sua complessità. In secondo luogo, ad ogni elemento individuato viene associato un parametro caratteristico (es. pressione, temperatura, portata, ecc.). Successivamente, ad ogni parametro, viene individuata una "parola chiave" che indica una condizione di deviazione dalle caratteristiche di funzionamento ordinario (es. parte 1, parola chiave "more" applicata al parametro "pressione" indica la condizione di deviazione che porta ad avere "alta pressione nella parte 1"). In fine, per ogni deviazione individuata viene associata una classificazione di pericolo. 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 (es. corto circuito o la sovraccarica del pacco batteria).
- Pericolo termico (es. elevate temperature, incendio).
- Pericolo meccanico (es. derivante da urti, penetrazioni del sistema batteria, cadute).
- Pericoli di sistema (es. malfunzionamento del fox-BMS).

Detto questo, per individuare la severità del danno associato un pericolo, per una singola deviazione di sistema, sono state individuate due categorie: "BASSA" e "ALTA". La prima comprende tutti quegli eventi che non possono avere ricadute al di fuori della cella o del modulo. La seconda racchiude tutte quelle sequenze incidentali che potenzialmente possono mettere a rischio le persone

Nello specifico del presente studio l'analisi HazOp è stata utilizzata per l'identificazione dei pericoli che possono essere associati all'utilizzo di un sistema di accumulo elettrochimico gestito dal fox-BMS. Il sistema

preso in considerazione è quello di una batteria da 30KWh utilizzabile in applicazioni automotive, composta da 96 celle, suddivise in 8 moduli da 12.

L'analisi sistematica è stata condotta secondo la procedura riportata dalla norma CEI IEC 61882 [8]. Per maggiori informazioni sulla procedura e sul flusso di lavoro condotto nell'analisi HazOp, si prega di consultare il documento *"Studio preliminare sulla gestione delle deviazioni dal normale funzionamento di un sistema di accumulo automotive da parte del BSM"* redatto dall'Università di Pisa in collaborazione con ENEA.

4.1 Scopo della presente analisi HazOp

La finalità dell'analisi HazOp condotta in questo studio è quella di determinare tutte le deviazioni di sistema potenzialmente pericolose che potrebbero verificarsi durante l'utilizzo del fox-BMS nella gestione di un sistema di accumulo di tipo Litio-ione, classificando la severità del danno di ogni evento inusuale.

4.2 Identificazione degli elementi che compongono il sistema fox-BMS

Come descritto precedentemente, all'inizio del capitolo 4 "Metodologia HazOp" la prima fase dello studio HazOp consiste nell'individuazione degli elementi basilari che compongono il sistema di interesse, in questo caso del fox-BMS. In Tabella 2, sono riassunti gli elementi, o sottosistemi del fox-BMS, individuati per l'analisi in questione.

Tabella 2 Elementi del fox-BMS

ELEMENTO / BLOCCO	***PARAMETRO CARATTERISTICO***
1 Master BMS MCU_0 (primario)	Elaborazione dati
2 Master BMS MCU_1 (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

4.3 Applicazione delle parole guida per l'identificazione delle deviazioni

Nella seconda fase della procedura sistematica HazOp sono state individuate, per ogni parametro caratteristico associato ad un elemento del sistema, le parole guida. L'applicazione di tutte le parole guida agli elementi del sistema, rappresenta la fase principale dello studio, in quanto porta all'identificazione delle possibili cause ed infine delle potenziali conseguenze associate agli eventi inusuali. In Tabella 3 viene mostra l'associazione del parametro caratteristico, alle parola guida e alle rispettive deviazioni associate ad ogni elemento del sistema fox-BMS.

Tabella 3 Parole guida e deviazioni associate ad ogni elemento del fox-BMS

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

4.4 Severità del danno

La classificazione della severità dell'evento inusuale è ispirata a quella utilizzata da EURCAR [9], nella quale il grado di severità viene rappresentato in una scala da 0 (nessun effetto) a 7 (esplosione). Per semplicità, nei paragrafi successivi, raggrupperemo i gradi di severità da 0 a 3 con il termine "BASSA" e da 4 a 7 con il termine "ALTA" vedi Tabella 4

Tabella 4 Classificazione di severità del danno secondo EUCAR e quella utilizzata nel seguente 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 resettare 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.

4.5 Schede analisi della procedura HazOp

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 fox-BMS 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.

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
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.
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

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
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		
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		

Id #	Elemento	Caratteristica	Parola guida	Deviazione	Possibile causa	Conseguenza	Severità del danno	Sistemi di sicurezza	Commenti
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	
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 fox-BMS 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.

4.6 *Gestione delle deviazioni a livello di cella di un sistema di accumulo Litio-ione da parte del fox-BMS*

Nel paragrafo precedente, è stato mostrato come il fox-BMS reagisce ad una possibile deviazione rispetto al funzionamento ordinario degli elementi che lo compongono. Tuttavia, il fox-BMS è stato progettato anche per gestire in sicurezza, gli eventi inusuali che possono portare a una deviazione, dal normale funzionamento del sistema, a livello di cella. Partendo da un precedente studio che sottopone ad analisi HazOp un sistema di accumulo elettrochimico composto da celle Litio-ione di tipo NMC [1], è stato possibile individuare le reazione del fox-BMS al presentarsi di un evento non ordinario, a livello di cella, durante l'analisi sistematica del sistema pacco batteria.

Tabella 5 Intervento del fox-BMS a una possibile deviazione dal normale funzionamanto di una cella Litio-ione

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 fox-BMS interviene non appena una cella all'interno del pacco batteria raggiunge il livello di tensione minimo consentito. L'intervento del fox-BMS consiste nell'apertura di tutti i contattori e della linea di interlock (questo avviene se il fox-BMS è attivo).
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.
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.
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 fox-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 fox-BMS verrebbe spento perché se non lo fosse scaricherebbe il pacco batteria nel giro di un mese. Comunque, ad ogni avvio, Il fox-BMS controlla lo stato di ogni cella del pacco batteria. Se è presente un'anomalia dovuta al lungo periodo di stoccaggio delle celle, il fox-BMS se ne accorge e provvede a dare una segnalazione di errore.

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 fox-BMS, il fox-BMS stacca il pacco. • Se la corrente massima che eroga il caricatore viene limitata a un valore inferiore rispetto al massimo consentito dal fox-BMS, il fox-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).
Sovra corrente durante la carica	Il BMS è progettato per inibire la ricarica del modulo se la corrente del caricatore è troppo elevata.	il fox-BMS interviene aprendo i contattori.
Malfunzionamento del BMS (perdita di equalizzazione)	Il BMS si accorge del malfunziamento nel sistema di bilanciamento e produce una segnalazione di errore	Il fox-BMS opera con sistema di bilanciamento di tipo passivo. Ogni cella può essere temporaneamente scaricata su due resistori da 68 Ω 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 fox-BMS Salve Board che attiva l'equalizzazione su comando del fox-BMS Master. In particolare, solo il chip monitor primario presente nel fox-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. Il fox-BMS può, quindi, discriminare un malfunzionamento nel sistema di bilanciamento ma nella versione base del SW non è previsto alcun tipo di intervento.

Causa	Ipotesi intervento BMS	Commenti gruppo di lavoro DII
Sovra carica 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	Se, nonostante l'equalizzazione, una o più celle raggiungono il limite superiore di tensione consentito, il fox-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 interviene, interrompendo la fase di utilizzo del pacco batteria.l	Il fox-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 fox-BMS consiste nell'apertura di tutti i contattori e della linea di interlock.
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 fox-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. E' più pericoloso perché dipende dalla zona della batteria interessata, cioè se colpisce il fusibile o no.

4.7 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 da:

Prof. Roberto Roncella (Dipartimento di Ingegneria dell'Informazione – Docente del corso di architetture dei sistemi elettronici)

Prof. Roberto Saletti (Dipartimento di Ingegneria dell'Informazione – Docente del corso di Elettronica digitale e Progettazione di Sistemi digitali)

Prof. Federico Baronti (Dipartimento di Ingegneria dell'Informazione – Co-docente del corso di Costruzioni elettroniche e Laboratorio di Elettronica Digitale).

Ing. Andrea Carloni (Dottorando di ricerca - Dipartimento di ingegneria dell'informazione).

Ing. Roberto di Rienzo (Dottorando di ricerca - Dipartimento di ingegneria dell'informazione).

Prof. Marco Carcassi (Dipartimento di Ingegneria Civile e Industriale – Docente del corso di Sicurezza ed Analisi del Rischio) .

Ing. Martino Schiavetti (HazOp leader).

Ing. Tommaso Pini (segretario).

5 Conclusioni

I risultati ottenuti dall'applicazione della metodologia HazOp al fox-BMS evidenziano come, in caso di malfunzionamenti del BMS, questo sia in grado di rilevare quasi la totalità delle situazioni indesiderate e di intervenire per evitare o limitarne gli effetti negativi. Grazie alla progettazione in accordo allo standard ISO 26262, risulta fondamentale l'architettura hardware che prevede elementi di ridondanza di sicurezza e di rilevazione degli errori. La capacità di individuazione delle situazioni indesiderate, viene decisa al momento della progettazione di un BMS. Ovviamente se il BMS dovrà essere utilizzato in applicazioni che richiedono un grado di affidabilità elevato, a livello di progettazione verranno aggiunti tutti i componenti elettrici e software necessari per l'individuazione dei malfunzionamenti previsti dallo standard di sicurezza a cui fa riferimento quel tipo di applicazione. Per questo motivo, si può affermare che le criticità più pericolose per l'incolumità dell'utilizzatore e del sistema sono quelle che avvengono a livello di cella. Infatti, un cortocircuito interno che riguarda una o più celle del pacco batteria potrebbe non essere rilevato dal BMS, e anche se lo fosse, il BMS, non sarebbe in grado di risolverlo in quanto non può agire a livello meccanico/chimico all'interno della cella e il guasto potrebbe degenerare portando il sistema a incendiarsi e/o all'emanazione nell'ambiente di sostanze chimiche anche tossiche. In conclusione, si può affermare che il grado di affidabilità di un sistema di accumulo elettrochimico, dipende fortemente dall'affidabilità intrinseca delle celle del pacco batteria, in quanto, l'affidabilità del sistema circuitale composto dal BMS rientra, come parametro nelle specifiche di progetto del gruppo di sviluppo di competenza.

5.1 Criticità

Le criticità insite nel presente studio risiedono nella mancanza di informazioni dettagliate sulla relazione esistente tra il fox-BMS 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, ad esempio, il posizionamento dei sensori che rilevano la temperatura potrebbe essere critico. Se posizionati male la misura di temperatura prelevata dal fox-BMS potrebbe non corrispondere con quella delle celle che compongono il pacco. 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 si dovrebbe studiare dal punto di vista probabilistico ogni componente circuitale del sistema, analizzare l'interazione tra sottosistemi e estrarre una valutazione complessiva sull'affidabilità del sistema.

L'assenza di dati riguardanti l'affidabilità dei componenti, rende impossibile ed impropria l'estensione del presente studio ad una più accurata analisi del rischio quantitativa. Il presente studio si è limitato a identificare le possibili sequenze incidentali che potrebbero riguardare un BMS utilizzato in applicazioni di tipo automotive, senza esprimersi sulla probabilità di presentazione di questi eventi incidentali.

6 Abbreviazioni, acronimi e definizioni

ADC	Analog Digital Converter
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)).
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
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
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
Elemento	Costituente della parte del quale si identificano una o più caratteristiche importanti per l'esercizio del sistema
Eventi Iniziatori	Evento (guasto, rottura, errore) che provoca una deviazione dal funzionamento ordinario del sistema, e che potrebbe dare origine ad una sequenza incidentale.
Funzionamento ordinario	Funzionamento dell'impianto/sistema secondo le specifiche del costruttore.
HAZOP	Hazard and Operability Analysis.
I^2C	Inter Integrated Circuit
LOPA	Layer of Protection Analysis
MCU	Monitor Control Unit
NMC	Nickel, Manganese, Cobalto
NTC	Negative Temperature Coefficient
Parola guida	Parola che aiuta il processo sistematico di ricerca di deviazioni dal normale funzionamento della caratteristica dell'elemento considerato
P&Id	Piping and Instrumentation Diagram
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 dalla condizione di funzionamento degli attrezzi, macchine, dispositivi ecc., potenzialmente in grado di causare danni ad un determinato target di riferimento (ambiente, popolazione etc.).
SOA	Safe Operation Area
SOC	State of Charge (Capacità disponibile della batteria o sistema in uso, utilizzato per stimare la corrente di carica di una batteria in uso).
SOH	State Of Health
SPI	Serial Peripheral Interface
SW	Software

7 Riferimenti

[1] M. C. M. Schiavetti, T. Pini, F. D'Errico, "Studio sulla caratterizzazione dei vari livelli di protezione di sistemi di accumulo litio-ione per uso automotive, mediante 'Layer Of Protection Analysis (LOPA)," 2017.

[2] A. Genovese, "Mobilità elettrica sostenibile," 2018.

[3] "fox-BMS." [Online]. Available: https://foxbms.org/.

[4] ISO/DIS 26262-2 road vehicles – functional safety – part 2: management of functional safety; 2009.

[5] K. S. Ng, C. S. Moo, Y. P. Chen, and Y. C. Hsieh, "Enhanced coulomb counting method for estimating state-of-charge and state-of-health of lithium-ion batteries," *Appl. Energy*, vol. 86, no. 9, pp. 1506–1511, 2009.

[6] L. Lu, X. Han, J. Li, J. Hua, and M. Ouyang, "A review on the key issues for lithium-ion battery management in electric vehicles," *J. Power Sources*, vol. 226, pp. 272–288, 2013.

[7] "SOX module." [Online]. Available: https://foxbms.readthedocs.io/en/latest/software_documentation/modules/sox/sox.html.

[8] M. Weber, "Some Safety Aspects on the Design of Sparger Systems for the," *Process Saf. Prog.*, vol. 25, no. 4, pp. 326–330, 2006.

[9] D. H. Doughty and C. C. Crafts, "FreedomCAR Electrical Energy Storage System Abuse Test Manual for Electric and Hybrid Electric Vehicle Applications," *Sandia Natl. Lab.*, no. August, pp. SAND2005-3123, 2006.

8 Curricula del gruppo di lavoro

Roberto Roncella

Il Prof. Roberto Roncella ha conseguito con lode la laurea in Ingegneria Elettronica nel 1984. Nel 1989 ha conseguito il titolo di Dottore di Ricerca. Ha poi prestato servizio come borsista del Consiglio Nazionale delle Ricerche (CSMDR, Pisa). Dal 1990 presta servizio presso il Dipartimento di Ingegneria dell'Informazione (DII) dell'Università di Pisa, prima come ricercatore e dal 1998 come professore associato, ricoprendo numerosi insegnamenti del raggruppamento di Elettronica.

Ha ricoperto il ruolo di responsabile scientifico di unità di ricerca dipartimentali nell'ambito di diversi progetti nazionali, con finanziamento da parte del Consiglio Nazionale delle Ricerche, del Ministero dell'Istruzione, dello Sviluppo Economico e da fondazioni bancarie. Svolge attività come referee per diverse riviste internazionali. Le sue attività di ricerca sono orientate al progetto e collaudo di circuiti integrati ad alta prestazione, quali circuiti per linee di ritardo ad alta risoluzione o circuiti a bassa dissipazione di potenza, alla proposta di nuove architetture VLSI per l'elaborazione numerica dei segnali e più recentemente, alla realizzazione di sistemi elettronici per la gestione e la sicurezza di sistemi basati su accumulatori al litio. In collaborazione con ENEA, è stato responsabile dello sviluppo di un sistema di BMS (*Battery Management System*) per un modulo costituito da celle al litio destinato ad applicazione in veicoli off-road. Nell'ambito di ricerche con finanziamento industriale, si occupa della progettazione di sistemi innovativi applicati all'ambito biomedicale, automobilistico e relativi alla gestione di sistemi di “energy storage” basate su accumulatori con chimica al litio per diverse applicazioni.

Sulle proprie attività ha pubblicato più di cento lavori su riviste o atti di congressi internazionali.

Roberto Saletti

Il Prof. Roberto Saletti ha conseguito con lode la laurea in Ingegneria Elettronica presso l'Università degli Studi di Pisa nel 1981. È stato ricercatore del Consiglio Nazionale delle Ricerche dal 1983 al 1992. Nel 1987 è stato *visiting scientist* presso la Cornell University, Ithaca, New York. In servizio dal 1992 al 2001 come professore associato e dal 2001 ad oggi come professore ordinario presso il "Dipartimento di Ingegneria dell'Informazione" nella Scuola di Ingegneria dell'Università di Pisa. Dal 2003 al 2010 è stato Presidente del Consiglio dei Corsi di Studio in Ingegneria Elettronica e responsabile regionale dell’Indirizzo Scientifico-Tecnologico della Scuola di Specializzazione per l’Insegnamento Secondario (SSIS). Dal 2016 è senatore accademico dell’Università di Pisa.

Ha collaborato alla fondazione, sviluppo e gestione del Centro per le Tecnologie e Applicazioni Microelettroniche (Centro TEAM) di Pisa Ricerche, finanziato dall'Unione Europea e responsabile scientifico di progetti di ricerca nazionali o su commessa di partner industriali quali Piaggio S.p.A, Pershing, Ferretti Yacht, Global Garden Products, FIAMM, etc..

Le sue attività di ricerca sono nell’area del progetto, collaudo e applicazione di sistemi elettronici ad alta prestazione, in particolare di “sistemi embedded”, per l’acquisizione ed elaborazione dati, l’interfacciamento di sensori e il controllo di attuatori su piattaforma elettronica a basso costo. Le principali applicazioni riguardano i sistemi elettronici per il mercato "automotive", sia esso nel campo dei veicoli a due e quattro ruote che delle imbarcazioni da crociera. Le attività recenti sono nel campo dell’elettrificazione dei veicoli, e in particolare verso il monitoraggio e la gestione dei sistemi di accumulo di energia basati su batterie di ultima generazione.

E’ Senior Member dello IEEE e co-fondatore dello IEEE-IES Technical Committee su “Energy Storage Devices and Systems”.

Federico Baronti

Il Prof. Federico Baronti ha conseguito con lode la laurea in Ingegneria Elettronica presso l'Università di Pisa nel 2001 e il titolo di Dottore di Ricerca, sempre presso la stessa università, nel 2005. Dopo il dottorato, ha prestato servizio presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Pisa, prima come assegnista di ricerca, poi come ricercatore universitario e dal 2017 come professore associato. Le sue attività di ricerca hanno riguardato lo studio e progetto di sistemi innovativi mirati a migliorare le prestazioni, sicurezza e comfort dei veicoli terrestri. Più recentemente sta lavorando alla modellizzazione delle batterie agli ioni di litio, allo sviluppo di algoritmi per la stima dello stato interno della batteria e alla progettazioni di "Battery Management System". È stato ed è responsabile di vari progetti finanziati dalla comunità europea e da aziende private. Sulle sue attività ha pubblicato più di 100 lavori su riviste e atti di conferenze internazionali. Baronti è *Senior Member* dell'IEEE, è stato chair dal 2015 al 2017 del comitato tecnico sull'Energy Storage dell'IEEE *Industrial Electronics Society* (IES), per la quale ha prestato servizio come *AdCom Member* dal 2015 al 2018. È associate editor per la rivista *Transactions on Industrial Informatics*. Ha svolto il ruolo di guest editor in diverse *special section* delle *Transactions on Industrial Electronics and Industrial Informatics*, *track chair* e organizzatore di *special session* in diverse conferenze sponsorizzate dall'IES, dove ha tenuto vari seminari su tematiche relative all' *energy storage*. Ha ricevuto il premio come miglior *paper dell'Industrial Electronics Magazine* nel 2013.

Roberto Di Rienzo

Si è laureato in Ingegneria Elettronica presso l'Università di Pisa nel 2014. Dopo una borsa di studio svolta presso il DII, ha conseguito nel 2018 il dottorato di ricerca in Ingegneria dell'Informazione. Attualmente è beneficiario di un assegno di ricerca cofinanziato dalla regione Toscana. Nelle sue attività di ricerca si è focalizzato sui sistemi di immagazzinamento dell'energia elettrica con particolare attenzione sulle batterie agli ioni di litio. In tale ambito, ha collaborato alla modellizzazione elettrica di diverse tecnologie di celle agli ioni di litio, allo sviluppo di algoritmi avanzati di stima dello stato di carica e salute di queste celle e alla progettazione e realizzazione di sistemi elettronici di gestione di batterie di medio e grande formato.
Attività di ricerca più recenti sono state svolte nell'ambito dell'agricoltura di precisione, in cui si è concentrato nello studio e sviluppo di un sistema di misura, basato sensori ultrasonici low-cost, in grado di eseguire una scansione tridimensionale di una coltivazione per estrarne informazioni sul volume vegetativo da utilizzare per ottimizzare le lavorazioni agricole da eseguire su di essa.

Andrea Carloni

Ha conseguito la laurea in Ingegneria Elettronica presso l'università di Pisa nel 2017. È attualmente al secondo anno del Dottorato di Ricerca in Ingegneria dell'Informazione presso la stessa università. Svolge attività di ricerca sul tema della ricarica senza fili di batterie e sullo sviluppo di strumentazione completamente open-source per la caratterizzazione di singole celle agli ioni di litio e in generale su sistemi di accumulo elettrochimico.