논문 2021-16-11

BMS의 위험우선순위 분석과 기능안전을 고려한 설계

(Analysis of Risk Priority Number and Functionally Safe Design of Battery Management System)

김 운 동, 이 순 구, 강 대 근*
(WoonDong Kim, SunGu Lee, DaeKeun Kang)

Abstract : In recent years, as ESS has become very popular, BMS related electric fires have occurring frequently. In this research we performed analysis of risk priority number (RPN) using Failure Mode and Effects Analysis (FMEA) technique to analyze the safety of BMS, which accounts for the most part in ESS electric fires. And the functional safety concept was used to eliminate or reduce failure modes that may cause overvoltage, overcurrent, and overheating for higher risk priorities of the analyzed BMS. The BMS hardware was redesigned so that the safety mechanism works for the high-priority risk modes, and the main firmware procedures were designed to control the battery against potential malfunctions. And we implemented the improved BMS hardware and experimentally verified that the safety mechanism works as designed. The test results have confirmed that the safety mechanism works normally and the battery can be controlled even if overvoltage, overcurrent and overheating occurs in the BMS, or major firmware procedures malfunction. Therefore we are confident that electric fires related to ESS can be prevented in advance by analyzing the safety of BMS in the way we used in this research to find high-priority risk factors and applying the concept of safety functions to the hardware and software design of BMS.

Keywords : Battery Management System, FMEA, Energy Storage System, Functional Safety, Risk Priority Number

Ⅰ. 서 론

최근에 모바일 기기, 전기 자동차 등 배터리를 사용하는 다양한 장치들이 급격히 증가함에 따라 에너지저장시스템 (Energy Storage System, ESS)에 대한 관심과 연구도 점점 증가하고 있다. ESS는 전기를 저장하였다가 필요한 때에 이용할 수 있도록 하는 장치를 말하며, 일반적으로 전기를 저장할 수 있는 배터리, 각 배터리 셀의 상태를 모니터링하고 오작동을 감지하는 배터리 관리 시스템 (Battery Management System, BMS)과 배터리에 충·방전하는 전력을 제어하는 전력변환시스템 (Power Conversion System, PCS), 배터리 충·방전 시간제어나 발전량과 수요량을 예측하고 최적의 운영을 위한 소프트웨어인 에너지관리시스템 (Energy Management System, EMS)로 구성되어 있다 [1]. 배터리는 여러 가지 종류가 있지만 에너지 밀도가 높고 효율이 우수한 리튬이온 배터리가 하이브리드 자동차, 전기자동차 등을 포함하는 산업전반에 널리 사용되고 있으며, 대량보급과 기술발전으로 생산원가가 점점 낮아지고 있다. 그러나 리튬이온 (Lithium-ion) 배터리는 종래 Ni-Cd나 Ni-MH 배터리와 비교하여 상대적으로 과열, 수분침투 및 단락시 화재나 폭발 위험성이 있어 안전한 사용을 위해 이에 대한 제어가 매우 중요하다 [2].

국내에서 최근 몇 년 전부터 ESS가 널리 보급되어 사용하고 있는 바 ESS 관련 화재가 2015년부터 2019년 6월까지 총 23건 보고되었다 [3]. 지금까지 발생한 화재는 ESS가 옥외에 설치되어 있어 인명피해는 발행하지 않았지만, 다중이용시설과 같은 옥내에 설치된 ESS에서 전기 화재가 발생한다면 재산적 손실 뿐 아니라 인명 피해까지 발생할 수 있다 [4]. ESS 화재발생시 설비가 대부분 전소되기 때문에 그 원인이 불분명하고 정확한 원인을 밝히는 것이 쉽지 않기 때문에 2019년 1월부터 공공기관의 ESS는 가동중지 조치가 내려진 상태이다 [3]. ESS 관련 화재사건에서 사고원인이 분석된 7건 중 4건이 BMS 오류에 의한 것으로 추정된 사실에서도 알 수 있듯이 ESS 관련 전기화재 중에서 BMS와 관련한 사고가 가장 높은 비율을 차지하고 있다 [5]. 이에 따라 2019년 10월부터 국가기술표준원에서 전기저장장치 발화·화재 사고 재발방지를 위한 안전관리 강화 대책의 일환으로 에너지저장장치용 리튬이차전지 시스템에 대한 기능안전 시험을 받도록 고시하고 있다 [6].

BMS는 각 배터리 셀의 충전상태, 온도, 전압, 전류를 상시 모니터링하고, 배터리의 충전량 (State of Charge, SOC)을 예측하거나 측정하고 각 배터리 셀의 충 방전 수준이 균형되도록 조정하는 셀 밸런싱 등의 기본적인 기능 뿐 아니

*Corresponding Author (dkkang@huconn.com)
Received: Feb. 15, 2021, Revised: Mar. 24, 2021, Accepted: Apr. 4, 2021.
W.D. Kim: Huconn Co., Ltd. (Senior Researcher)
S.G. Lee: Huconn Co., Ltd. (Senior Researcher)
D.G. Kang: Huconn Co., Ltd. (CEO)
※ 본 연구는 한국산업기술진흥원이 지원하는 지역특화산업육성+(R&D) 사업의 일환으로 수행되었습니다 (S2934696).

ⓒ IEMEK J. Embed. Sys. Appl. 2021 Apr. 16(2) 79-88
ISSN : 1975-5066
http://dx.doi.org/10.14372/IEMEK.2021.16.2.79

라 배터리 안전을 위해 과전압, 과전류, 과열 등을 방지하기 위한 기능 및 회로도 반드시 포함해야 한다. 또한 보호회로나 펌웨어 오동작으로 인해 과전압 (Over Voltage, OV), 과전류 (Over Current, OC), 과열 (Over Temperature, OT)이 발생하는 경우에도 배터리를 제어할 수 있는 시스템 설계가 요구된다. 따라서 BMS 부품 결함이나 펌웨어 오동작이 시스템에 미치는 영향을 분석할 필요가 있고, 랜덤 결함 혹은 에이징 (aging)에 의해 고장 발생빈도가 높은 부품 및 펌웨어 기능에 대한 위험수준을 분석하여 이를 제거하거나 줄이기 위한 하드웨어 및 소프트웨어 설계가 요구된다 [7].

지금까지 국내 ESS 산업은 에너지저장장치를 보급하는 단계였고, ESS의 용량을 늘리거나 경제성 및 효율에 대한 연구가 주로 이루어지고 상대적으로 배터리 안전에 대한 연구나 관리는 미흡한 수준이다. 그리고 최근에 BMS를 포함하는 전체 ESS의 위험우선순위 분석이나 ESS 구성부품별 화재 리스크평가에 대한 연구가 있었지만, ESS 관련 전기화재사고와 밀접한 관련이 있는 BMS의 안전성 분석이나 기능안전을 고려한 설계에 대한 연구는 아직 활발하게 이루어지지 않고 있다 [8]. 최근에 ESS에 대한 안전 리스크 평가에 제품이나 프로세스의 신뢰성 평가에 많이 사용되는 FMEA (Failure Mode and Effects Analysis, FMEA)나 FTA (Fault Tree Analysis, FTA) 기법을 사용하여 연구가 진행되었다 [3, 9].

따라서 본 연구에서는 시스템이나 프로세스의 잠재적인 고장위험을 찾아내고 분석하는데 일반적으로 많이 사용되는 FMEA기법에 대해 간략히 기술한 다음, 기본적인 BMS의 각 구성 부품에 대하여 고장모드영향분석 (FMEA)을 실시하고 위험우선순위지수 (Risk Priority Number, RPN) 분석을 하고자 한다. 그리고 분석결과를 통해 위험순위가 높은 고장모드를 찾고, 이를 제거하거나 줄이기 위해 기능안전 개념을 적용하여 BMS 하드웨어 및 펌웨어를 재설계하고자 한다. 그리고 이를 BMS 하드웨어로 제작하여 잠재적인 부품결함이나 펌웨어 오작동으로 인해 과전류나 과전압, 과열이 발생한 경우에도 BMS가 안전하게 배터리를 제어할 수 있음을 실험으로 검증하고자 한다.

Ⅱ. 본 론

1. FMEA 기법

FMEA는 부품이나 프로세스가 의도한 대로 기능하지 않을 잠재적인 고장원인을 찾아내서 그것이 전체 시스템의 동작에 미치는 영향을 평가하고, 고장위험의 원인되는 요소를 제거하거나 줄이기 위해 개발된 기법이다 [10]. FMEA의 목표는 제품 개발이나 제조공정 초기에 잠재적인 결함을 찾아냄으로써 고장을 미연에 방지하고, 안전성을 증가시기 위함이다. FMEA는 처음에 위험요소를 찾기 위한 도구로 개발되었지만, 회계나 재무 분야에서 신용이나 투자위험을 평가하거나 소프트웨어개발 분야에서 프로그램 버그나 오류를 찾아 개선하거나, 정보통신 분야, 마케팅, 의료 등의 분야에

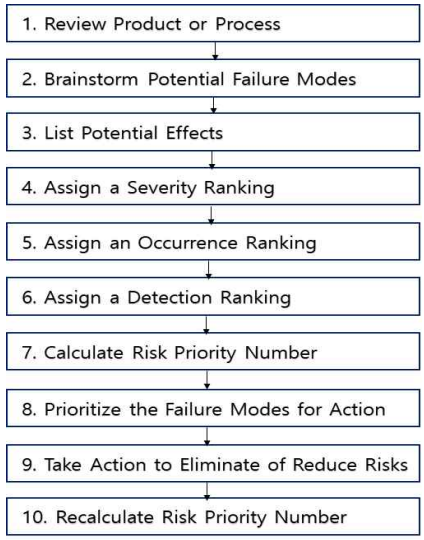

그림 1. FMEA 프로세스 단계
Fig. 1. Step of FMEA process

도 활용되고 있다 [10]. FMEA의 분석결과는 제품의 잠재적인 고장 및 위험발생 가능성을 찾아서 개선함으로써 제품의 사용수명을 연장시키거나 사용자 안전을 개선하는데 매우 중요한 자료로 활용된다. FMEA 기법에서 위험모드를 찾고 각 원인과 영향에 대한 평가는 주로 유사한 제품이나 프로세스에 대한 과거 경험 혹은 일반적인 고장 메커니즘에 근거하여 이루어진다. FMEA 프로세스는 그림 1에 주어진 순서에 따라 진행된다.

2. 위험우선순위지수 (RPN)

고장모드는 부품의 결함이나 고유 특성 변화, 프로세스의 오작동 등에 의해 발생된다. 그리고 이것은 부품이나 프로세스에 존재하는 고유한 고장발생 메커니즘을 검토함으로써 알 수 있다 [10]. 그러나 물리적 부품의 경우 고장모드 및 고장발생 원인 데이터는 제조사들이 사적 자산으로 관리하고 있어서 이에 대한 자료를 수집하는 것은 쉽지 않다. 따라서 신재생과 관련하여 미국의 “SEMATECH”에서 제시한 위험우선순위를 토대로 심각도, 발생도, 검출도의 등급을 제시하였다 [8]. 이것은 참고문헌 8에서 참고문헌 6의 “INTERNATIONAL SEMATECH, Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry, 1992” 논문을 인용한 것이다.

2.1 심각도 순위 기준 (Severity Ranking Criteria)

심각도 (Severity)는 해당 고장모드가 발생하면 일어나면 얼마나 심각한 영향이 있는지를 평가하는 척도이다. 본 연구에서는 BMS에 대한 개략적인 심각도를 판별하고자 하므로 표 1에 제시한 대로 분류 기준을 5단계로 구분하고자 한다. 참고적으로 일반적으로 제품이나 프로세스에 대해 정밀한 위험우선순위를 분석하고자 하는 경우 10단계로 구분한다.

표 1. ESS의 심각도 순위 기준
Table 1. Severity ranking criteria of ESS [8]

Rank	Description
1	Failure is of such minor nature that the customer (internal or external) will probably not detect the failure.
2	Failure will result in slight customer annoyance and/or slight deterioration of part or system performance.
3	Failure will result in customer dissatisfaction and annoyance and/or deterioration of part or system performance.
4	Failure will result in high degree of customer dissatisfaction and cause non-functionality of system.
5	Failure will result in major customer dissatisfaction and cause nonsystem operation or non-compliance with government regulation.

2.2 발생도 순위 기준 (Occurrence Ranking Criteria)

발생도 (Occurrence)는 해당 고장모드가 얼마나 빈번하게 발생할 수 있는지를 평가하는 척도이다. 부품의 예상 기대 수명 동안 잠재적으로 발생할 수 있는 고장으로 단위시간당 잠재발생률로 나타내었다. FMEA에서 사용하기 위한 순위 기준은 표 2에 제시하였다.

NOTE: Quantitative data were used if it is available.
For Example:
0.001 = 1 failure in 1,000 hours
0.01 = 1 failure in 100 hours
0.10 = 1 failure in 10 hours

2.3 검출도 순위 기준 (Detectability Ranking Criteria)

검출도 (Detectability)는 사고가 발생하기 전에 고장모드 혹은 고장의 영향을 얼마나 쉽게 미리 감지할 수 있는지에 대한 평가척도이다. 이것은 사고가 일어나기 전에 위험이나 고장의 잠재적인 원인이나 메커니즘을 감지하고 대응하는 운용능력과 관련이 있다. 감지순위 기준은 부품 및 펌웨어에서 감지확률을 5단계 평가기준으로 제시하였다. 1단계는 감지될 확률이 매우 높음을 의미하고, 5단계는 감지확률이 매우 낮거나 거의 감지될 확률이 없는 경우를 말한다. 표 3은 검출도 순위 기준을 나타낸다.

위험우선순위지수 (RPN)은 심각도, 발생도, 검출도에 동일한 중요성을 두고 식 (1)과 같이 평가한다.

$$RPN = 심각도 \times 발생도 \times 검출도. \quad (1)$$

각 기준을 1-5단계로 제시하였으므로, RPN 값은 1과 125 사이의 값이며 값이 크면 고장위험이 높거나 안전에 취약하므로 제거 및 개선의 대상이 된다. 위험우선순위 결정은 각 고장모드에 대한 RPN 값으로 결정한다. 일반적으로 RPN이 1~10은 무시할 수 있는 위험, 10~29는 경미한 위험, 30~63은 상당한 위험, 64~80은 중대한 위험, 81~125로 평가

표 2. 발생도 순위 기준
Table 2. Occurrence ranking criteria [8]

Rank	Description
1	An unlikely probability of occurrence during the item operating time interval. Unlikely is defined as a single failure mode (FM) probability < 0.001 of the overall probability of failure during the item operating time interval.
2	A remote probability of occurrence during the item operating time interval (i. e. once every two months). Remote is defined as a single FM probability > 0.001 but < 0.01 of the overall probability of failure during the item operating time interval.
3	An occasional probability of occurrence during the item operating time interval (i. e. once a month). Occasional is defined as a single FM probability > 0.01 but < 0.10 of the overall probability of failure during the item operating time interval.
4	A moderate probability of occurrence during the item operating time interval (i. e. once every two weeks). Probable is defined as a single FM probability > 0.10 but < 0.20 of the overall probability of failure during the item operating time interval.
5	A high probability of occurrence during the item operating time interval (i. e. once a week). High probability is defined as a single FM probability > 0.20 of the overall probability of failure during the item operating interval.

표 3. 검출도 순위 기준
Table 3. Detectability ranking criteria [8]

Rank	Description
1	Almost certain that the problem will be detected (chance 81 - 100%)
2	High probability that the problem will be detected (chance 61 - 80%)
3	Moderate probability that the problem will be detected (chance 41 - 60%)
4	Low probability that the problem will be detected (chance 21 - 40%)
5	None/minimal probability that the problem will be detected (chance 0 - 20%)

된 고장 모드를 허용불가 위험으로 분류한다 [3].

3. BMS 구성도 및 부품분류

ESS의 배터리관리시스템 (BMS)에 FMEA를 적용하기 위해서는 BMS의 작동 메커니즘에 대한 이해가 필요하다 [1, 11]. 본 연구에서는 기본적인 BMS의 작동 흐름도와 시스템 설계를 제시하고, 이에 대한 FMEA 분석을 실시하여 위험우선순위지수를 도출하였다. 그리고 BMS의 안전에 영향을 미치는 위험모드를 찾아서 이것들을 제거하거나 줄이기 위한 방안을 제시하고 기능안전을 고려한 BMS를 설계를 제안하고 제작하여 실험으로 검증하였다. 그림 2는 간략화한 BMS에 대한 동작 흐름도이다.

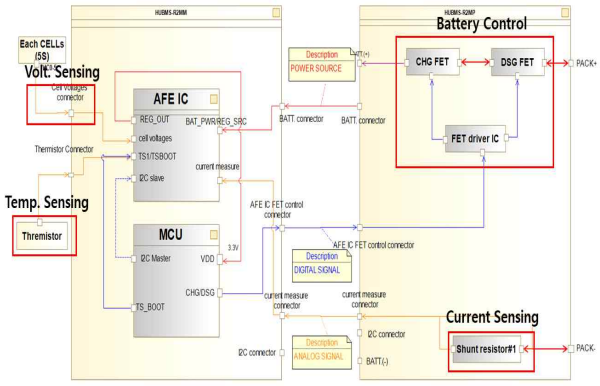

그림 2. 기본적인 BMS 동작 흐름도
Fig. 2. Basic BMS operation flow chart

표 4. BMS 주요 구성부품 고장률 데이터
Table 4. Main components failure rate for BMS

Component	Failure Rate 10^6 hr
Li-ion Battery	2.24
AFE IC	1.59
MCU	2.25
Charging FET	2.23
Discharging FET	2.23
FET Driver IC	2.00
Voltage Regulator	0.029
Thermistor	3.47
Shunt Registor	3.74

그림 2에서 BMS는 크게 배터리 모듈과 아날로그 프론트 엔드 (Analog Front End, AFE), MCU, 제어부로 이루어져 있다. 배터리 모듈은 여러 개의 셀들을 직렬 혹은 병렬연결하여 대용량을 구현한 것이며, AFE는 각 배터리 셀들의 전압, 전류, 온도 등을 측정하여 MCU에 전송하며, MCU는 이들 데이터를 바탕으로 과전압 (OV)나 과전류 (OC), 과열 (OT) 등이 발생하면 배터리모듈을 외부 회로와 연결을 차단하는 역할을 한다. AFE에서 전압은 배터리 셀 전압을 검출하고, 배터리 전류는 Shunt 저항을 통해, 배터리 온도는 써미스터를 사용하여 측정한다.

본 BMS 설계에 사용한 주요 구성부품에 대한 고장률은 표 4에 제시하였다. 그러나 BMS와 관련된 구성 부품에 대한 고장에 대한 정량적 정보나 통계는 제조사의 노하우로 인하여 공개를 꺼려하기 때문에, 표 4에 제시한 데이터는 국내 SCI 논문이나 각 부품 데이터시트 등을 검토하여 파악하였다 [8]. 각 부품에 대한 고장률은 RPN에서 각 위험모드에 대한 발생도 (Occurrence) 산출의 근거로 사용된다.

4. 위험우선순위지수분석

그림 2의 BMS의 동작 메커니즘과 표 4의 주요부품에 대한 고장률을 바탕으로 FMEA 분석을 수행한 결과는 표 5에 제시하였다.

표 5의 FMEA 분석에서 상당한 위험이나 중대한 위험에 해당하는 RPN값이 40이상인 경우에 대한 위험모드들을 표 6에 제시하였다.

표 5. 기본 BMS에 대한 FMEA 분석표
Table 5. FMEA results for basic BMS

Part. ID	Potential Failure Mode	Potential Causes	Potential Effects	SEV	OCC	DET	RPN
100	**Li-ion Battery**						
101	short circuit	cell balancing error	wrong battery connection	4	2	2	16
102	Abnormal output voltage	Low battery capacity, overheating	Load damage, battery explosion	5	2	3	30
103	No output	Poor performance	ESS malfunction	4	2	2	16
104	Cracking	lower battery capacity	ESS performance degradation	4	2	3	16
105	Discontinuous operation	lower battery capacity	ESS performance degradation	4	2	2	16
200	**AFE IC**						
201	AFE IC fault	component fault	Measurement monitoring and control impossible	5	1	5	25
202	Voltage measurement error	Measurement circuit component error	no overvoltage control	5	2	5	50
203	Current measurement error	Measurement circuit component error	no overcurrent control	5	2	5	50
204	Temperature measurement error	Measurement circuit component error	Fire or explosion	5	2	5	50
300	**MCU**						
301	Operation error	unstable voltage/clock	no battery control	4	2	5	40
302	Bits error (SRAM/FlASH)	unstable voltage/clock	no battery control	4	2	5	40
303	I2C Communication failure	I2C circuit fault, unstable voltage/clock	no receiving AFE current	4	2	2	16
304	ADC Read error	Measurement circuit error unstable voltage/clock	MCU temperature error	5	2	5	50
400	**Charging FET**						
401	Inoperative	component fault	no safety function	5	2	3	30
500	**Discharging FET**						
501	Inoperative	component fault	no safety function	5	2	3	30
600	**FET Driver IC**						
601	IC fault	IC 결함	No battery control	5	2	3	30
602	FET control failure	FET fault and control circuit abnormality	No battery control	4	2	3	24
700	**Thermistor**						
701	Abnormal resistance change	component fault	no battery voltage measurement	5	3	5	75
800	**Shunt Registor**						
801	abnormal behavior	component fault	battery current measurement error	5	3	5	50

표 6. 위험수준이 높은 고장모드
Table 6. Highly critical failure modes

Part ID	Potential Failure Mode	Potential Causes	Potential Effects	SEV	OCC	DET	RPN
300	**MCU**						
301	Operation error	unstable voltage/clock	no battery control	4	2	5	40
302	bits error (SRAM/FIASH)	unstable voltage/clock	no battery control	4	2	5	40
304	ADC Read error	Measurement circuit error unstable voltage/clock	MCU temperature error	5	2	5	50
200	**AFE IC**						
202	Voltage measurement error	Measurement circuit component error	no overvoltage control	5	2	5	50
203	Current measurement error	Measurement circuit component error	no overcurrent control	5	2	5	50
204	Temperature measurement error	Measurement circuit component error	Fire or explosion	5	2	5	50
700	**Thermistor**						
701	Abnormal resistance change	component fault	no battery voltage measurement	5	3	5	75
800	**Shunt Registor**						
801	abnormal behavior	component fault	battery current measurement error	5	3	5	75

표 6에서 BMS 각 부품들의 랜덤 결함이나 에이징에 의해 1) MCU의 클럭 불안정, 2) AFE IC에 의한 전압, 전류, 온도 측정 오류, 3) 써미스터의 비정상적인 저항값 변화로 배터리 셀의 과전류 측정 오류 등에 의해 BMS가 배터리 모듈을 제어를 할 수 없는 잠재적인 위험이 발생할 수 있음을 확인할 수 있다.

따라서 서론에 언급한 바와 같이 ESS의 안전한 운용을 위해서 BMS의 역할이 매우 중요한 만큼 과전압, 과전류, 과열이 발생할 수 있는 잠재적인 가능성에 대하여 상시 안전메커니즘이 작동하는 BMS 하드웨어 및 펌웨어 설계와 운용이 요구된다.

5. 기능안전을 고려한 BMS 하드웨어 및 펌웨어 설계

국가기술표준원에서는 에너지저장장치 발화·화재 사고 재발방지를 위한 안전관리 강화 대책의 일환으로 에너지저장장치용 리튬이차전지 시스템에 대한 기능안전 시험을 받도록 고시하고 있으며, 기술기준은 “KC 62619 Ed 1.0-제정고시 제2019-0309호의 부속서D”에 개념적으로 제시되어 있다 [6]. 이것을 참고하면 안전을 고려한 BMS 설계를 위해서는 하드웨어와 소프트웨어에 대하여 다음과 같은 사항들을 고려해야 한다 (KC 62619 부속서 D 세부기준 참고) [6].

1) 배터리 셀의 과전압, 과전류, 과열을 검출할 수 있어야 한다.
2) 시스템이 오작동이나 고장을 일으킬 경우에도 위험한 상황이 발생하지 않고 안전상태가 되도록 설계해야 한다.
3) 시스템 오작동에 대해 결함을 검출하거나 방지하기 위한 기술적 해결책을 구현되어야 한다.
4) 기능안전은 하드웨어 설계에만 해당되는 것이 아니라 펌웨어와 하드웨어 모두에 대하여 제어 흐름, 데이터 흐름, 타이밍을 고려하여 구조적인 설계가 이루어져야 한다.

즉, BMS는 배터리 셀의 전류, 전압, 온도에 대한 신뢰성 있는 값을 검출할 수 있어야 하며 과전압, 과전류, 과열이 발생하면 배터리를 외부 시스템과 차단하도록 설계되어야 한다. 기능안전 관점에서 그림 2의 BMS는 다음과 같은 문제점이 있다.

1) 배터리 셀의 전압, 전류, 온도 검출이 단일 채널이기 때문에 측정값의 신뢰성을 보장할 수 없다.
2) 전압, 전류, 온도에 대한 센싱이 단일채널이므로 센서 결함이나 고장이 발생하는 경우 전압, 전류, 온도를 센싱할 수 없거나 측정값이 신뢰할 수 없다.
3) 전압, 전류, 온도 측정값이 올바르게 센싱되더라도 MCU의 클럭 주파수 불안정한 경우 배터리를 제어할 수 없다.
4) MCU나 펌웨어 오류가 발생하는 경우 배터리를 제어할 수 없다.

따라서 본 BMS에 대한 FMEA의 위험우선순위지수 값이 높은 위험모드를 제거하거나 줄이기 위해 BMS의 하드웨어 및 펌웨어에 대하여 다음과 같은 사항들을 추가하거나 보완하였다.

1) 전압 센싱은 AFE에서 배터리 셀 전압을 측정할 뿐 아니라 추가적으로 MCU에서 전압 센서값을 검출하도록 하였다.
2) 전류 센싱도 AFE에서 Shunt 저항을 이용하여 센싱할 뿐 아니라, MCU에서도 전류센서를 통해 검출하도록 하였다.
3) 온도 측정은 2개의 써미스터를 사용하여 각각 AFE와 MCU에서 온도값을 측정하여 서로 비교함으로써 온도값의 신뢰성을 확보하도록 했다.
4) 제어부도 AFE와 MCU에 이중채널로 FET와 FET 드라이버를 제어하도록 함으로써 하나의 채널이 문제가 발생한 경우에도 배터리를 제어할 수 있도록 구성했다.
5) MCU 뿐 아니라 AFE에서도 과전류, 과전압, 과열이 검출되면 제어부의 FET 드라이버를 제어할 수 있도록 AFE Companion IC를 추가했다.
6) MCU의 사용시간이 오래되거나 랜덤 결함이 발생하여

클럭이 불안정한 경우에 대비하여 외부 수정발진기를 추가하고, 이 클럭 주파수를 MCU 클럭 주파수 값과 비교함으로써 클럭 주파수 불안정한 경우 배터리를 제어할 수 있도록 했다.

7) 펌웨어 주요 프로시저들도 동작에 오류가 발생하는 경우 정해진 시간 후에 배터리를 외부회로와 차단하도록 설계하였다.

위에 설명한 기술적 사항들을 바탕으로 기능안전 개념을 적용한 BMS의 시스템 구성도는 그림 3과 같다.

그림 3에서 재설계한 BMS 시스템에서 배터리 셀의 전압, 전류, 온도 센싱을 이중화하여 각 검출값을 비교함으로써 데이터의 신뢰성을 확보하였고, 두 개의 검출 값이 규정값 이상의 차이가 발행하는 경우 센서에 문제가 있는 것으로 판단하여 배터리 셀을 외부와 차단하도록 하였다. 또한 외부 수정발진기를 추가하여 MCU 내부 클럭주파수와 값을 비교하여 클럭 주파수의 신뢰성을 확보함으로써 잠재적인 연산오류나 비트오류, I2C 통신이나 ADC에 의한 전류, 전압값의 오류를 검출하여 배터리 셀을 제어할 수 있도록 했다. 배터리 제어부도 AFE와 MCU에서 이중채널로 구성함으로써 어느 하나의 FET나 FET 드라이브에 고장이 발생하는 경우에도 배터리 셀을 제어할 수 있도록 설계하였다 [1, 11-13]. 그러나 과전압, 과전류, 고온, 부품결함, 펌웨어 오류 등 위험요소가 발생하는 경우에 BMS가 배터리 팩을 외부회로와 차단하지만, 전압, 전류, 온도가 안전 수준 상태로 복귀하면 원래 ESS 기능을 수행하도록 펌웨어를 설계하고 작성하였다.

Ⅲ. 실험결과

1. 구현된 BMS 보드

그림 4는 상기 BMS의 안전성 문제를 해결하기 위해 부품 결함이나 펌웨어 기능 오작동 등이 발생하는 경우에도 안전메커니즘이 작동하도록 설계하고 구현한 BMS 보드이다. 또한 펌웨어 주요 프로시저에 대해서도 표 7에 제시한 명세에 따라 안전메커니즘이 작동하도록 설계하고 개발하였다.

2. 실험환경

그림 5는 구현된 BMS의 안전메커니즘을 테스트하기 위한 실험환경으로 BMS 보드, 부하기능을 위한 Electronic Load, 전원공급기, 오실로스코프 및 BMS 보드의 주요 부품의 전기적 상태를 모니터링하기 위한 로깅용 컴퓨터로 구성된다. 구현된 BMS의 안전메커니즘이 제대로 작동하는지 테스트하기 위해서는 BMS에 과전압, 과전류, 과열 상황을 고의적으로 발생시켜야 한다. 과전압은 배터리 셀에 전원공급기로 과전압을 인가하여 발생시키고, 과전류는 로드장비를 연결하여 고전류를 흐르도록 해서 발생시켰다. 또한 과열은 써미스터를 가변저항으로 대체하여 저항값을 변화시킴으로써 발생되도록 하였다.

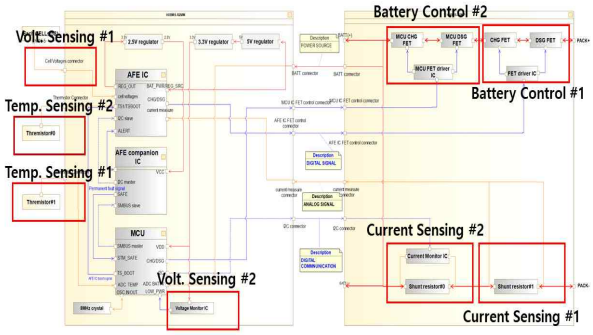

그림 3. 기능안전을 고려한 BMS 동작 흐름도
Fig. 3. Flow chart for the functionally safe BMS

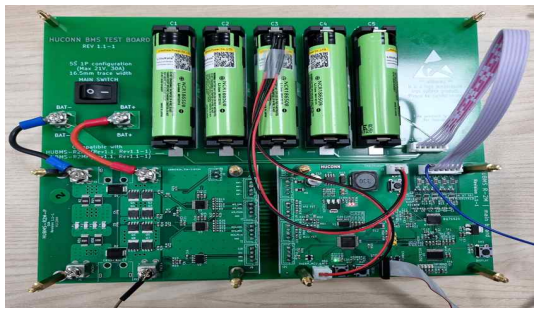

그림 4. 구현된 BMS 보드
Fig. 4. Embodied BMS board

표 7. BMS의 기능안전을 위한 주요 펌웨어 동작
Table 7. Main firmware operation for the functionally safe BMS

Detection target	**MCU IC CPU operation error**
prerequisite	After MCU initialization
diagnosis time	Periodic check of MCU software
safe state	MCU CHG/DSG FET OFF
Detection target	**MCU IC's built-in SRAM bit error**
prerequisite	After MCU initialization
diagnosis time	SRAM 1-bit error detection point
safe state	MCU CHG/DSG FET OFF
Detection target	**MCU IC's built-in FLASH bit error**
prerequisite	After MCU initialization
diagnosis time	Initialization of MCU and double error of FLASH
safe state	MCU CHG/DSG FET OFF
Detection target	**Software task not working or abnormal flow behavior**
prerequisite	After MCU initialization
diagnosis time	Periodic check of MCU software
safe state	MCU CHG/DSG FET OFF
Detection target	**Software task stackoverflow**
prerequisite	After MCU initialization
diagnosis time	Periodic check of MCU software
safe state	MCU CHG/DSG FET OFF

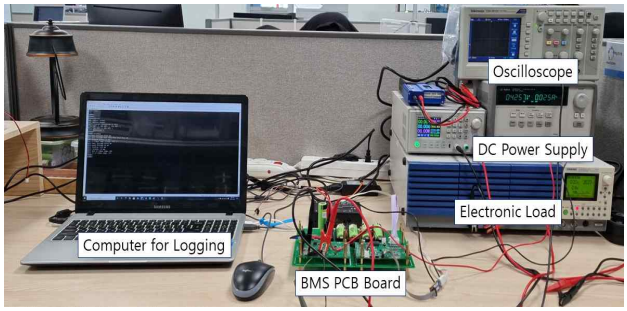

그림 5. BMS 안전메커니즘을 테스트하기 위한 실험환경
Fig. 5. Test setup for BMS safety mechanism

3. 실험결과

그림 6은 구현된 BMS에 대한 안전메커니즘 작동을 테스트한 결과이다. 그림 6 (a)는 과전압에 대한 테스트 결과로 배터리 셀 전압을 4.25V에서 과전압인 4.3V로 높여주면, 3초 뒤에 FET가 OFF된다. 그림 6 (b)는 방전 중 과전류 테스트이며, 방전 중 배터리 전압은 낮아지며, 연결된 로드 장치를 통해 과전류가 흐르는 경우 8초 뒤에 FET가 OFF 된다. 그림 6 (c)는 충전 중 과전류 테스트인데, 충전 중 배터리 전압은 높아지며, 전원공급기를 통해 배터리에 과전류가 흐르도록 했으며, 7초 뒤에 FET가 OFF 된다. 그림 6 (d)는 과열에 대한 테스트이며, 써미스터 전압이 낮아져서 과열이 발생하는 경우 2초 뒤에 FET가 OFF된다. 이상과 같이 배터리 셀에 과전압, 과전류, 과열이 발생하는 경우 설정된 시점 (초)이후에 FET를 OFF 시킴으로써 상시 안전메커니즘이 정상적으로 작동됨을 알 수 있다. 그리고 배터리팩의 전압, 전류, 온도값이 안전한 상태로 복귀하면 차단된 FET는 다시 ON되어 원래 ESS 기능을 수행하는 것을 확인하였다.

또한 펌웨어 기능함수의 안전메커니즘 테스트와 관련하여

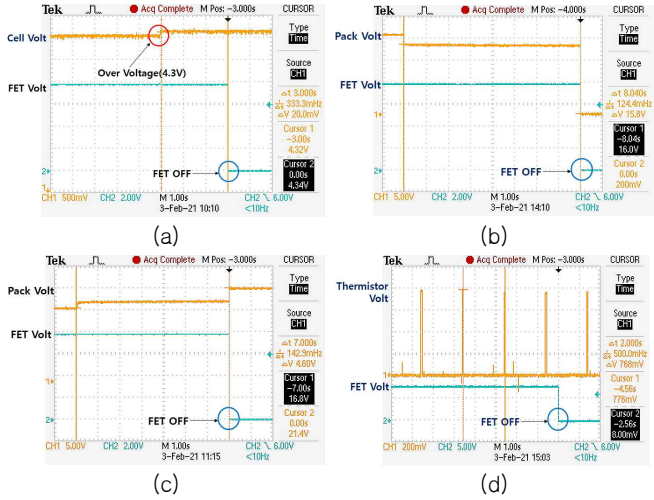

그림 6. 구현된 BMS 테스트 결과
(a) 과전압 테스트 (b) 방전 중 과전류 테스트
(c) 충전 중 과전류 테스트 (d) 과열 테스트
Fig. 6. Test result for the embodied BMS
(a) Over voltage test (b) Over current test for discharging
(c) Over current test for charging (d) Over temperature test

Task의 주기가 정해진 범위를 벗어나는 경우 와치독 동작을 확인했고, Task의 주기적 프로시저의 일부가 수행되지 않은 경우 Flow 체크 오류 발생과 FET 제어를 확인했고, Task의 stack overflow 상황시 오류 발생과 FET 제어를 확인함으로써 BMS의 펌웨어 주요 프로시저들도 안전메커니즘이 정상적으로 작동됨을 알 수 있다. 재설계한 BMS의 구성부품 뿐 아니라 소프트웨어의 주요 프로시저에 대해서도 FMEA 분석을 수행했으며, 그 결과는 표 8에 제시하였다 [14].

표 8. 기능안전을 적용한 BMS의 FMEA 분석표
Table 8. FMEA results for our functionally safe BMS

Comp ID	Failure Mode	Potential Causes	Potential Effects	SEV	OCC	DET	RPN
A100	**AFE IC**						
A101	AFE IC fault	component fault	Measurement monitoring and control impossible	5	1	1	5
A102	Voltage measurement error	Measurement circuit component error	no overvoltage control	5	2	1	10
A103	Current measurement error	Measurement circuit component error	no overcurrent control	5	2	1	10
A104	Temperature measurement error	Measurement circuit component error	Fire or explosion	5	2	1	10
A200	**AFE Companion IC**						
A201	IC fault	component fault	no monitoring in MCU	5	1	1	5
A202	I2C fault	AFE IC fault, circuit defect	no AFE monitoring/control	4	2	1	8
A203	I2C frame CRC error	I2C circuit defect	no AFE monitoring/control	4	2	1	8

B100	**MCU**						
B101	operation error	component fault, unstable voltage/clock	Battery control incorrect	5	2	1	10
B102	bit error(MCU SRAM)	component fault, unstable voltage/clock	Battery control incorrect	5	2	1	10
B103	bit error(MCU Flash)	component fault, unstable voltage/clock	Battery control incorrect	5	2	1	10
B104	I2C fault	I2C circuit defect unstable voltage/clock	no current measurement in MCU, no battery control	5	2	1	10
B105	SMBUS fault	SMBUS circuit defect unstable voltage/clock	no receiving AFE data no battery control	5	2	1	10
B106	SMBUS PEC error	SMBUS circuit defect unstable voltage/clock	no receiving AFE data no battery control	5	2	1	10
B107	Temperature ADC measurement error	Measurement circuit fault unstable voltage/clock	overheating control error	4	2	1	8
B108	Battery voltage measurements error	Measurement circuit fault unstable voltage/clock	voltage control error	4	2	1	8
C100	**AFE FET**						
C101	FET fault	component fault	safety mechanism not working	5	2	1	10
C200	**MCU FET**						
C201	FET fault	component fault	safety mechanism not working	5	2	1	10
D100	**AFE FET Driver IC**						
D101	IC fault	component fault	safety mechanism not working	5	2	1	10
D102	FET control failure	FET/control circuit failure	safety mechanism not working	4	2	1	8
D200	**MCU FET Driver IC**						
D201	IC fault	component fault	safety mechanism not working	5	2	1	10
D202	FET control failure	FET/control circuit failure	safety mechanism not working	4	2	1	8
E100	**Thermistor #1**						
E101	abnormal resistance change	component fault	safety mechanism not working	5	3	1	15
E200	**Thermistor #2**						
E201	abnormal resistance change	component fault	safety mechanism malfunction	5	3	1	15
F100	**Current Monitor IC**						
F101	IC fault	component fault	no AFE measurement data update	5	1	1	5
F102	measurement error	measurement circuit fault	MCU current measurement error	4	2	1	8
G100	**8Mhz Crystal Oscillator**						
G101	clock instability	component fault, MCU oscillator fault	MCU malfunction no battery control	5	2	1	10
G102	clock cycle mismatch	component fault, MCU oscillator fault	no battery control	5	2	1	10
H100	**Voltage Monitor IC**						
H101	IC fault	component fault	no battery voltage control	5	1	1	5
H102	abnormal output	component fault	no battery voltage control	4	2	1	8
I100	**Shunt Registor**						
I101	abnormal output	component fault	battery current	5	3	1	15

			measurement error				
S100	**freeRTOS: task scheduling**						
S101	Stack overflow	Software error	battery control error/disability	5	2	1	10
S200	**task_bq_monitoring: AFE Companion IC measurement and state monitoring**						
S201	task inactivity	task scheduling starvation, task block	no battery control, no sensing AFE companion IC fault, no AFE measurement data receiving	5	2	1	10
S202	no operation in a defined order/cycle	task내 scheduling error	no battery control	5	2	1	10
S300	**task_mcu_monitoring: current, voltage, temperature monitoring in MCU**						
S301	task inactivity	task scheduling starvation, task block	no safety mechanism / no MCU measurement data update	5	2	1	10
S302	no operation in a defined order/cycle	task scheduling error	safety mechanism operation delay	5	2	1	10
S400	**task_functional_safety: performing safety mechanisms requiring periodicity**						
S401	task inactivity	task scheduling starvation, task block	safety mechanism not working	5	2	1	10
S402	no operation in a defined order/cycle	task scheduling error	safety mechanism operation delay	5	2	1	10
S500	**task_supervisor: checking the periodic operation of tasks**						
S501	task inactivity	task scheduling starvation, task block	no safety mechanism, no watchdog refreshing	5	2	1	10
S502	no operation in a defined order/cycle	task scheduling error	sno safety mechanism, no watchdog refreshing	5	2	1	10

표 9. 기존 BMS와 재설계한 BMS의 RPN 비교
Table 9. RPN comparison of existing BMS and redesigned BMS

Part ID	Potential Failure Mode	RPN	
		Existing BMS	Redesigned BMS
300	**MCU**		
301	Operation error	40	**10**
302	bits error (SRAM/FIASH)	40	**10**
304	ADC Read error	50	**8**
200	**AFE IC**		
202	Voltage measurement error	50	**10**
203	Current measurement error	50	**10**
204	Temperature measurement error	50	**10**
700	**Thermistor**		
701	Abnormal resistance change	75	**15**
800	**Shunt Registor**		
801	abnormal behavior	75	**15**

기능안전을 고려해서 설계한 BMS가 기존 BMS에 비해 위험수준이 개선되었는지 확인하기 위해 RPN값을 비교하였으며 표 9에 주어져 있다. 비교를 위해 펌웨어에 대한 분석은 제외하였다.

표 9에서 BMS의 부품 결함이나 오작동 및 펌웨어 주요 기능의 오류를 감지하고 안전메커니즘이 상시 작동되도록 설계 및 구현함으로써 검출도(Detectability) 값이 낮아짐으로 높은 위험우선순위지수 (RPN) 값을 가지는 고장모드들이 개선되었음을 알 수 있다.

따라서 본 연구에서 기능안전 개념을 적용하여 설계하고 제작한 BMS 하드웨어 및 펌웨어가 과전압, 과전류, 및 과열이 발생하는 다양한 잠재적인 상황에서도 안전 메커니즘이 정상적으로 작동하고, BMS로 인해 전기화재가 발생할 수 있는 상황이 사전에 방지될 수 있음을 알 수 있다.

Ⅳ. 결 론

본 연구에서는 ESS 전기화재에서 가장 많은 부분을 차지하고 있는 BMS의 주요 부품들과 펌웨어 프로시저들에 대하여 FMEA 분석을 시행하고 안전에 영향을 미치는 위험모드를 찾고 이를 제거하거나 줄이기 위해 기능안전 개념을 적용하여 BMS 하드웨어와 펌웨어를 재설계하였다. 이를 BMS 하드웨어로 구현하고 과전압, 과전류, 및 과열이 발생하는 다양한 상황에서도 BMS가 안전하게 배터리를 제어할 수 있음을 실험적으로 테스트하여 확인하였다.

앞으로 정부의 친환경 정책과 편의성을 추구하는 소비자의 요구에 따라 하이브리드 자동차나 전기차 등과 같은 산업용 ESS 뿐 아니라 가정용 혹은 커슈머용 ESS가 폭발적

으로 보급될 것으로 예상된다. 따라서 ESS에 필수적인 장치이고 배터리 폭발이나 화재의 큰 영향을 미치는 BMS를 안전하게 설계 제작하고 보급하는 것은 매우 시급한 과제이다.

본 연구에서 제시한 대로 각 부품 및 펌웨어 프로시저들에 대한 FMEA 분석을 수행하고 위험수준이 높은 위험우선순위지수 (RPN)을 찾고 위험모드를 제거하거나 줄임으로써 잠재적인 부품결함이나 펌웨어 오류로부터 안전한 BMS 하드웨어 및 소프트웨어를 설계 제작할 수 있고, BMS 관련 전기화재를 사전에 방지할 수 있을 것이다.

References

[1] Rui Xiong, Weisiang Shen, "Advanced Battery Management Technologies for Electric Vehicles," John Wiley & Sons, 2019.

[2] Reiner Korthauer, "Lithium-Ion Batteries: Basics and Applications," Springer, 2019.

[3] E.S. Kim, "Fire Risk Assessment based on Risk Priority Number for Components of ESS," doctoral dissertation, Chungbuk National University, 2020 (in Korean).

[4] B.W. Lee, "A study on the Analysis and Solution of ESS System Fire Cause," master's thesis, Hanyang University, 2020 (in Korean).

[5] H.J. Jang, T.S. Song, J.Y. Kim, S.J. Kim, T.H. Jang, "Study on Analysis of Fire Factor and Development Direction of Standard/safety Requirement to Keep Safety for Energy Storage System (ESS)," Journal of Standards, Certification and Safety, Vol. 9, No. 3, pp. 25-49, 2019 (in Korean).

[6] https://www.kats.go.kr/content.do?cmsid=239&cid=21072&mode=view

[7] Jurgen Garche, Klaus Brandt, "Electrochemical Power Sources Fundamentals, Systems, and Applications Li-Battery Safety," Elsevier, 2018.

[8] D.H. Kim, S.C. Kim, J.S Park, E.J. Kim, E.S. Kim, "Analysis of Risk Priority Number for Grid-connected Energy Storage System," Journal of the Korean Society of Safety, Vol. 31, No. 2, pp. 10-17, 2016 (in Korean).

[9] D.H. Kim, S.C. Kim, E.S. Kim, K.G. Nam, C.K Jeong "Safety Assessment for PCS of Photovoltaic and Energy Storage System Applying FTA," Journal of the Korean Society of Safety. Vol. 34, No. 1, pp. 13-20, 2019 (in Korean).

[10] Michael R. Beauregard, Raymond J. Mikulak, Robin E. McDermott, "The Basics of FMEA," Productivity Press, 2008.

[11] Kirby W. Beard, "Linden's Handbook of Batteries, Fifth Edition," McGraw-Hill, 2019.

[12] John Warner, "The Handbook of Lithium-Ion Battery Pack Design: Chemistry, Components, Types and Terminology," Elsevier Science, 2015.

[13] S.B. Kim, S.H. Lee, "Design and Development of Less than 1Kw Lithium Eechargeable Battery Pack," International Journal of Internet, Broadcasting and Communication Vol. 10 No. 3, pp. 104-108, 2018.

[14] H.H. Kim, N.H. Lee, "The Case Study on Software FMEA for the Efficient Improvement of Functional Safety," The Korean Society of Automative Engineers Conference & Exhibition, Vol. 2012 No. 11, pp. 1303-1308, 2012 (in Korean).

WoonDong Kim (김 운 동)

1991 Electronics Engineering from Kyungpook National University (B.S.)

1993 Microwave Engineering form Kyungpook National University (M.S.)

Career:

2019~ Senior Reseacher in Huconn Co.,Ltd.

Field of Interests: ESS & Battery Management System, Machine Learning for IOT

Email: woondong.kim@huconn.com

SunGu Lee (이 순 구)

2002 Statistics in Yeungnam University (B.S.)

Career:

2020~ Senior Reseacher in Huconn Co.,Ltd.

Field of Interests: Embedded System, Realtime System, ESS & Battery Management System

Email: sungu.lee@huconn.com

DaeKeun Kang (강 대 근)

2003 Computer Engineering in Yeungnam University(B.S.)

2009 Multimedia Communication Engineering in Yeungnam University(M.S.)

Career:

CEO of Huconn Co.,Ltd.

Field of Interests: Safety Mechanism, ESS & Battery Management System