


2차년도 기술문서

(과제명) 대규모 분산 에너지 저장장치 인프라의 안전한 자율
운영 및 성능 평가를 위한 지능형 SW 프레임워크 개발

(과제번호) 2021-0-00077

- 기술문서명 : ESS의 사고 사례를 통한 안전무결성 등급
기준 수립 및 안전 SW 검증 모델 기술서
- 작성일자 : 2022년 11월 2일

과학기술정보통신부 SW컴퓨팅산업원천기술개발사업
“기술문서”로 제출합니다.

수행기관	성명/직위	확인
슈어소프트테크(주)	심정민 / 이사	

정보통신기획평가원장 귀하

ESS의 사고 사례를 통한 안전무결성 등급 기준
수립 및 안전 SW 검증 모델 기술서



2022년 10월 30일

슈어소프트테크(주)

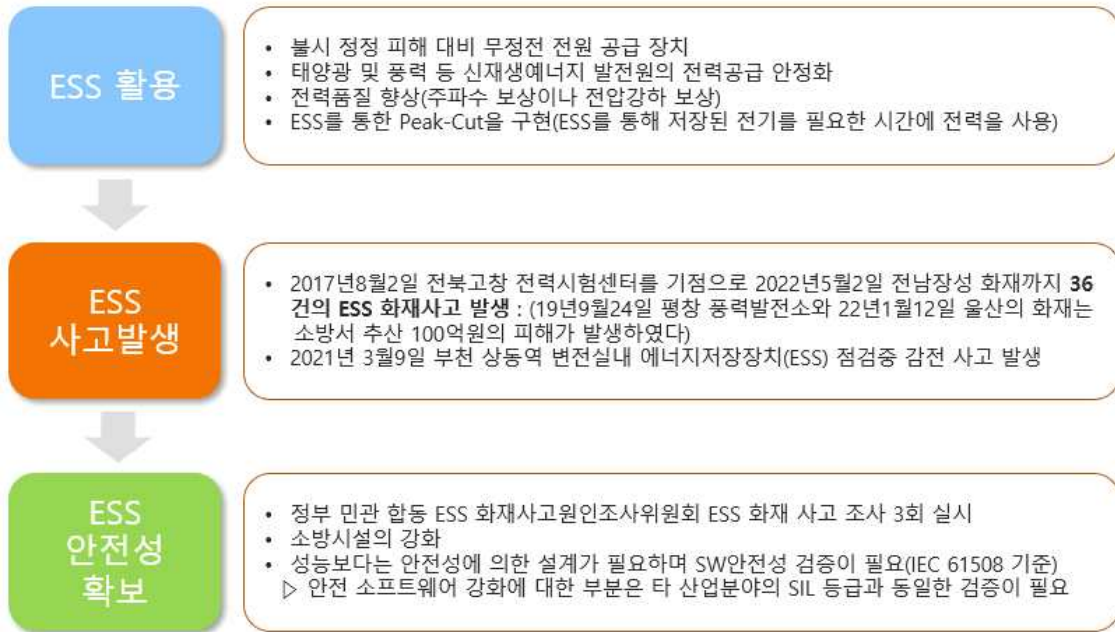
목 차

1. 개요	4
1.1 기후 위기 속 국내 탄소 중립 정책	4
1.2 탄소중립과 신재생에너지	4
1.3 ESS 화재발생과 안전조치	4
2. 에너지저장장치 SW안전 검증 모델	5
2.1 SW 안전 검증 모델의 대상 범위 지정	5
2.2 사고 사례를 통한 위험원 분석, 리스크 분석	5
2.3 IEC 61508 기반의 SW안전 검증 프로세스	9
2.4 SW안전 검증 지표 방법	11
3. 결론	12

<그림 차례>

그림 1 ESS활용 및 안전성 확보	4
그림 2 에너지저장장치 시스템 구성에서 검증 대상범위 지정	5
그림 3 국내 ESS화재 및 피해규모	5
그림 4 국내 및 해외 ESS 화재 사고 리스트	6
그림 5 위험원 분석을 통한 SW안전 등급 결정	7
그림 6 각 산업별 안전무결성(SIL) 등급 분류	7
그림 7 IEC 61508-5 안전무결성 등급의 결정 - 정성적 방법 예시	8
그림 8 ESS 규모별 시스템 및 통합업체 특징	8
그림 9 평가 항목 분류 시 고려되는 항목 구분	9
그림 10 리스크 파라미터에 기반한 정성적 안전 무결성 수준 결정	9
그림 11 IEC 61508 기반 SW개발 검증 프로세스	9
그림 12 SW개발 검증 프로세스 단계별 검증 대상	10
그림 13 수립된 항목을 기준으로 KC 62619에서의 수행여부 확인	10
그림 14 소프트웨어 설계 검증 - 검증지표	11
그림 15 소프트웨어 구현 검증 - 검증지표	11
그림 16 소프트웨어 모듈 시험 검증지표	11
그림 17 소프트웨어 통합 시험 검증지표	12
그림 18 시스템 통합 시험 검증지표	12

1. 개요



<그림1 ESS활용 및 안전성 확보>

1.1 기후 위기 속 국내 탄소중립 정책

이산화탄소는 태양으로부터 지구에 들어오는 짧은 파장의 태양 복사에너지는 통과시키는 반면 지구로부터 나가려는 긴 파장의 복사에너지는 흡수하므로 지표면을 보온하는 역할을 하여 지구 대기의 온도를 상승시키는 작용을 하는데 이를 온실효과라 하며, 기후시스템에서 온실효과는 필요하지만 산업혁명 이후 지속적으로 다량의 온실가스가 대기 중 배출됨에 따라 지구 대기 중 온실가스 농도가 증가하여 지구의 지표온도가 과도하게 증가하여 지구온난화라는 현상을 초래하게 되었다.

탄소중립이란 대기 중 이산화탄소 농도 증가를 막기 위해 인간 활동에 의한 배출량은 최대한 감소시키고, 흡수량은 증대하여 순 배출량이 '0'이 된 상태. 즉, 인간 활동으로 배출하는 온실가스는 최대한 줄이고, 배출되는 온실가스는 산림 흡수나 CCUS(Carbon Capture, Utilization, Storage: 이산화탄소 포집, 저장, 활용 기술)로 제거하여 실질적인 배출량을 '0'수준으로 낮추는 것을 탄소중립(Net Zero)이라고 한다.

1.2 탄소중립과 신재생에너지

이산화탄소의 원인이 되는 화석연료는 지금까지 따뜻한 원료였지만 언제부터인가 점점 애물단지가 되고 있다. 지구 온난화와 환경문제에 전 세계가 나서서 이산화탄소 발생을 줄이려 신재생에너지로의 전환을 앞 다투고 있다. 하루 종일 일정하게 전력원의 상태가 유지가 되지 않는 풍력과 태양광은 에너지저장장치가 필수적인 장비라고 볼 수 있다.

1.3 ESS 화재발생과 안전조치

정부에서는 2017년부터 잇따른 에너지저장장치(ESS)의 배터리 랙과 배터리 관리 시스템(BMS)의 SW 시스템 전반에 문제 또한 염두해두고 SW 기능안전을 국가표준에 도입하였다.

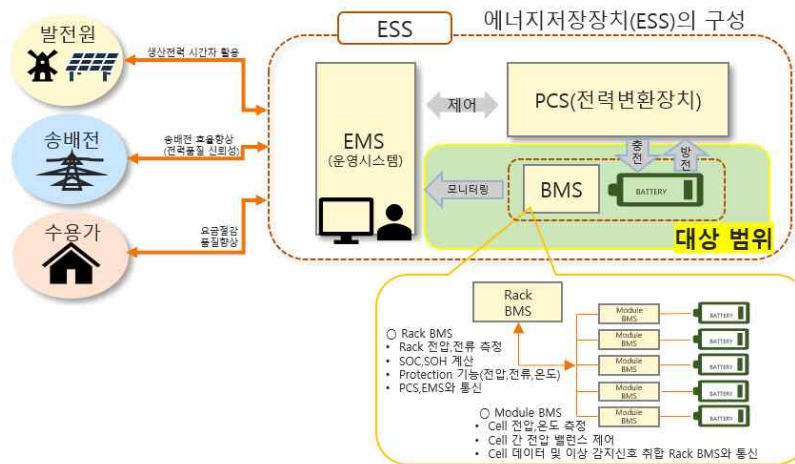
산업통상자원부 국가기술표준원에 따르면 2020년 4월부터 ESS 배터리 랙에 관한 SW기능안전시

험 제도를 정식 도입하고 안전확인신고증명서를 획득하지 못한 제품의 판매는 제한된다. 국내에서 법에 근거해 전력설비에 SW기능안전시험이 도입되는 건 ESS가 처음이다.

2. 에너지저장장치 SW 안전 검증 모델

2.1 SW 안전 검증 모델의 대상 범위 지정

전력 계통에 통합되어 배터리시스템 제어를 주목적으로 하는 에너지저장장치(ESS)의 원활한 수행을 위한 배터리관리시스템(BMS)을 대상 범위로 지정

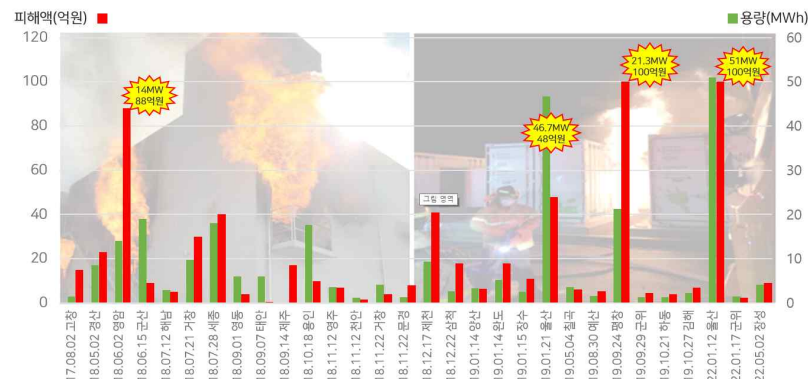


<그림2 에너지저장장치 시스템 구성에서 검증 대상범위 지정>

- 리튬이차전지를 사용하는 에너지저장시스템의 BMS에 대한 안전무결성 등급 적용 기준 명시
- 리튬이차전지를 사용하는 에너지 저장 시스템의 BMS 안전 적용 검사 항목 제시
- 검사 항목별 검사 접근 방식과 안전무결성 등급별 검사 항목 및 지표 명시

2.2 사고 사례를 통한 위험원 분석, 리스크 분석

2017년 8월2일 전력연구원 고창 전력시험센터를 기점으로 2022년 9월 6일 인천 현대제철 화재까지 37건의 ESS 화재사고가 발생하였다. 2019년 9월 평창 풍력발전소와 22년1월 울산의 화재는 소방서 추산 100억 원의 큰 피해가 발생하였으며, 최근 2022년9월 발생한 인천 현대제철의 화재는 300억 원 이상의 피해가 추정된다.



<그림3 국내 ESS 화재 및 피해규모>

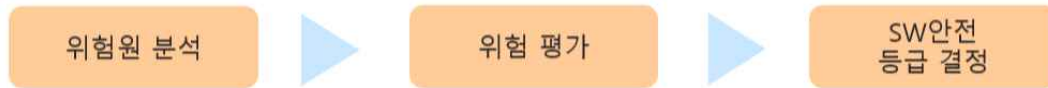
No.	사고일시	장소	용량 (MWh)	화재 진압 소요 시간(분)	운용기간 (월)	배터리상태	ESS 용도	피해(추정치)
1	17.08.02	전북 고창	1.46	531	-	설치중(보관)	풍력 연계	15억원
2	18.05.02	경북 경산	8.6	157	1년10개월	수리 점검 중	주파수 조정	23억원
3	18.06.02	전남 영암	14	197	2년5개월	수리 점검 중	풍력 연계	88억원
4	18.06.15	전북 군산	18.965	559	6개월	충전 후 휴지 중	태양광 연계	9억원
5	18.07.12	전남 해남	2.99	99	7개월	충전 후 휴지 중	태양광 연계	5억원
6	18.07.21	경남 거창	9.7	120	1년7개월	충전 후 휴지 중	풍력 연계	30억원
7	18.07.28	세종	18	424	-	설치 중(시공)	피크제어용	30억원
8	18.09.01	충북 영동	5.989	110	8개월	충전 후 휴지 중	태양광 연계	4억원
9	18.09.07	충남 태안	6	156	-	설치 중(시공)	태양광 연계	0.56억원
10	18.09.14	제주	0.18	22	4년	충전 중	태양광 연계	17억원
11	18.10.18	경기 용인	17.7	415	2년7개월	수리 점검 중	주파수 조정	10억원
12	18.11.12	경북 영주	3.66	75	9개월	충전 후 휴지 중	태양광 연계	7억원
13	18.11.12	충남 천안	1.22	122	11개월	충전 후 휴지 중	태양광 연계	1.5억원
14	18.11.22	경남 거창	4.16	128	11개월	충전 후 휴지 중	태양광 연계	4억원
15	18.11.22	경북 문경	1.331	118	7개월	충전 후 휴지 중	태양광 연계	8억원
16	18.12.17	충북 제천	9.316	108	1년	충전 후 휴지 중	피크제어용	41억원
17	18.12.22	강원 삼척	2.662	196	1년	충전 후 휴지 중	태양광 연계	18억원
18	19.01.14	경남 양산	3.289	811	10개월	충전 후 휴지 중	피크제어용	6.5억원
19	19.01.14	전남 완도	5.22	549	1년2개월	충전 중	태양광 연계	18억원
20	19.01.15	전북 장수	2.496	494	9개월	충전 후 휴지 중	태양광 연계	10.9억원
21	19.01.21	울산	46.757	475	7개월	충전 후 휴지 중	피크제어용	48억원
22	19.05.04	경북 칠곡	3.66		2년3개월	충전 후 휴지 중	태양광 연계	6억원
23	19.05.26	전남 장수	1.027		1년	충전 후 방전 중	태양광 연계	-
24	19.08.30	충남 예산	1.55	8시간	1년8개월	충전 후 휴지 중	태양광 연계	5.2억원
25	19.09.24	강원 평창	21.3	2시간30분	2년6개월	충전 후 휴지 중	풍력 연계	100억원
26	19.09.29	경북 군위	1.5		1년9개월	방전 초기	태양광 연계	4.6억원
27	19.10.21	경남 하동	1.33		1년3개월	충전 후 휴지 중	태양광 연계	4억원
28	19.10.27	경남 김해	2.26	3시간43분	1년6개월	충전 후 휴지 중	태양광 연계	7억원
29	20.05.27	전남 해남		5시간				4.67억원
30	20.09.03	충북 음성						
31	21.03.11	경북 영천						9.1억원
32	21.04.06	충남 홍성		3시간43분				4.4억원

No.	사고일시	장소	용량 (MWh)	화재 진압 소요 시간	운용기간 (월)	피해(추정치)
33	22.01.12	울산	51	8시간	3년2개월	100억원
34	22.01.17	경북 군위	15	5시간		2.35억원
35	22.05.01	전북 익산		8시간40분		2억원
36	22.05.02	전남 장성		14시간4분		9억원
37	22.09.06	인천	103	24시간57분		300억원이상

해외 ESS 화재 리스트

국가	지역	발생일	용도	용량 (MWh)	비고
호주	빅토리아주 (데슬라PJT)	21.07	PV	300	발화(컨테이너 1대, 전소)
미국	하와이	12.08	계통연계	12	배터리(납)
	아리조나	12.11	수요관리	1.5	변압기 화재
	워싱턴	13.07	계통연계	0.5	
	위스콘신	16.08	수요관리	-	
	아리조나	19.04	계통연계	2	LG화학
	일리노이주 라셀레	21.07	PV	36	발화(2MWh 소실)
	미시간주 스탠디쉬	21.04	PV	12	발화(1.5MWh 소실)
	캘리포니아	22.02	PV	100	LG냉각수 누수 단락
독일	에리조나 채들러변전소	22.04	계통연계	10	발화(전소)
	노히하르텐베 르크	21.07	PV	5	발화(전소)
	바덴뷔르템베 르크	22.03	가정용	-	가정용 소용량(일부)
중국	산지	17.03	수요관리	9	삼성 셀(일부)
	산지	17.12	수요관리	4.5	삼성 셀(일부)
	양충	18.07	수요관리	1.7	작업자 부주의
	베이징 정타이 구	21.04	PV	1.4	발화(전소) 사망 3명, 부상 1명
일본	이바라키	11.09	수요관리	2	열폭주(NaS)
오스트 리아	빅토리아	13.07	계통연계	0.5	
벨기에		17.11	주파수조정용	6	열폭주
영국	리버풀	20.09	-	-	

<그림4 국내 및 해외 ESS 화재 사고 리스트(2017.8 ~ 2022.9)>



<그림5 위험원 분석을 통한 SW안전 등급 결정>

IEC 61508에서 목표하는 안전을 달성하기 위해 안전 무결성 등급(SIL; Safety Integrity Level)을 결정하는 것은 소프트웨어 안전 확보를 위한 필수 활동이며, 소프트웨어 안전등급에 의해 효율적인 안전관리가 가능하다.

아래의 표는 산업 도메인별 안전무결성 등급(SIL)을 보여주고 있다.

각 산업별 표준 수립 시 대상 도메인의 위험원을 분석하고, 평가하여 SW안전 등급을 결정한다.

표준	산업 도메인	소프트웨어 안전무결성 등급(SIL)				
		위험도 매우 높음	높음	중간	낮음	SW 안전무관
IEC 61508	산업안전	SIL 4	SIL 3	SIL 2	SIL 1	-
NASA-STD-8719-13C	항공우주 (NASA)	FULL	MOD		MIN	-
MIL-STD-882E	미국방	CI 1	CI 2	CI 3	CI 4	CI 5
IEC 62279	철도	SIL 4	SIL 3	SIL 2	SIL 1	SIL 0
ISO 26262	자동차	ASIL D	ASIL C	ASIL B	ASIL A	QM
DO-178C	항공	A	B	C	D	E
IEC 62304	의료기기	Class C	Class B		Class A	

<그림6 각 산업별 안전무결성(SIL) 등급 분류>

IEC 61508에서 위험원 분석 및 리스크 평가의 목적은 기능 안전 평가 프로세스에서 안전관련 시스템이 허용 위험 기준을 충족할 가능성 또는 위험한 상황의 영향을 줄일 수 있도록 설계를 보장하는 역할을 하며 개념을 잡고 범위를 정의한 후 개발을 시작하는 가장 기초가 되는 단계이다.

안전 무결성 수준에 의해 요구되는 범위만큼, 주어진 소프트웨어 안전수명 주기 단계에서 얻은 산출물을 시험하고 평가함으로써, 해당 단계에 입력으로 제공된 표준과 그 출력에 따라서 정확성과 일치성을 보장할 수 있다.

리스크 계산 공식
$R = f \times C$ <p> <i>R</i> : 안전관련 시스템이 없는 경우의 리스크 <i>f</i> : 안전관련 시스템이 없는 경우의 위험한 사건 빈도 <i>c</i> : 위험한 사건의 결과 (건강과 안전 또는 환경 손상으로부터의 피해와 관련될 수 있다.) </p>

안전관련 시스템이 없는 경우 리스크는 '사건의 빈도 X 사건의 결과'라고 할 수 있을 것이다. 추가로 위대한 사건을 피할 가능성과 불의의 사건 발생 확률을 추가하여 IEC 61508에서 리스크 파라미터를 산정할 수 있다고 제시하고 있다.

리스크 파라미터		구분	비고
결과(C)	C ₁ C ₂ C ₃ C ₄	<ul style="list-style-type: none"> 경상 한명 이상의 사람이 심각하고 영구적인 상해, 한명 사망 몇 사람 사망 매우 많은 수의 사람 사망 	-구분 체계는 사람에 대한 상해와 사망에 따라 개발되었다. 환경 또는 물질 손상에 대해서도 기타 구분 계획을 개발할 필요가 있다. - C1, C2, C3, C4의 해석에 대하여, 사고의 결과와 정상적인 구제조치를 고려하여야 한다.
	F ₁ F ₂	<ul style="list-style-type: none"> 위해 구역에서의 노출이 드물거나 가끔 있음 위해 구역에서의 노출이 빈번하거나 항상 있음 	
위대한 사건을 피할 가능성(P)	P ₁ P ₂	<ul style="list-style-type: none"> 일정 조건에서 가능 거의 불가능 	-어떤 공정의 운영 감독 유무, 위대한 사건의 방지 유무 등
	W ₁ W ₂ W ₃	<ul style="list-style-type: none"> 불의의 사고 발생을 간과할 확률이 거의 적으며 불의의 사고 발생 가능성이 거의 없음. 불의의 사고 발생을 간과할 확률이 적으며 불의의 사고 발생 가능성이 약간 있음. 불의의 사고 발생을 간과할 확률이 비교적 높으며 불의의 사고 발생 가능성이 자주 있음. 	

<그림7 IEC 61508-5 안전무결성 등급의 결정 - 정성적 방법 예시>

ESS 용량	소형 (000W ~ 00kW급)	중형 (00~000kW급)	대형 (MW급)
사업 base	올인원 베이스(단일 시스템)		프로젝트 베이스
사업 특징	<ul style="list-style-type: none"> ESS 제조사 = Integrator 디벨로퍼, EPC, 금융조달 불필요 O&M 기능 필요 		<ul style="list-style-type: none"> SI, 디벨로퍼, O&M, EPC 기능 필요 금융조달 필요
요구 특성	<ul style="list-style-type: none"> 高 에너지밀도 요구(컴팩트화 가능) 실내 설치 가능성 높아 디자인 중요 수요처(가정, 상업)마다 평균 전력량 차이 존재하므로 용량대 선정 중요(ESS 확장성 필요) 개인이 구매자로 가격 중요(저가와 요구) 		<ul style="list-style-type: none"> 高 에너지밀도 요구(설치비용 절감) 성능의 신뢰성이 중요 프로젝트마다 환경/특성이 다르므로 ESS 엔지니어링 능력 중요
설치후 시장요구	O&M 및 A/S에 대한 신뢰할 수 있는 인프라 필요(설치 해당지역 업체가 유리)		
주요 참여업체	<ul style="list-style-type: none"> 가정용 전자기기(Consumer 제품) 제조사 전기전자 사업자 배터리 제조사 start-up 등 		<ul style="list-style-type: none"> 전력전자기기 제조사 배터리 제조사 충전기 제조사 start-up 등

<그림8 ESS 규모별 시스템 및 통합업체 특징(산업통상자원부, ESS 산업 생태계 강화 지원정책 및 전력개발 '17.3)>

에너지저장시스템의 배터리는 용량의 크기에 따라 열 폭주로 인한 화재 발생 시 더 큰 화재규모, 더 큰 피해규모가 발생할 수 있는 가능성이 내포되어있다고 볼 수 있다. 위 표는 산업통상자원부의 ESS용량에 따른 분류이다. 또한 전력 계통에 연계되는 시간과 위험으로 회피할 수 있는 가능성 여부에 따라 리스크 파라미터를 분류할 수 있다.

참고로 우리나라 4인 가구의 월평균 전력소비량 350kWh 이며, 가구당 하루 평균 전력 소비량은 11.7kWh 이다. 국내최대 ESS는 신안군 안좌도이며 배터리 용량은 340MWh 이다. 이는 2만9

천여 가구가 하루 동안 사용할 수 있는 전기를 저장할 수 있다.

리스크 파라미터		구분	비고
피해 규모 크기 (consequence)	C_1	20KWh 미만(가정용, 소형 ESS)	<ul style="list-style-type: none"> 에너지저장시스템의 고장으로 인한 화재사고 발생시 피해 규모는 배터리 용량에 비례, 위대한 사건의 결과를 배터리 용량으로 평가
	C_2	20KWh이상 1MWh 미만(중형)	
	C_3	1MWh 이상 100MWh 미만(대형)	
	C_4	100MWh 이상 용량(초대형)	
충방전 빈도 및 계통 연계 노출시간 (Exposure)	F_1	임시 (정전대비, UPS 용도)	<ul style="list-style-type: none"> 충방전 빈도 및 계통 연계의 시간을 기준으로 평가
	F_2	상시 (주파수 조정, 피크제어용, 신재생에너지 연계용)	
위험으로 인한 피해 회피 가능성 (Avoidance)	P_1	열폭주 저감 조치 : 배터리랙 내부 화재확산 방지 자체 소화시스템 추가 조치, 배기시설 조치	<ul style="list-style-type: none"> 화재확산 방지를 위한 자체 소화시스템 추가 조치, 배터리실 내 폭발을 예방하기 위해 위험한 내부압력이 발생한 경우 감압을 위한 배출 기능 설치한 경우 고장 회피 가능성이 증가한다고 평가 배터리랙 안에 소화시스템이 추가조치 되는 경우 위험 감쇄 가능
	P_2	열폭주 저감 미조치 : 배터리랙 내부 화재확산 방지 미조치, 자체 소화시스템 추가 미조치, 배기시설 미조치	

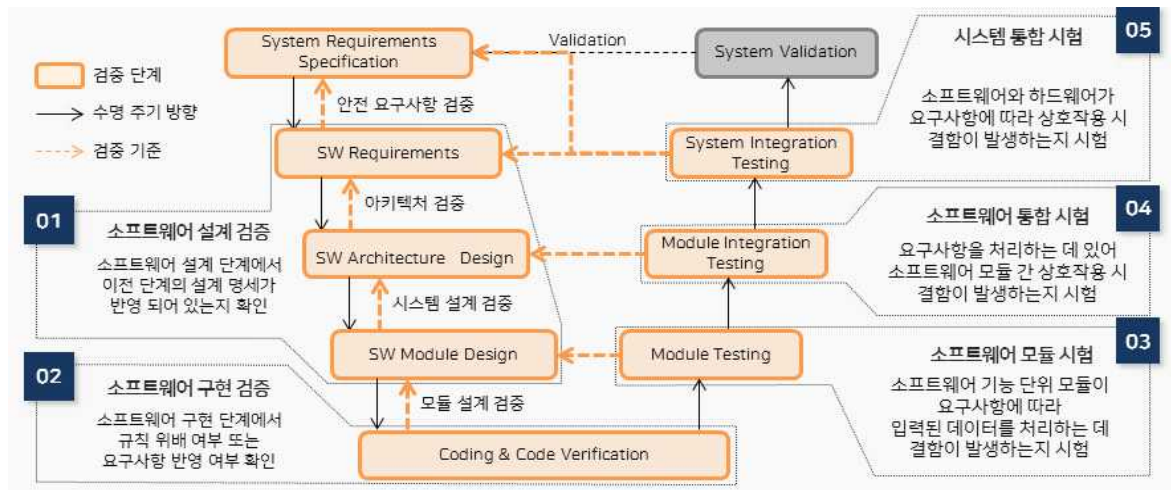
<그림9 평가 항목 분류 시 고려되는 항목 구분>

위의 리스크 파라미터 평가 기준을 적용하여 에너지저장시스템의 안전 무결성 등급을 아래와 같이 결정한다.

리스크 파라미터			
위해한 사건의 결과(C)	위해 구역의 빈도와 그에 대한 노출시간 (F)	위해한 사건으로 피할가능성(P)	
		P_1	P_2
C_1	F_1	QM	QM
	F_2	QM	SIL 1
C_2	F_1	SIL 1	SIL 1
	F_2	SIL 1	SIL 2
C_3	F_1	SIL 2	SIL 2
	F_2	SIL 2	SIL 3
C_4	F_1	SIL 3	SIL 3
	F_2	SIL 3	SIL 4

<그림10 리스크 파라미터에 기반한 정성적 안전 무결성 수준 결정>

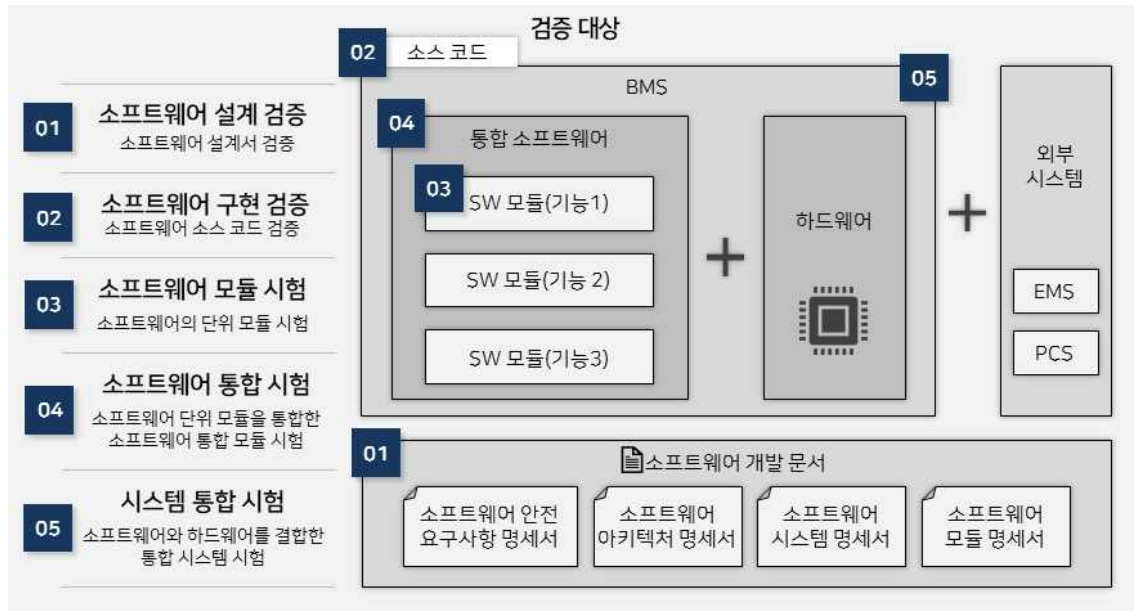
2.3 IEC 61508 기반의 SW안전 검증 프로세스



<그림11 IEC 61508 기반 SW개발 검증 프로세스>

안전 SW의 검증 단계별 검증대상은 아래와 같이 나타낼 수 있다.

- ① 소프트웨어 설계 검증 : 소프트웨어 설계 단계에서 산출된 소프트웨어 설계서 검증
- ② 소프트웨어 구현 검증 : 소프트웨어 구현 단계에서 산출된 소스 코드 검증
- ③ 소프트웨어 모듈 검증 : 소프트웨어의 단위 모듈 시험
- ④ 소프트웨어 통합 검증 : 소프트웨어 단위 모듈을 통합한 소프트웨어 통합 모듈 시험
- ⑤ 시스템 통합 검증 : 소프트웨어와 하드웨어를 결합한 통합 시스템 시험



<그림12 SW개발 검증 프로세스 단계별 검증 대상>

안전 SW 검증 단계 및 검증 대상을 도출하고, 검증 단계 별 검증 항목과 각 항목에 맞게 검증 지표를 도출하였다. 이후 도출된 검증 항목이 KC 62619에서 수행하는지 비교하였다.

단계 별 검증 항목				
검증 단계	검증 항목	설명	검증 지표	KC 62619
SW 설계 검증	SW 요구사항 추적성 검증	• SW 요구사항과 시스템 요구사항간 추적성 검증	상/하위 문서간 추적성 커버리지	X
	SW 아키텍처 요구사항 추적성 검증	• SW 아키텍처 요구사항과 SW 요구사항 추적성 검증		X
	SW 모듈 설계 요구사항 추적성 검증	• SW 모듈 요구사항과 SW 시스템 설계 요구사항 추적성 검증		X
SW 구현 검증	코딩 표준 준수 검증	• 소스코드가 코딩 표준을 준수하는지 검증	규칙 위반 개수	X
SW 모듈 시험	모듈 단위 시험	• 상세 설계서의 기능/비기능 요구사항을 충족하는지 시험	요구사항 커버리지	X
		• 기능/비기능 시험을 통해 소스 코드 상에서 시험 수행된 코드의 커버리지를 검증	코드 커버리지	
SW 통합 시험	모듈 통합 시험	• 소프트웨어 시스템 설계서의 기능/비기능 요구사항을 충족하는지 시험	요구사항 커버리지	X
		• 모듈간 인터페이스에 해당하는 함수간 호출의 코드 커버리지를 검증	함수 호출 커버리지	
시스템 통합 시험	시스템 기능 시험	• 시스템(SW)의 기능 요구사항을 충족하는지 시험	기능 요구사항 커버리지	△ KC 62619 8.2 안전기능시험에 일부 포함
	시스템 비기능 시험	• 시스템(SW)의 비기능 요구사항을 충족하는지 시험	비기능 요구사항 커버리지	X
	시스템 강건성 시험	• 악의 조건에서 시스템 무정지 강건성을 확인하는 시험	강건성	△ 부속서 D.5 에서 안전기능 기능시험 수행

<그림13 수립된 항목을 기준으로 KC 62619에서의 수행여부 확인>

2.4 SW안전 검증 지표 방법

소프트웨어 설계 과정에서는 SW 요구사항 설계, SW 아키텍처 설계 및 SW 상세 설계 단계가 있다. 소프트웨어 설계 검증에서는 각 설계 단계에서 상위 설계 과정에서 명세된 요구사항을 충족하였는지 확인하는 과정으로 각 설계 과정에서 도출된 설계서가 상위 요구사항을 반영되었는지 추적함으로써 확인할 수 있다. 해당 과정에서 검증 항목으로 요구사항 명세 단계에서의 추적성 확인, 아키텍처 설계 단계에서의 추적성 확인과 모듈 설계 단계에서의 추적성 확인을 제시한다.

소프트웨어 설계 검증 : 설계 단계에서 상위 설계 과정에서 명세된 요구사항을 충족하였는지 확인				KC 62619 수행 여부
검증 항목	설명	검증 지표	지표 산정 방법	
SW 요구사항 추적성 검증	명세한 SW 요구사항이 시스템 요구사항을 얼마나 충족하는지 비교한다.	상/하위 요구사항 추적성 커버리지	$\frac{\text{시스템 요구사항과 추적된 SW 요구사항 개수}}{\text{SW 요구사항 개수}}$	X
SW 아키텍처 요구사항 추적성 검증	명세한 SW 아키텍처 요구사항이 SW 요구사항을 얼마나 충족하는지 비교한다.	상/하위 요구사항 추적성 커버리지	$\frac{\text{SW 요구사항과 추적된 SW 아키텍처 요구사항 개수}}{\text{SW 아키텍처 요구사항 개수}}$	X
SW 모듈 설계 요구사항 추적성 검증	명세한 SW 모듈 요구사항이 SW 아키텍처 설계서의 요구사항을 얼마나 충족하는지 비교한다.	상/하위 요구사항 추적성 커버리지	$\frac{\text{SW 아키텍처와 추적된 SW 모듈 설계 요구사항 개수}}{\text{SW 모듈 설계 요구사항 개수}}$	X

<그림14 소프트웨어 설계 검증 - 검증지표>

소프트웨어 구현 검증 과정은 구현된 소스 코드가 코딩 표준을 준수하는지 확인한다. 해당 과정에서 검증 항목으로 코딩 표준 준수 검증을 제시한다.

소프트웨어 구현 검증 : 소프트웨어 구현 시 설계 단계에서 명세된 요구사항을 충족하는지 확인				
검증 항목	설명	검증 지표	지표 산정 방법	KC 62619
코딩 표준 준수 검증	검증 및 유지보수의 용이함을 위해 소스 코드가 코딩 표준에 위배되었는지 확인한다.	위배 개수	코딩 표준 위배 개수	X

<그림15 소프트웨어 구현 검증 - 검증지표>

소프트웨어 모듈은 소프트웨어가 작동하는 기능의 최소 단위를 의미한다. 소프트웨어 모듈 시험 과정에서는 소프트웨어 모듈이 명세된 요구사항을 수행하는지 확인하고 불필요한 구문이 존재하는지 확인한다. 해당 과정에서 검증 항목으로 코드 커버리지를 통한 모듈 단위 시험과 요구사항 커버리지를 통한 모듈 단위 시험을 제시한다.

소프트웨어 모듈 시험 : 기능의 최소 단위인 모듈의 데이터 처리 시 발생 가능한 결함 검증				
검증 항목	설명	검증 지표	지표 산정 방법	KC 62619
모듈 단위 시험	소프트웨어 단위 모듈이 기능 요구사항을 수행하는 중 구문 또는 분기 등 도달하지 않는 부분이 있는지 테스트 케이스를 생성하고 확인한다.	코드 커버리지 (구문, 분기, MC/DC)	$\frac{\text{시험에서 수행된 코드 수}}{\text{전체 코드 수}}$	X
	모듈 설계서에 명세된 값을 기반으로 테스트 케이스를 생성하고 소프트웨어 단위 모듈이 명세된 요구사항을 충족하는지 동작시켜 확인한다.	요구사항 커버리지	$\frac{\text{시험에서 충족된 요구사항 개수}}{\text{SW 모듈 설계 요구사항 개수}}$	X

<그림16 소프트웨어 모듈 시험 검증지표>

소프트웨어 통합 시험은 소프트웨어 모듈을 통합하면서 아키텍처 설계 단계에서 명세된 요구사항을 충족하는지 확인하고 호출되지 않은 함수가 존재하는지 확인한다. 해당 과정에서 검증 항목으로 코드 커버리지를 통한 모듈 통합 시험과 요구사항 커버리지를 통한 모듈 통합 시험을 제시한다.

소프트웨어 통합 시험 : 모듈간 상호작용 시 발생 가능한 결함 검출				
검증 항목	설명	검증 지표	지표 산정 방법	KC 62619
모듈 통합 시험	통합된 소프트웨어가 기능 안전 요구사항을 수행하는 과정에서 호출되지 않은 함수가 존재하는지 확인한다.	코드 커버리지 (함수 호출)	$\frac{\text{실제 호출된 함수 수}}{\text{전체 함수 수}}$	X
	아키텍처 설계서에 명세된 값을 기반으로 테스트 케이스를 생성하고 소프트웨어 통합 모듈이 명세된 요구사항을 충족하는지 동작시켜 확인한다.	요구사항 커버리지	$\frac{\text{시험에서 충족된 요구사항 개수}}{\text{SW 아키텍처 설계 요구사항 개수}}$	X

<그림17 소프트웨어 통합 시험 검증지표>

시스템 통합 시험은 BMS 소프트웨어와 하드웨어와 결합할 시 명세된 기능 및 비기능 요구사항을 충족하는지 확인하고 악의 조건에서도 요구사항을 어느 정도 동작할 수 있는지 확인한다. 해당 시험은 KC 62619에서도 오류 주입 시험을 통하여 일부 수행하고 있다. 해당 과정에서 검증 항목으로 시스템 기능 시험, 시스템 비기능 시험 및 악의 조건에서의 시스템 강건성 시험을 제시한다.

시스템 통합 시험 : BMS 소프트웨어와 하드웨어간 상호 작용 시 발생 가능한 오류 검출				
검증 항목	설명	검증 지표	지표 산정 방법	KC 62619
시스템 기능 시험	시스템 또는 SW 요구사항의 기능 명세를 충족하는지 시험한다.	기능 요구사항 커버리지	$\frac{\text{시험에서 충족된 기능 요구사항 개수}}{\text{기능 요구사항 개수}}$	Δ 9.2에서 안전기능 기능시험 수행
시스템 비기능 시험	시스템의 자원 사용량, 응답시간 등의 비기능 요구사항 명세를 충족하는지 시험한다.	비기능 요구사항 커버리지	$\frac{\text{시험에서 충족된 비기능 요구사항 개수}}{\text{비기능 요구사항 개수}}$	X
시스템 강건성 시험	결함 주입, 부하 등의 악의 조건에서 시스템이 정지 없이 동작 가능한지 시험한다.	강건성	$\frac{\text{시스템 무정지 TC 개수}}{\text{악의 조건 TC 개수}}$	Δ 부속서 D.5에서 안전기능 기능시험 수행

<그림18 시스템 통합 시험 검증지표>

3. 결론

대한민국 정부는 지구온난화 기후위기 속에서 탄소발생을 줄이고 단계적으로 원전과 석탄발전 가동을 중단하고 2030년까지 전체 발전량의 20%를 신재생에너지로 공급하는 것을 목표로 하고 있다.

생산된 전기를 이차전지에 저장했다가 전력이 필요할 때 공급하는 에너지저장장치는 주파수조정,

신재생에너지 연계 발전, 전력 피크 억제 효과, 전력 수급 위기 대응 등 많은 장점이 있다. 러시아 발 에너지 가격 상승 또한 전 세계의 에너지 가격 상승과 더불어 물가상승을 불러오고 있다.

세계의 기후위기 속에서 에너지저장장치는 꼭 필요하다. 2017년과 2018년 화재사고 이후 정부 지원은 줄고 규제는 늘어나서 국내 ESS 시장은 정체되어있다.

자동차, 철도, 항공, 전력, 국방, 금융, 의료 등 대부분의 분야에서 SW의 의존도가 높아지고 있고, SW 오류로 인한 사고의 피해가 그동안 발생하였고 위험 정도를 낮추고 재발을 막기 위한 활동은 제품의 안전도를 높이고 신뢰도 향상에 도움이 된다. 시스템의 안전 확보를 위해 기능안전 표준화가 국제적으로 활발히 이루어지고 있다.

선사시대 두려움에 떨던 불도 이젠 인류는 이롭게 쓰고 있다. 아니 없어서는 안 되는 요소이다. 에너지저장장치 또한 마찬가지라고 생각된다. 불이나 칼처럼 나쁘게만 쓰면 안 좋은 것들일 수도 있지만 좋게 칼로 요리를 하고 불로 따뜻하게 난방을 하는 우리 일상에 없어서는 안 될 존재들이다.

단순히 가져다쓰는 전기가 아닌 효율적으로 쓰는 전기가 돼야 될 것이다. 장난감에 갈아 끼는 건전지 정도로만 생각해서는 안 되고, 더 세밀히 물성을 파악하고 또 충전과 방전이 반복되는 에너지저장장치에서는 이를 제어하는 BMS의 SW 안전 강화 또한 필요하다.

화재 발생이후 ESS산업은 신뢰도 회복을 위해 안전 기준을 강화하고 있다. 위기를 기회로 삼아서 타 산업분야에서도 그렇듯이 산업이 발전함에 있어 사고를 많이 경험하고, 재발 방지를 하고 안전한 상황이 만들어지면 세계 ESS 시장에서 국내 기업이 선두할 수 있으리라 기대된다.

이처럼 현대 사회에서는 모든 분야에서 제품과 서비스 구조가 복잡해지고 기능이 많아짐에 따라 시스템이 오작동하거나 오류로 인한 사고가 발생하고 있다. 시속 300Km/h이상으로 달리는 고속열차에서 안전벨트를 매지 않아도 우리는 안전벨트를 매고 자동차를 타고 고속도로를 지날 때보다 더 안전하다고 느낄 수 있다. 사고 발생 후 신속한 원인 분석으로 위험(Risk)요소를 제거하고 피해의 가능성(Probability)과 심각성(Severity)을 낮추는 활동을 할 때 시스템에 대한 신뢰도는 높아지리라 믿는다.