


2차년도 주요 결과물

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

(과제번호) 2021-0-00077

- 결과물명 : 안전SW 검증 평가 모델
- 작성일자 : 2022년 12월 2일

과학기술정보통신부 SW컴퓨팅산업원천기술개발사업
“2차년도 주요 결과물”로 제출합니다.

수행기관	성명/직위	확인
슈어소프트테크(주)	심정민 / 이사	

정보통신기획평가원장 귀하

에너지저장장치 안전 SW 검증 모델



2022년 12월 2일

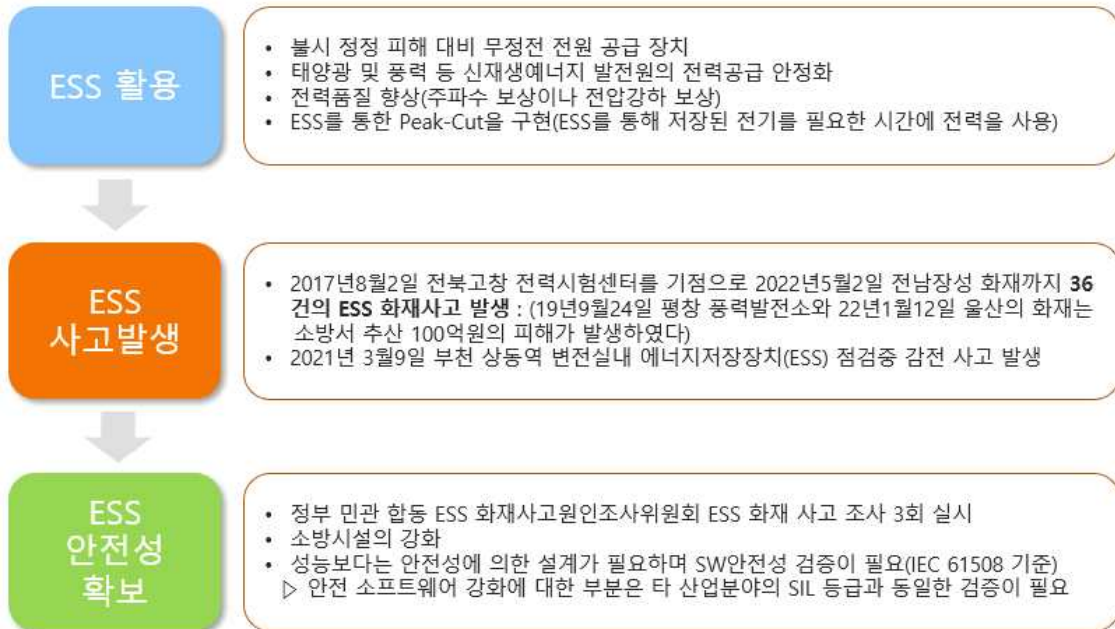
슈어소프트테크(주)

목 차

1. 개요	3
2. 에너지저장장치 SW 안전 검증 모델의 대상 범위 지정	4
3. 사고 사례를 통한 위험원 분석	5
4. 검증 활동 측면의 안전무결성 등급 기준 수립 필요성	5
5. 각 산업별 안전무결성 등급 결정 후 안전표준 수립	5
6. 안전무결성 기준 수립 파라미터	6
7. IEC 61508 기반의 SW안전 검증 프로세스	8
8. IEC 61508 대비 KC 62619 SW안전 검증 활동 비교	9
9. SW안전 검증 항목 및 지표 산정	10

1. 개요

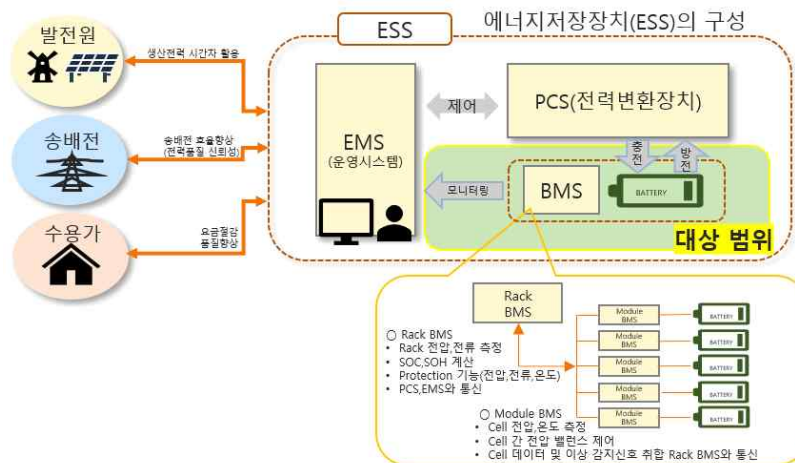
ESS의 활용과 화재사고 발생, ESS의 안전성 확보 및 SW 검증 강화 필요



<ESS활용 및 안전성 확보>

2. 에너지저장장치 SW 안전 검증 모델의 대상 범위 지정

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

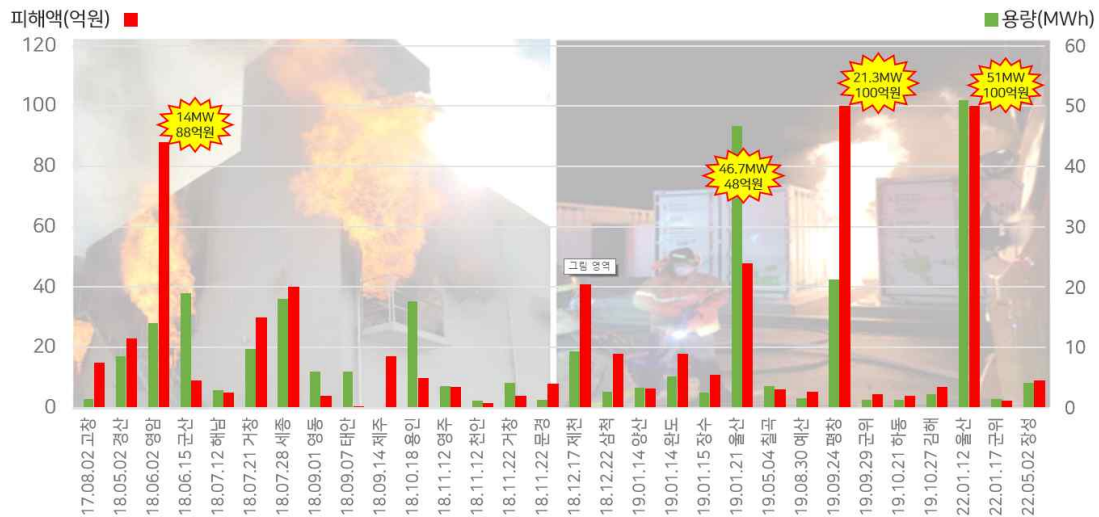


<에너지저장장치 시스템 구성에서 검증 대상범위 지정>

- 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

3. 사고 사례를 통한 위험원 분석

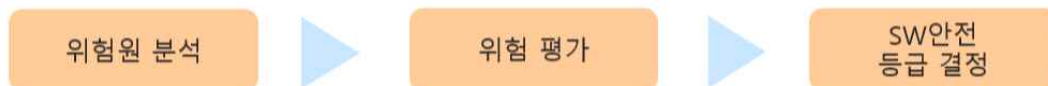
2017년 8월2일 전력연구원 고창 전력시험센터를 기점으로 2022년 9월 6일 인천 현대제철 화재까지 37건의 ESS 화재사고가 발생하였다. 2019년 9월 평창 풍력발전소와 22년1월 울산의 화재는 소방서 추산 100억 원의 큰 피해가 발생하였으며, 최근 2022년9월 발생한 인천 현대제철의 화재는 300억 원 이상의 피해 추정



<국내 ESS화재 및 피해규모>

4. 검증 활동 측면의 안전무결성 등급 기준 수립 필요성

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 안전관리 가능



<그림5 위험원 분석을 통한 SW안전 등급 결정>

5. 각 산업별 안전무결성 등급 결정 후 안전표준 수립

산업 도메인별 안전무결성 등급(SIL)은 각 산업별 표준 수립 시 대상 도메인의 위험원을 분석하고, 평가하여 SW안전 등급 결정

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	

<각 산업별 안전무결성(SIL) 등급 분류>

6. 안전무결성(Safety Integrity Level) 기준 수립 파라미터

- 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 단계
- 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 보장

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

리스크 파라미터		구분	비고
결과(C)	C ₁	• 경상	-구분 체계는 사람에 대한 상해와 사망에 따라 개발되었다. 환경 또는 물질 손상에 대해서도 기타 구분 계층을 개발할 필요가 있다. - C1, C2, C3, C4의 해석에 대하여, 사고의 결과와 정상적인 구제조치를 고려하여야 한다.
	C ₂	• 한명 이상의 사람이 심각하고 영구적인 상해;한명 사망	
위해 구역의 빈도와 그에 대한 노출 시간(F)	C ₃	• 몇 사람 사망	
	C ₄	• 매우 많은 수의 사람 사망	
위해 구역을 피할 가능성(P)	F ₁	• 위해 구역에서의 노출이 드물거나 가끔 있음	
	F ₂	• 위해 구역에서의 노출이 빈번하거나 항상 있음	
위대한 사건을 피할 가능성(P)	P ₁	• 일정 조건에서 가능	-어떤 공정의 운영 감독 유무, 위대한 사건의 방지 유무 등
	P ₂	• 거의 불가능	
불의의 사건 발생 확률(W)	W ₁	• 불의의 사고 발생을 간과할 확률 이 거의 적으며 불의의 사고 발생 가능성이 거의 없음.	-W 인자의 목적은 안전관련 시스템 (E/E/PE 나 기타 기술)을 추가하지 않고 기타 기술 위험 감소 시설만 포함시킨 경우의 불의의 사고 발생 빈도를 측정하는 것이다.
	W ₂	• 불의의 사고 발생을 간과할 확률 이 적으며 불의의 사고 발생 가능성이 약간 있음.	
	W ₃	• 불의의 사고 발생을 간과할 확률 이 비교적 높으며 불의의 사고 발생 가능성이 자주 있음.	

<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

<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 분류

참고: 우리나라 4인 가구의 월평균 전력소비량 350kWh 이며, 가구당 하루 평균 전력 소비량은 11.7kWh. 국내최대 ESS는 신안군 안좌도이며 배터리 용량은 340MWh 이다. 이는 2만9천여 가구가 하루 동안 사용할 수 있는 전기를 저장

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	

<평가 항목 분류시 고려되는 항목 구분>

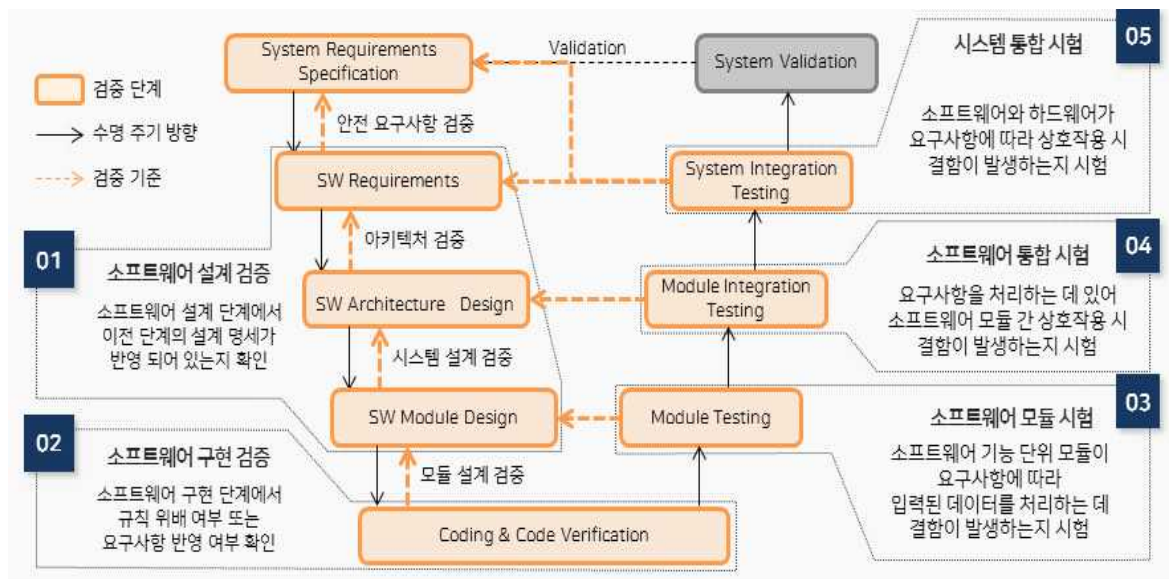
위의 리스크 파라미터 평가 기준을 적용하여 에너지저장시스템의 안전 무결성 등급을 아래와 같이

결정

리스크 파라미터			
위해한 사건의 결과(C)	위해 구역의 빈도와 그에 대한 노출시간 (F)	위해한 사건으로 피할 가능성 (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

<리스크 파라미터에 기반한 정성적 안전 무결성 수준 결정>

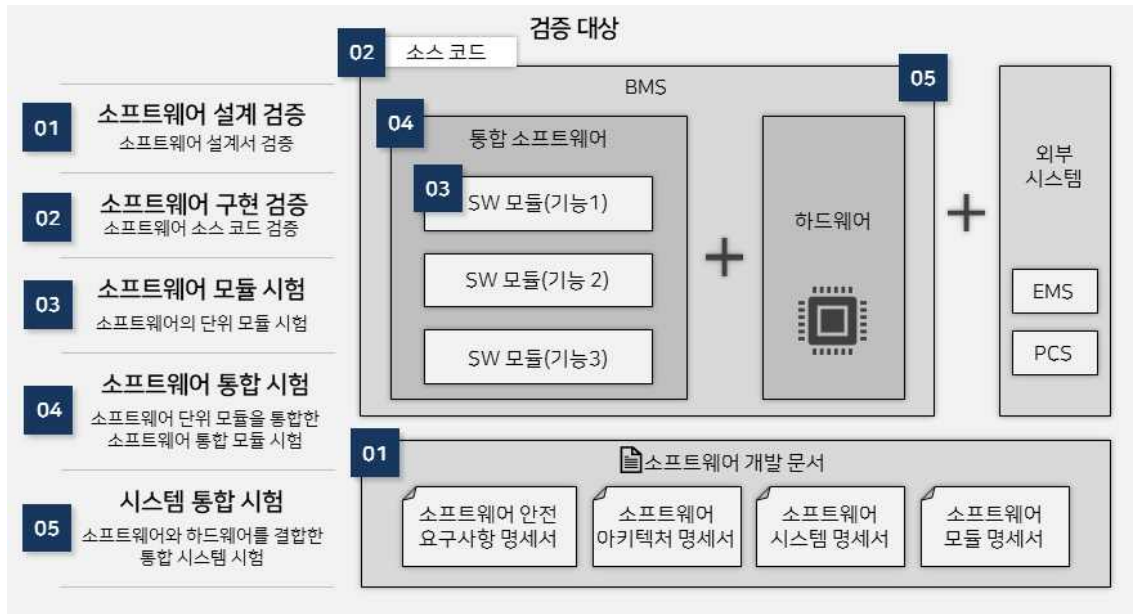
7. IEC 61508 기반의 SW안전 검증 프로세스



<IEC 61508 기반 SW개발 검증 프로세스>

안전 SW의 검증 단계별 검증대상의 설명

- 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



<SW개발 검증 프로세스 단계별 검증 대상>

8. IEC 61508 대비 KC 62619 SW안전 검증 활동 비교

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 비교

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

<수립된 항목을 기준으로 KC 62619에서의 수행여부 확인>

9. SW안전 검증 항목 및 지표 산정

소프트웨어 설계 과정에서는 SW 요구사항 설계, SW 아키텍처 설계 및 SW 상세 설계 단계가 있다. 소프트웨어 설계 검증에서는 각 설계 단계에서 상위 설계 과정에서 명세 된 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 제시

소프트웨어 설계 검증 : 설계 단계에서 상위 설계 과정에서 명세 된 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

<소프트웨어 설계 검증 - 검증지표>

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

소프트웨어 구현 검증 : 소프트웨어 구현 시 설계 단계에서 명세 된 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

<소프트웨어 구현 검증 - 검증지표>

소프트웨어 모듈은 소프트웨어가 작동하는 기능의 최소 단위를 의미한다. 소프트웨어 모듈 시험 과정에서 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 제시

소프트웨어 모듈 시험 : 기능의 최소 단위인 모듈의 데이터 처리 시 발생 가능한 결함 검출				
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 테 스트 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 케이스 를 생성하고 소프트웨어 단위 모듈이 명세된 요구사 항을 충족하는지 동작시켜 확인한다.	요구사항 커버리지	$\frac{\text{시험에서 충족된 요구사항 개수}}{\text{SW 모듈 설계 요구사항 개수}}$	X

<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 제시

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 않는 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

<소프트웨어 통합 시험 검증지표>

시스템 통합 시험은 BMS 소프트웨어와 하드웨어와 결합할 시 명세된 기능 및 비기능 요구사항을 충족하는지 확인하고 악의 조건에서도 요구사항을 어느정도 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 제시

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	$\frac{\text{시험에서 충족된 기능 요구사항 개수}}{\text{기능 요구사항 개수}}$	△ 8.2에서 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	$\frac{\text{시스템 무정지 TC 개수}}{\text{악의 조건 TC 개수}}$	△ 부속서 D.5에서 안전기능 기능시험 수행

<시스템 통합 시험 검증지표>