1차년도 주요 결과물

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

(과제번호) 2021-0-00077

- 결과물명 : 타 안전분야 대비 에너지 분야 GAP분석서
- 작성일자 : 2021년 12월 22일

과학기술정보통신부 SW컴퓨팅산업원천기술개발사업
"1차년도 주요 결과물"로 제출합니다.

수행기관	성명/직위	확인
슈어소프트테크(주)	심정민 / 이사	

정보통신기획평가원장 귀하

목 차

1. 개요 ····· 3
1.1 SW 안전이란 ····· 3
1.2 SW 오류로 인한 사고 ····· 3
1.3 안전(Safety)의 개념 ····· 6
1.4 기능안전(Function Safety)의 개념 ····· 6

2. 산업분야의 기능안전 표준 ····· 8
2.1 IEC 61508 일반적인 안전표준 ····· 9
2.2 철도 산업의 안전표준 ····· 10
2.3 항공 분야의 안전표준 ····· 10
2.4 원자력발전소의 안전표준 ····· 10
2.5 의료기기 안전표준 ····· 10
2.6 자동차분야 안전 표준 ····· 11

3. 전기 에너지 장치 관련 표준 동향 ····· 13
3.1 전기 에너지 장치의 국제 표준 동향 ····· 13
3.2 전기 에너지 장치의 국외 표준 동향 ····· 15

4. 타 산업 분야의 기능안전과 전기 에너지 장치의 기능안전 관련 GAP ····· 17

5. 결론 ····· 18

<표 차례>

표 1 산업 도메인 별 안전 관련 국제 표준 ····· 8
표 2 해외 ESS 배터리 인증평가 표준 ····· 15
표 3 국내 ESS화재 발생 리스트 ····· 16

한전시방서 ····· 19

1. 개요

이젠 자율주행 자동차라는 말이 어색하지 않은 시대가 도래하였다.

첨단 전자 산업의 발전과 함께 HW와 SW가 융합된 안전 시스템의 시장이 지속적으로 성장을 하고 있고, SW 결함으로 인한 사고의 피해 범위와 규모 또한 확대되고 있다.

모든 산업 분야에서 여러 위험요소를 최소화하기 위해 신뢰성 및 안전성에 대해 각 분야 별로 안전 관련 국제 표준을 준수하도록 요구하고 있다.

1.1 SW 안전이란

SW 오작동 및 안전 기능(사전에 위험성 분석 등을 통해 마련된 위험한 상황 발생을 방지하는 기능) 미비로 발생 가능한 사고(Accident)로부터 충분한 대비가 될 수 있도록 SW 위험원(Hazard)을 사전에 도출하여 제거한 상태를 말한다.

* 참조 : ISO/IEC Guide 51(Safety : freedom from risk which is not tolerable)

1.2 SW 오류로 인한 사고

현대 사회에서 다양한 분야에서 대부분의 시스템들이 소프트웨어를 내장하고 있고, 여러 분야에서 소프트웨어 의존도가 높아지고 있다. 또한 소프트웨어 오류로 인한 사고와 그로인한 피해 범위와 규모가 확대되고 있다.

그림 1 AECL의 방사선치료기 Therac-25

캐나다의 의료기업체인 AECL이 암 종양 제거를 위한 방사선 치료기인 Therac-25는 1985년 6월과 1987년 1월 사이에 환자 중 일부가 수십만 라드 노출되어 방사선 피폭되면서 5명 이상의 사람들이 사망했다. 턴테이블을 작동하는 변수 설정 오류(오버플로우 발생)로 턴테이블에 잘못된 위치에 놓일수 있고, 기타 여러 가지 잠재적인 버그와 오류로 인하여 이상동작을 하였다.

Therac-25 사건 이후, FDA는 안전이 중요한 시스템과 관련된 많은 문제에 대한 태도를 바꾸었으며 보고 시스템을 개선하고 소프트웨어를 포함하도록 절차와 지침을 보강하였다.

그림 2 렉서스 급발진 사고

2009년 8월 미국에서 일가족 넷이 타고 있던 렉서스 ES350이 급발진 사고로 탑승자 4명 전원으로 사망한 사고가 있었다. 사고 당시 차량이 통제 불능 상태이며 시속 120마일을 초고하여 주행하고 있다고 말했다. 이는 바(BARR) 그룹의 도요타 급발진 조사보고서로 전자제어장치(ECU)에 내장된 SW 내부 오류로 인한 것으로 밝혀 졌다. 초기 차에 맞지 않는 바닥매트로 인한 것으로만 치부했던 사건이었다. 스택 오버플로우가 발생할수 있으며 변수 손상 등 여러 SW 오류가 내포되어있었다. 2014년 3월19일, 미 법무부는 도요타가 지난 6년간 급발진을 부정하고 소비자를 기만했다는 이유로 자동차업계 역사상 최고 벌금인 약 1조 3천 억원이 부과되었다.. 이 사건은 급발진의 원인으로 전자제어장치의 오류를 인정한 사실상 최초의 사례라고 할수 있다.

그림 3 Ariane 5 Flight 501 로켓 사고

70억달러의 비용으로 10년에 걸처 구축된 유럽우주국(European Space Agency:ESA)의 로켓

Ariane 5 Flight 501 로켓이 1996년 6월 4일 발사 39초 후에 3700m 고도에서 비행경로를 이탈하면서 폭발하였다. 이는 로켓의 자세를 결정하는 관성기준시스템(Inertial Reference System)에서 오버플로우가 발생하였다. 수평 속도 데이터를 64비트 부동소수점 수 형식에서 16비트 부호가 있는 정수 형식에서 전환하는 과정에서 오버플로우가 발생하였다. 데이터 전환코드가 예상 못한 높은 값 같은 예외상황처리 또한 되어 있지 않았다.

그림 4 우버(Uber)의 자율주행차량 XC90 사고

최근 자율주행차의 오동작으로 인한 치명적인 사고가 잇따라 발생하고 있다.
기본적인 달리기위한 자동차에서 카메라(Camera),레이터(RADAR),라이더(LiDAR) 센서 등이 추가되어 자율주행을 하기위해서는 주변을 인지하고 판단하고 제어하는 과정의 연속이 될것이다.
2018년 3월 18일 밤 9시 58분경, 미국 애리조나(Arizona)주 템피(Tempe)에서 자율주행 시범 운행 중이던 우버 차량이 자전거를 끌고 길을 건너던 40대 여성을 43 mi/h(69 km/h) 속도로 치어 사망케 함에 따라 자율주행차로 인한 최초의 보행자 사망 사고로 기록되었다.

1986년 4월 26일 폭발사고가 발생했던 체르노빌 원전의 모습이다. 위키피디아 제공

그림 5 체르노빌 원전

1986년 구소련 체르노빌 원전사고, 2011년 일본 후쿠시마 원전 사고로 다량의 방사선, 방사선

물질이 환경으로 누출됐다. 지진으로 인해 후쿠시마 원전 사고가 발생하였지만 조금더 안전에 신경써서 설계했더라면하는 아쉬움이 남는다.

그림 6 플래스테이션3 게임기

2010년3월1일 갑자기 플래스테이션3(PS3) 게임기에서는 오류코드 '8001050F'가 뜨면서 제대로 작동하지 않았다. 이 오류코드는 PS3의 시계 소프트웨어가 '3월1일'을 '2월29일'로 계산했기 때문에 발생한 오류였다.

1.3 안전(Safety)의 개념

IEEE 1228에서는 소프트웨어 안전(Software Safety)을 '재해나 사고의 결과로 인해 사람의 사망,상해 또는 재산 피해의 원인이 될 수 있는 소프트웨어 위험원 으로부터의 자유로움(Freedom from Software Hazard)'이라고 정의하고 있다. SW 위험요소를 사전에 제거하고 오류로 발생 가능한 사고를 예방하는 것이다.

1.4 기능안전(Functional Safety)의 개념

기능안전이란 운용자 오류, 하드웨어 및 소프트웨어 고장, 환경적 변화 등에 대한 안전한 관리를 포함, 주어진 입력에 대하여 정확히 동작하는 안전 관련 시스템에 의존하는 하나의 시스템의 전체적인 안전성의 일환이다. 기능안전은 기존의 제품 안전 평가방법보다 더 높은 수준의 안전 평가로, 기술이 발전하고 복잡해짐에 따라 예기지 찮은 위험이 발생될 확률이 커져가는 현대 사회에서 안전을 보장하기 위해 사용할 수 있는 대표적인 평가 방법이다. 이로 인해 자동차, 철도, 의료기기, 발전소, 자동화설비 등 산업영역에서 그 중요성이 대두되고 있으며 일부 영역에선 점차 의무화 되고 있는 추세이다.

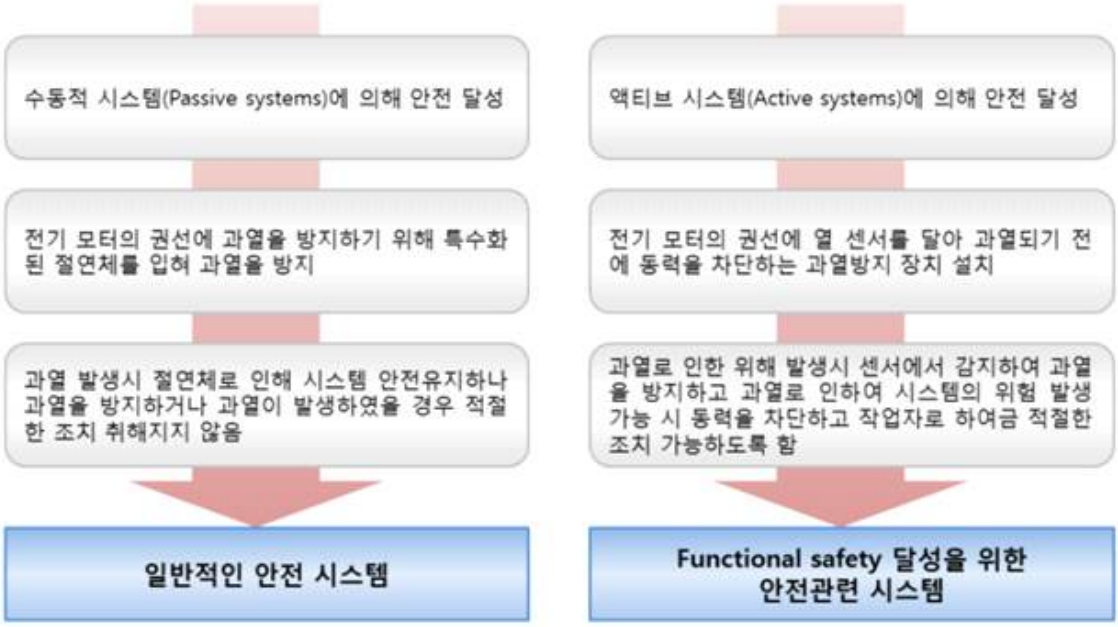


그림 7 일반적인 안전시스템과 기능안전시스템

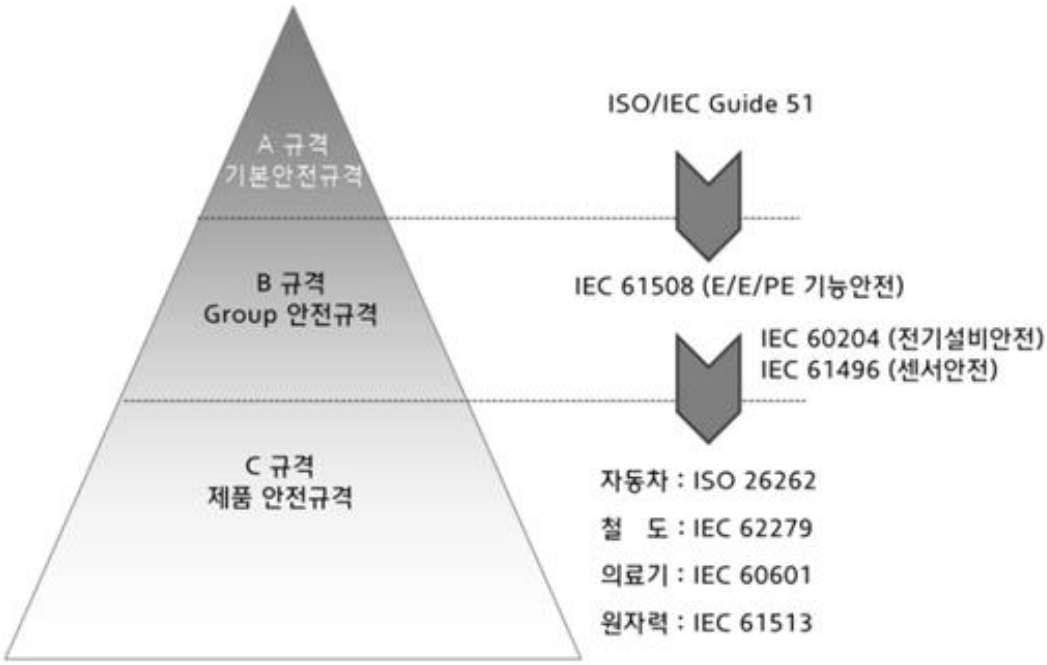


그림 8 SW 안전관련 국제표준 구성 체계

2. 산업 분야의 기능안전 표준

그림 9 IEC 61508 기반 도메인 별 안전 관련 국제 표준

분야	표준	설명
산업일반	IEC 61508	전기,전자,프로그램 가능한 전자시스템의 기능안전 표준
자동차	ISO 26262	자동차 전자제어장치의 오작동으로 인한 사고 및 인명 손실을 최소화하는 안전 표준
제조, 계측	IEC 62061	제조공정, 계측을 사용하는 전자제어시스템에 대한 기능안전 표준
의료기기	ISO 14971 IEC 62304	전자 의료장비(MRI, CT 등) 소프트웨어 안전 표준
항공기	DO-178C	항공 소프트웨어 고려사항과 유무인기/설비 품질 인증을 위한 표준
철도	IEC 62278 IEC 62279	RAMS(Reliability, Availability, Maintainability, Safety)의 기술적 내용과 철도시스템 관리원칙을 제공하는 국제표준
원자력	IEC 60880	원자력발전소의 안전 표준

표 1 산업 도메인 별 안전 관련 국제 표준

"사후약방문" 또는 "소 잃고 외양간 고친다" 이란 말이 있다. 원래의 뜻만 보면 사고가 나서 후회한다라는 뜻이겠지만 안전 개념에서 보면 한 마리의 소를 잃었을때 빨리 다시 외양간을 고치고 다시는 잃지 않겠다는 의미로 보는게 맞겠다. 즉 한번 난 사고는 다시는 나지 않게 예방한다.

더 나아가 미리 일어날수도 있는 사고 유형을 예상하고, 사전에 예방 할수 있는 방안을 마련하고 최소한의 허용할수 있는 피해가 발생할수 있는 활동을 안전 활동이라 할 수 있겠다.

각 산업분야도 먼저 발전을 하고 사고가 많이 발생하면서 안전 표준이 제정된다고 할 수있겠다.

2.1 IEC 61508의 일반적인 안전표준

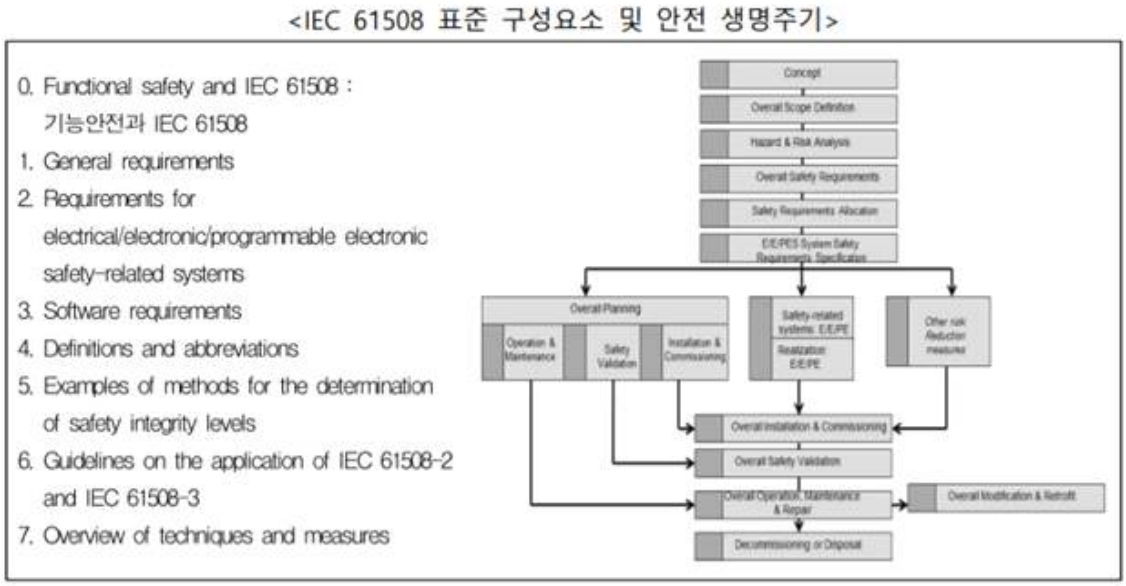


그림 10 IEC61508 표준 구성요소 및 안전 생명주기

IEC 61508 표준에서는 소프트웨어 안전등급에 따른 안전활동의 구분이 별도 존재하지 않는다. 소프트웨어 요구사항 정의 단계에서만 'Safety'가 언급되며, 이후 하위 활동에서는 정의된 안전 요구사항에 따른 설계 및 검증 활동을 설명하고 있다. 즉, 일반적인 소프트웨어 개발 활동들은 기본으로 수행된다는 가정 하에 안전 개발을 설명하고 있으며, 안전 특화된 활동들을 개발 단계별로 구분 지어 설명하고 있지는 않는다. 소프트웨어 안전등급에 따라 안전활동이 구분되지는 않으나, 안전 등급에 따른 안전기법 및 수단의 차등 적용을 제시하고 있다. 다루고 있는 기법 및 수단의 수가 매우 많으며, 안전 등급을 기준으로 세부 기법 및 활동, 방법론 측면에서 설명하고 있다.

허용 가능한 위험 수준의 SW안전 확보를 위해서는 정해진 SW 시스템 개발 프로세스에 따라 단계별로 SW 안전 확보 활동이 필요하다. 우선 전체 시스템 수준에서 위험성 분석을 선행하고 도출된 시스템 안전요구 사항을 바탕으로 SW 안전 요구사항을 도출한다.

위험원 분석(Hazard Analysis)을 통해 발생 가능한 위험원을 식별·제거하고 위험성 평가(Risk Assessment) 등을 통해 사고 발생 가능성과 영향을 정량화하여 SW시스템의 안전 목표수준 설정과 달성 여부를 추적 관리한다.

목표한 SW시스템 안전 수준에 맞도록 위험성을 낮추는데 필요한 안전 요구사항 설정을 위한 SW 시스템 안전 메카니즘 구현 및 달성여부 검증하고 확인한다.

2.2 철도 분야(EN 50128, IEC 62279) 안전표준

철도 시스템의 기본인 철도 신호와 관련된 제어(control), 명령(command) 및 보호(protection) 시스템의 안전성을 높이기 위한 활동을 정의하고 있다.

미국은 화물 및 저속 수송을 목적으로 하고 있고, 유럽연합은 승객 및 고속 수송을 목적으로 하고 있다. 미국(CFR49), 유럽(EN50128)은 안전요구 제품에 대해서는 국제표준에 맞는 객관적인 입증 자료를 요구하는 규제와 인증제도를 요구하고 있다.

국내의 경우 철도 안전법 및 시행령에 근거하여 SW 안전성 확보를 포함한 철도차량 기술기준을 가지고 있다. 국제표준·규격 등을 적용하고 있다. 또한, 한국철도기술연구원은 형식승인검사기관으로 국제·국내 표준 기반으로 관련 연구·시험·인증을 수행하고 있으며 SW 안전에 대한 철도 RAMS (Reliability, Availability, Maintainability, and Safety) 기술 교육을 기업에게 제공하고 있다.

2.3 항공 분야(DO-178,ED-12) 안전표준

항공기에 탑재되는 SWdp 대한 기능안전 표준으로, 시스템 수명 전주기에 걸쳐 요구되는 활동, 증거물(evidence) 등을 정의하고 있다.

DO-178(RTCA가 제정, 미국 FAA가 채택한 표준), ED-12(EUROCAE 제정, 유럽 EASA가 채택한 표준, RTCA와 EUROCAE는 상호 협조하며 표준화 작업중에 있다.

미연방항공청(FAA)과 유럽항공안전청(EASA)에서는 소프트웨어 안전 확보를 위한 표준으로 각 DO-178, ED-12를 명시하고 요구하고 있다.

국내 항공기 기술기준과 항행안전시설 성능적합증명 검사 기술기준에 SW는 미국(DO-178) 및 유럽(ED-12) 기준을 준수하도록 요구하고 있으며 주로 해외 도입 항공기 또는 장비에 적용하고 있다.

2.4 원자력 분야 안전표준

IEC 60880은 원자력 발전소의 컴퓨터 기반 계측제어 시스템 소프트웨어가 지녀야 할 요구사항을 기술한 표준이다. 소프트웨어 안전을 확보하기 위해 원자력 산업 특성에 맞게 제정된 표준이다. 설계시 고려하여야 하는 최소한의 기능과 성능에 관한 기준에 따라 지진이나 방사선 누출, 화재, 침수, 기타 고장들에 대해 안정상태를 유지하는데 목적이 있다. 과거 원전사고 사례를 분석하고 사고에 대처하기 위한 보호 기능을 제공하는 계통 및 사고시 발전소를 제어 상태로 유지하는데 필요한 계통이 포함된다.

2.5 의료기기 안전표준

관련표준으로는 ISO 14971, IEC 62304가 있다.

의료 분야의 안전체계와 SW 생명주기별 의료 분야에 특화된 활동을 요구사항을 기술한 표준이다. 제어, 측정, 분석, 진단, 데이터변환, 전송, 수신, 표시기능 등 의료기기 특성을 포함한 기술 및 개발 필수 사항이 명시되어 있다.

2.6 자동차 분야(ISO 26262) 안전표준

자동차에 탑재되는 전기·전자 시스템의 기능안전 표준으로, 시스템 수명 전주기에 걸쳐 요구되는 활동, 증거물(evidence) 등을 정의하고 있다. 해외 BMW, BENZ, Volkswagen, Volvo, PSA, GM, Ford, Toyota, Honda와 주요 협력사 보쉬, 콘티넨탈, 지멘스, 발레오, 델파이, 덴소, 오므론 등은 국제표준에 맞는 체계를 확보하고, 공급자에게도 SW 안전관련 국제표준 준수를 요구·확인하고 있다. 국내에서도 현대자동차, 현대모비스, 만도, LG 등 대기업 대부분은 국제표준 ISO 26262를 만족하는 전장부품 연구개발프로세스를 구축·운영하고 공급자에게도 기능 안전 준수를 요구하고 있다.

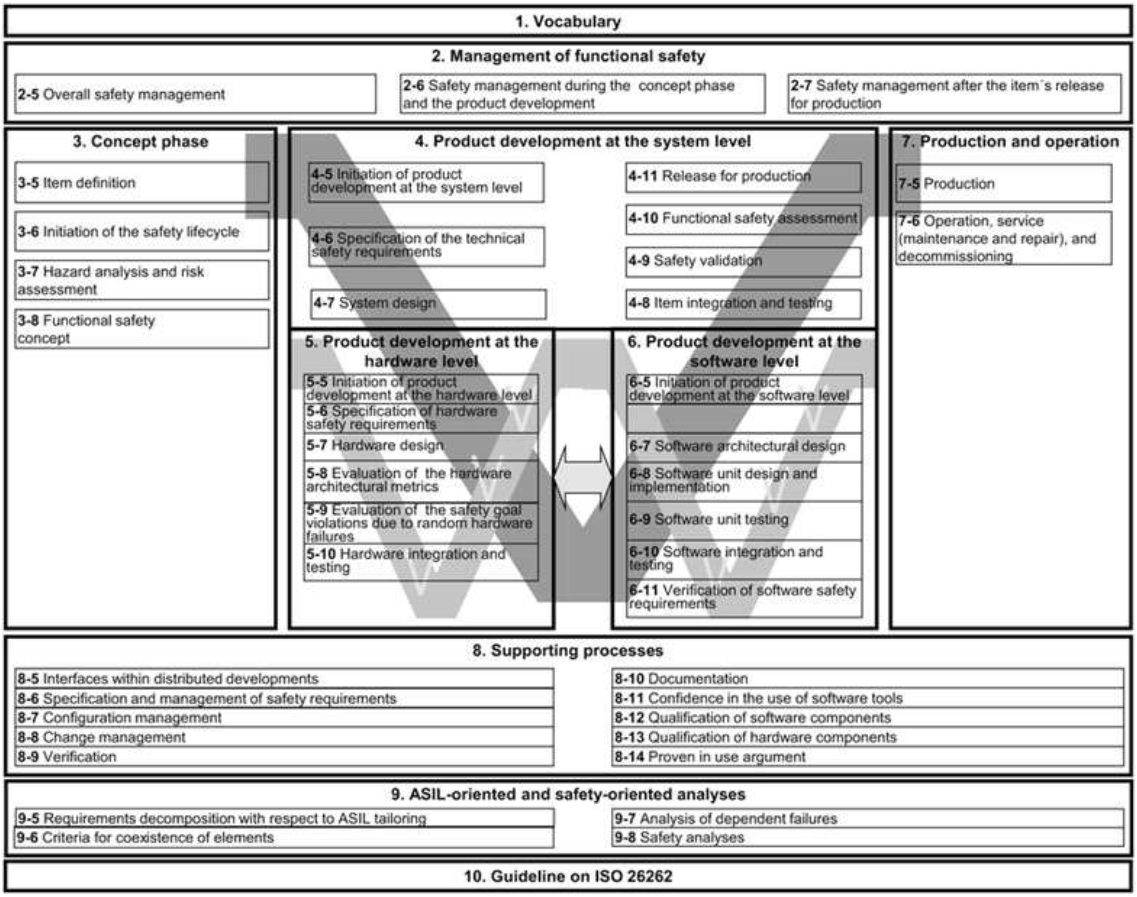


그림 11 ISO 26262

- 파트 1: 어휘
- 파트 2: 기능 안전 관리
- 파트 3: 개념 단계
- 파트 4: 시스템 수준에서 제품 개발
- 파트 5: 하드웨어 수준의 제품 개발
- 파트 6: 소프트웨어 수준의 제품 개발
- 파트 7: 생산 및 운영
- 파트 8: 지원 프로세스
- 파트 9: ASIL(Automotive Safety Integrity Level) 지향 및 안전 지향 분석

- 파트10: ISO 26262 지침

MISRA-C Coding rule을 적용하고 있다.
MISRA C는 MISRA(Motor Industry Software Reliability Association)에서 개발한 자동차 산업에 사용되는 임베이드 시스템 소프트웨어의 코드 안정성, 호환성, 신뢰성 향상을 위한 C 프로그래밍 언어에 대한 개발 가이드라인 (C++의 경우 MISRA C++가 있다)
MISRA C는 자동차 산업을 위해 개발되었지만, 우주/항공, 의료장비, 국방, 철도 등의 다양한 산업의 Best Practices로 진화되어 활용되고 있다.
MISRA C:2012의 경우 총 143 개 규칙과 16개의 지침으로 구성되어 있다.

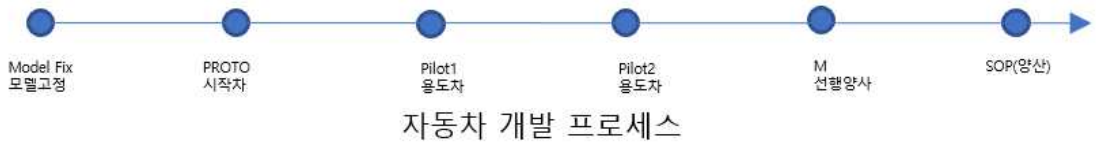


그림 12 자동차개발프로세스

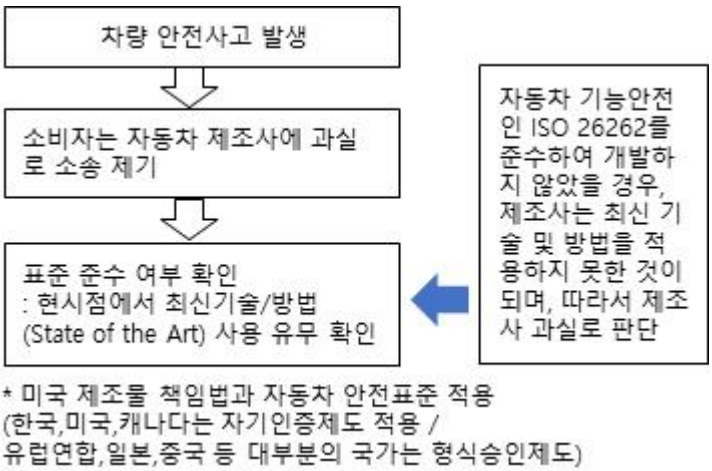


그림 13 자동차 안전사고 발생 및 제조물책임법

3. 전기 에너지 저장장치 관련 표준 동향

전기 에너지저장시스템(ESS)은 발전원에서 생산된 전기를 배터리 등의 저장장치에 저장한 후, 전력이 필요할 때 공급할 수 있는 시스템이다. 발전출력 변동이 심한 태양광, 풍력과 같은 신재생 에너지원과 연계하여 출력품질을 향상시키거나 야간 경부하 시간에 유휴 전력을 저장하여 피크부하에 방전하여 사용할 수도 있다.

기후위기 속 탄소중립 정책과 함께 화석연료를 줄이며 신재생에너지 연계 에너지저장장치 설치는 전세계적으로 자연스럽게 증가하는 추세라고 할수 있다.

3.1 전기 에너지저장장치의 국제 표준 동향

일본은 2011년 동일본 대지진 이후 원자력발전의 가동을 중단하고 약 466만 가구의 정전이 있었다. 하루 3시간씩 계약 정전이 실시되었으며 이로 인해 일본에서는 가정용 ESS가 활성화되었다. 이를 계기로 일본 전지협회 SBA A 1101 산업용 리튬 이차전지 성능과 안전성 시험 방법에 대한 단체표준이 제정이 되었다. 2012년에 일본은 이를 국제표준으로 IEC TC21에 제안하여 2014년 IEC 62620 산업용 리튬 이차 단전지와 전지의 성능요구 사항 국제표준이 제정되었으며, 이후 2017년에는 IEC 62619 산업용 리튬 이차 단전지와 전지의 안전성 요구사항이 제정되었다. IEC 62619는 초기 제정시부터 용도가 다양화되어 관련 표준이 명확화되기 전까지 Umblella 표준으로 발표가 되었다.

IEC 63056:2020 © IEC 2020 – 5 –

INTRODUCTION

This document covers safety requirements for secondary lithium cells and batteries for use in Electrical Energy Storage Systems and is under the umbrella standard IEC 62619 as shown in Figure 1. As an umbrella standard, IEC 62619 had been developed which covered various industrial applications in 2017.

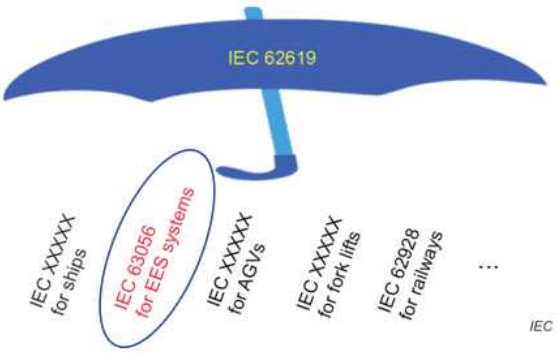


Figure 1 – IEC 62619 as umbrella standard to various industrial applications

그림 14 IEC 62619의 포괄적 응용 범위

2020년에는 EES Systems 용도로 IEC 63056 표준이 제정되었다.

IEC TC 21의 이차 전지, TC 22 의 전력변환장치, IEC TC 57 계통연계 등에서 요소별로 국제 표준화가 진행되고 있다. IEC TC 120에서는 ESS의 시스템 및 활용 측면에서의 표준화가 일부 제정 완료 되었고 목적에 따라 신규 표준은 개발중에 있다.
독립적인 시스템이 아니라 전력 개념으로 단순히 전기공급원이라 인식되던 에너지저장장치도 시스템 개념에서 논의가 되고 IEC TC 120에서 사용 목적에 따라 아래와 같이 IEC 62933 표준이 제정 완료 되거나 제정 중에 있다.

그림 15 IEC TC120 표준

전기 에너지장치의 안전표준은 리튬이차전지의 화재 발생에 중점을 두고 있다.
리튬이차전지의 높은 에너지 밀도로 인해 안전문제를 일으킬 우려가 있어 화재 및 폭발을 일으키는 열폭주 현상에 대해 접근하여 이를 토대로 성능시험과 안전시험이 이루어 지고 있다.

해외 각 지역별 ESS 배터리 인증평가 표준은 아래와 같다.

각 지역 ESS배터리 인증평가 표준

순번	인증/적용범위	인증규격	적용제품	비고
1	배터리 운송	UN38.3	배터리 셀, 배터리 모듈, 배터리 팩, ESS팩	전지팩/ESS팩이 6200Wh일 경우 배터리 모듈로 시험을 진행
2	CB인증	IEC 62619	배터리 셀 / 배터리 팩	안전
		IEC 62620	배터리 셀 / 배터리 팩	성능
		IEC 63056	전력저장시스템	배터리 셀 IEC 62619 참조
3	중국	GB/T 36276	배터리 셀, 배터리 팩, 배터리 시스템	CQC&CGC 인증
		YD/T 2344.1	배터리 팩	통신
4	EU	EN 62619	배터리 셀, 배터리 팩	
		VDE-AR-E 2510-50	배터리 팩, 배터리 시스템	VDE인증
		EN 61000-6시리즈 규격	배터리 팩, 배터리 시스템	CE인증
5	인도	IS 16270	PV축전지	
		IS 16046-2	ESS배터리(리튬)	500 Wh이하만 취급
6	북아메리카	UL 1973	배터리 셀, 배터리 팩, 배터리 시스템	
		UL 9540	배터리 팩, 배터리 시스템	
		UL 9540A	배터리 셀, 배터리 팩, 배터리 시스템	
7	일본	JIS C8715-1	배터리 셀, 배터리 팩, 배터리 시스템	
		JIS C8715-2	배터리 셀, 배터리 팩, 배터리 시스템	S-Mark
8	한국	KC 62619	배터리 셀, 배터리 팩, 배터리 시스템	KC 인증
9	호주	전기저장설비 전기안전요구	배터리 팩, 배터리 시스템	CEC 인증

표2 해외 ESS 배터리 인증평가 표준

3.2 전기 에너지 장치 관련 국내 표준

국내는 2017년도부터 여러 건의 에너지저장장치의 화재사고로 인하여 강화된 정책들이 시행중이다.

(제조 기준)

[KS]세계 최초 ESS 시스템 안전 국제표준 도입('19.5월)

[KC인증]배터리,PCS 등 주요부품 인증(19.8월)

[단체표준]배터리 보호장치 성능 및 통합 제어 프로토콜 규정 등 세부기분 마련

(설치 기준)

[설치장소]옥내는 설치용량을 총 600kW로 제한, 옥외는 별도 전용건물 설치

[안전장치]과전류,과전압 등 보호장치 의무화

[모니터링]이상징후 시 비상정지 및 관리자 통보, 운영 데이터 별도 저장·관리

(운영·관리)

[충전율]배터리 만충전 후 추가 충전 금지

[운영환경]제조사 권장범위 내 온·습도, 분진 관리

[관리제도]법정검사 주기단축)4년→ 1~2년), 임의 개보수시 제재조항 신설 등

(소방기준)

[특정소장대상물 지정]소장,방화시설 의무화 등('19,소방시설법 개정)

[화재안전기준]ESS에 특화된(소화설비,방화구획,이격거리) 소방기준 마련('19.9월)

화재 사고 이후 2019년 10월21일 KC 62619를 제정하였다. 국제표준인 IEC 62619를 인용채택하였다.(정격용량 300kWh 이하의 에너지저장장치의 리튬이차전지시스템)

배터리의 화재사고를 방지하기 위해 일반안전고려사항과 형식시험조건(외부단락시험, 충돌시험, 낙하시험, 고온시험, 과충전시험, 강제방전시험, 내부단락검토, 과충전전압 제어시험, 과충전전류제어시험,과열제어시험 등)의 시험조건과 합격기준이 명시되어있다. 배터리 시스템의 안전(기능 안전성 검토)은 부속서 D에서 인용표준으로 IEC 61508, IEC 60730-1 Annex H를 적용하고 있다.

안전개념에서 ESS BMS(Battery Management System)제어기 내에서는 최소한의 안전기능인 고전압 검출 기능, 과전류 검출기능, 과열 검출 기능을 설계되어야한다.

전기산업진흥회,스마트그리드협회,전지산업협회,관련업계 등 민간이 자율적으로 협력하여, 배터리시스템 보호장치 성능사항, ESS 통합관리 기준 등을 단체표준에 추가하고 고효율인증과 연계하여 실효성을 확보한다.

No.	사고 일시	장소	배터리용량 (MWh)	운용기간 (월)	배터리상태	설치 장소	용도	발화지점 / 비고
1	17.08.02	전북 고창	1.46	-	설치중(보관)	해안가	풍력 연계	리튬이온전지
2	18.05.02	경북 경산	8.6	22	수리 점검 중	산지	주파수 조정	배터리 추정
3	18.06.02	전남 영암	14	29	수리 점검 중	산지	풍력 연계	배터리실 중앙 랙 추정
4	18.06.15	전북 군산	18.965	6	충전 후 휴지 중	해안가	태양광 연계	ESS 설비 내부
5	18.07.12	전남 해남	2.99	7	충전 후 휴지 중	해안가	태양광 연계	배터리랙 2~3번 모듈
6	18.07.21	경남 거창	9.7	19	충전 후 휴지 중	산지	풍력 연계	랙 상단 1~2단의 모듈
7	18.07.28	세종	18	-	설치 중(시공)	공장지대	피크제어용	배터리 추정
8	18.09.01	강원 영동	5.989	8	충전 후 휴지 중	산지	태양광 연계	1~2번 랙 14모듈
9	18.09.07	충남 태안	6	-	설치 중(시공)	해안가	태양광 연계	배터리 추정
10	18.09.14	제주	0.18	48	충전 중	상업지역	태양광 연계	랙 상단 1~2단의 모듈
11	18.10.18	경기 용인	17.7	31	수리 점검 중	공장주변	주파수 조정	리튬이온전지
12	18.11.12	경북 영주	3.66	9	충전 후 휴지 중	산지	태양광 연계	배터리 내부
13	18.11.12	충남 천안	1.22	11	충전 후 휴지 중	산지	태양광 연계	배터리실 내부
14	18.11.22	경남 거창	4.16	11	충전 후 휴지 중	산지	태양광 연계	7번 랙
15	18.11.22	경북 문경	1.331	7	충전 후 휴지 중	산지	태양광 연계	3,4 번 랙으로 추정

16	18.12.17	충북 제천	9.316	12	충전 후 휴지 중	산지	피크제어용	배터리 랙
17	18.12.22	강원 삼척	2.662	12	충전 후 휴지 중	산지	태양광 연계	배터리실 내부 추정
18	19.01.14	경남 양산	5.22	14	충전 중	산지	피크제어용	배터리실 내부
19	19.01.14	전남 완도	3.289	10	충전 후 휴지 중	공장지대	태양광 연계	배터리실 내부
20	19.01.15	전북 장수	2.496	9	충전 후 휴지 중	산지	태양광 연계	8번랙 10~11번 모듈 추정
21	19.01.21	울산	46.757	7	충전 후 휴지 중	공장지대	피크제어용	64번랙 추정
22	19.05.04	경북 칠곡	3.66	-	충전 후 휴지 중	산지	태양광 연계	19년4월 배터리 교체후 재가동 이후 화재발생 SOC 96%
23	19.05.26	전남 장수	1.027	12	충전 후 방전 중	산지	태양광 연계	관할 소방서 미신고
24	19.08.30	충남 예산	1.54		화재시 충전율 93.5% 충전범위 0~95%		태양광 연계	배터리 단락 추정 저전압 및 이상 고온 신호 확인
25	19.09.24	강원 평창	21.3		화재시 충전율 98.0%충전범위 0~100%	산지	풍력 연계	배터리 단락 추정 저전압 및 이상 고온 신호 확인
26	19.09.29	경북 군위	1.36		화재시 충전율 86.5% 충전범위 0~95%		태양광 연계	배터리 단락 추정 저전압 및 이상 고온 신호 확인
27	19.10.21	경남 하동	1.33		화재시 충전율 94.5% 충전범위 0~95%		태양광 연계	절연감시장치 분석 결과, 급격한 절연저항 감소 확인
28	19.10.27	경남 김해	2.26		화재시 충전율 92.2% 충전범위 0~95%		태양광 연계	배터리 단락 추정 저전압 및 이상 고온 신호 확인

표3 국내 ESS화재 발생 리스트

ESS 설치 기준은 전기설비기술기준의 판단기준에 관리되며, 주요 관련 규정으로는 전기설비 기술기준의 판단기준 '제4절 이차전지를 이용한 전기저장장치의 시설'에 반영(제295조~제298조)되어 있다.

4. 타 산업 분야의 안전 표준과 전기 에너지 장치의 기능안전 관련 GAP

4.1 소스 코드 정적분석

정적분석은 소스코드를 실제로 수행하지 않고, 컴파일만 하고 결함을 찾아내는 기술을 말한다. 실제로 실행을 하지 않기 때문에, 수행된 실행 흐름 뿐만 아니라 실행될 가능성이 있는 소스코드의 구석구석의 결함을 검사하는데 매우 효과적이다. 의학, 원자력, 자동차 등 타 산업분야에서는 정적분석을 통해 소스 자체의 결함을 분석하고 품질을 보증하는 수단으로 사용된다.

'The Economics of Software Quality'에 따르면 소스코드 정적 분석은 결함을 예방하는 65가지의 다양한 방법 중 7위에 랭크 되었다.

(Reductions in defects per function point for 1,000 function points)			
Defect Prevention Methods (In Order of Effectiveness)	Defect Prevention Efficiency	Defects Potentials without Prevention	Defect Potentials with Prevention
1 Reuse (certified sources)	85.00%	5.00	0.75
2 Inspections (formal)	60.00%	5.00	2.00
3 Quality Function Deployment (QFD)	57.50%	5.00	2.13
4 Prototyping –functional	52.00%	5.00	2.40
5 Risk analysis (automated)	48.00%	5.00	2.60
6 PSP/TSP	44.00%	5.00	2.80
7 Static analysis of source code	44.00%	5.00	2.80
8 Root cause analysis	41.00%	5.00	2.95
9 Quality in all status reports	40.00%	5.00	3.00
10 Joint Application Design (JAD)	40.00%	5.00	3.00

표 4 Effectiveness of Software Defect Prevention Methods

정적 분석 기법을 사용하면 알려진 결함에 대한 검출 효율이 44% 나 된다고 한다. 37%의 검출 효율을 갖는 Test-driven development 와 CMMI5 를 획득할 정도의 프로세스를 갖는 경우의 검출 효율인 21% 보다 상대적으로 많은 결함을 예방할 수 있다는 사실을 알 수 있다. 또한, 정적 분석은 매우 다양하게 활용될 수 있습니다.

예를 들면, 소스코드 내의 오타를 찾아주는 것도 정적 분석이고, 미리 버그라고 알려진 코드 패턴을 검사하는 것도 정적 분석이다. 또한, 런타임 에러가 발생하면 치명적인 문제들을 발견하거나, 개발 시에 미리 정해진 코딩 가이드라인을 잘 따르고 있는지 검사하는 것도 정적 분석의 예라고 할 수 있다. 정적 분석은 그 범위가 매우 다양하기 때문에 이것들 중에 가장 빠르고 도입하기 쉬운 것을 먼저 선별하여 도입하는데, 대부분의 경우 코딩 가이드라인 검사를 선호한다.

코딩 가이드라인이란 코드에 안정성과 통일성을 주기 위해 정해진 규칙이다. 소프트웨어는 여러 개발자들이 동시에 개발할 수 있다.. 하지만 사람마다 성격이 다르듯이 개발자들의 코딩 방식도 각양각색이다. 이런 경우 좋은 코딩 가이드라인을 따른다면, 소스 코드 품질을 일정 수준 이상으로 올릴 수 있고 코드의 가독성을 높여 유지보수에 도움이 된다. 또한, 개발자의 작은 결함이 대형 사고가 되지 않도록 조기에 차단할 수 있다.

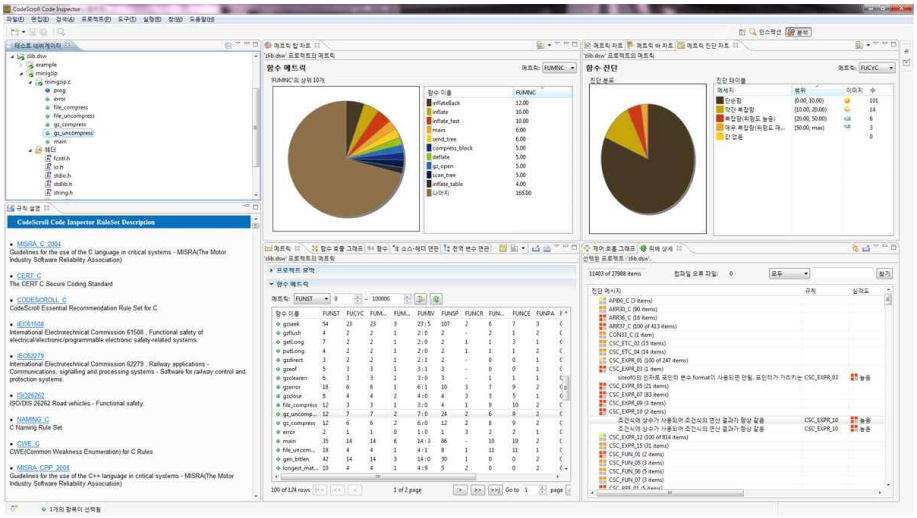


그림 16 정적분석 도구 Code Inspector

4.2 MISRA-C rule

MISRA-C는 MISRA(Motor Industry Software Reliability Association)에서 개발된 C 프로그래밍에 대한 개발 표준이다. "MISRA-C"의 목적은 ISO C 언어로 작성된 임베디드 시스템의 코드 안전성, 호환성, 신뢰성이다. C++언어에 대한 가이드라인으로는 MISRA C++가 존재한다.

"MISRA-C"는 자동차 산업으로부터 작성된 모델이지만 1998년 시행된 이래로, MISRA C에 대한 이해와 사용은 저자들의 원래 예상을 훨씬 뛰어넘었다. 위에서도 밝혔듯이, MISRA C는 원래 1994 MISRA 가이드라인의 언어 요건을 지원하기 위해 개발되었다. 그러나 이후 MISRA C는 철도, 우주항공, 군, 의료 부문 등 다양한 산업 및 응용분야에서 채택, 사용되고있다. 나아가 상당한 수의 MISRA C 규정을 이행할 것을 권장하는 툴을 사용할 수 있게 되었다.

MISRA Guideline Compliance Summary

Guidelines: **MISRA C 2012**

Checking tool: **PVS-Studio**

Result: **Not compliant**

Summary: There were violations of 5 mandatory guidelines, 29 required guidelines, 13 advisory guidelines. There were deviations of 1 required guideline, 1 advisory guideline.

Guideline	Category	Recategorication	Compliance
Rule 14.1	Required		Violations (14)
Rule 14.2	Required		Not Supported
Rule 14.3	Required		Compliant
Rule 14.4	Required		Compliant
Rule 15.1	Advisory		Violations (462)
Rule 15.2	Required		Violations (94)
Rule 15.3	Required	Mandatory	Violations (6)
Rule 15.4	Advisory		Violations (127)
Rule 15.5	Advisory		Violations (2647)
Rule 15.6	Required		Deviations (52)
Rule 15.7	Required		Violations (669)
Rule 16.1	Required		Not Supported
Rule 16.2	Required		Compliant
Rule 16.3	Required		Violations (175)
Rule 16.4	Required	Mandatory	Violations (178)
Rule 16.5	Required		Violations (4)
Rule 16.6	Required		Violations (13)
Rule 16.7	Required		Compliant
Rule 17.1	Required		Not Supported
Rule 17.2	Required		Violations (65)
Rule 17.3	Mandatory		Violations (2)
Rule 17.4	Mandatory		Violations (1)
Rule 17.5	Advisory	Required	Compliant
Rule 17.6	Mandatory		Compliant

그림 18 MISRA C 2012 Summary

4.3 테스트 주도 개발

IEC 62619의 배터리 관리 시스템 기능안전성 고려 사항은 기능안전 관련 표준인 IEC 61508과 IEC 60730 Annex H를 참고하고 있다. IEC 61508은 안전 시스템에 대한 요구사항 명세, 설계, 개발, 설치, 운영, 유지보수의 표준으로 원전, 항공, 의료, 철도, 장치산업 등에서 활용되는 디지털 제어 시스템의 안전을 위해 IEC 61508을 근간으로 기능 안전성 (Functional Safety) 검증을 요구하고 있다.

		Safety Integrity Level			
		SIL1	SIL2	SIL3	SIL4
1	Boundary value analysis	R	HR	HR	HR
2	Error guessing	R	R	R	R
3	Error seeding	-	R	R	R
4	Performance modeling	R	R	R	R
5	Equivalence classes and input partition testing	R	R	R	R
6	Structure-based testing	R	R	HR	HR

표 4 IEC 61508에서의 Dynamic Analysis and Testing 요건

표4는 IEC 61508에서 요구하는 테스트 방법을 타나내고 있는데, 여기서 R(Recommended)과 HR(Highly Recommended)은 필수적으로 수행해야 하는 요건을 의미한다. 표4에서 보는 것과 같이 IEC 61508 에서는 테스트 결과가 만족해야할 문장 (Statement) 커버리지나 결정(Decision) 커버리지와 같은 구체적인 구조적 커버리지 기준을 정하지는 않고 있다.
즉, IEC 61508은 특정 IT융합 제품 영역을 대상으로 하지 않고 있기 때문에, 각 테스트 단계에 대한 수행 결과의 Pass/Fail 기준을 테스트 계획수립 시 적절하게 설정하고 수행할 것을 요구하는 등 기법적인 준수 보다는 절차적인 준수 위주로 제시하고 있다.

		Application by SW Level			
		A	B	C	D
1	MC/DC Coverage	●			
2	Decision Coverage	●	●		
3	Statement Coverage	●	●	○	
4	Data Coupling and Control Coupling Coverage	●	●	○	

표 5 DO-178B에서의 Verification of Verification Process Results 요건

RTCA/DO-178B는 유럽연합과 미국에서 산업항공분야에 사용되는 소프트웨어에 대한 인증을

얻기 위해 사용되는 표준으로, 항공시스템에서 가져야 할 두 가지 주요한 목적 (소프트웨어의 항공운항 시스템과 장비들은 서로 호환되어야 하고, 내부 기능들이 안전하게 수행될 수 있도록 소프트웨어가 가져야 하는 지침을 제공해야 함)이기술되어 있다.
DO-178B의 안전 무결성 등급은 A~D로 나누어지며 A가 제일 높은 등급이다. <표 3>은 DO-178B에서 요구하는 코드 커버리지 요건으로, ○와 ●는 모두 커버리지가 달성되어야 함을 의미한다. 단, ●는 테스트 자체가 독립적으로 수행되어야 한다.
DO-178B에서는 IEC 61508과는 달리 안전 무결성 등급에 따라 달성되어야 하는 구조적 커버리지 기준을 제시하고 있기는 하지만, 해당 커버리지가 어떤 특정 테스트 단계(단위/통합/시스템)의 수행 결과로 만족해야 함을 요구하지는 않고 있다. 즉, 최고 안전 무결성 등급의 제품 개발 시 단위 테스트 단계에 MC/DC 커버리지를 만족하지 않아도 된다는 것을 의미한다.

ISO 26262는 자동차에 탑재되는 SW의 오류로 인한 사고를 미연에 방지하기 위해 제정한 기능안전 표준으로, IEC 61508이 일반 전기전자 장치의 안전에 관한 포괄적 표준이라는 한계를 보완하기 위해 만들어졌다. ISO26262에서는 재난상황 노출 가능성 (probability of exposure), 잠재적 심각도 (potential severity),그리고 통제 가능성 (controllability)을 고려하여 차량 안전 무결성 등급인 ASIL(Automotive SIL)을 결정한다. 이것은 자동차 제품의 특성을 반영한 것으로 ASIL은 최저 등급인 A부터 최고 등급인 D까지 4개 등급으로 구성되어 있다. BMW, GM, 보쉬, 현대자동차 등의 글로벌 자동차 메이커 및 부품 공급업체들은 ISO 26262를 자체 개발 프로세스 내에 적용하고 있다.

		Application by SW Level			
		A	B	C	D
1a	Statement Coverage	++	++	+	+
1b	Branch Coverage	+	++	++	++
1c	MC/DC (Modified Condition/ Decision) Coverage	+	+	+	++

표 6 ISO 26262에서의 Metrics for structural coverage at software unit testing 요건

표6은 ISO 26262의 소프트웨어 단위 테스트에 대한 결과 검증을 위해 사용되는 코드 커버리지 기준에 대한 요건을 나타낸다. +와 ++는 각각 IEC 61508의 R과 HR에 해당한다.
ISO 26262는 DO-178B보다 더 엄격해서 특정테스트 단계에서 달성해야 할 구조적 커버리지 요건을 제시하고 있다. 즉, 코드 기반의 단위 테스트는 물론, 모델 기반의 개발일 경우에도 모델에 유사한 구조적 커버리지 기준을 적용해야 하며, 통합 테스트 단계에서도 함수 (Function) 커버리지와 같은 구조적 커버리지를 적용한 결과를 요구하고 있다.

Test Report(Merge)

Project: zlib
Create Date : 2021-12-24 14:56:21
Controller Tester Version : 3.5

Total Coverage

Statement	Branch	Call	MC/DC	Function
41.81 %(1,670/3,994)	27.75 %(587/2,115)	43.85 %(164/374)	18.35 %(230/1,253)	100.00 %(114/114)

Unit Test

Total test	Succeed test	Total test case	Succeed test case
	Host/Target	Host/Target	Host/Target
114	67/0	938/0	657/0

Unit Test Summary

Test	Total test case	Success	Failure	Error	Statement	Branch	Call	MC/DC
	Host/Target	Host/Target	Host/Target	Host/Target				
_tr_align(struct internal_state *)_0	13/0	1/0	0/0	12/0	0.92 %(37/3994)	0.47 %(10/2115)	0.53 %(2/374)	0.23 %(3/1253)
_tr_flush_block(struct internal_state *, char *, unsigned	12/0	0/0	0/0	12/0	1.35 %(54/3994)	0.89 %(19/2115)	1.87 %(7/374)	0.55 %(7/1253)
_tr_init(struct internal_state *)_0	1/0	1/0	0/0	0/0	0.67 %(27/3994)	0.28 %(6/2115)	0.53 %(2/374)	0.23 %(3/1253)
_tr_stored_block(struct internal_state *, char *, unsigne	8/0	0/0	0/0	8/0	0.57 %(23/3994)	0.28 %(6/2115)	0.53 %(2/374)	0.15 %(2/1253)
_tr_tally(struct internal_state *, unsigned int, unsigned i	3/0	0/0	0/0	3/0	0.05 %(2/3994)	0.00 %(0/2115)	0.00 %(0/374)	0.00 %(0/1253)
adler32(unsigned long, const unsigned char *, unsigned	13/0	9/0	0/0	4/0	2.47 %(99/3994)	0.94 %(20/2115)	0.00 %(0/374)	0.63 %(8/1253)
adler32_combine(unsigned long, unsigned long, signed	11/0	11/0	0/0	0/0	0.45 %(18/3994)	0.37 %(8/2115)	0.00 %(0/374)	0.31 %(4/1253)
bi_flush(struct internal_state *)_0	11/0	5/0	0/0	6/0	0.22 %(9/3994)	0.18 %(4/2115)	0.00 %(0/374)	0.15 %(2/1253)
bi_reverse(unsigned int, signed int)_0	5/0	3/0	0/0	2/0	0.12 %(5/3994)	0.09 %(2/2115)	0.00 %(0/374)	0.07 %(1/1253)
bi_windup(struct internal_state *)_0	8/0	3/0	0/0	5/0	0.17 %(7/3994)	0.18 %(4/2115)	0.00 %(0/374)	0.15 %(2/1253)
build_bl_tree(struct internal_state *)_0	8/0	0/0	0/0	8/0	1.00 %(40/3994)	0.66 %(14/2115)	0.80 %(3/374)	0.55 %(7/1253)
build_tree(struct internal_state *, struct tree_desc_s *)_	7/0	0/0	0/0	7/0	2.00 %(80/3994)	1.08 %(23/2115)	1.33 %(5/374)	0.63 %(8/1253)
check_header(struct gz_stream *)_0	23/0	21/0	0/0	2/0	0.50 %(20/3994)	0.33 %(7/2115)	0.53 %(2/374)	0.15 %(2/1253)
compress(unsigned char *, unsigned long *, const unsig	3/0	3/0	0/0	0/0	10.41 %(416/3994)	6.80 %(144/2115)	14.17 %(53/374)	2.39 %(30/1253)
compress2(unsigned char *, unsigned long *, const uns	6/0	6/0	0/0	0/0	4.85 %(194/3994)	3.07 %(65/2115)	7.75 %(29/374)	1.03 %(13/1253)
compressBound(unsigned long)_0	3/0	3/0	0/0	0/0	0.02 %(1/3994)	0.00 %(0/2115)	0.00 %(0/374)	0.00 %(0/1253)
compress_block(struct internal_state *, struct ct_data_	8/0	1/0	0/0	7/0	0.60 %(24/3994)	0.28 %(6/2115)	0.00 %(0/374)	0.15 %(2/1253)
copy_block(struct internal_state *, char *, unsigned int,	5/0	0/0	0/0	5/0	0.32 %(13/3994)	0.23 %(5/2115)	0.26 %(1/374)	0.07 %(1/1253)
crc32(unsigned long, const unsigned char *, unsigned in	7/0	6/0	0/0	1/0	1.05 %(42/3994)	0.61 %(13/2115)	0.26 %(1/374)	0.47 %(6/1253)
crc32_big(unsigned long, const unsigned char *, unsign	10/0	9/0	0/0	1/0	0.95 %(38/3994)	0.47 %(10/2115)	0.00 %(0/374)	0.47 %(6/1253)
crc32_combine(unsigned long, unsigned long, signed lo	9/0	7/0	0/0	2/0	1.02 %(41/3994)	0.85 %(18/2115)	1.87 %(7/374)	0.71 %(9/1253)
crc32_little(unsigned long, const unsigned char *, unsig	10/0	9/0	0/0	1/0	0.90 %(36/3994)	0.47 %(10/2115)	0.00 %(0/374)	0.47 %(6/1253)
deflate(struct z_stream_s *, signed int)_0	32/0	27/0	0/0	5/0	2.72 %(109/3994)	1.98 %(42/2115)	2.67 %(10/374)	0.71 %(9/1253)
deflateBound(struct z_stream_s *, unsigned long)_0	6/0	6/0	0/0	0/0	0.17 %(7/3994)	0.09 %(2/2115)	0.00 %(0/374)	0.00 %(0/1253)
deflateCopy(struct z_stream_s *, struct z_stream_s *)_	3/0	0/0	0/0	3/0	0.17 %(7/3994)	0.04 %(1/2115)	0.53 %(2/374)	0.00 %(0/1253)
deflateEnd(struct z_stream_s *)_0	26/0	19/0	0/0	7/0	0.17 %(7/3994)	0.18 %(4/2115)	0.26 %(1/374)	0.55 %(7/1253)
deflateInit2_(struct z_stream_s *, signed int, signed int,	20/0	20/0	0/0	0/0	0.15 %(6/3994)	0.04 %(1/2115)	0.00 %(0/374)	0.00 %(0/1253)
deflateInit_(struct z_stream_s *, signed int, const char *	5/0	5/0	0/0	0/0	0.17 %(7/3994)	0.04 %(1/2115)	0.26 %(1/374)	0.00 %(0/1253)
deflateParams(struct z_stream_s *, signed int, signed i	12/0	12/0	0/0	0/0	0.65 %(26/3994)	0.47 %(10/2115)	0.26 %(1/374)	0.47 %(6/1253)
deflatePrime(struct z_stream_s *, signed int, signed int	5/0	5/0	0/0	0/0	0.10 %(4/3994)	0.04 %(1/2115)	0.00 %(0/374)	0.00 %(0/1253)
deflateReset(struct z_stream_s *)_0	5/0	5/0	0/0	0/0	0.07 %(3/3994)	0.04 %(1/2115)	0.00 %(0/374)	0.00 %(0/1253)
deflateSetDictionary(struct z_stream_s *, const unsigne	14/0	9/0	0/0	5/0	2.20 %(88/3994)	1.37 %(29/2115)	0.53 %(2/374)	1.03 %(13/1253)

그림 19 CONTROLLER TESTER 단위/동합 테스트 도구

그림19는 CONTROLLER TESTER를 이용한 단위/통합 테스트의 결과이다. 자동차, 국방에서는 실제 타깃 환경에서 테스트를 통해 구조적인 커버리지 목표를 달성해야한다. 유닛 테스트를 통해 문장, 분기, 함수, 함수 호출 커버리지 및 MC/DC 측정이 가능하다. 자동차, 국방, 철도, 원자력 금융, 통신 산업 분야별 도메인에서 요구하는 MC/DC 목표 달성을 요구하며 소프트웨어 품질을 향상 시킬 수 있으며 고객의 신뢰를 확보 할 수 있다.

에너지저장장치의 BMS시스템에서도 SW Code의 만족해야할 문장 (Statement) 커버리지나 결정(Decision) 커버리지와 같은 구체적인 구조적 커버리지 기준을 타 산업분야 만큼 강화하여 테스트할 때 무너진 신뢰감을 되찾을 수 있으리라 기대한다.

5. 결론

정부는 기후위기 속에서 탄소발생을 줄이고 단계적으로 원전과 석탄발전 가동을 중단하고 2030년까지 전체 발전량의 20%를 신재생에너지로 공급하는것을 목표로 하고있다.

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.
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.

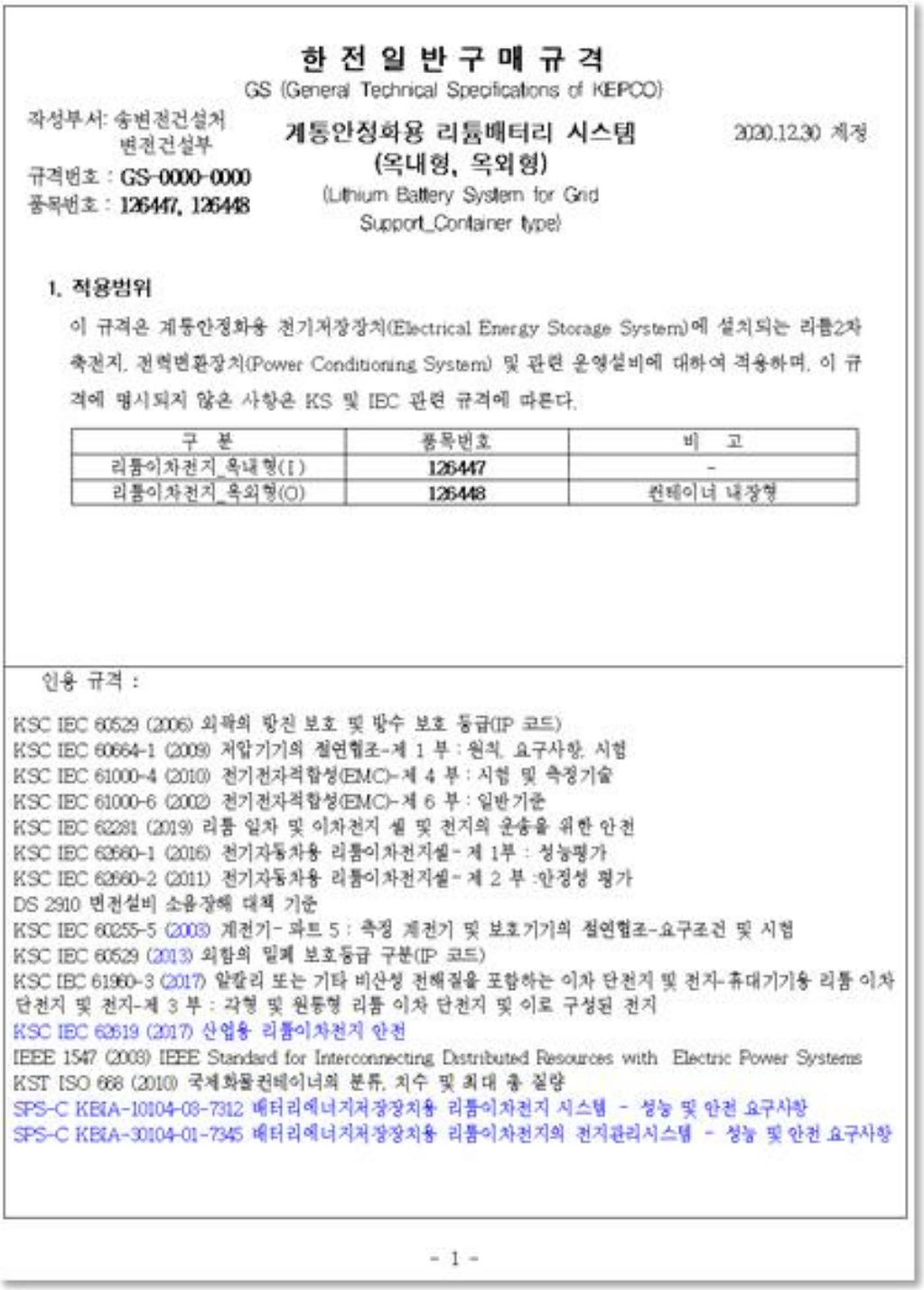
선사시대 두려움에 떨던 불도 이젠 인류는 이롭게 쓰고 있다. 아니 없어서는 안되는 요소이다.
에너지저장장치 또한 마찬가지라고 생각된다. 불이나 칼처럼 나쁘게만 쓰면 안좋은 것들일수도 있지만 좋게 칼로 요리를 하고 불로 따뜻하게 난방을 하는 우리 일상에 없어서는 안될 존재들이다.

단순히 가져다쓰는 전기가 아닌 효율적으로 쓰는 전기가 되야 될것이다.
장난감에 갈아끼는 건전지 정도로만 생각해서는 안되고, 더 세밀히 물성을 파악하고 안전 기준을 강화해야 할 것이다.

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.

우버(Uber)의 자율주행차량(2017년형 볼보 XC90 개조)이 자전거를 끌고 길을 건너던 40대 여성을 치어 사망케 했던 사고가 있었다. 그리고 테슬라의 모델X 차량이 자율주행 중 고속도로 충격흡수장치를 들이받고 연이은 추돌사고로 운전자가 사망한 사고 사례도 있었다. 자율주행을 위해 첨단운전지원시스템(ADAS)은 카메라,레이더,라이더(LIDAR)등의 추가적인 부품 및 관련 기술이 사용되며 이는 시스템의 복잡도(complexity)를 필연적으로 상승시키며 주행중인 차량이 다른 차량의 운행정보 도로,시설물과 네트워크 통신을 이용하여 정보를 공유하기 때문에 SW는 더욱더 안전설계가 요구되고 있다.

이처럼 현대 사회에서는 모든 분야에서 제품과 서비스 구조가 복잡해지고 기능이 많아짐에 따라 시스템이 오작동하거나 오류로 인한 사고가 발생하고 있다. 시속 300Km/h이상으로 달리는 고속열차에서 안전밸트를 메지 않아도 우리는 안절밸트를 메고 자동차를 타고 고속도로를 지날때보다 더 안전하다고 느낄수 있다. 사고 발생 후 신속한 원인 분석으로 위험(Risk)요소를 제거하고 피해의 가능성(Probability)과 심각성(Severity)을 낮추는 활동을 할때 시스템에 대한 신뢰도는 높아지리라 믿는다.



한 전 일 반 구 매 규 격

GS (General Technical Specifications of KEPCO)

작성부서: 송변전건설처
변전건설부

규격번호 : GS-0000-0000
품목번호 : 126447, 126448

계통안정화용 리튬배터리 시스템 (옥내형, 옥외형)

(Lithium Battery System for Grid Support_Container type)

2020.12.30 제정

1. 적용범위

이 규격은 계통안정화용 전기저장장치(Electrical Energy Storage System)에 설치되는 리튬2차 축전지, 전력변환장치(Power Conditioning System) 및 관련 운영설비에 대하여 적용하며, 이 규격에 명시되지 않은 사항은 KS 및 IEC 관련 규격에 따른다.

구 분	품목번호	비 고
리튬이차전지_옥내형(I)	126447	-
리튬이차전지_옥외형(O)	126448	컨테이너 내장형

인용 규격 :

KSC IEC 60529 (2006) 외곽의 방진 보호 및 방수 보호 등급(IP 코드)
KSC IEC 60664-1 (2009) 저압기기의 절연협조-제 1 부 : 원칙, 요구사항, 시험
KSC IEC 61000-4 (2010) 전기전자적합성(EMC)-제 4 부 : 시험 및 측정기술
KSC IEC 61000-6 (2002) 전기전자적합성(EMC)-제 6 부 : 일반기준
KSC IEC 62281 (2019) 리튬 일차 및 이차전지 셀 및 전지의 운송을 위한 안전
KSC IEC 62660-1 (2016) 전기자동차용 리튬이차전지셀- 제 1부 : 성능평가
KSC IEC 62660-2 (2011) 전기자동차용 리튬이차전지셀- 제 2 부 :안정성 평가
DS 2910 변전설비 소음장해 대책 기준
KSC IEC 60255-5 (2003) 계전기- 파트 5 : 측정 계전기 및 보호기기의 절연협조-요구조건 및 시험
KSC IEC 60529 (2013) 외함의 밀폐 보호등급 구분(IP 코드)
KSC IEC 61960-3 (2017) 알칼리 또는 기타 비산성 전해질을 포함하는 이차 단전지 및 전지-휴대기기용 리튬 이차 단전지 및 전지-제 3 부 : 각형 및 원통형 리튬 이차 단전지 및 이로 구성된 전지
KSC IEC 62619 (2017) 산업용 리튬이차전지 안전
IEEE 1547 (2003) IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems
KST ISO 668 (2010) 국제화물컨테이너의 분류, 치수 및 최대 총 질량
SPS-C KEIA-10104-03-7312 배터리에너지저장장치용 리튬이차전지 시스템 - 성능 및 안전 요구사항
SPS-C KEIA-30104-01-7345 배터리에너지저장장치용 리튬이차전지의 전지관리시스템 - 성능 및 안전 요구사항

- 1 -

그림 17 한전 에너지저장장치 시방서

한국전력의 일반구매규격 시방서에서는 인용규격을 명시하고 있다.

< 자료 출처 >

전기에너지 저장 시스템 국제 표준화 동향, ETRI 정상진

SW안전 국제표준화 동향과 시사점, 정도균(SW공학팀 ICT생태계본부) 정보통신산업진흥원

“원자력 안전의 소프트웨어를 바꾸다”, 원자력신문
(http://www.knpnews.com/news/articleView.html?idxno=10888)

티유브이슈드코리아(TUV SUD Korea) BLOG 기능안전이란
(https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=tuv-sud&logNo=220603281295)

MISRA C (misra.or.kr)

SW 오류, 대형 사고 원인 될 수 있다, 사이언스타임즈
(https://www.sciencetimes.co.kr/news/sw-%EC%98%A4%EB%A5%98-%EB%8C%80%ED%98%95-%EC%82%AC%EA%B3%A0-%EC%9B%90%EC%9D%B8-%EB%90%A0-%EC%88%98-%EC%9E%88%EB%8B%A4/)