SW 안전 적용사례 10








과학기술정보통신부 Ministry of Science and ICT
nipa 정보통신산업진흥원 National IT Industry Promotion Agency

SW 안전
적용사례
10

CONTENTS

01 SW 안전 적용사례

02 SW 안전 기술의 이해

LG전자

다른 제품의 안전성 보장하는 검증된 테스트 자동화 솔루션

LG전자 TestPresso IEC 61508.ISO 26262 검증 가능 도구로 각광 배터리/팩 등에 적용해 검증률 제고 및 검증시간 단축 효과 톡톡

▲ 'LG전자' CTO 부분 선행R&BD 이상용 센터장

LG전자 기본 정보

회사명	LG전자 주식회사	전화번호	02-3777-1114
대표자명	권봉석	홈페이지	https://www.lge.co.kr/
설립연도	1958	종사자	39,745명
주소	서울시 영등포구 여의대로 128 LG트윈타워		
주요제품	TV · AV, PC, 주방가전, 생활가전, 에어컨 · 에어케어, 뷰티/액세서리		

LG TestPresso

TestPresso는 LG가 자체 개발한 테스트 자동화 SW 솔루션으로 2004년 모바일 핸드폰(일명 피처폰)을 시작으로 지난 15년간 스마트폰, 자동차, 가전, 홈엔터테인먼트, 웹 애플리케이션, 사물인터넷(IoT) 등 다양한 LG 제품군에 적용되어 왔다. 기능성은 물론 신뢰성이나 안정성과 같은 비기능성 특성에 대해서 안정적이고 효율적인 동적 테스트를 수행하는 것이 장점이다. TestPresso의 적용 범위는 이제 LG 계열사를 넘어 다른 기업의 다양한 제품군으로 확대되고 있으며, 최근에는 디지털 전환 제품인 클라우드, AI, 로봇, 가상화 기술, 융복합 제품 등에도 적용되고 있다. 심지어 디지털 산불 사전 예방에도 기여하고 있다. 특히 TestPresso는 글로벌 인증기관인 독일의 TUV SUD로부터 전기·전자 시스템 기능안전 국제표준 'IEC 61508'와 자동차 기능안전 국제표준 'ISO 26262'을 검증할 수 있는 도구로 인증받음으로써 검증 솔루션으로서의 안전성을 확보했다.

TestPresso는 최근 AI/머신러닝(ML) 기반 이미지 처리 기술을 적용해 화면 객체들을 인식하고 자동으로 테스트 스크립트를 생성하는 기능을 추가 제공하게 되었으며 스마트 TV, 사이니지, 자동차 IVI 적용을 통해 우수성을 입증했다. 또한 데이터 수집 및 빅데이터 분석 기술을 기반으로 제품 품질 취약점, 고객 만족도, 시장 상황 등을 파악하여 제품이 앞으로 나아갈 방향을 제시하는 제품 품질분석 서비스도 제공한다.

아울러 테스트 환경의 빠른 변화에 대응할 수 있는 클라우드 기반 테스트 통합 관리 도구를 제공해 사용자들이 원격 검증 시스템 구축, 품질 데이터 수집/분석, 사용자 맞춤형 리포트 시스템 등을 쉽게 이용할 수 있도록 지원하고 있다. 특히 코어와 애플리케이션(플러그인)으로 분리되어 있는 아키텍처를 설계하여 플러그인 개발만으로 다양한 타 환경에 쉽게 적용할 수 있고 안전하게 확장할 수 있다.

배터리

적용 표준	적용 안전 기법(Techniq & Measure)
ISO26262 IEC61508	• 글로벌 SW 기능안전 표준을 준수한 테스트 자동화 자체 솔루션 개발 • ISO26262/IEC61508 규격에 맞는 7단계 체계적인 인증 프로세스 적용 • ISO26262 규격 및 IEC61508 규격에 맞는 2개 제품 적용 사례 제시

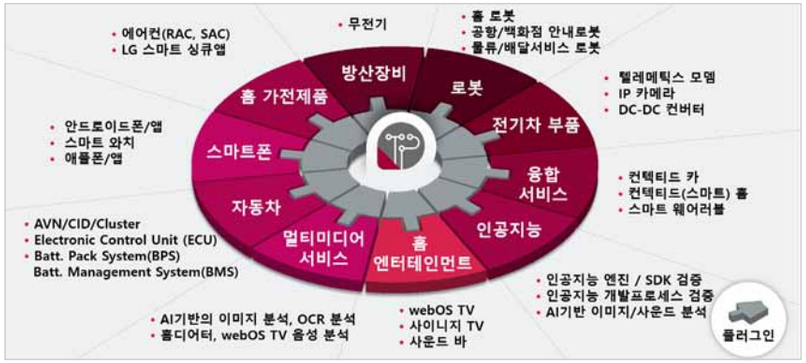
다른 제품 안전성을 검증하려면 가능안전 인증 필수

최근 글로벌 산업 전반에 걸친 제품 기술 고도화와 부품 미세화로 복잡성이 증가하면서 제품의 안전성(Safety)이 더욱 중요해지고 있다. 각국의 기업과 기관들이 법제화 및 인증 제도를 통해 제품 안전성을 확보하고자 하는 노력도 치열해지고 있다.

이러한 글로벌 흐름에 맞춰 TestPresso는 여러 분야의 제품 안전성 검증을 수행해왔다. 이 중에서 제품 및 부품에 대한 안전성이 가장 중요시되고 있는 분야는 자동차 산업이다. 자동차 부품의 결함으로 인한 사고가 발생하거나 사람의 생명을 위협할 경우 제조사의 브랜드 이미지와 신뢰도는 큰 타격을 입게 된다. 이에 따라 제조사는 자동차 기능안전 표준인 ISO26262를 개발 초기, 생산, 폐기 등 자동차 라이프사이클 전반에 걸쳐 적용하고 있으며 OEM 부품 업체에도 ISO 26262 인증을 요구하고 있다.

ISO 26262 인증은 시스템, 하드웨어, SW 레벨에 걸쳐 기능 안전을 관리하고 제품 개발에 관여하며, 자동차 안전 수명 주기에 따른 위험 유형을 결정하는 위험 기반 접근법과 허용 가능한 잔류 위험도를 위한 안전 요구사항, 안전성을 보장하기 위한 검증 및 확인 조치에 대한 요구사항 등을 제공한다. ISO 26262 인증을 통해 자동차에 사용되는 전기/전자 장치 부품에 대해 높은 수준의 안전성을 보장함으로써 사전에 부품에 대한 문제를 방지하여 자동차 사고를 예방할 수 있게 된다.

TestPresso는 전기/전자 장치 부품을 단일 및 통합 테스트하는 만큼 TestPresso 자체에 대한 신뢰성 및 안전성이 중요하다. 제조사에 납품하는 부품 자체에 대한 안전성 및 신뢰성뿐 아니라, 해당 부품을 테스트하는 SW 솔루션인 TestPresso에 대해서도 ISO26262 인증을 획득함으로써 제조사에 납품하는 부품에 대한 신뢰성 및 안전성을 한층 제고할 수 있다.



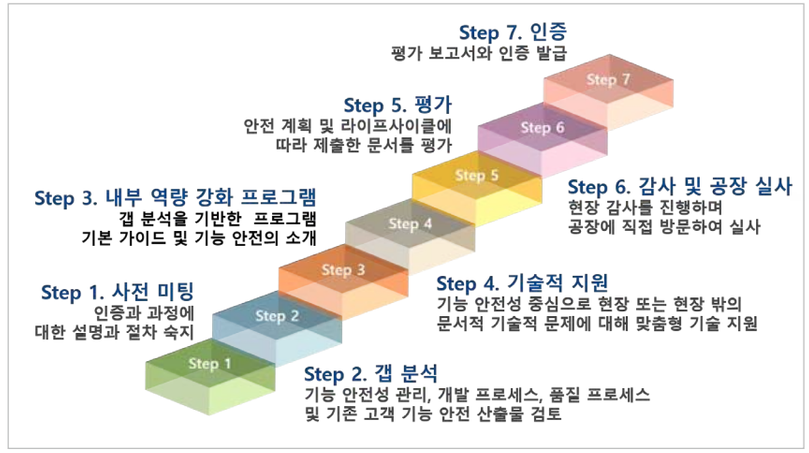
▲ LG TestPresso 다양한 분야 적용사례

갭분석 등 7단계 과정 거쳐 인증 취득

인증 과정은 총 7단계로 사전 미팅, 갭 분석, 내부 역량 강화 프로그램, 기술적 지원, 평가, 감사 및 공장 실사, 인증 발급의 순서로 진행되었다. 첫 단계인 사전 미팅에서는 인증 과정에 대한 설명을 듣고 절차를 숙지하는 내용이 진행됐다.

두 번째 갭 분석 단계에서는 ISO26262/IEC61508 규격에서 요구하는 수준과 TestPresso 수준과의 차이를 분석해 갭 분석 보고서를 작성하였다. 세 번째로 내부 역량 향상 프로그램 단계에서는 갭 분석 보고서를 기반으로 내부 개발 인원 교육 프로그램을 설계하고 수행하여 구성원들의 안전기능에 대한 이해를 높였다.

네 번째인 기술적 지원 단계에서는 개발팀에서 작성한 산출물들의 문서적/기술적 문제에 대해 한국지사(TUV SUD Korea)로부터 맞춤형 기술 지원을 받아 수정 보완함으로써 산출물들을 완성했다. 그 다음 평가 단계에서는 보완한 산출물들을 인증기관(TUV SUD 본사) 평가자(Assessor)의 피드백을 받은 후 TestPresso에 모두 반영하여 최종 완성했다. 여섯 번째 감사 및 공장검사(Audit/Factory Inspection)에서는 본사 평가자가 LG전자 현장에 직접 방문해 실사를 진행하였다. 마지막 인증(Certificate) 단계에서는 실사 단계 피드백을 반영하여 최종 검증을 거쳐 평가 보고서와 인증서를 발급받았다.

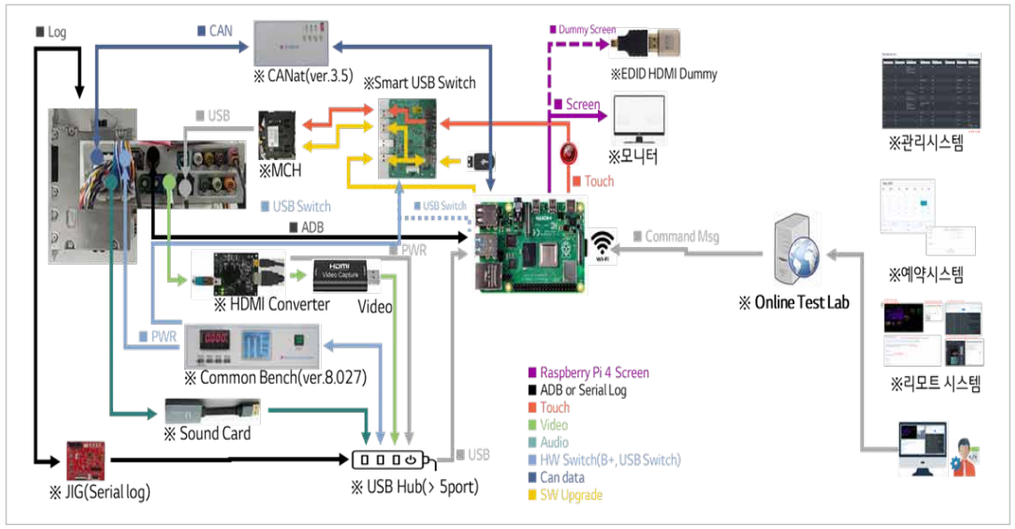


▲ LG전자 TestPresso의 안전 인증절차 및 과정

적용사례로 본 TestPresso 1. IVI(In-Vehicle Infotainment)

IVI는 각종 차량 정보를 입력받아 표시하고 제어하는 시스템으로 탑승자에게 주행에 필요한 정보와 즐길 거리를 동시에 서비스할 수 있는 차량 내 환경을 제공한다. 과거에는 계기판을 통해 속도와 연료 등의 기초 정보를 제공하고, 오디오나 미디어박스를 통해 극히 수동적이고 제한적인 엔터테인먼트(Entertainment)만 가능했다면 이제는 커넥티드 및 자율주행 등의 기술 등장으로 차량 자체가 하나의 이동 수단 겸 휴식공간, 업무공간으로 탈바꿈하는 SW/HW 통합 플랫폼으로 발전해나가고 있다. 이러한 기술 변화의 핵심엔 SW가 있으며 SW 비중의 증가와 함께 이들의 품질보증, 특히 안전성 품질 강화를 위한 다양한 연구와 개발이 필요하게 되었다.

이에 TestPresso를 도입하여 AUTOSAR(Automotive Open System Architecture) Classic Platform에 기초한 서비스 지향 인터페이스 및 로그파일 추적 기능을 적용하였고, 통합개발 검증 랩을 활용하여 개발자와 테스터들이 직접 검증 인프라를 구축하지 않고도 원격으로 기본기능, 신뢰성 검증, 안전성 검증을 수행할 수 있도록 하였다. 이를 통해 검증 시간과 비용을 절감하고 리소스 관리의 효율성을 개선하였으며 그 결과, 신뢰성 검증률 80%, 기능성 자동화율 60% 이상의 효과를 얻을 수 있었다.



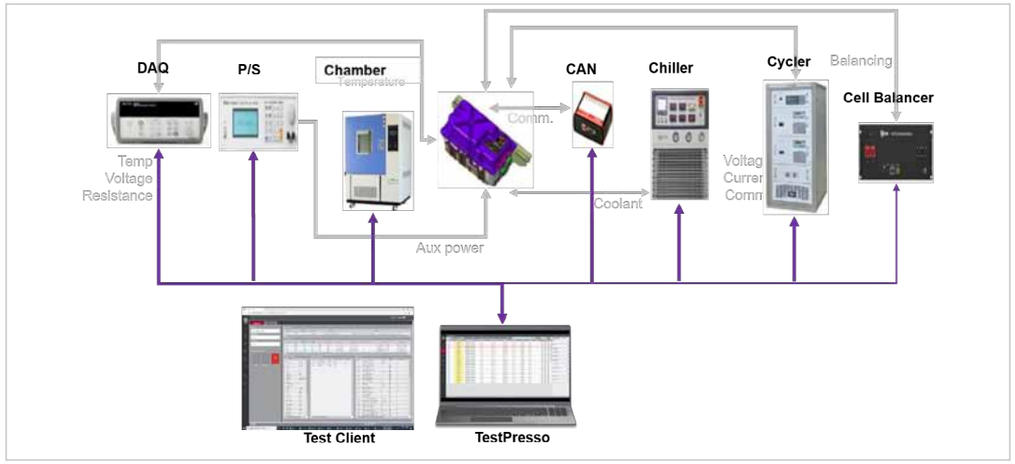
▲ 원격 검증 인프라 구축 사례

적용사례로 본 TestPresso 2. 배터리/팩 시스템

전기자동차의 핵심 부품인 BMS(Battery Management System)와 팩 시스템은 전기자동차나 하이브리드 전기자동차에 사용되는 이차전지의 전류, 전압, 온도 등 여러 요소들을 센서를 이용해 측정하고 배터리의 충/방전 상태와 잔여량을 제어하는 시스템으로, 전기 자동차 내부의 제어시스템과 연동하여 전지가 최적의 환경에서 작동하게 한다.

기존의 HIL(Hardware-in-the-loop) 기반 반자동화 검증 환경이 고가인데다 자동차 OEM들의 품질 요구 사항이 날로 강화되면서 규모는 갈수록 커지고 복잡해지는 등 다양한 이슈 대응에 어려움을 겪는 상황이었다. 이에 새로운 대안으로 TestPresso 도입을 고려하게 되었고 적용을 통해 한계 상황을 돌파할 수 있었다.

TestPresso는 시험 수행을 자동화하여 수동 검증 수행 대비 모델 당 검증시험 시간을 82시간 단축했고, 사용자 GUI 클라이언트를 이용한 시험 제어 및 모니터링 기능을 제공하여 사용자 편의성을 강화했다. 특히 통합 로그 저장으로 실시간 그래프를 갱신하여 육안 또는 자동으로 시험 진행 사항을 확인하고 결과를 판정할 수 있도록 하였다. 또한 시험 안전성 강화를 위해 이상 작동(자동 방전 전환, 작업 멈춤, 온도 조절, 가동 중단 등)을 자동으로 감지하여 제어 조치하고 테스터나 관련자에게 이상 상태를 통보해 주는 기능을 제공하고 있다.



▲ 배터리/팩 시스템 적용 사례

핵심 산출물인 Safety Plan 작성과 준수 가장 중요

ISO26262 인증 심사는 주로 산출물 리뷰를 통해 이루어졌다. 개발 과정 산출물(SRS, SAD, STS 등)도 물론 평가 대상에 포함되었지만 가장 중요한 산출물은 Safety Plan 이었다. TestPresso 및 SW 공학적 도메인지식이 풍부한 Safety Leader(SL) 및 Safety Manager(SM)를 선정하여 인증 프로세스 관리 및 산출물을 철저하게 점검하는 것 역시 중요했다.

Safety Plan에는 안전한 제품을 개발하기 위해 필요한 모든 활동과 프로세스, 업무분장, 교육 계획 등이 포함된다. Safety Plan을 작성하고 부족한 부분을 보완할 계획을 세우는 것으로부터 인증이 시작되었는데 이것이 가장 중요한 과정이다. Safety Plan을 작성하는 것도 중요했지만 그에 못지 않게 Safety Plan에서 계획한 프로세스와 활동이 제대로 실행되는지 점검하는 활동도 매우 중요하게 평가되었다.

이에 모든 산출물에 대해 사소한 변경 이후에도 검증 리뷰(Verification Review)에 따라 심사하였고, 심사 결과는 별도의 검증 리포트에 기록하였다. 형상 관리가 제대로 이루어지고 있는지도 주기적으로 심사했으며 변경 요청 또한 별도의 위원회에서 변경이 안전에 미치는 영향을 면밀히 검토한 후 승인하였다. 제품 개발의 중간 혹은 마무리 단계에서는 Safety Plan에 명시된 모든 활동들에 대해 내부 심사를 통해 이를 점검하고 보완하는 활동이 수행됐다. Safety Plan의 작성과 준수는 가장 어려운 활동이었지만 안전 개발에 있어 가장 필수적이고 중요한 과정이기 때문에 인증 획득을 목적으로 하지 않더라도 안전개발을 위해서 Safety Plan을 구축하는 것이 바람직하다. 아래 그림은 TestPresso 과제에서 작성한 Safety Plan의 구성 항목을 보여준다. ALM(Application Lifecycle Management)에 따르는 모든 활동과 ISO26262 Part8에서 요구하는 Supporting Processes 관련 활동 등을 포함하였다.

▲ TestPresso Safety Plan 구성 항목

참여자 소감 및 향후 진행 방향

"TestPresso는 이미 만들어서 사용하고 있는 제품이었기 때문에 안전 관점에서 기존 프로세스를 개선하는 것이 쉽지 않았다. 그러나 개발팀의 적극적인 협력 하에 프로세스를 개선해 나가면서 큰 보람을 느낄 수 있었다. 앞으로 지속적인 모니터링을 통해 TestPresso가 계속해서 안전한 제품으로 발전해나갈 수 있도록 협력할 계획이다."

- 기능 안전 담당자(Safety Manager)

"인증 과정은 TestPresso를 어떻게 하면 안전한 제품으로 개발할 수 있을까에 대해 많은 고민과 실천을 해볼 수 있는 소중한 시간이었다. 안전 개발이 쉽지 않은 과정인 것은 분명하지만 LG 화학 등 안전이 필수적인 제품들에 TestPresso가 활용되는 만큼 힘들더라도 사명감을 가지고 안전 개발에 힘쓰도록 하겠다."

- 제품 개발 담당자(Project Manager)

LG전자 CTO(Chief Technology Officer; 최고기술책임자) 박일평 사장은 "TestPresso의 글로벌 규격 인증은 LG전자의 SW 경쟁력을 더욱 높이게 될 것"이라며 "LG전자의 차별화된 기술이 고객에게 실질적인 혜택으로 이어질 수 있도록 지속적으로 노력할 것"이라고 말했다.

HYUNDAI AutoEver

미래 자동차 기능안전, 효율성과 효과성 모두 잡았다

현대오토에버의 AUTOSAR 표준 기반 모빌진 SW 플랫폼 제조업체는 시간과 비용 절감, 소비자는 안전한 탑승

▲ '현대자동차그룹의 전문 ICT 기업' 현대오토에버 서정식 대표

현대오토에버 기본 정보

회사명	현대오토에버주식회사	전화번호	02-6296-6000
대표자명	서정식	홈페이지	https://www.hyundai-autoever.com/
설립연도	2000. 4. 10	종사자	4,585명
주소	서울 강남구 테헤란로 510		
주요제품	차량전장SW, 차량응용SW, 스마트IT서비스		

기술 발전으로 다양한 기능의 차량용 제어기가 개발되면서 이에 따른 차량용 소프트웨어의 종류 및 복잡성도 증가하고 있다. 이러한 복잡성 증가로 인해 개발 및 관리 효율의 필요성은 더욱 커졌고 이는 차량용 소프트웨어의 아키텍처 표준화 요구로 이어진다. 즉, 차량의 출시를 위해 다양한 협력 부품 업체로부터 공급받는 다수 제어기 간의 상호 연동성을 표준화함으로써 개발 효율성, 상호 호환성, 재사용성을 구현하는 소프트웨어 표준 플랫폼이 필요하게 된 것이다. 그 결과, 차량용 제어기 소프트웨어를 위한 아키텍처의 표준화를 통해 차량용 소프트웨어의 복잡성을 해결하는 AUTOSAR[1]가 2003년 출범하게 되었다.

AUTOSAR는 제어기 별로 서로 다른 소프트웨어 설계에 따른 개발 품질의 저하, 재사용성의 문제 등 기존 단점을 해결하기 위해 계층 아키텍처(Layered Architecture) 컨셉의 표준 플랫폼을 제공한다. 소프트웨어 계층(Software Layer)은 실제 소프트웨어가 동작하는 MCU(Micro Controller Unit) 상에서 Application(ASW), Runtime Environment(RTE), BasicSoftware(BSW)의 3개 계층으로 구성된다. BSW 계층은 자동차 내 전자제어기(ECU: Electronic Control Unit)에서 공통으로 사용하는 기능이 구현된 컴퓨터 운영체제 역할을 한다. ASW는 각 제조업체와 여러 공급업체들이 개발해야 할 실제 ECU가 동작하는 상세 기능이 구현된 응용 프로그램 계층이다. RTE는 BSW와 ASW 간 데이터 통신을 담당한다.

이러한 AUTOSAR의 계층적 구조는 소프트웨어의 하드웨어 종속적인 부분과 응용 소프트웨어 부분을 계층으로 분리 개발하도록 해준다. 장점은 명확하다. 응용 소프트웨어 개발을 수행하는 완성차 업체(OEM)나 공급업체가 하드웨어 구조에 독립적인 소프트웨어를 설계할 수 있게 돼 재사용성을 크게 높일 수 있다. 또한 응용 소프트웨어 개발자가 하드웨어 없이 소프트웨어를 설계할 수 있으며 기본 소프트웨어 개발도 동시에 진행할 수 있는 장점이 있다.

1) AUTOSAR(AUTomotive Open System Architecture) : 주요 OEM 및 Tier1이 모인 AUTOSAR 컨소시엄이 SW 재사용성 및 시스템의 유연성을 높이기 위해 수립한 표준화된 개방형 자동차 SW 아키텍처

	적용 표준	적용 안전 기법(Techniq & Measure)
자동차	ISO26262	• SEooC 기반의 기능안전 컨셉 도출 및 SW 안전 요구사항 개발 • AUTOSAR 표준 아키텍처 기반의 안전 분석(FMEA, DFA) 수행 • ASPICE 기반의 소프트웨어 프로세스 수립 및 기본 품질 관리 체계 구축

AUTOSAR 표준 기반의 모빌진 클래식 R4.4 SW 플랫폼

현대차그룹의 표준 플랫폼을 담당해 온 현대오토에버는 AUTOSAR 표준 사양에 기반한 표준 플랫폼 개발을 수행하고 있다. 2016년 그랜저에 전자 아키텍처를 적용한 것을 시작으로 현대차 표준 SW 플랫폼의 내재화 및 양산을 수행하고 전장 분야의 공통 기능에 대해 표준 인터페이스를 제공하는 역할을 하고 있다.

현대오토에버의 모빌진(Mobilegene) 클래식은 Classic AUTOSAR 표준 사양 기반의 표준 플랫폼으로 현재 양산 주력 제품으로 고객사에 제공하는 것은 R4.0.3 버전이지만 지난해 하반기 AUTOSAR Classic 표준 R4.4를 만족하는 플랫폼 개발에 성공하면서 기대감이 커지고 있다.

모빌진 클래식 R4.4 플랫폼은 2018년 제정된 AUTOSAR Classic R4.4 표준을 기반으로 개발되었으며 자율주행 차량 등과 같은 기능 안전(Functional Safety) 대응 제어기 개발의 시장 수요에 대비해 만들어졌다. 현재 R4.0.3 버전은 BSW의 경우 단일 코어(파티션)에 배치하여 사용해야 했지만 R4.4 버전에서는 통신 부하 증가에 따른 MCU의 부하를 분산 관리하기 위해 BSW의 분산 배치를 지원한다. 이를 통해 CAN(controller Area Network), Ethernet을 각각의 단일 코어에 배치해 독립 수행이 가능하도록 했다.

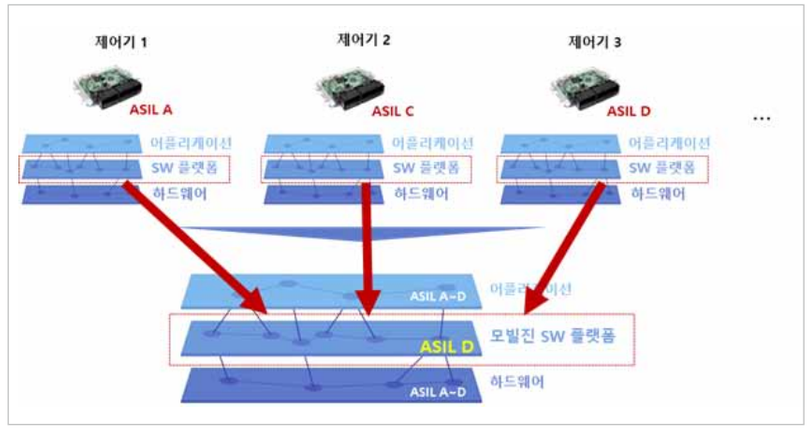
▲ 현대오토에버의 모비젠 로고

모빌진 클래식 SW 플랫폼과 기능안전 개발 적용의 복잡성

차량 개발의 패러다임이 기계 중심에서 전기/전자 시스템으로 변화되면서 전자 제어장치(ECU) 하드웨어 및 소프트웨어 결함 발견 빈도가 높아지는 것은 물론 사고의 직접적인 원인이 되고 있다. 따라서 전자 제어 시스템 전반의 오동작으로 인한 사고를 최소화하기 위해 하드웨어, 소프트웨어, 반도체 각 분야에서 ISO26262 자동차 기능 안전성 국제 표준을 적용하기 위한 노력이 지속적으로 이루어지고 있다.

현대오토에버 역시 파워트레인, 샤시 부분 전자 제어장치(ECU)에 각각 탑재된 SW 플랫폼을 대상으로 기능안전 적용을 우선 수행하고 있으며 OEM의 기능안전 평가를 통해 적용 여부를 확인하고 있다. 모빌진 클래식 SW 플랫폼도 차량 제어기 시스템에 포함되기 때문에 기능안전 적용이 필요하다. 그러나 다양한 도메인 제어기에 대응 가능하도록 설계된 모빌진의 특성상 높은 복잡성으로 인해 기능안전 적용의 어려움이 존재하는 것도 사실이다.

타겟 도메인 제어기의 다양성 및 ASIL(Automotive Safety Integrity Level) A, B, C, D 각기 다른 기능안전 요구사항을 모두 대응하기 위해 높은 수준의 소프트웨어 개발 및 관련 메커니즘 설계가 요구되기 때문이다. 결과적으로 모빌진 클래식 SW의 기능안전 적용에 있어 효율적이면서도 최대의 효과를 내기 위한 전략이 더욱 중요해지게 됐다.



▲ 기능안전 필요성

ASIL-D 인증을 취득하기 위한 기능안전 적용 전략의 수립

우선 다양한 도메인에 적용이 가능한 모빌진 클래식 R4.4 SW 플랫폼의 특성을 반영한 기능 안전 적용을 위해 체계적인 전략을 수립했다. SW 플랫폼의 모든 모듈을 ASIL-D에 따라 개발하는 것은 각 HW 마다의 의존성, 기능안전 연관성이 낮은 모듈 존재 등으로 인해 효율성과 효과성 측면에서 모두 좋은 전략이 아닌 것으로 분석됐다.

이에 ISO26262 자동차 기능 안전성 국제 표준의 SEooC[2] 방법을 적용해 기능안전 요구사항을 가정하고 전 제어기에 공통 적용 가능한 필수 모듈에 집중해 기능안전 컨셉을 도출했다. 또 기능안전 표준에서 요구하는 수준의 프로세스 수행을 위해 ASPICE(Automotive Software Process Improvement and Capability dEtermination)에 따라 내부 개발 프로세스를 정립 및 내재화했으며 기능안전 표준에서 요구하는 개발 활동 및 산출물을 위해 관련 역량을 확보하는 활동을 진행했다. 특히 ASIL 할당된 기능안전 모듈과 QM(Quality Management) 모듈이 공존하고 있어 SW 플랫폼 내에서 상호 간섭이 없음을 보장하는 FFI[3]설계와 검증으로 SW 플랫폼의 기능안전이 충족될 수 있도록 프로젝트를 수행했다.

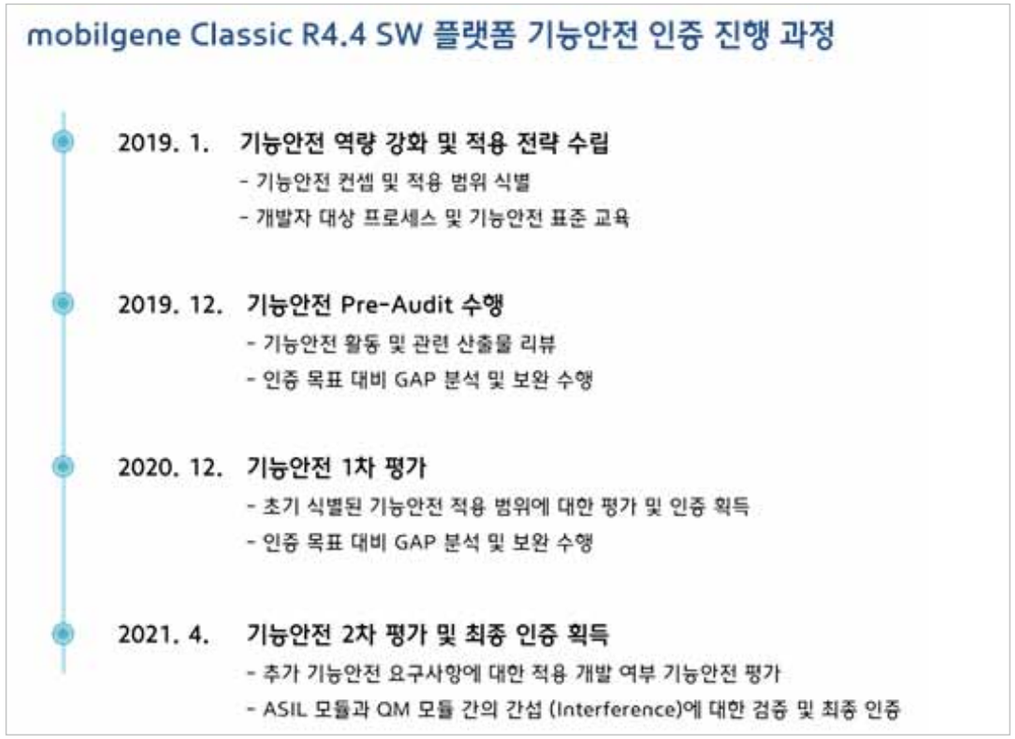
2) SEooC(Safety Element out-of-Context) : 선행 개발 또는 특정 고객을 타겟으로 하지 않는 제품의 개발에도 ISO26262 적용이 가능해야하기에 ISO26262 Part. 10에 기능안전 요구사항을 가정하여 개발하는 방법에 대해 정의
3) FFI(Freedom From Interference) : 서로 다른 ASIL 레벨 SW 컴포넌트들 간의 간섭이 없는 상태. ASIL 별로 잠재된 Systematic Fault 정도가 다르고, 높은 ASIL SW 컴포넌트에 영향을 끼치지 않아야 하기에 해당 상태 충족 필요

▲ 현대오토에버의 mobilgene Classic SW 플랫폼 기능안전 적용

모빌진 SW 플랫폼의 기능안전 평가 및 인증 획득 과정

이 과정에서 SW 플랫폼 개발팀과 기능안전 엔지니어링을 전문적으로 수행하는 기능안전팀의 협업은 기능안전을 충실히 적용할 수 있는 큰 힘이 됐다. 프로젝트 초기 두 팀이 협업하여 수립한 기능안전 적용 전략에 따라 개발팀은 기능안전 표준에서 언급된 방법론을 적용해 요구사항, 설계, 개발, 테스트를 수행했다. 기능안전팀은 기능안전 컨셉 보완, 프로세스 활동 감사(Audit), 기능안전 산출물 검토 및 가이드 등을 통해 실제로 기능안전 활동과 산출물이 작성되는지를 모니터링하고 가이드하는 역할을 했다.

다만 모빌진 클래식 R4.4 SW 플랫폼은 타겟 제어기가 정해져 있지 않기 때문에 관련 OEM 또는 협력업체로부터 평가를 받기가 어렵다. 따라서 자동차 기능안전 분야에서 오랜 경험과 공신력이 있는 인증 기관을 통해 전체적인 기능안전 프로세스, 산출물들을 평가받고 이슈 사항들을 해결함으로써 SW 플랫폼의 ASIL-D 기능안전 충족 여부를 확인할 수 있었다.

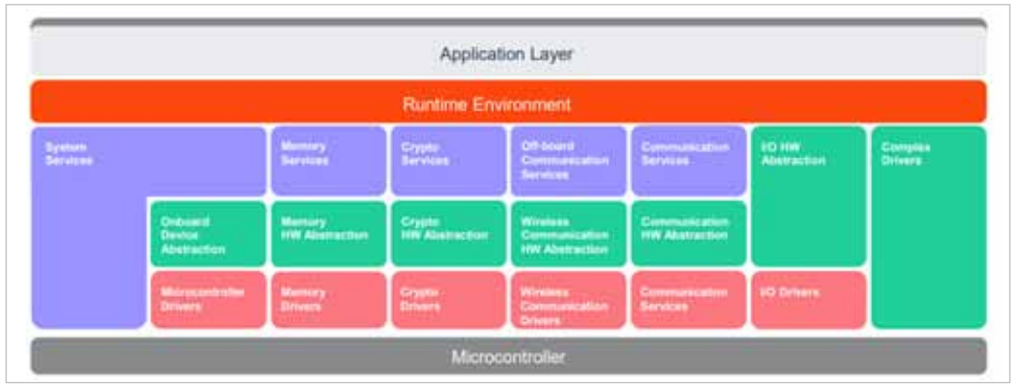


▲ 기능안전 인증 진행 과정

> *ASIL-D 기능안전 적용 및 인증을 위한 과정은 쉽지 않았지만 ISO26262 자동차 기능 안전성 표준을 제대로 이해하고 적용할 수 있는 계기가 되었다.*

참여자 소감 “ASIL-D 기능안전 적용 및 인증을 위한 과정은 쉽지 않았지만 ISO26262 자동차 기능 안전성 표준을 제대로 이해하고 적용할 수 있는 계기가 되었다. 이번 인증 경험을 기반으로 지속적인 SW 플랫폼 기능안전을 통해 고객의 제어기 및 차량 기능안전 만족에 도움을 드릴 수 있도록 계속 노력할 계획이다.” - 현대오토에버 기능안전 담당자

“현대오토에버의 자동차 기능안전 국제표준 대응 개발 역량은 가장 까다로운 안전 요구 수준인 ASIL-D를 만족했다. 현대오토에버 모빌진 클래식의 이번 적합성 인증 과정에 요구된 기능안전 개발 및 규격 세부 요건 대응 조치 역량을 높이 평가한다.” - 기능안전 인증업체 대표



▲ mobilgene Classic SW 플랫폼 구성

향후 계획 현대오토에버는 모빌진 클래식 R4.4 SW 플랫폼의 성공적인 기능안전 적용 및 인증 경험을 기반으로 기능안전 모듈을 업그레이드하고 다양한 제어기에서 필요로 하는 기능안전 모듈을 확대 개발할 예정이다. 또 제어기 SW 플랫폼 통합 경험 및 기능안전 엔지니어링 역량을 통해 사용자(애플리케이션) 관점의 기능안전 컨셉을 적용하고 고객의 눈높이에서 안전성을 보장할 수 있는 SW 플랫폼을 지속 개발한다는 방침이다.

향후 여러 제어기들이 통합된 도메인 제어 유닛(DCU (Domain Control Unit))에 대응하는 작업과 함께 일부 애플리케이션의 기능을 SW 플랫폼에 공용화, 표준화하는 작업도 진행하고 있다. 궁극적으로 필요 기능안전 메커니즘 발굴을 통해 한층 진보된 기능안전 역량을 가진 기업으로 자리매김한다는 목표를 세우고 있다.

현대오토에버 차량 전장 소프트웨어 사업부장 임양남 상무는 “모빌진 클래식은 현대오토에버가 2015년 개발·완료해 지속적으로 업데이트하고 있는 소프트웨어 플랫폼으로, 현재까지 거의 무결점에 가까운 품질을 자랑하고 있다”며 “고객은 모빌진 클래식 소프트웨어 플랫폼을 통해 시스템 안전 입증에 필요한 시간과 비용을 단축할 수 있고 최종 소비자들은 안전한 미래차에 탑승할 수 있는 이점이 있다”고 말했다.

OBIGO

안전 수준까지 높인 스마트카 소프트웨어 플랫폼

오비고, 글로벌 수준의 기능 안전 역량까지 확보
플랫폼부터 제작도구, 애플리케이션 원스톱 제공

▲ 미래자동차를 위한 '스마트카 소프트웨어 플랫폼 기업' 오비고 황도연 대표

오비고 기본 정보

회사명	(주)오비고	전화번호	031-8033-3000
대표자명	황도연	홈페이지	http://www.obigo.com
설립연도	2003. 3. 20	종사자	10명
주소	(13493) 경기도 분당구 판교로 338번지 3층		
주요제품	스마트카 소프트웨어 플랫폼		

전기차 시대가 도래하고 자율주행이 보편화될수록 자동차는 단순 이동 수단이 아닌 제2의 생활 공간이 될 가능성이 커진다. 그만큼 차안에서 보내는 시간이 길어지고 차에서 해야하는 일들이 많아지게 된다. 차량용 네트워크에 연결된 애플리케이션 서비스가 중요해지고 매우 다양해져야 하는 이유이다.

오비고는 세계 최초 휴대폰 WAP(Wireless Application Protocol, 무선 응용 프로토콜) 브라우저 솔루션 회사로 출발해 17년 간 축적된 임베디드 브라우저 기술을 바탕으로 다양한 OEM별 차량 인터페이스 및 OS 환경과 연동을 통해 스마트카 소프트웨어 플랫폼 및 전문 서비스업체로 자리매김하고 있다. 차량용 애플리케이션 설치·업데이트·삭제·실행 등의 환경을 제공을 제공하는 스마트카 소프트웨어 플랫폼, 차량용 서비스를 위한 애플리케이션 제작도구와 스토어를 제공하고 있다. 또 사용자가 보다 편리하게 자동차 정비 및 관리, 금융, 보험, 충전 등 주요 서비스를 사용하거나 쇼핑, 배송, 스트리밍, 음식주문, 다중 모빌리티 등의 맞춤형 모빌리티 라이프를 누릴 수 있도록 다양한 차량 애플리케이션 서비스를 개발하고 있다.

특히 오랜 노력 끝에 차량의 커넥티드 서비스 제공을 위한 소프트웨어 플랫폼 상용화에 성공해 이 분야 선두기업으로 부상했다. 자동차용 운영체계(OS) 1위인 블랙베리 QNX 소프트웨어에 HTML5 기반의 차량용 브라우저를 공급했으며 르노/닛산/마힌드라/쌍용차 등에 스마트카 소프트웨어 플랫폼과 다양한 애플리케이션을 개발, 공급하고 있다.

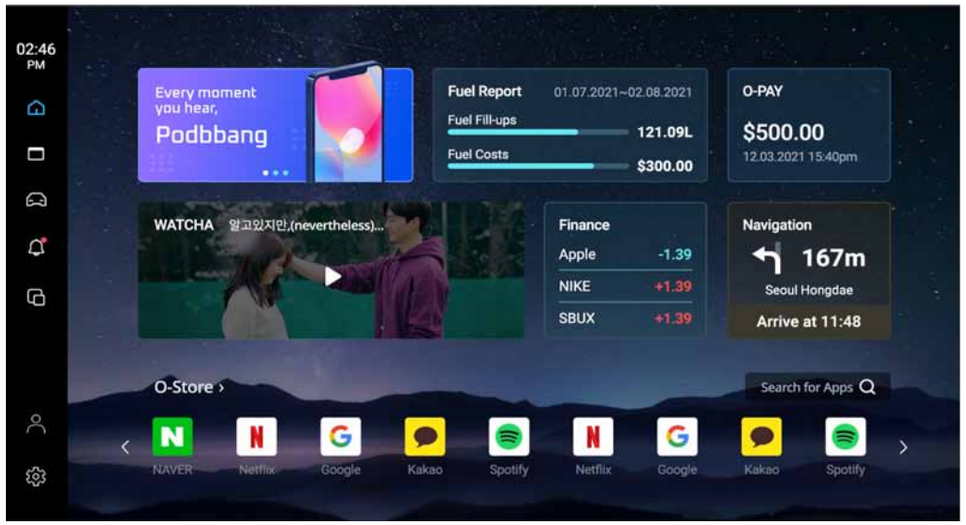
자동차

적용 표준	적용 안전 기법(Techniq & Measure)
ISO 26262	• ISO 26262기반 기능안전 개발 체계 구축 및 가이드 개발 • 차량 SW 코딩 표준 적용을 통한 정적분석 수행 및 자동화된 통합 빌드 환경 구축 • 사전결함 예방을 위한 DRBFM 가이드 개발 및 테스트 체계 구축

시장 요구에 맞는 기능안전 달성을 위한 역량 절실

자동차는 전세계에서 가장 많은 사람들이 활용하는 이동수단으로, 기능도 기능이지만 안전에 대한 이슈가 가장 큰 산업이다. 차량용 애플리케이션 실행을 위한 오비고의 스마트카 소프트웨어 플랫폼은 차량의 AVN 시스템에 장착되어 안전에 중요한 영향을 미치게 되는데 여기서 오비고의 고민이 시작됐다. 장착 차량 환경에 따라 ASIL(Automotive Safety Integrity Level, 자동차 안전 무결성 수준) B 수준에 그치고 있어 토요타를 비롯해 국내외 완성차 업체(OEM) 요구사항인 ISO 26262 기능안전 표준 지침 적용 및 도구 적용에 대한 준수가 미흡했기 때문이다.

따라서 OEM에 제품을 공급하고 해외 수출에 성공하기 위해서는 ISO 26262 도입이 절실히 요구되었다. OEM에서 요구하는 글로벌 수준 개발 및 품질 요구사항 대비 부족한 역량(회사 규모 및 품질비용 우려 등)을 비약적으로 키우면서 품질관리체계를 확보하는 것이 절실한 상황이었던 것이다.



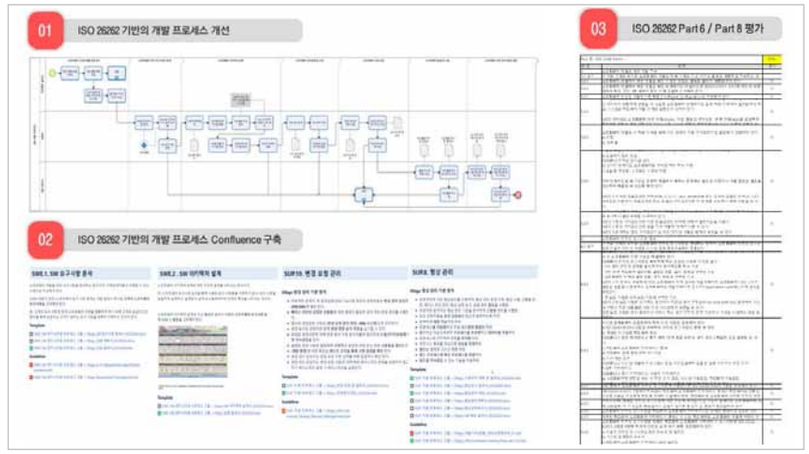
▲ 오비고 차량 어플리케이션 서비스 화면

ISO 26262 기능안전 개발 체계 구축 및 가이드 개발

ISO 26262는 해외 OEM(독일, 미국, 일본 등)과 국내(현대자동차, 현대모비스, 쌍용자동차에서 도입하고 있으며 차량에 탑재되는 전기/전자(E/E)시스템의 오류로 인한 자동차 사고를 줄이기 위해 제정된 차량용 기능 안전에 대한 표준이다.

오비고는 먼저 ISO 26262/SW공학전문가(TUV SUD FCSP 전문가)의 ISO 26262 공학수준 진단 및 갭분석을 통해 문제점을 체계적으로 분석했다. 수행해야 하는 고객사 프로젝트가 있는 상황을 감안해 도입 추진 시급성 및 중요성 관점에서 ISO 26262 Part 6(SW 개발 프로세스)와 Part 8 (지원에 관한 프로세스) 위주로 프로세스 구축과 적용 내재화를 수행하도록 우선순위를 결정했다.

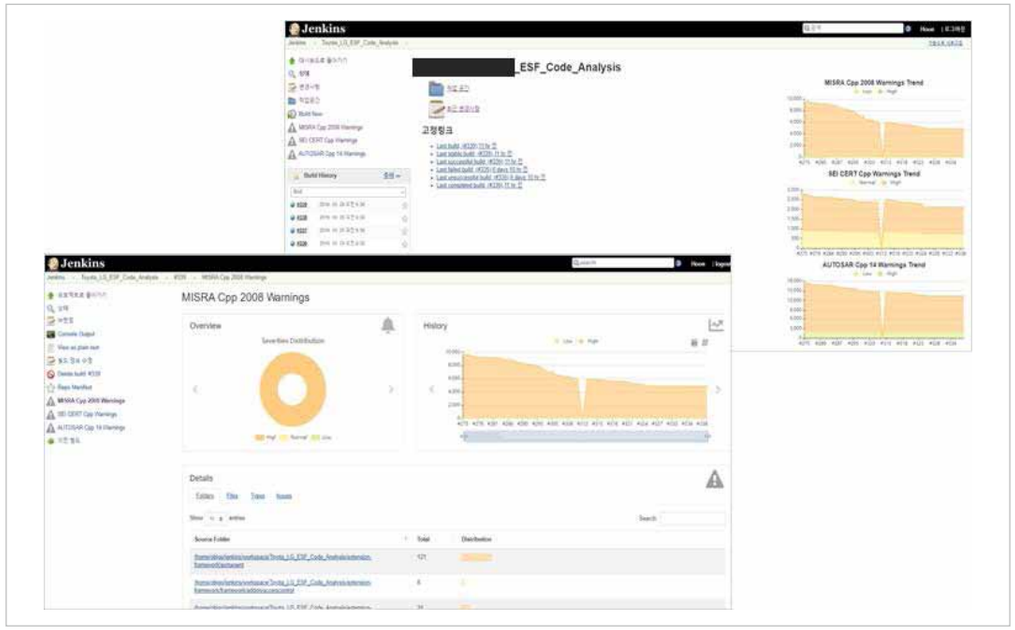
특히 ISO 26262를 수행하려면 프로세스 및 개발 방법에 있어 기존보다 엄격한 활동 및 산출물이 요구돼 이에 따른 저항감, 신규 도구 도입에 대한 경험 부족 및 시행착오가 흔히 일어나게 된다. 이를 해결하기 위해 ㈜브이웨이 컨설팅사의 실무 위주 가이드 지원 및 경영진의 적극적인 지원을 통해 ISO 26262 활동이 내재화될 수 있도록 노력했다. 또한 NIPA에서 배포한'자동차 전자제어장치 분야 SW 신뢰·안전성 확보를 위한 가이드 개발'가이드를 활용해 ISO26262 요구사항 적용에 필요한 기법 및 템플릿 가이드를 산출했다.



▲ ISO 26262 개발 체계 구축 및 가이드 개발

차량 SW 코딩 표준 적용을 통한 정적분석 수행 및 자동화된 통합 빌드 환경 구축

ISO 26262에서 요구하는 SW 안전성을 위한 코딩 표준을 정의하고 정적분석 도구와 Jenkins 도구를 연동하여 자동화된 Daily 빌드 및 정적분석 수행 환경을 구축하였다. 자동차 OEM의 요구사항인 MISRA(Motor Industry Software Reliability Association, 자동차 산업 소프트웨어 신뢰성 협회)-C:2012, MISRA-C++:2008, SEI CERT-C, SEI CERT-C++, AUTOSAR(AUTomotive Open System Architecture, 개방형 자동차 표준 소프트웨어 구조) C++ 14 규칙을 기준으로 정의하여 개발 가이드로 표준화하였고, 소스코드의 사이버 보안 취약점(CWE, CERT) 탐지 기능 실행, 품질지표(Quality Metric) 분석 기능 실행, 메모리 접근 에러, 누수, corruptions 등에 대한 런타임 에러 탐지 기능 실행 등 Parasoft C/C++ Test 정적분석 도구를 활용했다. 또 정적 분석 도구와 Jenkins 연동을 통한 Daily build 자동 수행 및 결함 발생 시 개발자/관리자에게 자동 보고가 이뤄지도록 환경을 구축했다. 특히 이 활동은 개발자의 만족도가 매우 높았는데 코딩 표준을 산출하여 학습 및 유지보수에 효과적이었고 소스 코드의 안정성 향상을 가져왔기 때문이었다.



▲ Jenkins 연동을 통한 정적분석 수행 예시

DRBFM 가이드 개발 및 수행 역량 강화

ISO 26262는 안전 분석을 개발 초기부터 적용해 안전 요구 사항을 추출하고 설계 검증하라고 권고하고 있다. DRBFM[1]은 OEM 업체중 하나인 토요타가 개발한 품질 경영 관리 기법 중 하나로, 변경되는 곳에서 문제(위험원)가 발생할 가능성이 크다는 점에 착안해 설계 단계에서 잠재된 문제를 사전 분석함으로써 위험원을 식별하고 문제 발생을 미연에 방지해준다.

오비고는 초기에는 테크니컬 리뷰 등 일반적인 동료 검토를 통해 설계 결함을 도출하였는데 고객사(토요타) 요청에 따라 DRBFM(Design Review Based Failure Mode) 수행을 시작하게 됐다. DRBFM 수행에 대한 사전지식이 없었기 때문에 활동순서, R&R, 실시방법, 워크시트 작성 방법 등에 대한 가이드를 개발했고 프로젝트 구성원 대상으로 5차 연수 및 DR 리뷰 절차, 워크시트 작성법을 교육했다. 어려움도 있었지만 성공적으로 해당 활동을 수행하고 품질 검증을 무사히 통과하는 성과를 거뒀다.

1) DRBFM(Design Review Based Failure Mode) : 토요타가 개발한 품질경영관리 기법 중 하나로 설계 품질 향상을 위한 활동

▲ DRBFM 프로세스 및 수행 테스트 전략

> *본 사업을 통해 SW 공학 역량이 강화되었고 자동차 SW 안전 개발 및 품질 활동 대응체계를 체계적으로 구축할 수 있게 되었다고 생각한다.*

테스트 전략 및 테스팅 체계 구축

ISO 26262에서 권고하는 테스트 프로세스를 구축하기 위해 SW Validation 단계별 활동 및 세부 활동 프로세스를 정의하고 수행하였다. 그동안 테스트라고 하면 프로젝트 일정에 맞춰 테스트 케이스를 작성하고 수행 결과 리포트를 전달하는 것이 일반적이었는데 ISO 26262 테스트 프로세스 구축을 통해 테스트 계획 및 설계 활동을 보다 체계적으로 수행할 수 있게 되었다.

특히 기존에는 공식 적용하지 않았던 테스트 케이스 설계기법(경계값 설계 적용, Negative 테스트 케이스 개발, 상태 전이 적용)을 공식적으로 적용해 테스트 커버리지를 넓혔고 테스트의 효과성 및 효율성을 확보할 수 있게 된 것이 큰 소득이었다.

참여자 소감

“수준의 자동차 소프트웨어 안전 및 프로세스가 무엇인지 알 수 있는 계기가 되었다. 본 사업을 통해 SW 공학 역량이 강화되었고 자동차 SW 안전 개발 및 품질 활동 대응체계를 체계적으로 구축할 수 있게 되었다고 생각한다.”

“안전기술 중에서 정적분석 도구 도입에 대한 요구가 항상 있었는데 여러가지 이유로 도입을 못하던 중 이번 기회로 다양한 코딩 표준(MISRA, CERT, AUTOSAR 코딩 규칙)을 확보할 수 있었다. 또한 정적분석 도구의 지속적인 통합(CI: Continus Integration)에 의한 개발 프로세스 효율성을 향상하고 가시성을 확보함으로써 코드 품질 향상에 큰 도움이 되었다.”

향후 계획

오비고 솔루션은 2013년 글로벌 자동차 제조사를 시작으로 한국, 중국, 인도, 유럽, 미국, 일본등 세계 각국의 다양한 제조사의 자동차에 탑재되고 있다. 오비고는 소프트웨어 안전기술 적용을 통해 글로벌 고객들이 자동차, 집, 주변 공간, 스마트 기기, 나아가 도시 전체를 연결해 자동차에서 안전하면서도 자신만의 라이프스타일을 누릴 수 있는 서비스를 제공한다는 방침이다.

오비고 CTO는“스마트카 시장에서 점차 중요해지는 소프트웨어의 안정성에 대비해 글로벌 표준 프로세스를 도입하여 소프트웨어 품질역량을 강화하고 있다”며 “앞으로 글로벌 시장에서 완성도 높은 제품으로 인정받고 세계적인 스마트카 소프트웨어 플랫폼 기업으로 도약하는 것이 목표”라고 말했다.

SKY AutoNet

안전 개발 체계 확보로 세계 TOP 5 자율주행 시스템 업체 부상

스카이오토넷, 첨단 기술 개발 역량에 안전을 위한 개발 체계까지 구축
2년간 노력 끝에 ASIL B등급, SP인증 획득...12월 스쿨존 세이버 출시

▲ '자동차 안전운전 단말기와 서비스를 제공하는 전문기업' 스카이오토넷 김태근 대표

스카이오토넷 기본 정보

회사명	스카이오토넷	전화번호	02-2279-1400
대표자명	김태근	홈페이지	http://www.adasone.com/
설립연도	2017. 9. 12	종사자	34명(2018년 한)
주소	서울특별시 서초구 방배로 114, 301호 (방배동, 다이치 빌딩)		
주요제품	ADAS, 스쿨존세이버 등		

스카이오토넷은 컴퓨터 비전과 센서 융합기술을 활용한 안전운전 단말기와 서비스를 제공하는 기업이다. 2014년 한양정보통신의 임베디드비전연구소로 출발해 2017년 9월 분사한 이후 총 92억원 규모의 국책연구개발사업의 주관기관으로 선정돼 스마트카 분야 기술력을 인정받은 바 있다(과제명: 교차로 AEB 등을 지원하기 위한 HD급 다중화각 전방 카메라 시스템 개발).

컴퓨터 비전 기반 ADAS(Advanced Driver Assistance System, 첨단 운전자 지원시스템) 기술과 딥러닝(Deep Learning), AEB(Autonomous Emergency Breaking, 긴급제동시스템), 차량제어 기술, 센서 융합 기술 등을 확보하고 있는 스카이오토넷은 스마트폰에서 사용하는 차로이탈방지 제품인 'AONE'과 상용차용 ADAS 단말기 'HM310', 첨단 차로이탈경고 시스템 'AXON 3.2', AEB 지원 카메라시스템, Personal Mobility(개인형 이동수단)용 자율주행 플랫폼 등의 제품을 선보이고 있다.

이 가운데 AEB 시스템은 2018년 1월 세계 최초로 완성차를 개조해 장착할 수 있는 애프터마켓용 제품으로 출시됐으며 같은 해 12월 제주도 대형버스 운전자 졸음감지 및 대응서비스 구축 사업에 납품되는 성과를 거두었다. 현재 제주도에서 운행되는 ICT 대형버스 20대에 ADAS와 함께 설치되어 있다.

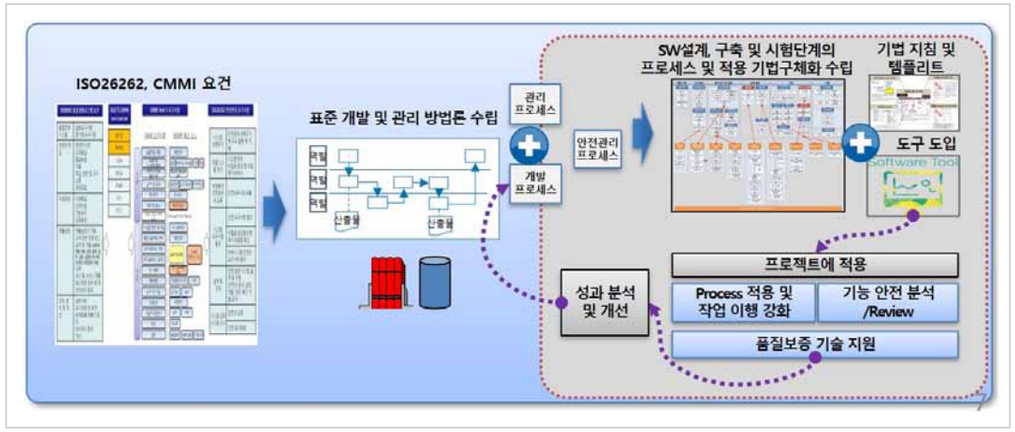
스카이오토넷은 미래 자동차의 큰 화두인 자율주행과 관련해 세계적인 수준의 반 자율주행(Semi Autonomous Driving) 시스템 업체로 부상하고 있다. 그러나 안전 기술 고도화와 체계 적인 시장 대응 등을 위해 최근 투자사 및 관련 공급사로부터 ISO 26262를 만족하는 체계 구축과 안전 개발 프로세스에 대한 요구가 높아지면서 이를 충족시켜야 하는 새로운 과제를 안게 됐다.

자동차

적용 표준	적용 안전 기법(Techniq & Measure)
ISO26262	• 안전 개발을 위한 자체 SW 안전관리 방법론 개발 • 안전기능 검증 및 관리를 위한 위험원 분석 및 리스크 평가 • 개발 기법 및 공학 원칙 적용을 위한 지침을 기반으로 정적 분석 수행

자율주행 관련 SW에 대한 안전 요구 개발 체계의 구축 시급

자동차 안전운전 단말기와 서비스를 제공하기 위한 많은 전문기술을 보유하고 있는 스카이오토넷이지만 안전성을 보장하기 위한 개발체계는 미흡한 부분이 있었다. 투자사 및 관련 공급사의 요구 수준도 점점 높아졌다. 투자 및 제품 공급을 위한 제품 검증 및 개발관리 프로세스 능력에 대한 테스트 및 실사 요구가 급증하면서 이에 대비해 ISO 26262를 만족하는 체계를 구축하고 그 역량을 입증할 필요성이 생겨난 것이다. 특히 그동안 SW 개발방법론 및 프로젝트 관리방법론을 도입하고 ISO9001 인증을 획득하는 등 노력을 기울여 왔으나 임베디드 시스템 개발에 적합하고 기능안전 관리(Functional Safety Management)를 포함하는 프로세스의 수립 및 적용에는 다소 미흡한 상황이었다. 무엇보다 스카이오토넷이 개발하고 있는 ADAS(Advanced Driver Assistance System) 및 AEB(Autonomous Emergency Brake) 제품이 기본적으로 ISO 26262의 ASIL(Automotive Safety Integrity Level) B~C 단계를 요구하고 있어 이에 대한 대응은 더 이상 미룰 수 없는 과제가 됐다.

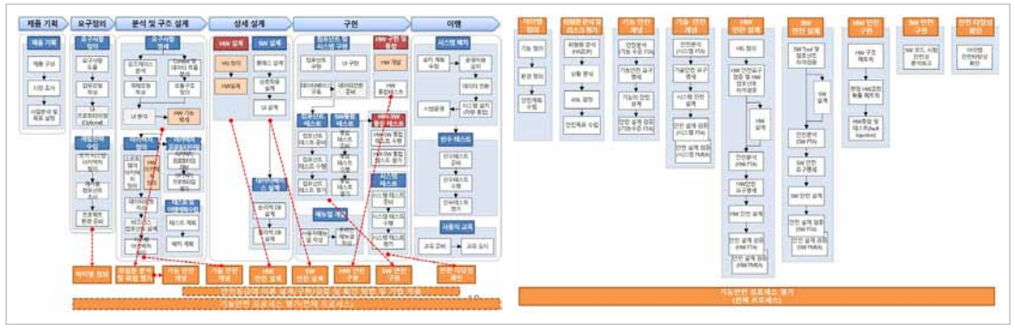


▲ ISO26262 ASIL B 등급을 만족하는 체계 수립 방안

ACBED(AdasOne Component-based Embedded System Development methodology) 개발

이같은 진단에 따라 CMMI[1] level 3와 ISO26262 ASIL B등급을 만족하는 수준으로 임베디드 시스템 개발 시 손쉽게 활용할 수 있는 스카이오토넷만의 방법론을 만들었다. 이는 ASIL B 등급을 만족하는 개발 및 관리 방법론으로, 실제 개발 프로젝트에서 적용의 효과성을 높이기 위해 단계별, 작업별 체크리스트, 표준산출물을 포함한 업무수행 가이드를 경량화해 작성되었다. 임베디드 시스템 구축 사업에 맞는 품질보증 절차를 수립하고 기능안전 관리를 위한 절차와 작업수행가이드 및 산출물 템플릿을 포함하고 있으며 SW 개발뿐만 아니라, HW 개발을 위한 작업의 업무수행가이드 및 산출물 템플릿도 포함하고 있다. 특히 기능안전관리 프로세스는 NIPA에서 공개한 『SW안전성공통개발가이드』를 참고해 개념 단계 및 시스템 개발 단계의 활동과 작업을 구체화하고 이를 설명하는 작업별 업무수행가이드를 수립하였다.

1) CMMI(Capability Maturity Model Integration) : 미국 카네기멜론대학 소프트웨어 공학연구소(SEI)와 산업계가 공동으로 개발, 보급하고 있는 소프트웨어 및 시스템 품질관리 인증



▲ ACBED 방법론(좌) 기능안전관리 프로세스(우)

▲ HARA 분석 쉬트 주요 내용

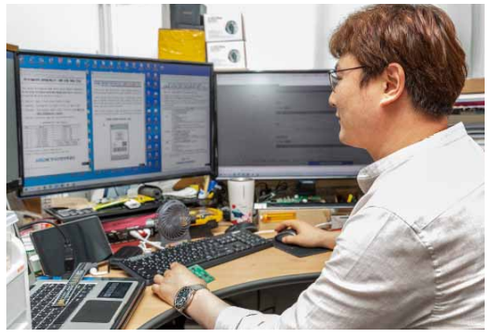
▲ HARA 분석 쉬트 주요 내용

기능안전관리를 위한 위험원 분석 및 리스크 평가

스카이오토넷은 무인이송시스템 개발을 시범사업으로 설정하고, 자체 작성한 기능안전관리 프로세스 적용을 위해 위험원 분석 및 리스크 평가를 우선 수행했다. 위험원 분석을 위해 Hazard와 운영상황을 도출한 결과, 주요 Hazard는 7개, 주요 운영상황(기본상황인 도로조건, 차량속도, 운행상태와 특정 운영상황인 눈길, 빗길, 야간, 역광 등)을 조합한 변수는 9,710개가 각각 도출되어 총 Hazardous Event는 6만 7,960개로 집계됐다. 이를 분석하면 ASIL C 등급을 충족시켜야 한다는 결론이 도출됐다.

개발 기법 및 공학 원칙 적용을 위한 지침 및 가이드 수립

스카이오토넷은 이를 감안해 ACBED 방법론 적용시, ASIL B 등급이 요구하는 개발 기법의 적용을 위한 다양한 기법 및 가이드를 수립하였다. NIPA에서 공개한 『자동차 SW안전가이드』, 『SW안전가이드-공통분야』를 활용해 모델링 가이드, 코딩 가이드, 명명 가이드, 시험 가이드, 테스트케이스 작성 가이드, 동료검토 가이드, 정적 분석 가이드, 통합시험(요구사항 기반, 인터페이스 시험) 가이드, 차량네트워크 기반 시험 가이드 등 총 32개의 개발 지침 및 개발 기법 적용에 필요한 가이드를 수립했다. 특히 기법 적용을 위한 가이드는 구체적인 기법별 적용 절차, 사례 등을 포함하고 산출물 템플릿과 연계해 수립하였으며 회사 내 현행 프랙티스의 약점과 단기간의 도입 가능성 등을 고려해 ISO26262에서 요구하는 SW공학 기법 및 원칙을 지침 혹은 가이드로 확정하였다.



> *2년간 회사에 맞는 프로세스를*
> *정립해나갈 수 있었고*
> *그 결과로 CMMI,*
> *ISO 26262 ASIL B등급,*
> *SP인증까지 받을 수 있게 되었다.*

참여자 소감 “ 2년간 회사에 맞는 프로세스를 정립해나갈 수 있었고 그 결과로 CMMI, ISO 26262 ASIL B등급, SP인증까지 받을 수 있게 되었다. 물론 그렇다고 해서 당장 눈에 띄는 변화가 생긴 것은 아니기 때문에 정량적으로 얼마나 좋아졌는지 정확한 수치를 말하기는 어렵지만 개발 역량이 15% 정도는 상승한 것 같다. 15%라는 수치가 크지 않다고 생각할 수 있겠지만 이로 인해 우리가 어떤 부분이 부족했는지 알게 되었다. 개선하려면 무엇이 부족한지를 아는 게 제일 중요하다는 점에서 매우 긍정적인 신호인 것이다.”

“제품의 안전성 확보를 위해 SW 공학을 적용한 프로세스를 만들어 내고 그것을 계속해서 현장에 적용해 보려고 노력하는 과정 속에서 정말 많은 것을 배울 수 있었다. 고객의 요구사항에 대해 보다 더 정확하게 파악할 수 있었고 일정 관리도 체계적으로 할 수 있었으며 동료 리뷰와 정적분석툴 사용을 통해 코드 결함을 조기에 찾아 수정함으로써 소프트웨어 품질까지 향상시킬 수 있었다.”

“프로젝트의 각 과정들을 문서화해 자료로 남겨놓음으로써 이후 신규 개발자가 오더라도 과거 작업과 연계성을 가지고 손쉽게 작업을 시작할 수 있는 기반을 만든 것이 큰 성과라고 볼 수 있습니다.”

향후 계획 스카이오토넷이 현재 가장 주안점을 두고 있는 제품은 ‘스쿨존 세이버’라고 불리는 ‘AXON 1.2’로 올해 12월부터 본격 판매를 앞두고 있다. 운전자가 스쿨존 내의 규정속도인 시속 30km를 준수할 수 있도록 속도를 제어해주는 장치로 올해 3월부터 시행된 ‘민식이법’을 준수할 수 있도록 해준다. 이 법에 따라 스쿨존 내 교통사고 시 특별범죄 가중처벌 대상으로 강화됐기 때문에 AXON 1.2을 활용하면 스쿨존 내 교통사고 및 안전사고를 효과적으로 예방할 수 있다.

소프트웨어 개발팀 이성호 수석연구원은 “스쿨존 세이버를 제작하면서 짧은 일정내에 개발해야 했기 때문에 어려움이 많았다”면서도 “SP인증을 받으면서 얻게 된 여러가지 체계화된 프로세스가 있었기 때문에 부담스러운 업무량 속에서도 헤매지 않고 비교적 효율적으로 작업을 진행할 수 있었다”고 소감을 밝혔다.

스카이오토넷은 이 제품을 시작으로 다양한 시장 친화적인 제품을 출시해 2022년까지 ‘세계 TOP5 자율주행 시스템 업체’, 2023년까지 ‘ADAS 단말기 및 안전운전 플랫폼 1억 달러 매출 달성’이라는 목표를 달성해나갈 계획이다.

HUCONN

SW 안전 설계로 BMS 넘어 ESS 강자 노린다

휴컨, SW 안전 아키텍처 구현으로 정적.동적 커버리지 100% 달성
2022년 자체 ESS, 이동형 전기차 충전 로봇까지 다양한 라인업

▲ '에너지 스토리지 시스템 전문기업' 휴컨 강대근 대표

휴컨
기본 정보

회사명	휴컨	전화번호	053-341-2613
대표자명	강대근	홈페이지	
설립연도	2016. 12. 15	종사자	
주소	대구시 북구 호암로 51, 벤처오피스동 501호		
주요제품	에너지 스토리지 시스템		

글로벌 에너지저장시스템(Energy Storage System, ESS)의 폭발적 성장으로 한국 ESS 시장 역시 2018년 이후 큰 폭의 성장을 거듭하고 있으며 ESS의 핵심 기술인 배터리관리시스템(BMS) 제어기술 또한 동반 성장하는 중이다.

현재 BMS의 요소기술별 기술 수준을 살펴보면 HW에 비해 배터리 모니터링, 계산 및 SW 제어 기술이 상대적으로 취약한 편이다. 현재 BMS의 SW 안전설계 부문은 전기자동차를 중심으로 진행되고 있으며 이마저도 대기업 수준의 역량을 갖춘 규모에서나 진행이 가능한 상황이기 때문이다.

그러나 소형 모빌리티 및 휴대용 전력기기의 출현으로 인해 BMS의 안전 설계에 대한 다양성 요구는 더욱 증가하고 있다. 앞으로 중소기업 규모에서도 수요자의 특성에 따라 커스터마이징 될 수 있는 기능 안전설계 기술의 체계적인 시스템 도입이 반드시 필요한 이유이다.

휴컨은 그동안 자체 연구인력 및 네트워크를 활용해 R&D 기술개발을 끊임없이 진행해 ESS 솔루션과 자동차 전장(Automotive Electronics System) 소프트웨어에서 뛰어난 개발력을 갖추고 있다. 국내 대기업과도 제휴관계를 맺고 있고 사용자 요구에 맞는 커스텀 소프트웨어 솔루션을 설계부터 구현까지 모든 부분을 체계적으로 개발하고 있다. 그러나 휴컨이 BMS 제품의 경쟁력 강화를 통해 ESS 분야 최강자로 부상하기 위해서는 중요한 과제가 있었다. 바로 안전 기능 설계와 구현에 대한 개선 활동이 이뤄져야 하는 상황이었다.

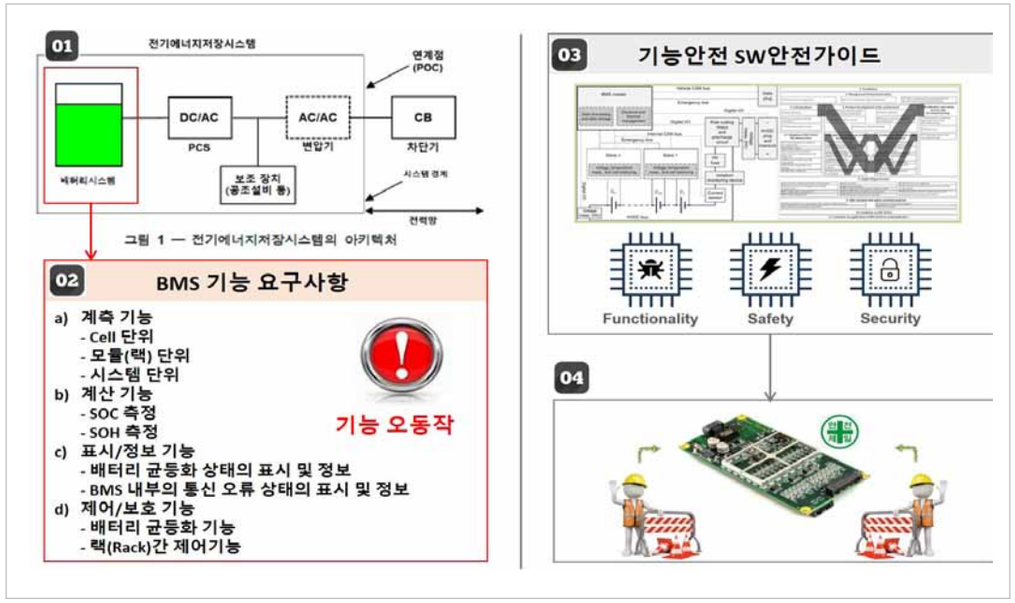
배터리

적용 표준	적용 안전 기법(Techniq & Measure)
IEC61508	• SW안전 가이드 기반 소프트웨어 안전 개발 활동 및 기법 수립 • 시스템 수준 안전 분석으로 SW 안전 요구사항 도출 및 아키텍쳐 설계 • IEC 61508 기반 SW 코드의 안전성 강화를 위한 SW 시험 (정적/동적)

안전 기술 적용을 통한 사업 경쟁력 확보가 관건

2017년 8월 전북 고창 한국전력 실증단지에서 풍력발전 연계용 ESS 화재가 발생한 이후 화재 사고는 지속적으로 발생하고 있다. 이러한 폭발과 화재로 인한 인명과 재산의 피해를 줄이기 위해 국내에서는 ESS 안전강화 대책의 일환으로 ESS 주요 구성품(리튬이차전지 셀, 시스템 및 전력변환장치)에 대한 KC 인증강화가 발표되었고 ESS의 안전한 상태를 확보하기 위한 과전압, 과전류, 과열 상황을 감지해 제어하는 안전기능 구현이 매우 중요한 과제로 부상했다.

특히 BMS 자체의 안전기능을 설계하였더라도 안전기능 수행에 관여하는 HW 및 SW의 결함으로 인해 안전기능의 무결성(Integrity)이 훼손될 수 있다. ESS 및 전동 킥보드 등 소형 모빌리티 시스템의 안전성 고도화를 위해 과전압, 과전류, 과열 상황에 대한 안전기능을 단순히 구현만 해서는 안되며 이 기능들이 SW 안전가이드 국제표준에 부합하는 무결성을 갖추고 동작하는 설계가 필요하게 되었다. 이에 IEC 61508 SW안전가이드 기반 배터리 운용상태(전압, 전류, 온도, SOC, SOH 등) 감시, 제어, 보호 관리할 수 있는 고신뢰성/고안전성 BMS 개발이 휴컨의 당면 과제가 되었다.



▲SW 안전가이드 기반 고신뢰성/고안전성 배터리관리시스템 개발 필요

산업일반 분야 SW안전 가이드의 SW안전 개발 활동 및 기법 적용

이전까지 휴컨에 없었던 SW 안전 개발 프로세스 적용은 IEC 61508 기반 산업일반 분야 SW 안전 가이드에서 제시한 SW 안전 수명주기 활동을 적용하는 것으로부터 시작되었다. SW 안전 계획서 내에 안전 수명주기 활동을 WBS(Work Breakdown structure)로 도출하였으며 프로젝트 관리 도구(wrike)를 활용해 관리하도록 구성되었다.

또한 SIL2 수준에서 각 활동에 적용되어야 하는 기능 안전 검증기법(Technique/Measures) 중에서 휴컨에 적용할 수 있는 것을 정의하였다(예: 소프트웨어 안전요구사항 작성 기법:Semi-formal methods, Computer-aided specification tools). 개발 중 발생하는 모든 산출물과 소스코드의 형상 변경을 체계적으로 관리하고 유지하기 위해 소프트웨어 형상관리를 적용하는 작업도 진행했다.

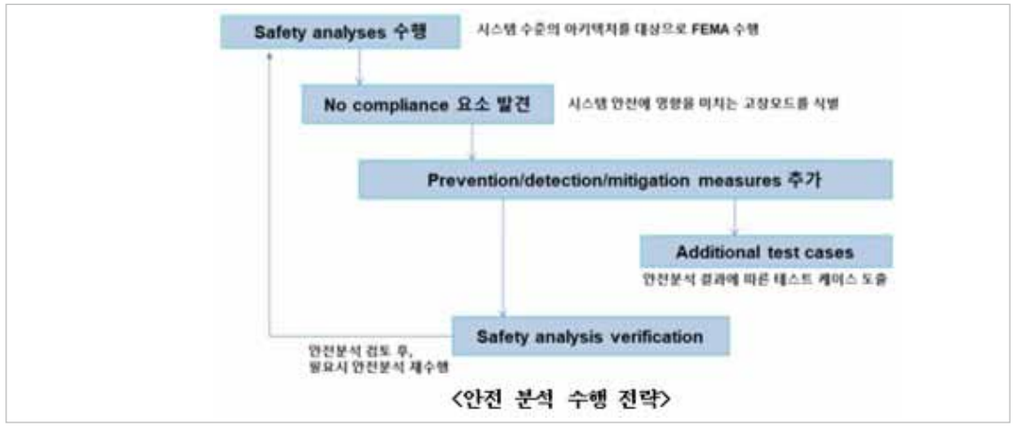
IEC 61508 표 / 항목		기법 및 조치	SIL2 수준	적용 여부
IEC 61508-3, 표A.1(소프트웨어 안전 요구사항 작성)	1a	Semi-formal methods	R	적용
	1b	Formal methods	R	미적용
	2	Forward traceability	R	적용
	3	Backward traceability	R	적용
	4	Computer-aided specification tools	R	적용
IEC 61508-3, 표A.2 (소프트웨어 설계 및 개발 – 소프트웨어 아키텍처 설계)	1	Fault detection	R	미적용
	2	Error detecting codes	R	미적용
	3a	Failure assertion programming	R	미적용
	3b	Diverse monitor techniques	R	미적용
	3f	Backward recovery	R	미적용
	4a	Re-try fault recovery mechanisms	R	미적용
	4b	Graceful degradation	R	미적용
	7	Modular approach	HR	적용
	8	Use of trusted/verified software elements (if available)	HR	미적용
	9	Forward traceability	R	적용
	10	Backward traceability	R	적용
	11a	Structured diagrammatic methods	HR	미적용
	11b	Semi-formal methods	R	적용
	11c	Formal design and refinement methods	R	미적용
	11d	Automatic software generation	R	미적용
	12	Computer-aided specification and design tools	R	적용
	13a	Cyclic behaviour, with guaranteed maximum cycle time	HR	미적용
	13b	Time-triggered architecture	HR	미적용
	13c	Event-driven, with guaranteed maximum response time	HR	미적용
	14	Static resource allocation	R	미적용
IEC 61508-3, 표A.3 (소프트웨어 설계 및 개발 – 지원도구 및 프로그래밍 언어)	1	Suitable programming language	HR	적용
	2	Strongly typed programming language	HR	적용
	3	Language subset	-	적용
	4a	Certified tools and certified translators	HR	적용
	4b	Tools and translators	HR	적용
IEC 61508-3, 표A.4 (소프트웨어 설계 및 개발 – 상세 설계)	1a	Structured methods	HR	적용
	1b	Semi-formal methods	HR	적용
	1c	Formal design and refinement methods	R	미적용
	2	Computer-aided design tools	R	적용
	3	Defensive programming	R	미적용
	4	Modular approach	HR	미적용
	5	Design and coding standards	HR	적용
	6	Structured programming	HR	미적용
	7	Use of trusted/verified software elements (if available)	HR	미적용
	8	Forward traceability	R	적용
IEC 61508-3, 표A.5 (소프트웨어 설계 및 개발 – 소프트웨어 모듈 시험 및 통합)	1	Probabilistic testing	R	미적용
	2	Dynamic analysis and testing	HR	적용
	3	Data recording and analysis	HR	미적용
	4	Functional and black box testing	HR	미적용
	5	Performance testing	R	미적용
	6	Model based testing	R	미적용
	7	Interface testing	R	미적용
	8	Test management and automation tools	HR	적용
	9	Forward traceability	R	적용
IEC 61508-3, 표A.6 (연 통합)	1	Functional and black box testing	HR	적용
	2	Performance testing	R	미적용
	3	Forward traceability	R	적용
IEC 61508-3, 표A.7(시스템 안전 검증(Validation)의 소프트웨어 측면)	1	Probabilistic testing	R	미적용
	2	Process simulation	R	미적용
	3	Modelling	R	미적용
	4	Functional and black-box testing	HR	미적용
	5	Forward traceability	R	미적용
	6	Backward traceability	R	미적용
IEC 61508-3, 표A.9 (소프트웨어 검증(Verification))	1	Formal proof	R	미적용
	2	Animation of specification and design	R	미적용
	3	Static analysis	HR	적용
	4	Dynamic analysis and testing	HR	적용
	5	Forward traceability	R	적용
	6	Backward traceability	R	적용
	7	Offline numerical analysis	R	미적용

▲SIL2 수준 안전 검증기법 적용

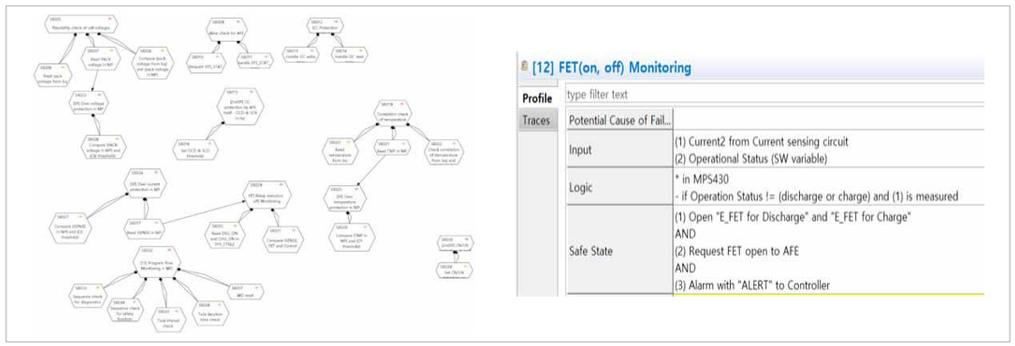
시스템 수준 안전 분석을 통한 소프트웨어 안전 요구사항 도출

ESS를 운영하기 위한 ESS BMS는 고전압, 저전압, 과전류, 과열의 위험원에 대응하기 위해 고/저전압 검출 안전기능, 과전류 검출 안전기능, 과열 검출 안전기능이 필요하다. 이러한 안전기능이 무결하게 동작하도록 SW 설계 요구사항을 도출하기 위해 시스템 설계 수준에서 안전 분석을 수행하였다. 안전 분석 방법은 FMEA[1]를 적용하였고 반복적으로 수행했다. SW 안전 요구사항은 사양서와 안전 요구사항 간의 관계도를 그려가면서 SW 안전 요구사항의 완성도를 높였다. 이렇게 도출된 안전 요구사항을 안전 아키텍처에할당함으로써 안전 아키텍처를 효율적으로 설계할 수 있게 되었다.

1) FMEA(Failure Mode and Effect Analysis) : 고장모드 영향분석. 도표 등을 사용하지 않고 미리 정해진 서식에 따라서 고장모드가 타 부품과 시스템 및 사용자에게 미치는 영향과 고장의 원인을 조사하는 기법



▲안전 분석 수행 전략

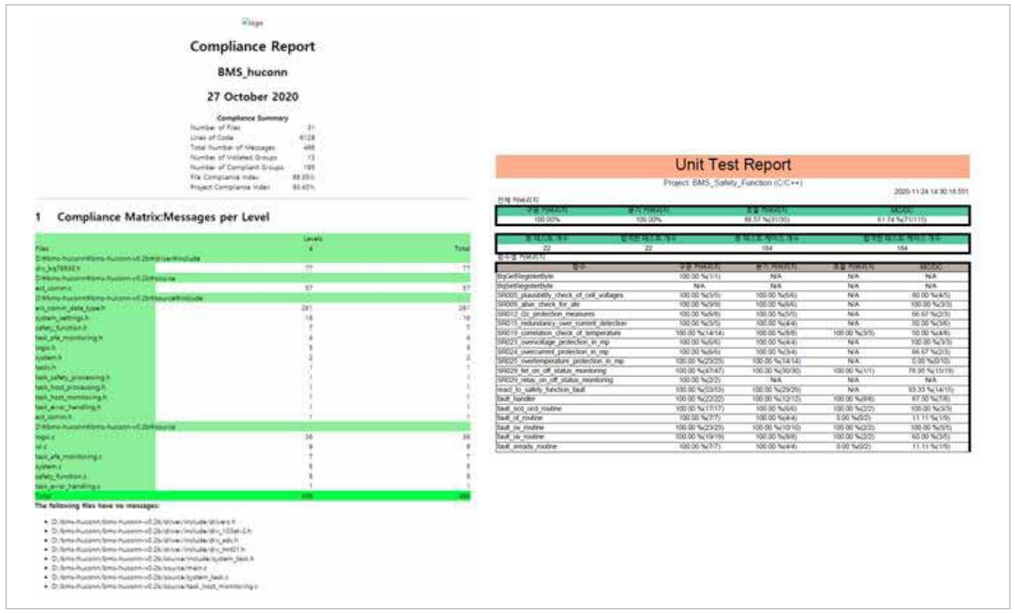


▲안전 요구사항 관계도(좌) 안전 요구사항(우)

IEC 61508 기반 산업일반 분야 SW안전 가이드를 적용한 SW 시험

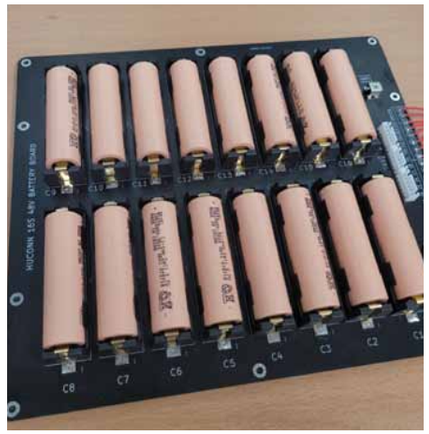
SW 안전 요구사항이 반영된 SW가 올바르게 구현되었는지를 확인하기 위한 작업도 필요했다. 유닛시험과 통합시험 목적을 고려해 적절하게 시험 전략을 수립하고 단기간에 효과적으로 SW에 대한 검증을 위해 코드작성과 병행하면서 정적시험과 동적시험을 수행했다.

먼저 정적분석은 소프트웨어 통합 시 개발된 코드를 대상으로 MISRA-C 규칙 준수 여부 확인하는 활동으로 이뤄졌는데, QA C Version 8.1.1-R을 사용하여 2차에 걸쳐 규칙 준수율을 확인한 결과 MISRA C 규칙 준수율이 99.35%로 매우 높은 신뢰성을 보였다. 또한 코드 수준의 무결성 확보를 위해 구문 커버리지 및 분기 커버리지 목표를 100%으로 하고 동적 시험을 수행했는데 CodeScroll Controller Tester로 측정한 결과 두 개 커버리지 모두에서 목표치 100%를 달성함에 따라 소스코드에 대한 안전 요구사항이 모두 충족했음을 확인할 수 있었다.



▲정적분석 / 동적시험 결과

> *기능안전이 적용된 BMS를 개발하면서 개념도 잡히고, 의료기기와 같은 제품에 왜 SW 안전이 적용되어야 하는지 알게 되는 계기가 되었다.*



참여자 소감 “가장 많이 받는 질문이 휴컨에서 만든 제품은 폭발하지 않는지에 대한 것이다. 그럴 때마다 KC 62619를 만족하는 수준의 제품이라고 자신있게 소개한다. 물론 부연 설명이 필요하지만 안전한 제품에 대한 인증을 받았다는 것만으로도 자부심을 가지고 소개할 수 있게 된 것이다.”

“SW 안전은 신입사원이었을 때 국방과제를 하면서 들어본 적이 있었다. 그 때는 선배들이 시키는 것만 해서 도무지 이해가 가지 않았다는데 이번에는 기능안전이 적용된 BMS를 개발하면서 개념도 잡히고, 의료기기와 같은 제품에 왜 SW 안전이 적용되어야 하는지 알게 되는 계기가 되었다. 스스로 레벨업이 된 것 같아 기분이 좋다.”

“우리와 같은 작은 기업에서는 SW 공학적 접근이 쉽지 않다. 개발 방법론이나 형상 관리, 심지어 소스관리도 툴이 없어 관리가 안되는 문제가 있었다. 이번 과제를 통해 여러가지 개발 방법론과 툴을 사용해 보았는데 생각보다 어렵지 않게 적응할 수 있었다. 또 해외 사업자와도 협업하는 기회가 있었는데 조금은 익숙해진 애자일(agile) 개발 방법을 사용해 다행이라는 생각이 들었다.”

“SW 품질에 대해 요구사항을 제시하는 고객사가 있었는데 정적, 동적 시험을 거친 경험이 있고 필요한 경우 이에 대한 리포트로 SW 품질을 평가할 수 있도록 하겠다고 했더니 매우 흡족해 했다. 특히 실제 적용 사례를 이야기할 수 있어서 매우 좋았다.”

향후 계획 배터리를 포함한 에너지 분야는 지금도 매우 빠르게 성장하는 분야이고 미래에는 더 폭발적으로 시장이 확대될 분야이다. 하지만 시장이 확대될수록 배터리가 무분별하게 사용되면서 크고 작은 사고로 이어질 우려도 커지고 있다. 휴컨은 배터리가 적용되는 제품이 안전하게 출시돼 소비자가 안심하고 사용할 수 있도록 SW 안전 연구개발에 최선을 다할 계획이다.

휴컨 강대근 대표는 “튼튼하고 안전한 BMS를 개발하고 이를 기반으로 다양한 제품에 빠르게 적용할 계획”이라며 “시장은 점점 더 안전과 성능이라는 두 가지 필요성을 함께 요구하고 있으며 휴컨은 그 두 마리 토끼를 모두 잡아냈다고 자부한다”고 강조했다. 휴컨은 앞으로 BMS 제품의 시장 확대는 물론 2022년에는 자체 ESS 제품, 이동형 전기차 충전 로봇까지 다양한 제품으로 시장에 진출한다는 목표를 세우고 있다.

하늘을 나는 무인비행체의 안전을 책임진다!

용비에이티, 항공기 수준의 SW 비행제어 인증 달성
미래형 비행제어 시스템 개발로 시장 점유율 확대 자신

▲ '하늘을 나는 무인비행체 SW 개발 기업'용비에이티 박원용 대표

용비에이티 기본 정보

회사명	용비에이티	전화번호	070-4895-1130
대표자명	박원용	홈페이지	www.yongbeeat.com
설립연도	2005. 11. 17	종사자	11명(2020년 기준)
주소	인천 연수구 갯벌로 12, 테크노파크 시험생산동 205		
주요제품	무인비행체 비행제어SW(FCS)		

세계적으로 항공산업이 급격하게 발전하면서 항공기에 적용되는 새로운 전자시스템이 개발되고 있지만 최근 몇 년 사이 소프트웨어 오류로 인한 대형 사고도 발생하고 있다(인도네시아와 에티오피아에서 추락한 보잉 737 맥스 항공기는 비행통제와 관련된 신기술인 조종특성향상시스템(MCAS) 자동항법장치의 SW 오류가 사고원인으로 추정되었는데 이후 보잉사에서는 해당 장치의 SW 오류를 수정했다고 발표한 바 있다).

사람을 수송하는 민항기의 경우 항공기에 탑재되는 모든 SW는 국제 항공기 SW 안전 규격인 RTCA DO-178C에 적합한 지 여부를 미국연방항공청(FAA)으로부터 승인받도록 되어있으나 무인비행체(무인항공기, 드론)에 대해서는 일부 비행 규제(비행가능 영역, 고도제한 등)만 하고 있을 뿐 탑재되는 SW 안전성에 대한 국제 수준의 규제는 아직 명확하지 않은 실정이다. 무인비행체가 비행 중 추락하게 될 경우, 무인비행체 손실뿐 아니라 지상 인명에 피해가 발생할 수 있으며 전기 시설 등 산업 시설의 파괴를 야기함으로써 다양한 피해가 발생하게 된다.

물론 항공기 SW 안전성 국제 규격을 기준으로 무인비행체 안전성을 보증하는 것은 관련 개발업체에 엄청난 부담으로 작용한다. 그럼에도 불구하고 용비에이티는 무인비행체 SW 안전성(Safety)을 보증하기 위해 RTCA DO-178C를 준수하기로 결정했다. 안전등급(Safety Level) A에 해당하는 71개 목표(Objective) 달성을 통해 안전성이 보장된 무인비행체 SW를 만들어야 한다고 판단했기 때문이다.

항공	적용 표준	적용 안전 기법(Techniq & Measure)
	DO-178C	• 안전한 무인비행체 소프트웨어 개발을 위한 프로세스 구축 • Target 기반의 시험 자동화 적용(테스트, 정적분석)

무인비행체의 안전을 확보하기 위한 목표 설정

고객사의 다양한 요구조건에 따라 개발된 제품의 SW는 DO-178C 기준을 적용하기에는 부족하기 마련이고 DO-178C 안전등급 A 수준을 확보하기 위해서는 추가적인 검증 및 시험을 수행하는 작업이 필요하다.

용비에이티가 그동안 개발한 무인비행체 탑재용 SW의 안전기능이 DO-178C 안전등급 A에 해당하는 안전 수준을 달성하기 위해서는 안전성을 보장하는 SW 개발 체계와 시험 자동화 도구 등의 확보가 필요한 상황이었다. 또한 용비에이티의 고객들이 항공기 감항 인증을 위한 SW 안전 규격인 DO-178C 적합성 증명을 요구하게 되면서 DO-178C를 준수하여 안전성 목표를 달성하는 것이 큰 과제로 부상했다. 회사의 역량 부족, DER 검토[1] 및 시험 자동화 도구 도입 등 비용 부담이 있었지만 무인비행체 시장은 점점 커질 것이기 때문에 안전 인증은 반드시 필요해질 것이라 판단을 했다.

특히 국방용 무인비행체의 경우 설계 단계부터 SW 안전인증 기준을 명확히 하고 있기 때문에 민간용 무인비행체도 이러한 안전 인증이 당연한 수순이 될 수밖에 없었다. 용비에이티는 DO-178C에서 요구하고 있는 안전등급 A 수준의 71개 목표(Objective)를 달성하는 방안에 대해 이 분야 전문기업인 모아소프트의 도움을 받아 전문 컨설팅을 받게 됐다.

1) DER(Designated Engineering Representatives) 검토 : 미국 연방항공국이 권한을 위임한 DER 을 통해 개발 및 검증과정에 참여하여 수행하는 공식검토

< RTCA DO-178C Process Objectives >

Annex Table A	Processes	Level A	Level B	Level C	Level D	Verifications
A-1	Software Planning	7	7	7	2	2
A-2	Software Development	7	7	7	7	
A-3	Verification of Software Requirements	7	7	6	3	7
A-4	Verification of Software Design	13	13	9	1	13
A-5	Verification of Software Coding & Integration	9	9	8	1	9
A-6	Testing of Outputs of Integration	5	5	5	3	5
A-7	Verification of Verification Results	9	7	6	1	9
A-8	Software Configuration Management	6	6	6	6	
A-9	Software Quality Assurance	5	5	5	2	
A-10	Certification Liaison	3	3	3	3	
Total		71	69	62	29	45

< 항공기 분야 SW안전가이드>

▲ 무인비행체 안전 확보를 위한 지침 현황

안전한 무인비행체 SW 개발을 위한 프로세스 구축

안전성을 보장하는 SW 개발 체계를 위해 먼저 개발 프로세스를 구축했다. NIPA에서 발간한 'DO-178C 기반 항공기 분야 SW안전가이드(2020, NIPA)'는 국제 수준의 무인비행체 SW 안전성을 확보하는데 매우 유용했다. 항공분야에 종사하는 중소기업에서 DO-178C를 적용하는데 필요한 가이드로, DO-178C에서 요구하고 있는 SW 개발 생명주기별 산출물 작성 시 필요한 구체적인 수행 지침과 산출물 예시를 제공하고 있어 이를 활용하면 SW 개발 과정에서 발생할 수 있는 많은 부담을 줄여준다. 이를 활용해 용비에이티는 비행제어소프트웨어(FCS, Flight Control Software) 개발 과정에'SW안전가이드'를 적용함으로써 개발 산출물과 검토 체크리스트를 포함하는 무인비행체 SW 개발 프로세스를 구축할 수 있었다. 이는 총 9개의 프로세스 단계로 구성되어 있는 개발지침서 1세트와 산출물 템플릿 22종, 프로세스와 산출물 검토 체크리스트를 포함하고 있다.

No	DO-178C Documents	약자	문서명	비고
1	Plan for Software Aspects of Certification	PSAC	SW 인증 계획서	
2	Software Development Plan	SDP	SW 개발 계획서	
3	Software Verification Plan	SVP	SW 검증 계획서	
4	Software Configuration Management Plan	SCMP	SW 형상관리 계획서	
5	Software Quality Assurance Plan	SQAP	SW 품질보증 계획서	
6	Software Requirement Standards	SRStd	SW 요구사항 표준서	
7	Software Design Standards	SDStd	SW 설계 표준서	
8	Software Code Standards	SCStd	SW 코드 표준서	
9	Software Requirement Data	SRD	SW 요구사항 명세서	SRS
10	Design Description	DD	SW 설계 기술서	SDD
11	Source Code			
12	Executable Object C			
13	Software Verificatio			
14	Software Verificatio			
15	Software Life Cycle			
16	Software Configurat			
17	Problem Reports			
18	Software Configurat			
19	Software Quality As			
20	Software Accomplis			
21	Trace Data			
22	Parameter Data Iten			

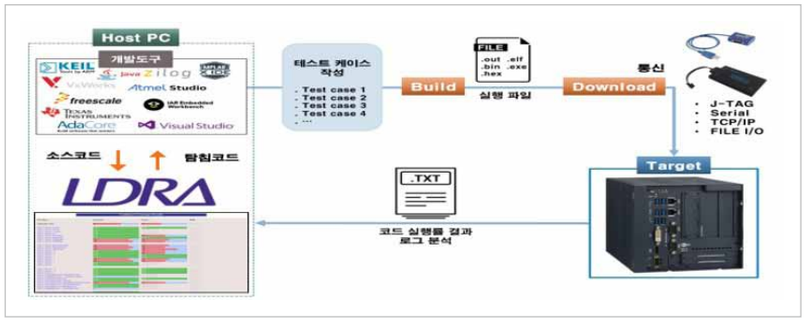
No.	Checklist
1	Appendix A: Software Planning Review Checklist
2	Appendix B: Software Requirements Review Checklist
3	Appendix C: Software Preliminary Design Review Checklist
4	Appendix D: Software Critical Design Review Checklist
5	Appendix E: Software Code Review Checklist
6	Appendix F: Integration Review Checklist
7	Appendix G: Software Verification Review Checklist
8	Appendix I: Peer Review Checklist - Planning
9	Appendix J: Peer Review Checklist - Requirements
10	appendix K: Peer Review Checklist - Design
11	Appendix L: Peer Review Checklist - Code
12	Appendix M: Peer Review Checklist - Integration
13	Appendix N: Peer Review Checklist – Test Procedures
14	Appendix N: Peer Review Checklist – Test Results

▲ 소프트웨어 개발 프로세스 및 기법/산출물

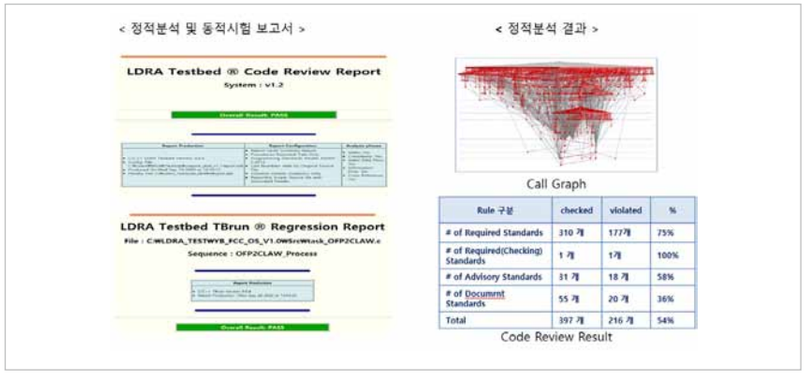
Target 기반의 시험 자동화 적용

무인비행체에 탑재되는 비행제어소프트웨어(FCS, Flight Control Software)를 시험하기 위해서는 타겟 기반의 시험환경을 구축하고 안전 요구사항 기반의 시험을 수행해야 한다. DO-178C에서 안전등급 A 수준의 시험 충분성 기준은 문장 커버리지[2], 분기결정 커버리지[3], 다중조건/결정 커버리지[4], 데이터 커플링(Data Coupling), 제어 커플링(Control Coupling)의 5 가지 구조적 커버리지를 모두 달성하도록 요구하고 있다. 이러한 시험 충분성을 달성하기 위해서는 SW 시험 자동화 도구를 도입해 시험환경을 구축하고, 시험 케이스를 도출하고, 시험을 수행해야만 한다. 이를 위해 테스트 자동화 도구인 LDRA Tool Suite을 도입해 자동화된 시험 환경을 구축하는 성과를 거뒀다. LDRA Tool Suite은 항공기 SW 감항 인증을 받은 제품이며 모든 산업 분야의 SW 안전성 검증을 지원하는 도구이다. 용비에이티는 이를 활용해 소스코드에 대한 코딩 규칙 검사와 타겟 기반의 동적시험을 통해 소스코드에 대한 구조적 커버리지를 확인하고 SW요구사항에 대한 추적성을 확보할 수 있었다.

2) 문장 커버리지(Statement Coverage) : 프로그램을 구성하는 모든 구문이 실행되도록 테스트 하는 방법
3) 분기결정 커버리지(Decision Coverage) : 프로그램 내 모든 분기문을 테스트 하는 방법
4) 다중조건/결정 커버리지(Modified Condition/ Decision Coverage) : 개별 조건식이 다른 개발 조건식에 영향을 받지 않고 전체 조건식에 독립적으로 영향을주도록 하는 테스트 방법



▲시험 자동화 체계



Rule 구분	checked	violated	%
# of Required Standards	310 개	177개	75%
# of Required(Checking) Standards	1 개	1개	100%
# of Advisory Standards	31 개	18 개	58%
# of Documnt Standards	55 개	20 개	36%
Total	397 개	216 개	54%

▲시험 수행 결과

무인비행체 비행제어SW의 안전성 인증 획득

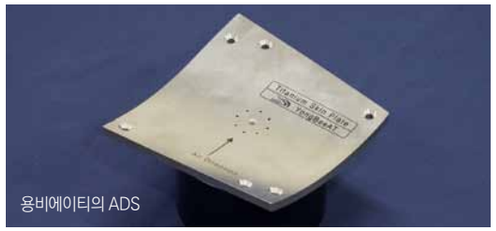
무인비행체의 안전성에 대한 확실한 증명은 인증 자체를 획득하는 것이다. 지금껏 수립한 개발 프로세스와 자동화된 시험을 통해 용비에이티가 가진 무인비행체 비행제어 SW에 대한 안전성을 확보했고 이를 검증받기 위해 RTCA DO-178C에 대한 인증(Complinace)을 준비하였다. 인증 절차는 DO-178C 기준의 산출물 작성과 활동 수행 결과에 대해 DER(FAA 인증심사원:Designated Engineering Representative)의 검토의견을 받아 필요한 시정조치를 완료한 후 이를 확인하여 FOPC(Finding of Process Compliance)를 받는 절차로 진행되었다.

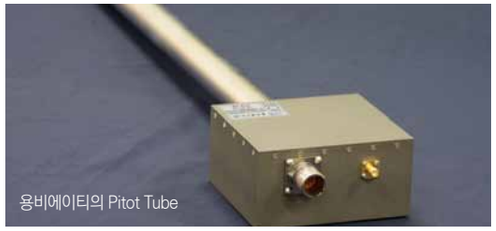
DER 검토는 SW 리뷰 체크리스트를 사용하여 각 단계별 산출물과 활동 결과가 DO-178C 목표에 부합하는지를 체크하고 이에 대한 코멘트 리포트를 발행하게 되는데, SW 개발 조직에서는 이같은 지적사항에 대한 조치를 수행하고 조치결과를 다시 DER에 제출, 확인받는 과정을 반복하게 된다. 용비에이티는 3번에 걸친 DER 검토 및 코멘트 리포트에 대한 조치를 완료한 후 마침내 비행제어 SW에 대한 FOPC(Finding of Process Compliance)를 획득하게 되었다.

▲RTC /DO-178C Level A 인증

> *SW안전이 무엇인지*
> *알 수 있는 계기가 되었다.*
> *조금만 살핀다면 사전에*
> *적은 노력과 시간으로 SW 안전을*
> *제공할 수 있다고 생각한다.*


용비에이티의 FLCC


용비에이티의 ADS


용비에이티의 Pitot Tube


용비에이티의 FCS

참여자 소감 “필요한 시점에 LDRA를 적용함으로써 프로그램의 오류 및 신뢰성 검증이 무사히 진행될 수 있었다.”

“생각하지 못한 코드 상 버그, 발생할 수도 있는 버그, 사용하지 않는 불필요한 코드를 제거할 수 있어 무인항공기/드론에 적용되는 코드가 한층 더 신뢰성을 확보할 수 있게 됐다.”

향후 계획 모든 산업 분야에서 안전은 매우 중요한 키워드이지만 특히 하늘을 나는 항공 산업에서 안전을 빼놓고 제품을 논할 수 없다. 과거에는 HW 중심의 안전을 강조했지만 현재는 SW 안전이 더욱 중요해지고 있다. 이같은 상황에서 무인비행체 비행제어 SW로 국제 안전성 인증을 획득함으로써 용비에이티는 SW 안전 품질을 한층 더 높일 수 있게 됐다.

특히 국내외 안전 표준에 적합한 개발 프로세스를 구축하고, 자동화 시험 도구를 적용하고, SW 안전성 검증을 위한 시험 및 품질 인력의 역량 향상을 이루는 성과를 거뒀다. 앞으로 항공기 감항 인증 관련 SW 개발사업 뿐만 아니라 국방항공 사업에 참여해 무인비행체의 비행제어 SW 분야에서 최고가 되는 것이 이 회사의 목표이다.
용비에이티 관계자는“현재 무인비행체 자동 제어 시스템, 지상 제어 시스템, PILS / HILS 시뮬레이터 등 무인항공기를 운용하면서 쌓은 기술력에다 새로운 플랫폼에 맞는 개선된 비행 제어 시스템과 센서 데이터를 바탕으로 앞으로 SW 안정성을 높이고 운용성을 획기적으로 개선하는 기술을 개발할 것”이라고 밝혔다.

이를 통해 시장이 급성장하고 있는 무인비행체 시장에서 새로운 플랫폼에 적용할 수 있는 비행제어 시스템을 제공하는 한편 보안성 문제로 중국산 비행 제어 시스템 사용이 금지된 상황에서 국산 비행제어 시스템과 안정성을 높힌 SW를 통해 시장 점유율을 높인다는 계획이다.

OSSTEM IMPLANT

국내 1위를 넘어 디지털 치과 SW의 글로벌 리더!

25개국 진출해 글로벌 경쟁…치과 진료의 토탈 솔루션 제공 목표
SW 개발 안전 프로세스 정립해 디지털 치과 솔루션의 품질고도화 구현

▲ '세계속의 임플란트 전문기업' 오스템임플란트 엄태관 대표

오스템임플란트 기본 정보

회사명	오스템임플란트	전화번호	02-2016-7000
대표자명	엄태관	홈페이지	http://www.osstem.com/
설립연도	1997. 1. 8	종사자	1,885명(2020년 8월 기준) 3,682명(2019년 12월, 글로벌 임직원수 기준)
주소	서울시 강서구 마곡중앙12로 3		
주요제품	Digital Dentistry Solution		

오스템임플란트는 임플란트, 치과치료 기자재 제조/판매, 치과의원용 SW, Digital Dentistry Solution 기술을 개발·공급하는 기업이다. 2015년 생산액 기준 국내 1위 의료기기 제조사로 자리매김했으며 아시아 1위 및 글로벌 세계 5위 임플란트 기업으로 성장했다. 지속적인 연구개발(R&D) 투자와 브랜드 가치 상승을 통해 2036년 매출 10조원을 달성, 세계 1위 기업으로 올라선다는 목표를 세우고 있다.

오스템임플란트는 지난 2006년 글로벌 시장에 처음 진출해 현재 28개국에서 70개 해외법인을 운영하고 있다. 해외 진출 초기 현지 기업들과의 치열한 경쟁을 통해 기반을 마련했으며 지난 15년간 꾸준한 역량 강화를 통해 최근에는 글로벌 경제의 중심축이라 할 수 있는 미국과 중국 현지에서도 영업이 호조를 보이고 있다. 이에 따라 미국, 중국, 러시아, 대만 등 대형 해외법인의 매출 역시 지속적으로 성장할 것으로 기대된다.

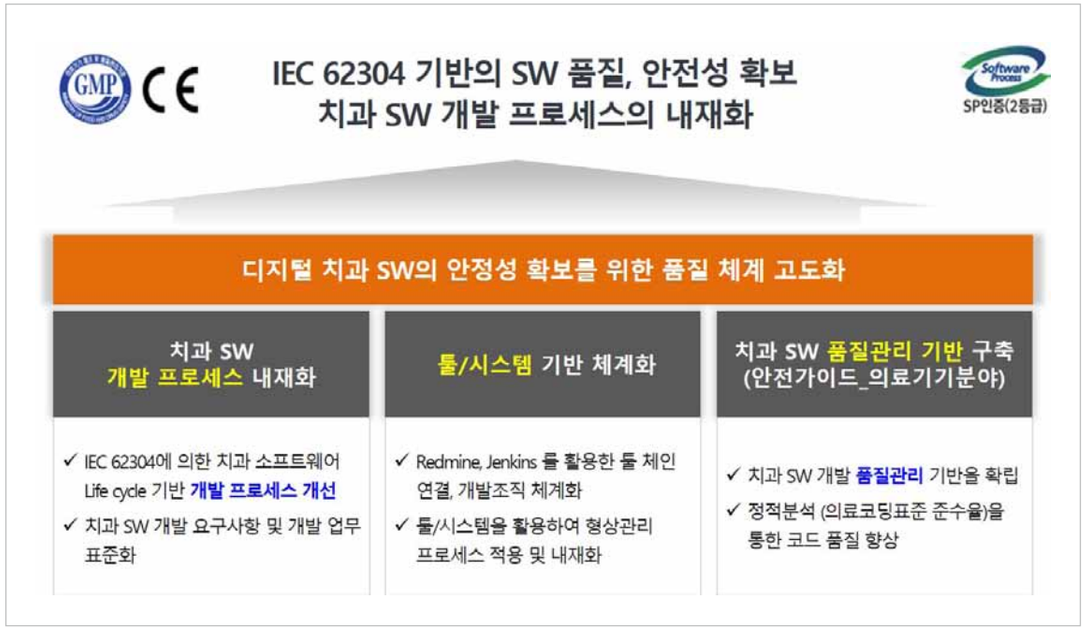
이같은 성과를 바탕으로 오스템임플란트는 앞으로 치과에서 필요한 다양한 품목군을 직접 제조, 공급하는 치과계 토탈 솔루션 제공 회사를 목표로 사업구조 고도화를 준비하고 있다. 치과 IT 사업의 경우 1997년 회사 설립 후 지속적인 연구개발을 통해 치과 IT 기술의 보급 확산을 이루었고 그 결과 국내 치과 청구 SW 및 치과관리 SW 시장의 75% 이상을 점유하고 있다. 또한 IT 기술기반의 Digital Dentistry Solution 기술 개발을 위해 디지털 영상처리 기술, 3D 영상 구성 및 처리 기술, 덴탈 CAD를 위한 그래픽 기술을 연구하고 있으며 SW뿐만 아니라 3D 구강 스캐너 및 모델스캐너와 같은 HW 연구개발에도 박차를 가하고 있다. 특히 웹기반 고객서비스와 모바일 통합 서비스를 통해 언제 어디서든지 치과와 고객을 관리할 수 있는 서비스도 함께 제공하고 있다.

의료	적용 표준	적용 안전 기법(Techniq & Measure)
	IEC62304, IEC29119	• 안전성 확보를 위한 오스템임플란트만의 개발 프로세스 수립 • 개발 프로세스와 연계된 툴 체인 확보(CI환경, 형상관리, 테스트) • 소스코드의 신뢰성 강화를 위한 자동화된 정적분석 환경구축

높은 신뢰성과 안전성을 요구하는 Digital Dentistry Solution

하지만 오스템이 미래 시장을 대비하기 위해 필요한 과제들도 적지 않았다. Digital Dentistry 솔루션은 의료기기 SW의 특성상 높은 신뢰성과 안전성이 필요하다. 그런 만큼 국내외 제조 및 판매를 위한 인허가 규정준수가 필수이며 SW에 대한 품질요구 사항이 까다로운 편이다. 또한 오스템임플란트가 선보인 치과용 임플란트, 치과용 장비(CT/파노라마 등의 영상장비, 치과용 유니트체어), 치과재료 등의 경우 20여 개 국가에 수출되고 있는 만큼 디지털 치과 솔루션(CT Viewer, Implant Guide SW, 교정진단/치료계획 SW 등)의 글로벌 경쟁력 강화가 반드시 필요한 상황이었다.

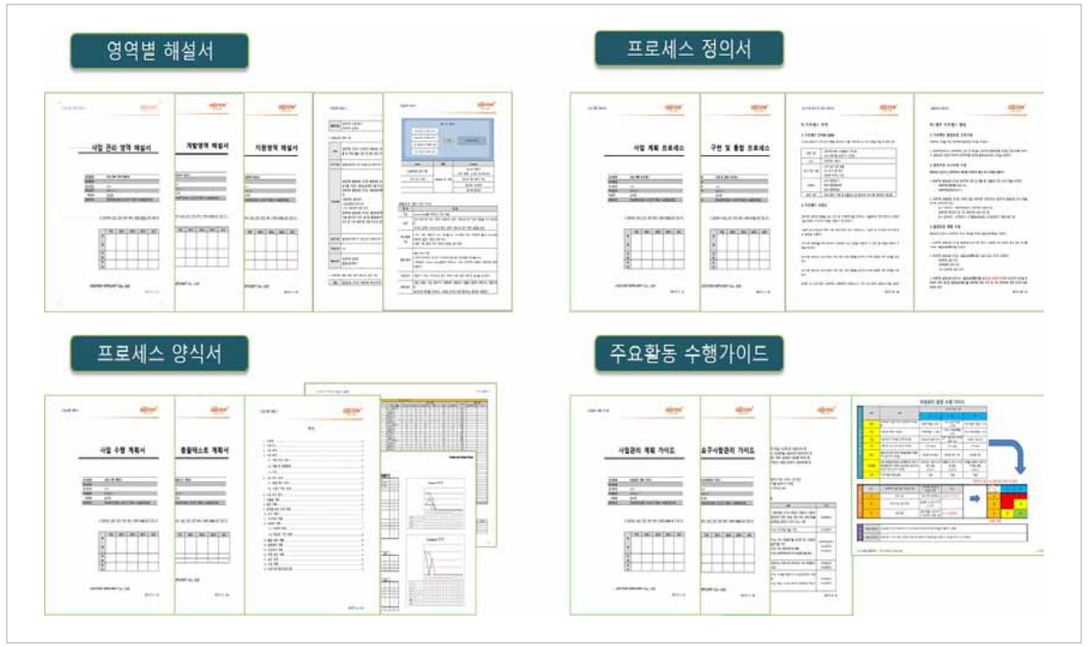
이를 위해 2009년 EU의 의료용구지침 적합성 보증을 위한 교정치료/진단 SW '브이셉(V-Ceph)'제품이 CE와 ISO13485 인증을 획득했으며 북미 수출을 목표로 FDA 인증도 준비한 바 있다. 더 나아가 오스템의 Digital Dentistry Solution의 품질경쟁력 강화 및 품질시스템 고도화를 실현하기 위해서는 IEC62304 기반 의료기기 SW 개발 프로세스에 대한 내재화가 반드시 요구되었다.



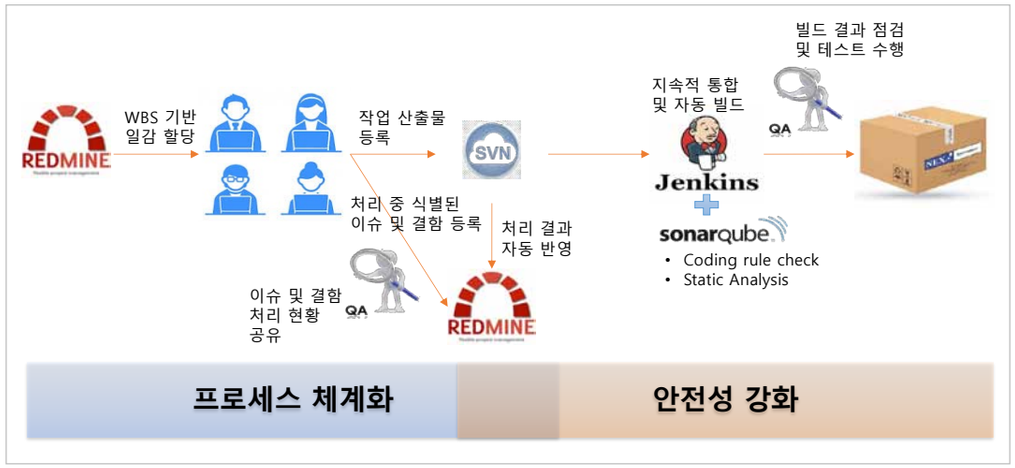
▲ Digital Dentistry Solution 안전성 확보를 위한 목표 수립

Digital Dentistry Solution의 안전성 확보를 위한 개발 프로세스 수립

그러나 솔루션 개발을 담당하는 SW제품연구소의 역량을 분석한 결과 체계적 SW 프로세스 이해가 부족하고, 형상관리, 품질보증, 테스트 프로세스가 취약한 것으로 파악되었다. 이에 SP 프로세스와 테스팅 표준(ISO/IEC29119)을 기반으로 의료기기용 SW 개발 표준(IEC 62304)을 포함하는 활동을 정의함으로써 SW 제품의 신뢰성과 안전성을 확보할 수 있도록 했다. 특히 업무 프로세스에 대해 충분한 인터뷰와 자료조사를 거쳐 디지털치과 SW 개발 프로세스와 영역별 해설서, 주요 활동 수행 가이드, 프로세스별 양식을 마련했으며 리뷰를 통해 개선점을 도출하고 이를 반영한 디지털치과 SW 개발 프로세스를 정립할 수 있었다.



▲ 디지털치과 SW 개발 프로세스 및 가이드/양식(총 90종)



▲ 가시화(Visualization) 툴체인의 모습

개발 프로세스와 연계된 툴 체인 확보

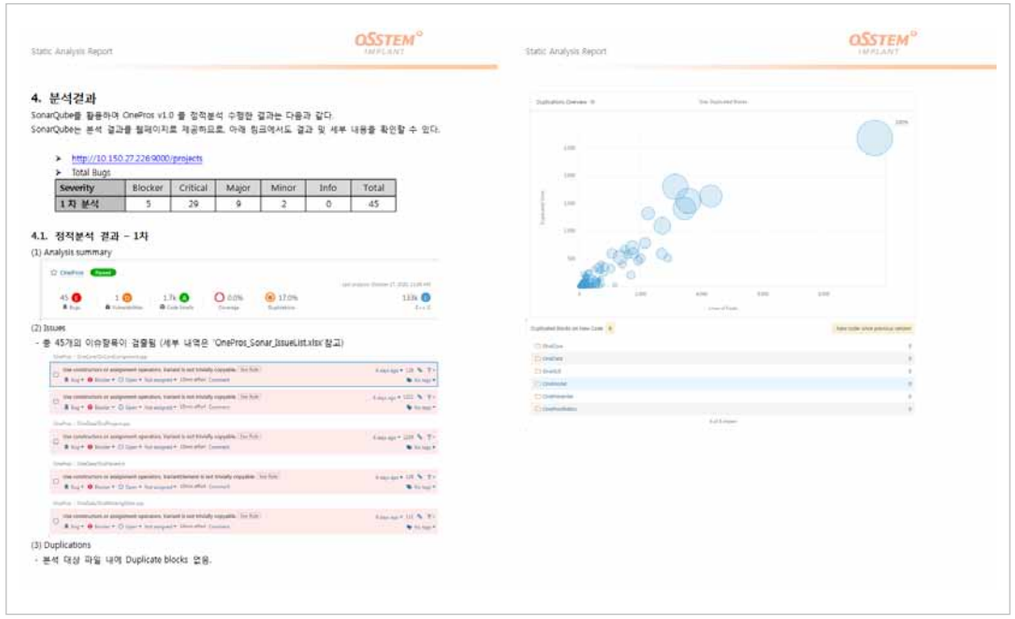
안전한 SW를 개발하기 위한 프로세스가 만들어져 있다하더라도 프로세스는 빠른 시간에 내재화되기 어렵다. 오스템은 이러한 문제를 해결하기 위해 기존에 활용 중인 redmine과 SVN, jenkins를 이용하여 CI[1] 환경을 구축하고, SW 단위 검증 도구인 SonarQube를 도입하여 정적분석과 코딩 rule 체크 결과에 대한 자동화 인프라를 구성했다. 테스트 결함에 대하여 개발팀과 QA팀의 협업 절차를 Redmine에 정의함으로써 코드의 안전성을 확인할 수 있는 가시화된 인프라를 구축한 것이다. 이를 통해 개발자들의 코드들을 통합 관리하고, 1일 단위의 지속적인 빌드를 수행하여 배포가 가능한 코드를 유지하도록 하였으며, 통합된 코드에 대한 현황 모니터링과 지속적인 결함 개선 작업을 수행할 수 있게 되었다.

1) CI(Continuous Integration) : 지속적 통합이 가능한 개발 환경. 모든 소스코드를 개발 완료후 한꺼번에 통합하는 것이 아니라 주기적으로 수행함으로써 통합시 발생하는 오류를 사전에 해결하기 위한 개발 환경

개발자가 직접 소스코드의 안전성 강화를 위한 정적분석 적용

개발된 제품의 안전성을 확보하기 위해 분석/설계/구현/테스트의 각 단계를 어떻게 진행할지, 어떤 산출물을 작성할지, 어떤 기법을 사용할지 등과 같은 프로세스 적용은 매우 중요하다. 그러나 분석/설계단계를 지나 개발단계를 진행함에 있어서는 소스코드에 대한 안전성과 기능성을 확인할 수 있는 것이 훨씬 더 중요하다.

이전에는 개발된 소스코드에 대한 검증은 테스트로만 확인할 수 있다는 생각을 가지고 있었지만 기 구축한 CI환경에 빌드시 정적분석을 자동으로 수행함으로써 소스코드의 품질을 확보할 수 있음을 확인했다. 이를 위해, SonarQube를 도입하였고 코딩 룰 체크, 보안 규칙 지원, 실행 시간 버그 찾기 등을 수행했다. 또한 정적분석 모니터링을 위해 플로우 기반 정적분석과 메트릭스 분석을 수행하였으며 이를 Jenkins를 활용해 가시화할 수 있었다.



▲ 정적분석 결과

> *치과환자정보, 진료정보의 안전한 관리를 위해 정적분석, 동적분석이 필요했는데, SW 품질 프로세스 구축과 안전 컨설팅을 통해 큰 도움을 받았다.*

참여자 소감 “컨설팅을 통해 SW 프로세스를 구축하였고 이 과정을 통해 SP 인증을 취득하게 되었다. 안전 프로세스를 체계적으로 준비하는 계기를 마련한 것에 큰 의미를 두고 있다.”

“사내에서 SW를 부가 서비스로 인식하는 시각이 있었기 때문에 SW 시각화(Visualization) 체계를 구축하는 건 쉽지 않은 일이었다. 경영진의 지원이 필수적인 상황이었는데 이번 과제를 통해 연구소장이 관심을 갖고 환경을 조성해주었으며 실제 진행과정에 적극적으로 참여하는 계기가 되었다. 특히 SW 프로세스 개선을 통한 단기, 중기 효과에 대해 직원들과 집중적으로 소통함으로써 프로세스 개선 및 자동화 필요성에 대한 공감대와 동기부여를 이룰 수 있었다.”

“디지털 치과 솔루션은 의료기기 인허가 필수이므로 국내의료기기 인증 및 CE는 취득했지만 기업 내에 의료기기SW 안전가이드 기반 프로세스는 내재화되지 않은 상태였다. 그 결과 지속적인 리팩토링 수행 과정 시 코딩 표준 룰이나 보안 지침을 위배하는 코딩이 증가하고 SW품질이 저하되는 문제가 발생했다. 치과 SW 특성상 환자정보 보호, 진료정보 보호를 위한 코드 보안 적용이 필요했는데 SW 품질 프로세스 구축과 안전 컨설팅을 통해 제품 품질향상에 큰 도움을 받았다.”

향후 계획 오스템임플란트는 과제수행을 통해 확보한 프로세스와 솔루션을 기반으로 솔루션 개발 프로세스를 표준화한 후 이후 개선 활동을 지속적으로 추진하고 있다. 툴 체인 기반의 회귀 테스트 자동화 및 정적 분석 도구를 순차적으로 도입, 적용해 제품 품질향상을 위해 노력하고 있다.

SW제품연구소장인 김승기 전무는“치과 솔루션 선두 주자로서, 향후 치과 진료 분야의 디지털화를 추구하는 디지털 덴티스트리 시장에서 글로벌 경쟁력을 확보하는 것이 목표”라며 “국내 시장에서 확고한 우위를 선점한 후 해외 SW업체와의 경쟁에서도 앞서나갈 것”이라고 말했다.

오스템임플란트는 의료분야 SW 오동작으로 인한 안전성 위협에 적극적으로 대응하기 위해 이후 안전성 확보를 위한 프로세스를 체계화하고 이를 산출물의 형태로 반영할 수 있도록 관련 업체와의 협업을 지속 추진해나갈 방침이다.

범아기전(주)

열차상태 정보 실시간 전송으로 철도 안전을 지키는 파수꾼

범아기전, HW에서 탈피해 기차 상태정보 전송 등 SW 업체로 변신
SW 안전 위해 SIL2 인증 추진…몽골 철도 현대화 사업 '노크'

▲'철도차량 부품 생산 전문기업'범아기전 남상헌 대표(하단 좌측에서 세번째)

범아기전 기본 정보

회사명	범아기전	전화번호	031-353-3074
대표자명	남상헌	홈페이지	http://bumahltd.co.kr
설립연도	1975. 9월	종사자	50명
주소	경기도 화성시 향남읍 한두골안길 87-2		
주요제품	철도차량 전장품		

범아기전은 45년 전통의 철도 차량부품 생산업체로서 캡 모듈, 하네스 모듈, 데스크 모듈, LB박스, 전자개폐기, 브러시 홀더 등 열차 하드웨어를 주력 제품으로 생산해왔다. 최근 사업다각화의 일환으로 부품·소재 중심의 HW 제조업에서 철도 소프트웨어 개발 분야로의 진출을 모색하고 있는데 그 일환으로 2016년부터 2019년까지 철도 관련 국책 과제 2개를 수행하기도 했다. 달리는 열차 안의 장치 상태 관련 데이터를 열차 관제센터에 실시간으로 전달해주는 열차상태정보 실시간전송장치(TSMD: Train Safety Monitoring Device) 개발과 전자식 입출력 접점방식의 철도차량 배선절감 로직회로 개발 사업이 바로 그것이다.

범아기전이 만든 TSMD는 철도안전 관제실로 철도 차량 내 운행정보와 상태정보를 실시간으로 제공함으로써 사고 위험성 및 사고 발생시 적절한 대응을 할 수 있도록 돕기 위해 고안된 기술이다. 범아기전이 처음 이 제품을 기획해 개발에 들어간 당시만 해도 국내에는 관련 제품이 없었으나 현재는 유사한 기능의 제품이 출시되어 있는 상태다. 그러나 타사 제품이 TCMS(Train Control and Monitoring System)등 기존 운행 장치의 차량제어에 직접적으로 개입해 데이터를 전송받는 데 반해 범아기전의 접근 방식은 열차 내부의 상태정보를 중간에서 스니핑(Sniffing)하여 안전관제실로 실시간 무선 전송을 한다는 점에서 차별성이 있다.

범아기전은 이 TSMD 제품을 가지고 한국국제협력단(KOICA) 공적개발원조(ODA) 사업인 '몽골철도교통인프라 현대화 마스터플랜 수립 및 통합 통제 시스템 구축' 프로젝트에 참여할 예정인데 이를 위해서는 안전인증 획득이 필수적으로 요구되는 상황이었다.

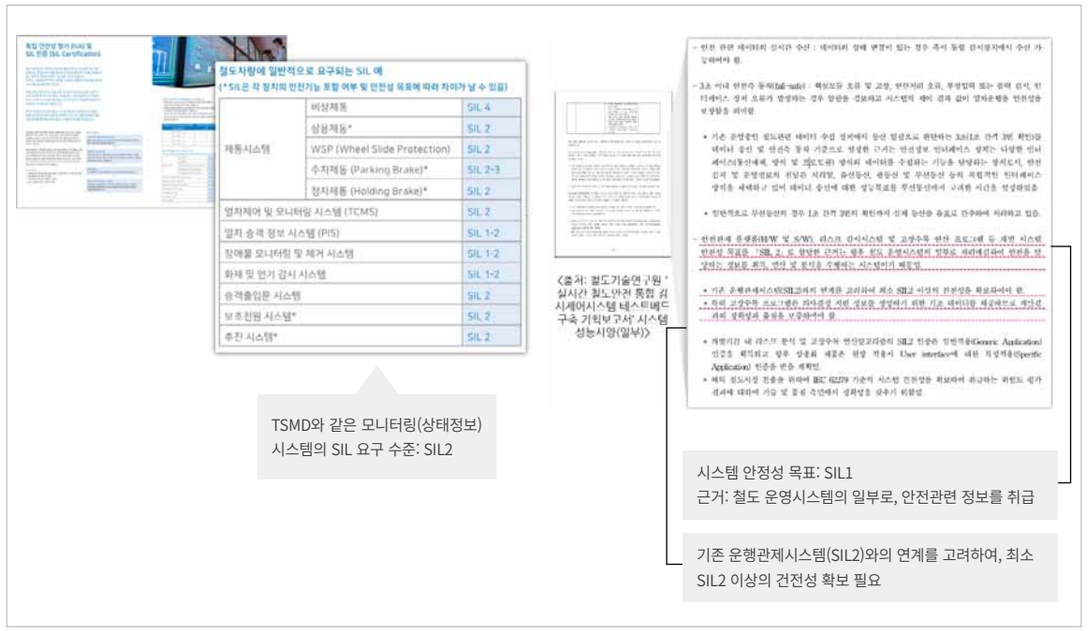
철도

적용 표준	적용 안전 기법(Techniq & Measure)
IEC62279	• 모든 위험원을 고려하여 안전하게 개발하기 위한 프로세스와 위험 분석 수행 • SW 품질 검증을 통한 솔루션의 품질은 확보 및 요구사항 관리 실시 • 품질보증기법 적용을 위한 정적 분석 도구 활용과 형상관리 도구 적용

안전한 TSMD 제작을 위해 당면한 이슈들

안전 인증은 최근 철도관련 사고 및 인명 피해가 증가하고 있는 상황에서 더욱 중요해지고 있다. 특히 4차 산업혁명의 흐름으로 SW 중요성이 커지는 만큼 SW 오류로 인한 문제점에 대한 인식도 높아지고 있는 상황이다. 철도, 원자력 등 다양한 분야에서 안전성 평가를 수행하고 있는 'TÜV 라인란드'에서는 TSMD와 같은 제어 및 상태 모니터링 시스템의 SIL 요구 수준을 SIL2로 정의하고 있고, 국내 철도기술연구원에서는 TSMD를 포함한 '실시간 철도안전 통합 감시제어시스템'의 시스템 성능사양에서 관련 SW의 안전성 수준을 SIL2로 규정하고 있다.

범아기전은 몽골 철도 현대화 사업 참여의 가능성을 높이고 TSMD의 수출 경쟁력을 향상하기 위해 솔루션의 품질과 안전성을 향상하는 것이 필요하다고 보고 SIL2 수준의 안전성 인증 획득을 추진키로 했다. 이를 위해 국제표준(IEC 62279)에 부합하는 체계적인 SW 개발 체계 및 인프라 구축과 이를 내재화하는 작업이 시급한 상황이었다.



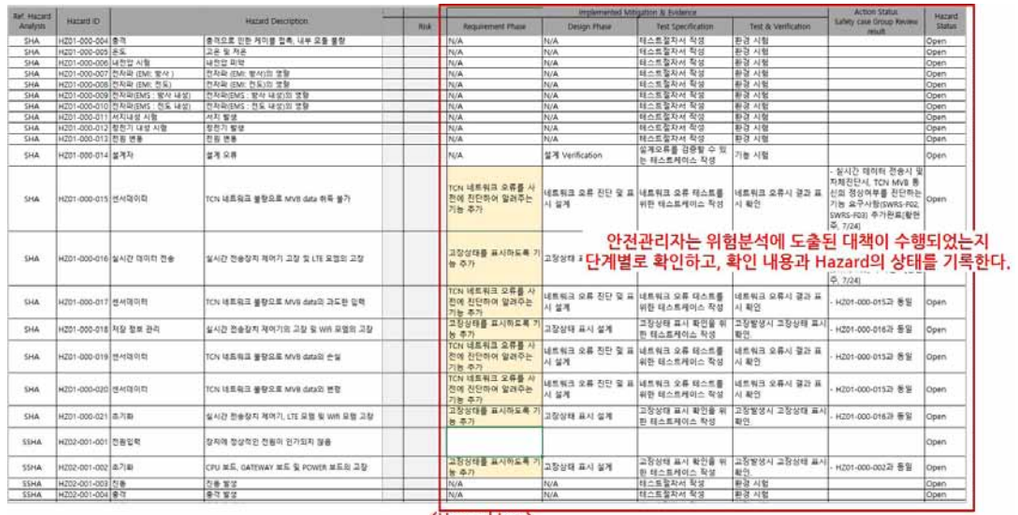
▲ 국내/국외 철도 관련 SW에 대한 안전성 수준요구 내용

모든 위험원을 고려한 안전한 개발에 초점

먼저 컨설턴트와 함께 TSMD 솔루션에 대한 안전성 검증 및 위험관리체계를 확인했다. 그동안 Hazop[1] Study를 통해 Hazard를 식별·분석한 후 Risk 평가에서 안전성 분석을 수행하고 있었지만 개발기간 동안의 설계변경 사항에 대한 안전성 분석은 진행되지 않고 있었음이 확인됐다. Hazop 보고서의 내용에는 시스템(SW)의 품질을 위해 반드시 예방해야 하는 오류 또는 수행되어야 하는 오류 예방 활동이 중심으로 적혀있긴 했지만 안전을 위한 내용은 아니었다.

따라서 Hazard Log를 통해 안전대책들이 조치되었는지 확인할 필요성이 대두됐고, 시험항목이나 기능요구사항 반영을 통해 시험결과를 확인하는 활동이 수행될 필요가 있었다. 이에 SW 품질 및 안전관리자가 시스템개발 생명주기동안 안전에 영향을 미치는 변경을 관리할 수 있도록 보장을 공식화했으며 기 분석된 Hazard의 Hazard Log를 만들고 단계별 조치여부를 기록/관리함으로써 위험원에 대한 분석 및 대응 활동이 개발 주기동안 일관성있게 진행될 수 있도록 하였다.

1) HAZOP(Hazard and Operability): 공정에 존재하는 위험요인과 공정의 효율을 저해 할 수 있는 운전상의 문제점을 찾아내어 그 원인을 제거하는 방법



▲ 위험분석에 대한 추적관리

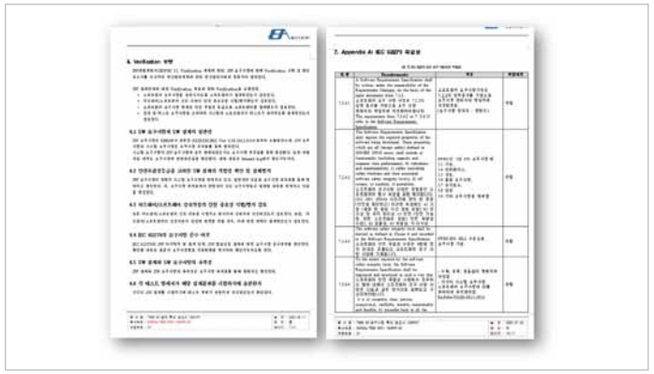
SW 품질 검증을 통한 솔루션의 품질 확보에도 만전

안전인증을 획득할 때 평가자가 가장 중요하게 점검하는 활동은 단계별 품질 활동이다. 범아기전은 조직의 품질관리 역량을 높이기 위해 품질관리 역량이 뛰어난 관리자를 선임해 품질보증 기법 및 활동을 수행하는 품질관리체계를 수립했다. 품질관리자의 역할, 품질관리 계획, 절차, 검증(Verification), 확인(Validation) 활동에 대한 교육을 실시했으며 SIL2 수준에서 요구하는 조직의 품질보증기법 중 추가해야 할 항목을 선정하여 적용했다.

IEC 62279의 요구사항을 반영해 산출물별 체크리스트와 동료 검토를 통한 품질검토를 수행하는 것은 물론 요구사항이 생명주기의 모든 단계에 적용되었음을 추적하고, 품질 향상을 위한 품질관리 지표 정의 및 지속 측정을 통해 확인이 가능하도록 하였다. 특히 품질관리자는 단계별 검증 활동을 수행한 후 리포트를 작성하고, IEC 62279의 관련 요구사항에 대한 적합성 여부를 검토한 결과는 부록으로 첨부하도록 했다.

SW품질보증기법 (표 별첨 6-9) 기법 및 대책		참조	SIL Level					현황 및 개선사항
			0	1	2	3	4	
1	ISO 9001 인증		R	HR	HR	HR	HR	• 필수: 품질경영시스템 인증서 확인
2	ISO 9001 준수		M	M	M	M	M	• 필수: 품질경영시스템에 따라 내부 심사 후 보고서를 제출했음.
3	ISO/IEC 90003 준수		R	R	R	R	R	
4	회사 품질 시스템		M	M	M	M	M	• 필수: 범아기전(주) 품질보증 매뉴얼(BAQM - 9001) 있음.
5	소프트웨어 형상 관리	별첨 7-48	M	M	M	M	M	• 필수: 적용 필요
6	체크리스트	별첨 7-47	R	HR	HR	HR	HR	• 필수: 적용 필요
7	추적성	별첨 7-58	R	HR	HR	M	M	• 필수: 적용 필요 → 요구사항이 생명주기의 모든 단계에 적용되었음을 추적
8	데이터 기록 및 분석	별첨 7-12	HR	HR	HR	M	M	• 필수: 적용 필요 → 품질목표와 정량지표를 정의하여 달성여부를 관리

▲ SIL2에서 요구하는 SW품질보증기법



▲ Verification Report의 IEC 62279 적합성 검토 내역

안전 가이드라인 내 품질보증기법 적용을 위한 도구

이와 함께 프로세스 관리 도구 , 의사소통 지원 도구를 포함해 안전 가이드라인의 품질보증기법 요구 필수 도구인 형상관리 도구를 적용했다. 또 상대적으로 적용이 어렵지 않으면서도 효과가 입증된 정적분석 도구도 함께 포함시켰으며 개발자의 통합개발환경(IDE)에 적용함으로써 개발 시 주기적으로 수행할 수 있도록 했다.

JIRA를 활용해 프로세스의 진행상태(할일, 진행 중, 완료)를 직관적으로 알 수 있는 칸반보드로 프로세스 가시성이 향상되었고 시스템과 관련된 형상(소스코드, 개발툴, 설계서 등)을 Subversion 통해 형상관리함으로써 안정된 유지보수가 가능하도록 했다. 또한 Confluence를 활용해 사내 표준 프로세스를 공유하면서 동시에 사내 게시판으로도 활용하고 있어 정보 공유가 활성화되었다.

개발자의 경우에는 IDE[2]에 설치된 CppCheck Plugin으로 개발단계 또는 유지보수 시 주기적으로 정적분석을 수행할 수 있다. 이밖에 복잡도 분석을 위해 NSIQCollector를 통해 복잡도가 상대적으로 높은 몇 개의 모듈을 대상으로 코드 개선작업을 수행하는 성과를 거뒀다.

2) IDE(Integrated Development Environment): 효율적으로 소프트웨어를 개발하기 위한 통합개발환경 소프트웨어 애플리케이션 인터페이스

▲ 안전가이드라인의 품질보증기법 요구 필수 도구

> *SW안전기술 확보를 바탕으로*
> *글로벌 시장으로 진출,*
> *100년 기업의 꿈을 향해*
> *나아간다는 계획이다.*

참여자 소감 “컨설팅 업체인 ㈜나이스컨설팅과의 협업이 정말 좋았다. 담당 컨설턴트가 일주일에 한 번씩은 꼭 회사에 방문해 장시간 교육 및 컨설팅을 해주었고 평소에도 수시로 비대면 상담을 통해 궁금한 내용들에 대해 친절하게 설명해 주었다. 호흡이 잘맞아 컨설팅 받는 내내 즐거웠고 도움이 많이 되었다. NIPA에 주관한‘SW 안전가이드 활용교육’을 통해 시스템 SW 안전성 교육을 받았던 것도 기억에 많이 남는다. 모 병원에서 항암치료 시 방사선 세기를 조절하는 SW프로그램이 잘못되어 한 환자가 항암 치료 도중 방사선에 장시간 노출된 나머지 사망에 이르게 된 사례를 들었을 때 충격을 받았다. SW 개발자로서 정말 안전한 SW를 만들어야겠다는 다짐을 새롭게 하는 계기가 됐다. 다만 사업기간이 2020년 5월부터 11월까지 7개월밖에 되지 않아 사내에 SW 공학기술의 내재화를 안정적으로 구현하기에는 너무 짧다는 아쉬움이 있다. 다음 해(앞 프로젝트 기간과 연관됨)에도 연속성을 가지고 현장적용 지원을 받을 수 있었으면 좋겠다.”

- 범아기전 기술연구소 황현주 수석연구원

향후 계획 범아기전은 올해 과제 수행으로 SP 인증획득을 통해 수행기관의 역량 내재화를 달성하고 이를 바탕으로 열차 상태정보 실시간 전송장치의 고도화를 통한 안전 인증을 획득할 예정이다.

또한 몽골 철도 현대화 사업을 성공적으로 수행해 몽골 철도 산업 진출의 교두보로 삼는 한편 이 사례를 발판으로 글로벌 시장으로 진출, 100년 기업의 꿈을 향해 나아간다는 계획이다.

LAB02

안전한 커넥티드 선박을 위한 미래기술의 요람

랩오투원 실시간 선박운항 정보분석에서 미래 예측까지 제공 , 해양 분야 선도적인 안전 기술 적용으로 글로벌 시장 진출

▲ 빅데이터 기반 '선박운항 정보분석 기업'랩오투원 이상봉 대표(윗줄 왼쪽에서 세번째)

랩오투원 기본 정보

회사명	랩오투원	전화번호	051-462-1021
대표자명	이상봉	홈페이지	http://www.lab021.co.kr/
설립연도	2015. 1. 7.	종사자	10명
주소	부산 중구 충장대로5번길72, 본관동 4층		
주요제품	선박운항솔루션		

랩오투원은 IoT 기반 기술을 활용해 선박 내 수 백 개 센서에서 쏟아져 나오는 정보를 실시간으로 수집, 분석하고 여기에서 모이는 거대한 데이터에서 선박 운항에 도움을 주는 귀중한 정보를 찾아낼 수 있는 간결하고 강력한 분석 도구와 서비스를 제공한다. 이러한 노하우를 바탕으로 지속적인 R&D를 진행해 실시간 선박 성능 모니터링 및 분석, 운항정보(ISO19030), 선박 진단, 해상 예보 등 관련 분야의 대표 기업으로 성장하고 있다. 특히 선박 운항 솔루션은 국내외 대형 선사를 비롯해 350척의 대형 선박에 탑재되어 실시간으로 선박 운영 정보와 미래 예측 정보를 제공하고 있으며 해외 선사에 수출도 준비하고 있다.

랩오투원은 글로벌 선박 운항 관련 이슈에 주목하고 있다. 최근들어 중요성이 커지고 있는 선박 e-내비게이션은 도입 시스템이 점점 복잡해져 단위 제품들의 안전성 보증이 국제기구에서도 이슈로 등장하고 있는 상황이다. 유럽의 대표적인 선급 인증기관들(DNV, LlOYD, EXIDA, TUV 등)은 이러한 추세를 반영해 국제기구가 요구하는 품질 및 안전성에 대한 적용 절차 및 표준화를 빠르게 진행하고 있었다.

국제해사기구(IMO, International Maritime Organization)에서는 선박 안전사고 예방을 위해 e-내비게이션 SQA/HCD(Software Quality Assurance / Human Centred Design) 가이드라인(IMO SQA/HCD)을 제정, 조선해양 분야에 들어가는 SW의 품질 및 안전 보증을 위한 강제 규정을 준비하고 있었다. SW 안전 세부 규격은 기능 안전 국제표준인 IEC61508을 따르도록 규정하고 있었는데 이에 따라 선박 운항 솔루션도 IEC61508, IMO SQA/HCD 등 국제 안전 규격에 맞는 SW 신뢰성 결과를 제공하는 것이 요구되었다.

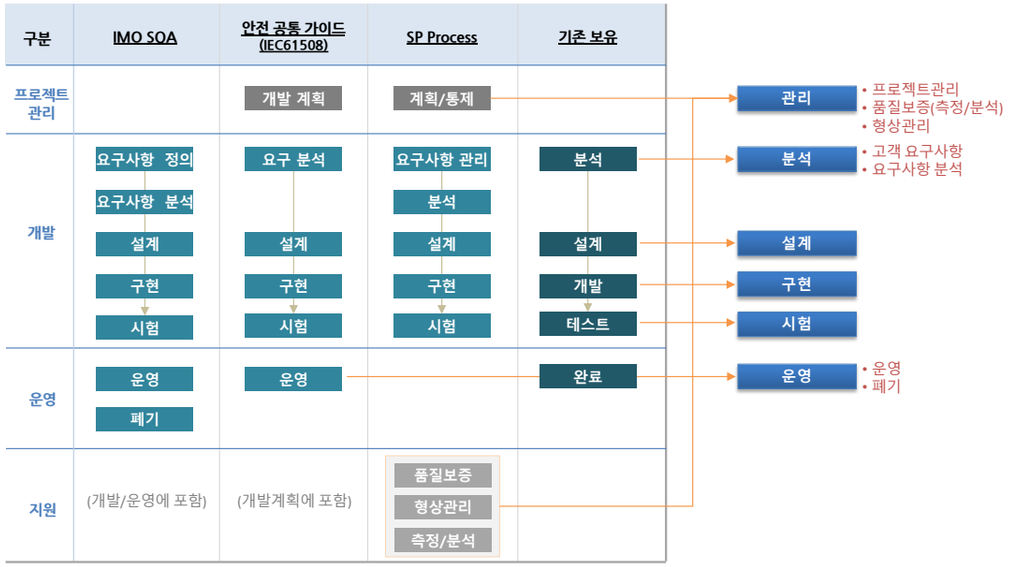
조선해양

적용 표준	적용 안전 기법(Techniq & Measure)
IMO SQA/HCD, IEC61508	• IMO SQA와 IEC 61508을 참조 안전보증 프로세스 수립 • HAZOP을 이용한 대상제품 위험분석 및 안전기능 도출 • 검증된 SW 정적분석 도구를 활용한 소스코드 안전성 확보 • 협업 도구를 이용한 엔지니어 및 고객간 의사소통 강화

분석을 통한 안전한 솔루션을 만들기 위한 기초 작업

랩오투원은 안전기술을 적용하기 위해 먼저 솔루션 개발 및 현재 운영 상태에 대한 분석을 수행하였다. 현 수준에 대한 객관적인 분석을 통해 조선해양 분야의 IMO SQA/HCD 및 IEC61508 수준에 어느 정도 도달했는지 갭 분석을 시행하면서 향후 사내에 적용 가능한 SW 품질·안전 보증체계를 수립하였다. SW 개발 및 운영 과정 전반에 대한 관리가 가능한 품질·안전 보증체계 수립을 통해 회사 솔루션의 안전성과 신뢰성 확보하는 것이 좋은 SW를 개발하는 관건이 된다.

NIPA에서 발간한 SW 신뢰 안전 공통 가이드를 참조해 내부 프로세스를 정립하고 제품의 안전 무결성 등급에 맞는 절차와 세부적인 활동 및 안전기술을 설계하였다. 회사의 프로세스에 신규 적용 또는 변경되는 부분이 많아 자체 수행이 어려웠기 때문에 한국해양대학교 이서정 교수님과 나이스컨설팅의 도움을 받았다. 적용해야 할 프로세스, 산출물, 안전기술 등에 대한 세부적인 적용 방법과 함께 사내 엔니지어 교육도 큰 도움이 됐다.



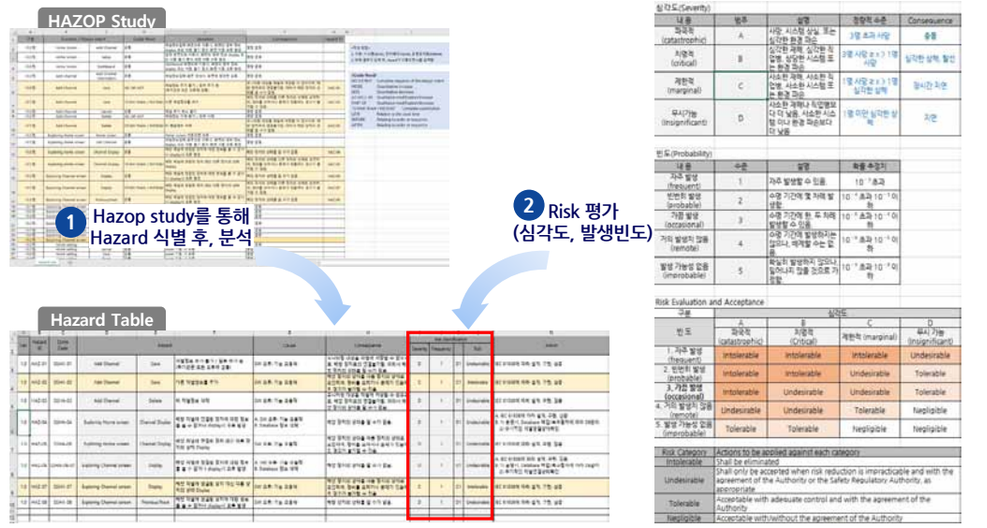
▲ 랩오투원의 품질 · 안전 보증체계 수립 방안

일반 위험관리로는 SW 안전 보장 못해 새롭게 접근

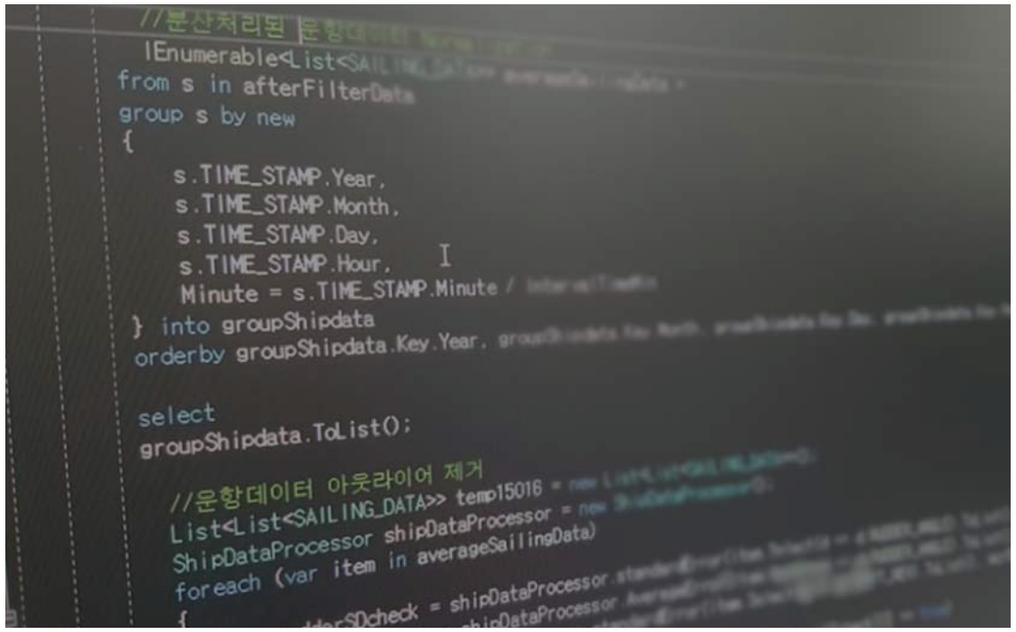
SW에 안전을 적용한다고 할 때 고민이 적지 않았다. 이전에도 위험관리라는 형태로 유사한 활동을 하고 있었다고 생각했으나 '안전한 제품을 만들고 있는가'라는 질문에 자신있게 답하기위해서는 안전을 위한 위험을 체계적으로 분석하고 평가하는 부분이 필요하다는 것을 알게 되었다. 안전한 SW를 만들기 위한 위험 분석 및 관리 절차가 별도로 추가됐다.

선박 운항 정보 습득 경로에 존재하는 많은 센서, 유량기 등 위험 요소에 대한 식별을 위해 Hazop[1] study를 실시하였으며 발견된 Hazard를 제거 또는 감소시키기 위한 각 안전기능을 분석하고 심각도, 발생빈도를 고려한 위험 평가를 시행하였다. 이를 통해 그동안 발견하지 못한 추가적인 안전기능을 도출해 안전이 강화되었다. 특히 체계적인 분석 및 이후 설계/구현/시험/운영을 진행하는 동안 관리해야 할 안전관리 항목을 선정하고 지속적인 검토 추적이 가능하게 됐다.

1) HAZOP(Hazard and Operability): 공정에 존재하는 위험요인과 공정의 효율을 저해 할 수 있는 운전상의 문제점을 찾아내어 그 원인을 제거하는 방법



▲ 랩오투원의 위험분석 절차 및 산출물 관계



▲ 랩오투원의 솔루션 소스 분석 화면 예시

정상 동작하는 SW코드도 자동화된 적정분석 도구로 검증 필요

오랫동안 고민하여 만든 코드에 대해 내부에서는 막연한 신뢰를 하고 있었을 뿐이었기 때문에 정상적으로 잘 동작하는 SW 코드에 대해서도 안전성을 높이고 객관적으로 검증할 방법을 적용하는 것이 필요했다. SW로 인한 대형 사고의 많은 부분은 정적분석을 거치면 해결되는 부분이 많았는데 특히 단순한 코딩 실수에 대한 자동화된 사전 분석 방법이 반드시 필요했다.

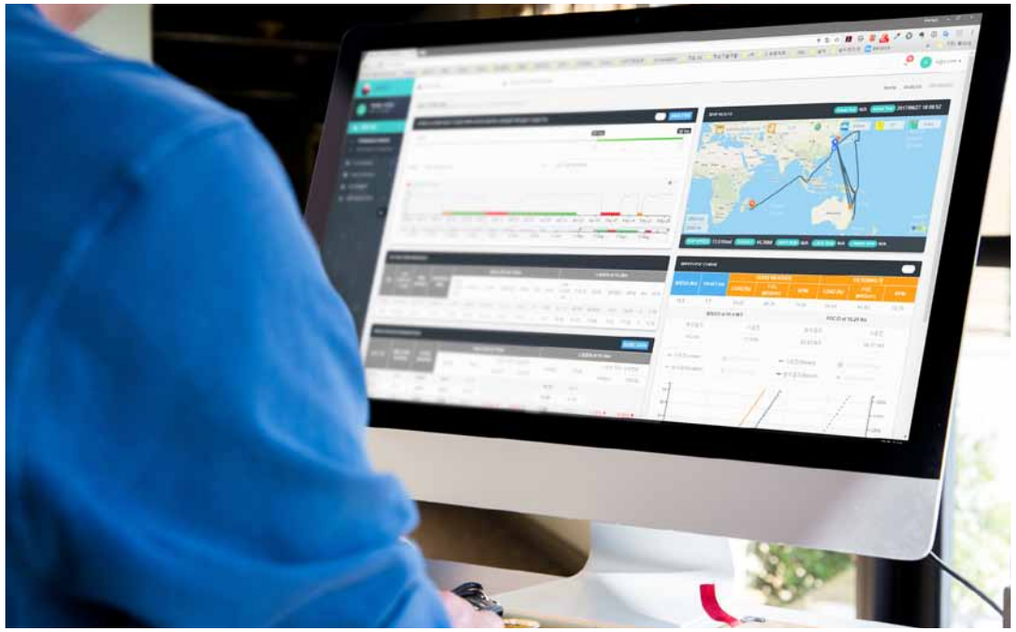
정적분석은 코드의 실행이 필요하지 않아 완성되지 않은 코드에도 적용이 가능해 결함을 빨리 발견할 수 있다. 자동화된 정적분석 도구를 사용하면 오랫동안 축적된 경험많은 개발자들의 노하우나 이미 필드에서 많이 발생하는 다양한 런타임 오류들에 대한 규칙들을 사용할 수 있다. 이를 위해 적용한 도구는 코드 표준에 FxCops, 백엔드 부분은 sonarLint for VisualStudio 등이다. IEC 61508에서는 경계값 분석, 제어 흐름 분석, 데이터 흐름 분석, 런타임 오류 분석 등의 안전기술을 적용하도록 제시하고 있다.

고객과의 소통 툴을 통한 요구사항의 효율적인 반영

SW 일은 상호 의사소통이다. 의사소통이 잘 된다면 고객이 원하는 요구사항과 개발 및 운영단계에서 해야 할 일들이 명확해져서 원하는 제품, 원하는 서비스를 제때 제공할 수 있다.

요즘들어 조선해양 분야의 고객들은 SW 부분에 대해 매우 다양하고 복잡한 요구사항을 제시한다. 특히 제품 및 서비스 제공 장소가 제품이 장착된 선박, 제품의 설치와 보수가 이루어지는 조선소, 제공 정보 및 데이터를 활용하는 선사 사무실 등 다양해지고 있어 요구사항도 시간과 공간을 가리지 않는다. 이러한 복잡다양한 요구에 대한 수용과 관리는 제품의 품질과 안전성 향상에 매우 중요한 항목이다.

랩오투원은 Atlassian사의 Trello를 활용해 언제 어디서든지 접속하여 실시간으로 요구사항을 등록하고 진행현황을 관리할 수 있었고 SW 결함이 생기면 즉시 개발팀에 넘겨 신속한 대응이 가능해졌다. 이러한 도구 적용을 통해 IEC 61508에서 요구하는 요구사항에 대한 기록, 추적성을 제공할 수 있었다.



▲ 랩오투원의 제품 화면-실시간 추적 예시

> *SW안전이 무엇인지*
> *알 수 있는 계기가 되었다.*
> *조금만 살핀다면 사전에*
> *적은 노력과 시간으로 SW 안전을*
> *제공할 수 있다고 생각한다.*

참여자 소감 “SW 안전이 무엇인지 알 수 있는 계기가 되었다. 평소 SW 개발 중에 문제가 있다고 생각했지만 관리하지 않아 이후 문제가 되었던 경험을 생각하면 이러한 습관 하나 하나가 SW 안전에 매우 중요한 활동임을 느낄 수 있었다. 조금만 살핀다면 사전에 적은 노력과 시간으로 SW 안전을 제공할 수 있다고 생각한다.”

“안전기술 중에서 정적분석 도구 도입에 대한 요구가 항상 있었지만 여러 가지 이유로 도입이 되지 않았는데 이번 기회로 도입할 수 있게 되어 기뻤다. 도입 초기에는 다소 어려움이 있었지만 지원 사업을 통해 빠르게 개발 프로세스에 반영할 수 있었고 자체적인 개선 작업이 가능해졌다. 지금은 이러한 프로세스가 완전히 회사 문화에 정착되어 SW 안전을 모든 구성원이 공유하고 우리가 만드는 제품을 신뢰할 수 있다는 자부심을 가질 수 있게 되어 뿌듯하다.”

“최근 디지털 제품의 시장 트렌드는 고객 스스로 많은 학습을 선행한다는 점이다. 과거와 달리 SW 안전에 대한 요구사항과 어떻게 제품에 반영되었는지 먼저 문의하는 고객이 많아진 것이 큰 변화이다. 해양 분야에서 비교적 초기에 SW 안전 개념을 적용한 덕분에 현재는 고객 제안 시 경쟁력 우위 확보는 물론 회사 이미지를 제고에도 큰 효과를 보고 있다.”

향후 계획 국내외 많은 선사와 선원들이 선박운항 솔루션이 장착된 선박으로 전세계의 모든 바다를 항해하고 있다. 랩오투원은 SW 안전기술을 통해 글로벌 고객들에게 선박과 육상을 하나로 연결해 선박이 안전하게 항해할 수 있도록 돕고, 해운 업무를 쉽고 편하게 만드는 서비스를 제공하고 있다. 특히 보이지 않는 곳의 안전까지 미리 대비하고 글로벌 규격에 맞는 탁월한 제품을 만들기 위해 끝없이 도전함으로써 최고의 역량을 갖춘 기업이 되겠다는 목표를 세우고 있다.

랩오투원의 이상봉 대표이사는 “해양 분야에서는 빠르게 디지털 전환이 일어나고 있어 SW 안전 및 품질에 대한 중요성이 커지고 있다”며 “이번 SW 안전기술 적용을 계기로 랩오투원이 개발하는 SW는 혁신적이고 신뢰성이 높다는 평가를 얻을 수 있게 됐다”고 말했다. 랩오투원은 이 같은 SW 역량을 기반으로 글로벌 시장에 도전해 2025년에는 아시아의 해양 디지털 리더로 성장한다는 계획이다.

|주| 미주하이텍

승강기의 안전을 책임지는 국민 안전 지킴이

잦은 안전사고에 대비해 강화된 국제 안전 인증 적용 필수
KTL의 도움 받아 IEC 22201 관련 표준 적용한 프로세스 정립

▲ '승강기 안전 기술 기업' 미주하이텍 이호연 대표

미주하이텍 기본 정보

회사명	미주하이텍	전화번호	02-2652-8741
대표자명	이호연	홈페이지	http://www.mijuhitech.co.kr
설립연도	2011. 11. 14	종사자	29명(2017년 기준)
주소	서울특별시 양천구 중앙로32길 67, 204호		
주요제품	승강기 설치 운영 솔루션		

미주하이텍은 우리가 하루 한번 이상 이용하는 승강기(엘리베이터, 에스컬레이터, 무빙워크 등)를 설치 및 운영하는 회사이다. 이렇게 자주 접하는 승강기에서 가장 중요한 이슈는 안전사고이다. 승강기 안전사고는 주변에서 흔히 발생하고 있다. 이 가운데 엘리베이터 문이 열릴 때 도어와 문틀 사이에 손이 끼어 발생하는 안전사고는 누구에게나 노출되어 있으며 특히 주의력이 약한 노약자나 어린이에게 더 빈번하게 발생하고 있다.

미주하이텍은 이런 상황을 개선하기 위해 엘리베이터 손 끼임을 방지하는 안전장치를 개발했고 제품의 안전성과 우수성을 인정받아 국내에 적극 도입되고 있으며 수출 시장도 노크하고 있다. 현장에서 반복적으로 발생하는 안전 사고를 그냥 지나치지 않고 끊임없는 R&D를 진행한 결과 기술 혁신으로 생활 안전을 구현하게 된 것이다.

미주하이텍은 설립할 때부터 세계 시장의 진출을 목표로 삼았다. 안전 기술은 국내뿐만 아니라 해외에서도 반드시 필요하기 때문이다. 유럽과 미국을 중심으로 한 해외 선진국에서는 IEC22201(승강기 제어 안전 국제표준) 관련 표준을 참조하여 엘리베이터와 에스컬레이터의 안전제어기를 포함한 자동제어 시스템에 대한 안전인증을 강제 규제로 시행하고 있다. 따라서 미주하이텍이 설립부터 염두에 둔 해외 진출을 위해서는 국제 안전규격에 맞는 안전 기술을 보장해야 했다.

특히 ISO 22201-2:2013 기반 PESSRAE[1] 인증을 받은 중국 제품들이 급격히 국내 시장에 수입되면서 중소기업 위주의 국내 제조업체들이 빠르게 대응하지 않으면 해외시장에서도 기회를 잃을 수 있는 상황이 나타나게 된 것이다.

1) PESSRAE(Programmable electronic systems in safety related applications) : 에스컬레이터/엘리베이터용 안전관련 프로그램 가능한 전자시스템에서 PES를 기반으로 한 소프트웨어 응용 프로그램

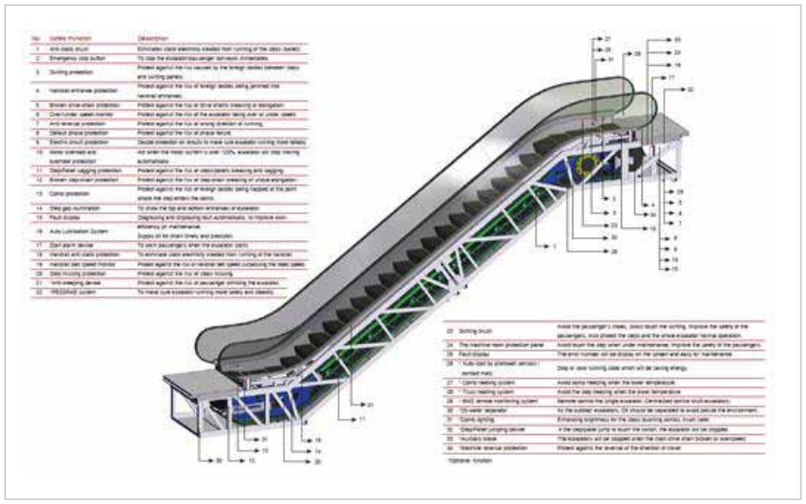
엘리베이터

적용 표준	적용 안전 기법(Techniq & Measure)
IEC61508, ISO22201	• 안전 기술 SW 요구사항 정의부터 설계 사양으로의 전개 • SW 소스코드의 변경 및 통제를 위한 형상 관리 적용 • 안전 요구사항 검증을 위한 안전보증 절차 및 시험 실시

국내외 안전기술 현황과 시각

앞서 말한 바와 같이 에스컬레이터와 무빙워크 관련 사고가 자주 발생하고 있는데 심각한 것은 사망 사고로 이어지고 있다는 점이다. 그러나 이러한 승강기 관련 사고 중 다수는 SW 기반 제어기의 안전 기능을 통해 예방/감소/완화가 충분히 가능하다는 점에 주목해야 한다. 이러한 승강기 안전 기술과 관련해 2013년 국제 표준으로 ISO 22201-2:2013 (PASSRAE)가 제정되어 있다. 이 표준은 SW 기반의 안전 제어기(이하 PESSRAE)가 에스컬레이터와 무빙워크를 안전하게 동작시키기 위해 필수적인 안전기능을 정의하고 있다. 상세히 살펴보면 PESSRAE에 의해 구현되는 안전 기능에 대한 목표 고장률을 SIL(Safety Integrity Level)로 정의하도록 하고 있으며, 각 안전등급(SIL1,2,3,4)을 만족하기 위해 필요한 설계/검증 기술과 방법, HW와 SW의 설계를 상세화하는 기술적 방법, HW와 SW의 안전검증(Safety Validation)에 관련된 요구사항의 기준을 제시하고 있다.

국내에는 KTL 인증이 있는데 이는 개발 초기부터, PESSRAE 표준 ISO 22201-2:2013을 준수하여 SW 설계 산출물을 작성하고 이를 통해 개발된 안전제어기에 대한 승강기부품안전인증기관의 PESSRAE 인증 획득하도록 되어 있다.



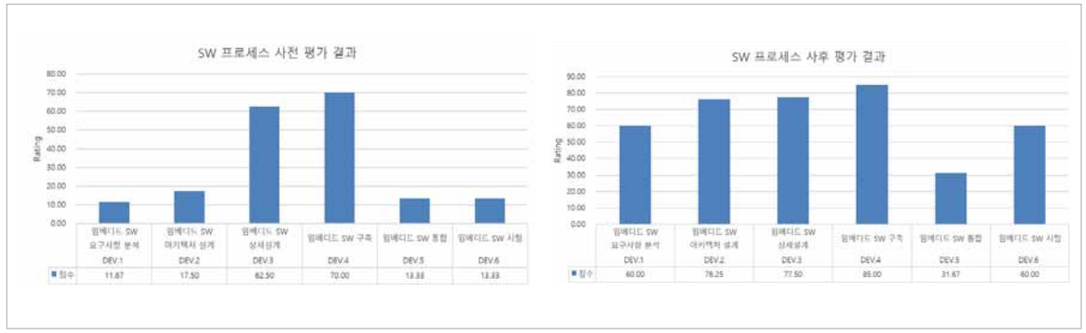
▲ 에스컬레이터 관련 안전기능

안전 기술 개발을 위한 당사의 강/약점 분석

안전 기술에 대한 국제 표준을 적용하려면 먼저 회사 내부의 개발 현황을 파악하는 것이 필요했다. 이를 위해 국내 안전 기술 인증부분의 전문가인 한국산업기술시험원(이하 KTL)의 도움을 받아 과거 진행된 프로젝트에 대한 프로세스 평가를 수행했다.

KTL에서 개발한 체크리스트를 활용해 각 SW 개발 프로세스에 대한 산출물 검토 및 인터뷰를 진행한 결과, 시스템 수준의 요구사항 문서가 잘 정의되어 있고, SW 아키텍처 설계 문서에 정적 설계가 기술되어 있으며, 아키텍처 문서에 따라 코드 개발이 수행되고, 유닛 설계 사양에 따라 Unit Test가 수행되는 장점이 확인됐다. 반면 시스템 요구사항은 정의되어 있으나 SW 요구사항의 식별이 어렵고 SW 컴포넌트에 대한 자원 소요량, 인터페이스 정의가 필요하다는 지적이 제기됐다. 또 SW 요구사항 – 아키텍처 설계 – 상세 설계 – SW 통합 – SW 시험 단계에 대한 추적성이 확인되지 않고, Unit Test 결과에 대한 Test Coverage를 확인할 수 없다는 보완 사항도 도출되었다.

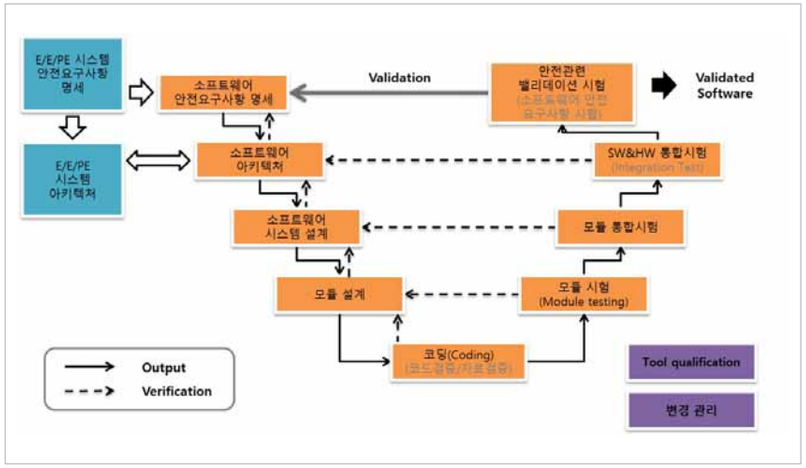
이 결과를 반영하여 안전 기술 SW 개발을 위해 개선할 부분과 목표를 설정하고 진행했고 보완 사항에 대한 개선활동을 수행한 후 재측정한 결과 SW 개발 프로세스 능력이 골고루 향상됨을 확인할 수 있었다.



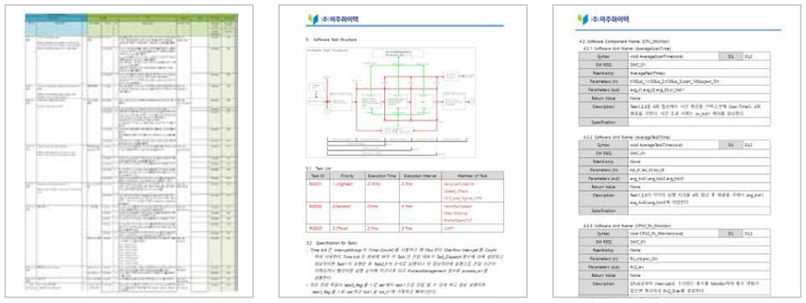
▲ SW 프로세스 사전/사후 평가 결과

체계적인 방법을 통한 안전 기술 SW 요구사항 정의부터 설계 사양으로의 전개

시스템 요구사항으로부터 안전 기술 SW 요구사항을 도출하고 이를 설계하기 위해 IEC 61508-3 SW 개발 라이프 사이클을 참고하여 『소프트웨어 안전 요구사항 – 소프트웨어 아키텍처 설계 – 소프트웨어 유닛 설계』 활동을 통한 SW 개발 프로세스를 수립하였다. SW 안전요구사항 단계에서는 ISO 22201-2에 식별한 안전기능에 대해 SW 수준으로 요구사항을 식별하고, SW 아키텍처 설계 단계에서는 SW 정적 구조와 동적 구조, SW 컴포넌트 사양을 정의했으며 SW 유닛 설계에서는 C언어를 사용하여 상세한 수준으로 모듈 단위의 설계 사양 기술하였다. 이런 절차를 따르면 안전 기술 SW 요구사항이 무엇인지, 어떻게 설계되어 구현될 것인지를 명확히 알 수 있어 안전 기술 요구사항이 누락되지 않고 체계적으로 안전 기술 SW설계가 가능해진다.



▲ IEC 61508-3의 소프트웨어 개발 라이프 사이클



▲ 체계적인 방법을 통한 에스컬레이터 안전 제어기 소프트웨어 설계 (소프트웨어 안전요구사항 / 아키텍쳐 / 상세 설계 내역)

소스코드에 대한 형상 관리 적용과 안전 요구사항 검증을 위한 시험 실시

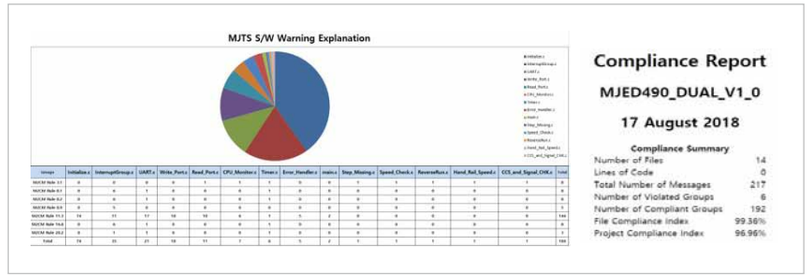
SW를 개발하고 운영하면서 가장 어려운 일은 SW 형상을 유지하는 일이다. SW는 HW와 달리 형상에 대한 관리가 엄격히 이뤄져야 한다. 미주하이텍은 소스코드에 대한 버전관리를 위해 SVN를 도입하였다. 소스코드에 대한 버전관리가 가능해지면서 SW가 가지는 잠재적인 결함을 탐지하고 개선하기 위하여 정적 분석, 설계에서 의도된 대로 정확히 작동하는지 확인하기 위한 동적 시험 수행이 가능해졌다.

정적분석 도구인 QAC를 활용하여 - MISRA C:2004에 대한 코딩 rule을 체크하였고, Compliance index를 96.96% 달성하였다. 동적 테스트는 Controller Tester를 통해 Target 환경과 유사한 환경을 만들어 수행함으로써 테스트 커버리지[2])를 확인할 수 있었다.(Statement Coverage :99.30% / Branch Coverage : 96.28% 달성)

또한 임베디드 SW 관점에서 SW 안전요구사항 검증을 위한 시험을 수행하여 PESSRAE에서 요구하는 안전 요구사항의 정의부터 설계, 개발, 시험까지의 추적성을 확보할 수 있게 되었다.

---

2) 테스트 커버리지(Test Coverage) : 테스트 대상인 프로그램이 일련의 시험 데이터에 의한 실행에서 범위를 어느정도 테스트하였는지를 정량적으로 나타내는 척도



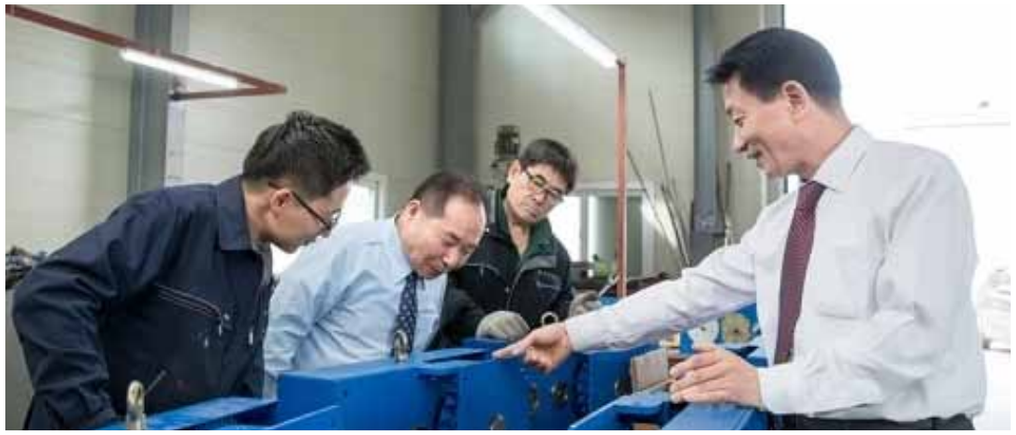
▲ 정적분석 수행 결과

▲ SW안전요구사항 검증 보고서

> *현장 적용 지원사업은 시험·분석·평가·컨설팅을 해주고 애로 사항과 인증에 대한 종합적인 지원을 해줘 더 나은 기술개발에 힘을 실을 수 있게 한다.*

참여자 소감 “미주하이텍은 설립할 때부터 세계 시장 진출에 목표를 둔 기업이다. 올해 홍콩 쇼핑몰 랭햄플에이스의 대형 에스컬레이터에서 역주행 사고가 발생하는 안타까운 사고가 있었고 그로 인해 많은 인명 피해도 일어났다. 승강기, 에스컬레이터는 세계적으로 같은 구조로 이뤄져 있기 때문에 이 같은 사고 예방을 위해서라도 우리의 기술이 세계적으로 꼭 필요하다고 생각했다. 우리가 세계로 나아가야 하는 이유이기도 하다.”

“현장 적용 지원사업은 우리 같은 중소기업들에 오아시스 같은 역할을 해주고 있다. 전담 연구원이 현장을 방문해 시험·분석·평가·컨설팅 등의 기술 지원을 해주고 제품 개발에 대해 애로 사항과 인증에 대한 종합적인 지원을 해주기 때문에 더 나은 기술개발에 힘을 실을 수 있다.”



향후 계획 국내 승강기 인증 분야에도 국제 기준 도입이 점차 가속화되고 있다. 전 세계가 유럽을 중심으로 한 제품 표준을 따르고 있고 정부도 안정된 기준을 가진 유럽 안전인증 제도를 도입하고 있다. 에스컬레이터의 안전한 이용과 안전사고 예방을 위해 강화된 법제도에 발맞춰 다양한 안전 기술 제품이 앞다퉈 출시되고 있지만 안전 품질이 뛰어난 제품들을 필두로 업계가 상생 가능한 시장을 형성하는 것이 무엇보다 중요하다. 미주하이텍은 안전 기술로 국민의 안전을 지키고 그 기술을 인정받아 세계로 진출하는 기업이 되겠다는 목표를 세우고 있다.

미주하이텍의 이호연 대표이사는“앞으로도 승강기 안전 기술을 개발해 나아가는 데 있어 NIPA의 안전기술 컨설팅 지원은 큰 힘이 될 것”이라며 “이 힘을 바탕으로 안전기술 연구개발에 더욱 박차를 가해 세계에서도 인정받는 기업이 되겠다”고 말했다.

SW 안전기술의 이해와 분야별 SW 안전 표준

02

SW 안전기술의 이해와 분야별 SW 안전 표준

SW 진흥법 개정

SW산업진흥법이 20년 만에 내용과 형식에서 큰 변화를 맞았다. 법안 이름이 SW산업진흥법에서 SW진흥법으로 바뀌었으며 내용도 전면 개정돼 SW산업 성장뿐 아니라 디지털전환 시대를 맞아 SW가 곳곳에 뿌리내리는 데 큰 역할을 할 것으로 기대된다.

기존 SW산업진흥법은 5장 48개조로 구성되었으나 새 법안은 조항이 30개 늘어난 8장 78개조와 부칙으로 이뤄져 있으며 특히 SW안전, SW품질, 상용SW, 지역SW, 공공SW시장 발주문화에 긍정적 변화를 가져올 전망이다.

SW 안전에 관해서는 4장 30조에서 SW안전 확보를 위한 관련 지침을 만들어 고시하게 했다. 고시 내용은 첫째, SW안전 관련 위험 분석, 둘째, SW안전 확보를 위한 설계 및 구현 방법, 셋째, SW안전 검증 방법, 넷째, 운영 단계의 SW안전 확보 방안, 다섯째, 기타 SW안전 확보에 필요하다고 인정되는 사항이다.

이어 31조에서는 과기정통부 장관이 SW안전 산업을 진흥하고, 국가 전반의 SW안전을 확보하기 위해 기술연구, 인력 양성, 산업 기반 조성, 안전사고 대응 지원, SW안전 정보 축적 및 활용 등의 사업을 하도록 했다.

SW 안전기술 활용서

SW 역할 확대 및 복잡화로 인해 SW 결함에 의한 안전 사고의 발생 가능성이 높아지고 있으며 이로 인해 SW 안전의 중요성이 증가하고 있다. 또한 국내외 SW 안전에 관한 규정과 표준, 법규가 강화되는 추세에 따라 국내 중소기업의 SW 안전기술에 대한 역량 강화 및 이에 대한 지원이 필요해지면서 SW 안전기술 활용서를 제작하게 되었다. 이 활용서는 SW 안전에 대한 개념 설명 및 안전 확보를 위한 접근 전략 제시를 통한 ‘SW 안전에 대한 공감대 형성’과 다양한 SW 안전활동 및 안전기법에 대한 구체적인 수행 방안 제공에 따른 ‘SW 안전기술 실무 적용 역량 강화’를 목적으로 한다.

SW 안전기술 활용서는 SW 안전기술 역량 강화를 위한 다양한 활용 방안을 제시하고 있다. 특히 시스템 및 SW 개발자, 안전 및 품질보증 엔지니어, 프로젝트 관리자 등 다양한 역할자의 역량 향상과 국내 SW 안전기술 확산 촉진 및 경쟁력 강화를 위해 SW 안전활동, 안전기법, 산출물 작성법, 다양한 적용 사례 및 고려사항 등을 수록하고 있다.

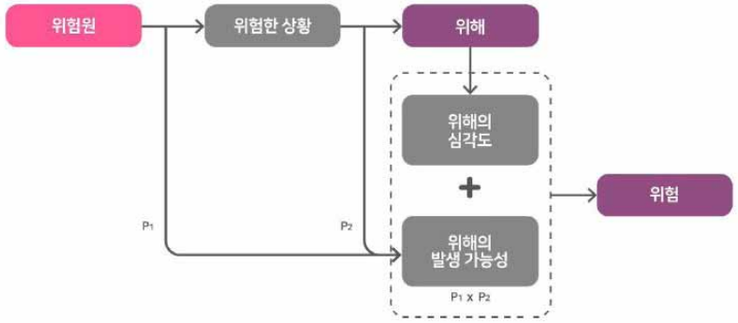
SW 안전기술 활용서 다운로드

버튼을 클릭하시면 해당 파일로 이동합니다

1. 안전(Safety)의 이해

국제 표준 'ISO/IEC Guide 51'에서는 안전을 허용할 수 없는 위험으로부터의 자유(Freedom from Risk which is not Tolerable) 라고 정의한다.

국내외 안전 관련 표준 및 법규에서는 공통적으로 안전에 대해 허용 가능한 수준의 위험 또는 위험 요인에 대해 충분한 대비가 되어 있는 상태를 조건으로 제시하고 있다.



- 위험원(Hazard): 피해의 잠재적 요인, 위 사고를 일으키는 원인을 의미
- 위험한 상황 (Hazardous Situation): 사람, 자산, 환경이 하나 또는 그 이상의 위험에 노출된 상황
- 위해(Harm): 신체에 대한 물리적 부상 또는 환경·자산에 대한 물리적 피해
- 위험(Risk): 피해 외 발생 확률과 피해의 심각도의 조합, 위험원이 위해 또는 사고로 이어질 수 있는 가능성(Probability)과 위해 발생 시의 삼각도(Severity)를 조합하는 것을 의미

[그림 1] 위험, 위해, 위험원의 관계

2. 기능 안전(Functional Safety)과 안전(Safety)

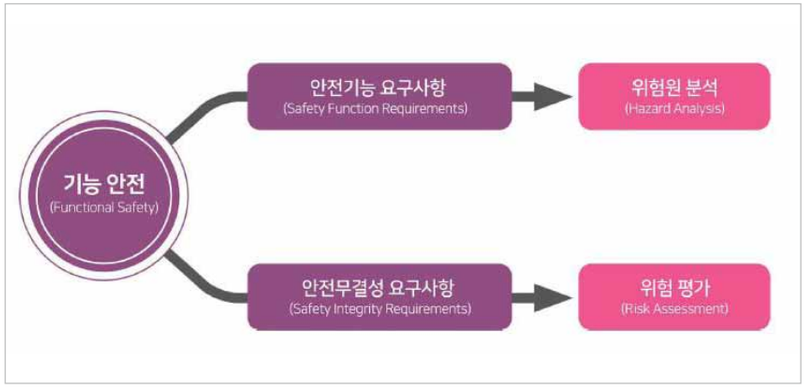
기능 안전은 전체적인 안전의 일부분으로 입력에 정확하게 동작해야 하는 시스템 또는 장비에 의존하는 안전을 의미한다. 기능 안전은 안전 확보를 위해 하나 이상의 자동 보호 기능(Automatic Protection Function) 또는 안전 기능(Safety Function)을 구현하여 사람의 신체적 상해 및 건강 손상을 발생시키는 위험에 대응하는 것이다.

	안전(Safety)	기능 안전(Functional Safety)
정의	허용할 수 없는 위험으로부터의 자유 Freedom from risk which is not tolerable	전체적인 안전의 일부분으로 입력에 정확하게 동작해야 하는 시스템 또는 장비에 의존하는 안전 잠재적으로 위험한 조건을 탐지하여 위험 사건의 발생을 줄이거나 완화함으로써 위험 사건의 영향을 줄이도록 보호하는 조정 장치 또는 메커니즘을 활성화하는 것
출처	ISO/IEC Guide 51	IEC 61508

기능 안전과 일반적인 안전의 예를 보면, 화재 발생 시에 센서의 연기 감지를 통해서 화재 진압 시스템을 활성화하거나 가연성 액체가 포함된 탱크에 액체 수위가 위험한 수준에 도달하는 경우, 잠금 스위치를 활성화하여 액체가 유입되는 것을 막는 것이 기능 안전이다. 이러한 방식으로 위험 사건의 발생을 줄이는 시스템을 기능 안전에서는 능동적 시스템(Active System)이라고 한다. 반면에 화재에 견딜 수 있는 내화성 문이나 불연재 등 수동적 방식(Passive System)으로 확보된 안전은 기능 안전이라고 하지 않는다. 이것은 앞서 연기 감지 센서 사례와 같이 동일하게 화재 위험으로부터 사람을 보호할 수 있지만 기능 안전에 해당하지는 않는다. 이처럼 일반적인 안전과 달리 기능 안전은 능동적 시스템에 의존하는 점이 가장 큰 특징이다.

기능 안전의 능동적인 시스템은 [그림 2]과 같이 안전 기능 요구사항(Safety Function Requirements)과 안전무결성 요구사항(Safety Integrity Requirements)에 의해 실현된다.

여기서 안전 기능 요구사항은 시스템에 대한 위험원 분석을 통해서 식별되는 위험원 감소 대책과 관련한 요구사항이며, 안전무결성 요구사항은 시스템 위험 평가를 통해서 결정되는 허용가능한 위험의 수준과 관련한 요구사항이다.



▲[그림 2] 기능 안전 확보 방법

3. SW 안전(Software Safety)

IEEE 1228에서는 SW 안전(Software Safety)을 재해나 사고의 결과로 인해 사람의 사망, 상해 또는 재산 피해의 원인이 될 수 있는 SW 위험원으로부터 자유로움(Freedom from Software Hazards) 이라고 정의하고 있다. 이는 시스템 또는 장비가 허용 가능한 수준의 위험에서 벗어나 사고로 이어지는 SW 상태가 되어서는 안된다는 것을 의미한다.

다양한 기관에서 제시하는 정의 및 개념에 기반하여 SW 안전을 다음과 같이 정의할 수 있다.

> SW 시스템의 안전 사고 발생 위험이 SW 역량을 통해 허용 가능한 수준으로 억제, 제거 또는 감소되어 있는 상태

SW 안전을 확보하기 위해서는 시스템 장비에서 예상되는 위험원을 필요에 따라 SW를 활용하여 제거, 감소하거나(예: 시스템의 기능 안전 확보를 위해 SW로 안전 기능 구현), SW 자체 문제로 인한 사고 위험 수준을 허용 가능한 수준으로 낮추는 노력이 필요하다. 이를 위해 사전에 위험원 분석 등을 통해 위험한 상황을 미리 식별하여 SW 방식으로 처리가 가능한 부분에 대하여 적절한 수준의 위험 감소 대책을 적용하거나, SW 품질 수준을 확보하여 SW 문제로 발생 가능한 사고로부터 충분한 대비를 해야 한다. 이러한 관점에서 SW 안전은 'SW를 통한 안전(Safety through software)'과 'SW의 안전(Safety of software)'을 모두 포함한다.

■ SW를 통한 안전(Safety through Software)

: 시스템 또는 장비에서 예상되는 사고를 필요에 따라서 SW를 활용하여 감소시키거나 예방하는 것을 의미하며, 이를 위해서는 시스템에서 발생 가능한 위험원의 분석과 필요한 SW 안전 기능(Safety Function)의 식별, 그리고 이에 대한 적용을 수행해야 한다.

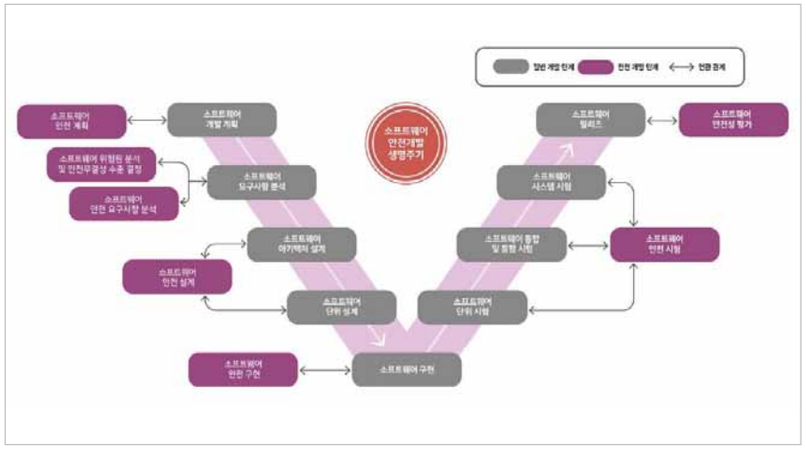
■ SW의 안전(Safety of Software)

: SW로 인한 사고가 발생하지 않도록 SW 품질 수준을 확보하는 것을 의미하며 이를 위해서는 SW 안전 기능이 만족스럽게 수행될 수 있도록 SW 안전무결성(Safety Integrity) 확보를 위한 다양한 SW 안전 활동을 수행해야 한다.

4. SW 안전 확보를 위한 주요 기술

주요 SW 안전기술은 안전이 중요시되는 SW 개발에 필요한 안전활동으로 구성된 SW 안전개발 생명주기와 안전 활동에서 위험원 제거 또는 감소를 위해 적용하는 SW 안전기법을 포함한다.

SW 안전개발 생명주기는 [그림 3]과 같이 SW 안전 계획, SW 위험원 분석 및 안전무결성 수준 결정, SW 안전 요구사항 분석, SW 만전 설계와 구현, 안전 시험 및 안전성 평가의 7개 단계로 구성된다.



▲ [그림 3] SW 안전개발 생명 주기

안전기법은 SW 안전개발 생명주기의 안전활동 수행 시 활용 가능한 위험원 분석, 위험 감소 대책, 위험 감소 검증 및 평가 관련 기법들이다. 예를 들면, SW 안전 설계를 위해 안전 아키텍처 패턴, 안전 매커니즘 등의 안전 기법을 활용할 수 있다. 안전활동과 기법, 산출물의 상세 내용은 우측 표를 참조한다.

안전활동	안전기법	산출물
소프트웨어 안전 계획		
• 소프트웨어 안전 계획 준비 • 소프트웨어 안전활동 테일러링 • 소프트웨어 안전활동 역할 및 책임 정의 • 소프트웨어 안전활동 WBS 작성 • 소프트웨어 안전 계획서 작성 및 검토설립연도	• 소프트웨어 안전활동 및 안전기법 테일러링 • 소프트웨어 안전 조직의 독립성 수준 결정	• 소프트웨어 안전 계획서 • 소프트웨어 안전활동 WBS • 소프트웨어 안전 계획 검토 결과서
소프트웨어 위험원 분석 및 안전 무결성 수준 결정		
• 소프트웨어 위험원 분석 • 소프트웨어 안전 무결성 수준 결정	• 소프트웨어 위험원 분석 기법 - 기능 위험원 분석(FHA) - 인터페이스 위험원 분석 (IHA) • 소프트웨어 안전 무결성 수준 결정 방법 - 시스템 안전무결성 수준 상속 - 소프트웨어 특화 평가요소를 추가한 결정 - 소프트웨어 위험 심각도 기반 결정	• 소프트웨어 위험원 분석 및 안전 무결성 수준 결정 결과서
소프트웨어 안전 요구사항 분석		
• 소프트웨어 안전 요구사항 도출 • 소프트웨어 안전 요구사항 추적성 수립 • 소프트웨어 안전 요구사항 검증	• 소프트웨어 안전 요구사항 명세 기법 - 비정형, 준정형 명세 - 안전 요구사항 명세 패턴	• 소프트웨어 안전 요구사항 명세서 • 소프트웨어 안전 요구사항 검증 결과서
소프트웨어 안전 설계		
• 소프트웨어 안전 아키텍쳐 설계 • 소프트웨어 안전 단위 설계 • 소프트웨어 안전 설계 검증	• 소프트웨어 안전 아키텍처 패턴 - 페일 세이프 아키텍쳐 패턴 - 페일 오퍼레이셔널 아키텍쳐 패턴 • 소프트웨어 안전 메커니즘 - 기능 엘리먼트 안전 메커니즘 - 동작환경 엘리먼트 안전 메커니즘	• 소프트웨어 안전 아키텍쳐 설계서 • 소프트웨어 안전 단위 설계서 • 소프트웨어 안전 설계 검증 결과서
소프트웨어 안전 구현		
• 소프트웨어 안전 단위 구현 • 소프트웨어 정적 분석 수행 • 소프트웨어 정적 분석 결과 검토 • 소프트웨어 안전 구현 검증	• 소프트웨어 코딩규칙 - MISRA 코딩 규칙 • 소프트웨어 코드 메트릭 - HIS 코드 메트릭 • 소프트웨어 코드 분석 기법 - 데이터 구조/흐름 분석, 제어 흐름 분석 등	• 소프트웨어 정적 분석 결과서 • 소프트웨어 안전 구현 검증 결과서
소프트웨어 안전 시험		
• 소프트웨어 안전 시험 계획 • 소프트웨어 안전 시험 명세서 작성 • 소프트웨어 안전 시험 수행 • 소프트웨어 안전 시험 검증	• 소프트웨어 안전 시험 유형 - 요구사항 기반 시험, 결함 주입 시험 등 • 소프트웨어 안전 시험 설계 기법 - 명세/구조/경험 기반 시험 설계 • 소프트웨어 안전 시험 커버리지 - 구문, 분기, 변경 조건/결정 커버리지 - 함수/콜 커버리지	• 소프트웨어 안전 시험 계획서 • 소프트웨어 안전 시험 명세서 • 소프트웨어 안전 시험 결과서 • 소프트웨어 안전 시험 검증 결과서
소프트웨어 안전성 평가		
• 소프트웨어 안전성 평가 준비 • 소프트웨어 안전성 평가 수행	• 소프트웨어 안전성 평가 기법 - 위험원 감소 검증 및 잔존 위험 평가 - 안전 케이스(Safety Case)	• 소프트웨어 안전성 평가 결과서

▲ [표] SW 안전활동과 기법, 산출물 상세 내용

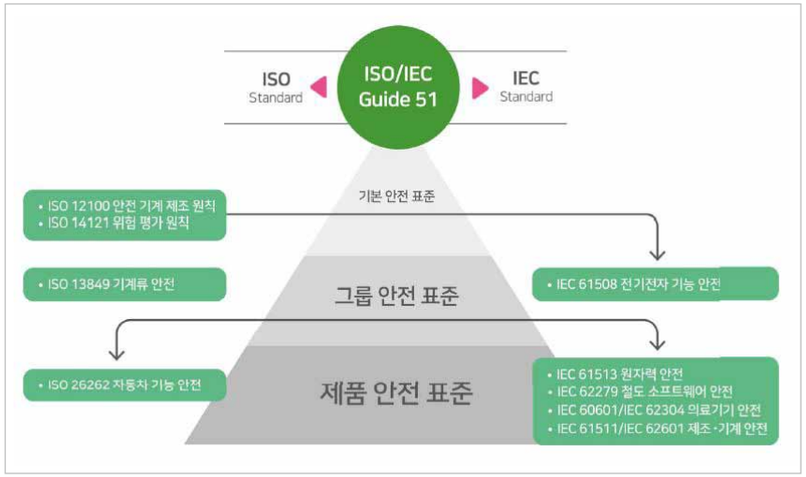
5.1 ISO/IEC Guide 51

개요

ISO/IEC Guide 51은 표준에 안전 관점의 규정을 도입할 경우 지켜야 하는 원칙에 대한 기본적인 가이드라인으로, 대부분의 안전 관련 국제 표준은 ISO/IEC Guide 51 에서 제시하는 개념 및 요건에 따라 안전을 확보하기 위한 기준을 제시하고 있다.

각 표준별 상관관계

ISO/IEC Guide 51 에서는 [그림 4]과 같이 만전 관련 표준을 분류하는 기준을 추가로 제시한다. 안전 관련 표준은 기본 안전 표준, 그룹 안전 표준, 제품 안전 표준으로 분류되며, 하위 표준의 경우 상위 표준에서 산업 분야별로 파생되거나 상위 표준을 기반으로 제·개정된 표준들로 구성된다.



[그림 4] ISO/IEC Guide 51의 안전 관련 표준 분류

* 기본 안전 표준: 광범위한 제품, 프로세스 및 서비스를 대상으로 하는 표준
  - 1S0 12100(안전 기계 제조 원칙), ISO 14121(위험 평가 원칙) 등 일반 안전 표준
* 그룹 안전 표준: 한 무리의 유사한 제품, 프로세스, 서비스를 대상으로 하는 표준
  - ISO 13849(기계류 안전), IEC 61508(전기전자 기능 안전) 등 특정 산업 분야에 한정하지 않고 기계류 또는 전기전자 장치 등을 대상으로 폭넓게 적용되는 안전 표준
* 제품 안전 표준: 특정 분야의 제품, 프로세스, 서비스를 대상으로 하는 표준
  - ISO 26262(자동차 기능 안전), IEC 61513(원자력 안전), IEC 62279(철도 소프트웨어 안전), IEC 60601/IEC 62304 (의료기기 안전), IEC 61511/EC 62601(제조 기계 안전) 등의 산업 분야별 안전 표준

5.2 IEC 61508

개요

1998년 IEC(국제전기 표준회의)에서는 전기, 전자 및 프로그램 가능한 전자 시스템의 기능 안전 표준으로 IEC 61508(Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) 발표하였으며, 국내외에서는 안전 관련 시스템의 의도된 기능 수행에 대한 확신을 마련하기 위하여 IEC 61508 표준에 대해 주목하고 있다. IEC 61508은 또한 ISO/IEC Guide 51에서 정의하고 있는 안전 관련 표준 분류에서 기능 안전 표준의 모표준 역할로 '그룹 안전 표준'의 범주에 속하며, 다양한 산업 분야의 여러 안전 관련 표준들이 IEC 61508을 기반으로 파생되었다.

구성

PART 0	기능 안전성과 IEC 61508	PART 4	정의와 약어
PART 1	일반 요구사항	PART 5	안전무결성 수준 결정 방법
PART 2	전기/전자/프로그램 가능한 전자시스템 및 장치의 안전과 관련된 시스템의 요구사항	PART 6	IEC 61508 Part 2와 Part 3의 적용 지침
PART 3	소프트웨어 요구사항	PART 7	기법과 수단의 개요

IEC 61508과 SW 안전

IEC 61508 Part 3에서는 안전 관련 시스템에 포함되는 SW를 위해 요구되는 안전활동 및 안전기법 관련 요건을 정의하고 있다. 안전 관련 시스템의 구성 중 SW의 경우 실제 고장률을 측정하는 것은 불가능하므로 주로 시스템이 결합되는 하드웨어 및 시스템의 전체 고장 또는 허용 가능한 범위의 고장률을 기반으로 하는 안전무결성 수준을 결정 후, IEC 61508 Part 3에서 제시하는 SW 개발 단계별 요건을 따르도록 하고 있다. 즉, SW에 대해서는 고장률 기반의 안전무결성 수준에 대한 달성 정도를 증명하는 대신 개발 단계별로 안전무결성 수준에 따라 요구되는 항목에 따라 수행한 활동에 대한 증거를 확인함으로써 목표하는 안전무결성 수준을 달성한 것으로 간주한다. 이는 SW의 경우 생명주기 단계에 따라 필수적으로 수행해야 할 활동들을 제대로 수행함으로써 결함이 추가될 가능성을 낮추거나 결함에 대한 예방이 가능하다는 것을 전제로 하고 있다.

5.3 ISO 26262

개요

ISO 26262(Road vehicles-Functional Safety)는 기능 안전 모표준인 IEC 61508을 바탕으로 제정된 자동차 분야의 기능 안전 표준으로서 자동차 내 전기전자 장치의 오동작으로 인한 사고 및 인명 손실 최소화를 목적으로 하는 자동차 전장부품의 안전 개발과 관련된 표준이다.

ISO 26262는 자동차에 탑재되는 전장부품의 개발, 관리, 생산, 운영, 서비스, 폐기 단계를 포함하는 생명주기 단계에 따라 적용이 요구되는 안전활동 및 안전기법을 포함한다.

구성

PART 1	Vocabulary	142개의 용어 및 정의, 53개의 약어 설명
PART 2	Management of Functional Safety	기능 안전 관리를 위한 요구사항의 정의, 개발 활동의 계획, 조정, 추적하는 요건에 대한 기술
PART 3	Concept Phase	제품 및 아이템 정의를 기반으로 위험원 분석과 위험성 평가를 통해 안전무결성 수준(ASIL)을 판정하여, 안전 목표 및 안전 메커니즘 정의
PART 4	Product Development at the System Level:	시스템 레벨에서의 제품 개발 단계에서 수행해야 할 일련의 활동에 대한 명시
PART 5	Product Development at the Hardware Level	개발, 통합, 검증에 대한 요구사항을 포함한 HW 레벨의 개발 활동에 대한 명시
PART 6	Product Development at the Software Level	개발, 통합 검증에 대한 요구사항을 포함한 SW 레벨의 개발 활동에 대한 명시
PART 7	Production and Operation	제품의 생산, 운명, 서비스, 폐기를 위한 요구사항에 대한 요건 정의
PART 8	Supporting Processes	형상관리, 변경관리, 검증, 문서화, 소프트웨어 도구 사용에 대한 신뢰와 사용 증명의 논거 및 주장 등에 대한 요구사항 정의
PART 9	Automotive Safety Integrity Level(ASIL)-oriented and Safety-oriented Analysis	안전무결성 수준(ASIL)과 안전의 분석을 위한 요구사항의 기술
PART 10	Guideline on ISO 26262	ISO 26262의 전반적인 이해에 도움을 주기 위한 주요 개념, 안전 케이스, 안전무결성 수준(ASIL) 분해 등과 같은 정보에 대한 요약 설명 기술
PART 11	Application of ISO 26262 to Semiconductor	차량용 반도체 개발에서의 ISO26262 적용

ISO 26262와 SW 안전

ISO 26262에서는 SW 안전과 관련하여 SW 안전 생명주기 단계를 구분하고, 각 단계별로 안전무결성 수준에 따라 적용이 필요한 활동 및 기법을 제시한다.

5.4 IEC 62279

개요

철도 분야에서는 사용되는 제어, 명령 및 보호 시스템(Control, Command and Protection System)의 안전을 높이기 위해 다양한 국제 표준을 제정하였다. 철도 선진국인 유럽에서 주도하며 유럽 표준인 CENELEC EN 50126, EN 50128. EN 50129, EN 50159를 먼저 제정하고 이후 이들 유럽 표준은 각각 IEC 62278, IEC 62279, IEC 62425, IEC 62280으로 국제 표준화되었다. 이 중 철도 분야 제어 및 보호 시스템의 SW 개발과 관련된 표준인 IEC 62279에서 SW 안전 개발에 필요한 SW 안전활동 및 기법을 정의하고 있다.

구성

PART 1	Scope	표준의 범위, SW의 개발을 위한 프로세스와 기술적 요구사항
PART 2	Normative references	IEC 62278, ISO/IEC 90003, ISO/IEC 25010 등을 명시
PART 3	Terms, definitions and abbreviations	표준 내 사용되는 용어 및 정의, 약어
PART 4	Objectives, conformance and software safety integrity levels	안전무결성 수준에 대한 설명 및 안전무결성 수준을 충족하기 위한 원칙
PART 5	Software management and organization	안전무결성 수준에 따른 조직, 역할 및 책임의 독립성 요구사항, 안전활동 수행을 위한 역량 요구사항, SW 개발 생명주기 구성
PART 6	Software assurance	검증(Verification), 확인(Validation), 안전성 평가, 품질 보증, 변경 관리, 지원 도구 및 언어 관리를 포함한 SW 개발 결과물 전반의 품질 보증을 위한 요구사항 기술
PART 7	Generic software development	SW 개발 생명주기 단계를 소프트웨어 요구사항, 아키텍처 디자인, 컴포넌트 디자인, 컴포넌트 구현 및 테스트, 통합, 확인 단계로 구분하고 각 단계별 활동 및 산출물에 대한 요구사항 기술
PART 8	Development of application data or algorithms	별도 설정을 통해 기능이 구성되는 시스템의 경우 적용되어야 하는 설정 데이터 및 알고리즘 개발과 관련한 요구사항 기술
PART 9	Software deployment and maintenance	SW 배포 이후의 유지보수 관련 요구사항 기술

IEC62279와 SW 안전

IEC 62279의 경우 표준의 적용 범위가 SW로 한정되어 있기 때문에 '7. Generic software development'에 기술된 SW 개발 생명주기 단계별 안전활동 및 산출물에 대한 요구사항을 포함하여 IEC 62279에 기술된 모든 요구사항은 철도 분야의 안전 관련 SW 개발 시 반드시 만족해야 한다.

5.5 IEC 62304

개요

IEC 62304(Medical device software - Software life cycle processes)는 의료기기 SW 생명주기와 관련된 요구사항을 다루는 표준이다. 여기서 의료기기 SW란 개발된 의료기기 내에 통합되는 목적으로 개발된 SW 시스템 또는 의료기기로의 사용이 의도된 SW 시스템을 의미한다.

IEC 62304에서는 의료기기 SW를 개발 및 관리하기 위해 Class라는 안전 등급 분류 방식으로 SW 안전무결성 수준을 정의하고 있다. Class는 해당 의료기기 SW에 의해 위험이 발생할 경우 환자에게 얼마만큼의 피해를 야기하는지를 판단하여 구분하며, IEC 62304에서 제시하고 있는 Class별 피해 상태는 다음과 같이 정의된다.

- Class A: SW 시스템이 위험한 상황을 야기하지 않음
- Class B: SW 시스템이 위험한 상황을 야기할 수 있고 식별된 위험이 수용 불가능한 상태이며, 위험 발생 시 환자에게 경상 발생 가능함
- Class C: SW 시스템이 위험한 상황을 야기할 수 있고 식별된 위험이 수용 불가능한 상태이며, 위험 발생 시 환자에게 중상 또는 환자 사망 발생 가능함

구성

PART 1	Scope	표준의 범위
PART 2	Normative references	본 표준과 연관된 표준
PART 3	Terms, definitions and abbreviations	표준 내 사용되는 용어 및 정의, 약어 기술
PART 4	General requirements	품질관리 요구, 위험관리 요구, SW 안전 등급 분류
PART 5	Software development process	SW 개발 프로세스별 안전 활동
PART 6	Software maintenance process	SW 유지보수 프로세스별 안전 활동
PART 7	Software risk management process	위험 관리를 위해 수행되어야 하는 활동
PART 8	Software Configuration management process	형상관리 활동
PART 9	Software problem resolution process:	문제의 해결을 위해 수행되어야 하는 활동

IEC 62304와 SW 안전

IEC 62279와 마찬가지로 IEC 62304의 경우도 표준의 적용 범위가 SW로 한정되어 있다. 때문에 의료기기 SW 개발 시에는 '5. Software development process'에 기술된 SW 개발 생명주기 단계별 안전활동 관련 요구사항을 반드시 만족해야 하며 기타 IEC 62304에서 언급하고 있는 유지보수 및 형상관리와 같은 SW 개발 지원 활동과 관련한 요구사항 또한 만족해야 한다.

5.6 RTCA DO-178C

개요

항공 SW의 오동작 혹은 결함 등을 최소화하기 위해 항공기에는 항공기 충돌 방지장치(Airborne Collision Avoidance System, ACAS)와 공중 충돌 방지장치(Traffic Collision Avoidance System, TCAS) 등과 같은 항공 전자장비가 내장돼 있는데 SW 안전과 안전성 확보는 항공산업에 있어 매우 중요하다. 이에 항공기와 항공기에 탑재되는 항공 전자장비의 안전에 관한 여러 표준이 제정되었고, 항법에 영향을 미치는 항공기 탑재 장비의 감항 요구사항[1] 준수를 목표로 하는 항공기 형식 인증의 표준으로 활용되고 있다. 미연방항공청(Federal Aviation Administration, FAA)과 국제 민간 항공기구(International Organization, ICAO) 등의 규제 당국에서 요구하는 항공기의 안전에 관한 표준이 있다.

1) 감항 요구사항 : 항공기가 항공하기에 적합한 안전성과 신뢰성을 갖추는 것

구성

Section 1	Introduction	DO-178C 소개
Section 2	System Aspects relating to Software Development	시스템 관점의 SW 개발 활동
Section 3	Software Life Cycle	SW 개발 생명주기와 시스템 개발 생명주기 간의 연관성
Section 4	Software Planning Process	SW 계획 프로세스
Section 5	Software development process	SW 개발 프로세스
Section 6	Software Verification Process	SW 검증 프로세스
Section 7	Software Configuration Management Process	SW 형상관리 프로세스
Section 8	Software Quality Assurance Process	SW 품질보증 프로세스
Section 9	Certification Liaison Process	SW 인증 연계 프로세스
Section 10	Overview of Certification Process	인증 프로세스 개요
Section 11	Software Life Cycle Data	SW 생명주기 정보
Section 12	Software problem resolution process:	추가 고려사항(도구 자격 인증, 대안 방법 등)

RTCA DO-178C와 SW 안전

항공기의 경우 사고 발생 시 막대한 재산 및 인명 피해를 유발하기 때문에 항공기 SW 개발에 있어 감항 요구사항의 준수는 매우 중요하다. D0-178C는 항공기 시스템과 장비용 SW 개발 시 감항 요구사항을 충족시키는 수준의 안전성을 갖출 수 있도록 지침을 제공하는 것을 목표로 개발되었다. 미연방항공(FAA)는 DO-178C 표준을 항공기 SW 인증을 위한 용도로 사용하는 것을 인정하였으며 관련 산업계에서는 상용 항공기에 탑재되는 항행안전시스템의 SW 개발을 위한 산업계 표준(De facto)으로 활용하고 있다.

SW안전 적용사례 10선

○ “후원 : 과학기술정보통신부 정보통신진흥기금”

○ “이 SW안전 적용사례 10은 「과학기술정보통신부 정보통신진흥기금」을 지원받아 제작한 것입니다”

○ “이 SW안전 적용사례 10은 「과학기술정보통신부 정보통신진흥기금」을 지원받아 제작한 것으로 과학기술정보통신부의 공식의견과 다를 수 있습니다”

SW안전 적용사례 10

과학기술정보통신부 Ministry of Science and ICT
nipa 정보통신산업진흥원 National IT Industry Promotion Agency

(27872) 충청북도 진천군 덕산읍 정통로 10
TEL. 043-931-5000 FAX. 043-931-5129

발간일 : 2021.12
발간인 : 정보통신산업진흥원
편집인 : 나이스컨설팅