상상을 현실로,
소프트웨어가 미래다

2018 SW산업 제조 안전가이드

2018 SOFTWARE SAFETY GUIDE

nipa 정보통신산업진흥원
National IT Industry Promotion Agency

CONTENTS

표 목 차

그림 목차

제 1 장 서론

서론

1.1. 배경 및 필요성

소프트웨어(이하 SW)가 사회 각 분야를 주도하는 SW 중심사회가 도래하면서 국민 안전 확보를 위한 핵심요소로 부각되고 있다.

철도, 항공, 제조, 의료 등 국가 기반시설 및 주요 산업분야에서 비중이 나날이 증가하고 있는 기능안전과 관련 된 SW의 결함 발생 시 대형 인명사고 및 엄청난 경제적, 사회적 비용을 유발할 수 있으며, 이러한 SW 안전성 확보는 국민 안전과 대규모 경제적, 사회적 손실 방지를 위해서도 매우 중요하다 할 수 있겠다.

또한 산업의 수출 확대 측면에서도 SW 안전성 확보는 중요한 과제이다. 선진국이나 개발도상국의 경우 자국의 안전을 위해 주요 산업 분야에서 SW 안전성이 확보된 제품을 사용하도록 하고 있으며, 이를 위해 별도의 법이나 규정으로 표준 규격과 기술 기준을 준수하도록 하고 있다.

제조분야의 시스템 안전표준의 경우, 4차 산업혁명의 핵심인 스마트공장 분야의 자동화 시스템에서 발생 가능한 위험을 식별하고 이를 저감, 회피, 예방 할 수 있는 안전 요건을 제시해 안전사고 및 인명손실의 최소화를 목적으로 하고 있는 IEC 62061(Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems), IEC 61511(Safety instrumented systems for the process industry sector)의 국제 안전표준을 제정해 준용하고 있는 추세이다.

하지만 이러한 표준은 기법과 목표 수준만을 명시하고 있어 관련 중소기업들이 실무에서 해당 표준을 적용해 제품을 개발하는데 있어 어려움이 있다. 이를 해결하기 위해 실무차원의 수행 기법 및 목표 수준 달성을 위한 가이드라인과 현장에서 용이하게 활용 가능한 적용사례가 필요하며, 이론적인 수준에서의 개발이 아닌 실무 적용 후 사용성과 내용이 검증 된 가이드라인이 필요하다.

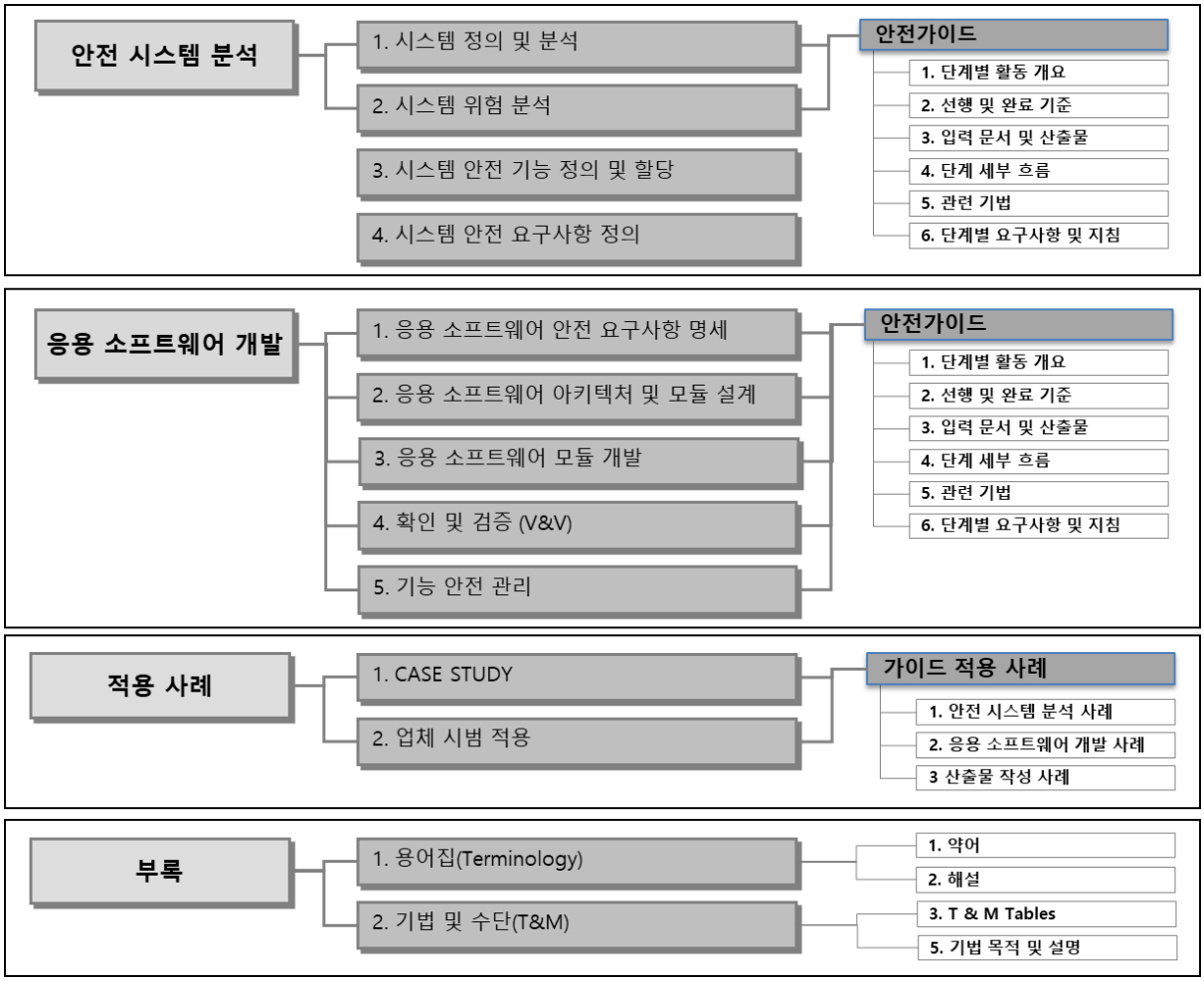
1.2. 목적

제공 공정에 사용되는 기계 장비 시스템의 기능안전 표준인 IEC 62061과 공정 장치 산업의 계장시스템의 기능안전 표준인 IEC 61511는 관련 시스템을 개발, 제작하는 국내 중소 기업체의 실무현장에서는 안전표준을 충분히 이해하고 적용할 수 있는 조직역량이 부족하여 관련 안전 표준을 적용하는데 어려움이 있다.

따라서 본 과제를 통해 IEC 62061 및 IEC 61511 기반으로 현장에서 쉽게 이해하고, 적용이 가능한 제조분야 안전가이드를 개발, 배포함으로써 국내 제조분야의 중소기업체들이 관련 산업군의 시스템을 개발함에 있어 신뢰성과 안전성을 확보하여, 국내 및 국제 시장에서의 경쟁력을 제고하는데 그 목적이 있다.

1.3. 가이드 범위 및 구성

본 제조분야 소프트웨어 안전 가이드에서 다루는 내용의 범위와 구성은 [그림] 과 같다. 가이드는 크게 제조 분야 안전 시스템의 분석을 다루는 "안전 시스템 분석" 영역과 안전 시스템의 제어 역할을 수행하는 "응용 소프트웨어 개발" 영역으로 나뉜다. 안전 시스템 분석과 응용 소프트웨어 개발에 대한 가이드의 적용 방법은 "적용 사례" 영역에서 다루며 전체 가이드와 관련 된 용어와 가이드 적용에 필요한 기법 및 수단은 "부록" 영역에서 다루고 있다.



1.4. 참고 표준

본 가이드는 [표 1]의 표준을 참고하여 개발하였다.

표 1 참고 표준

작성	문서 번호	문 서 명
IEC/ISO	61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC/ISO	61511	Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework definitions, system, hardware and application programming requirements
IEC/ISO	62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
ISO	12100	Safety of machinery — General principles for design — Risk assessment and risk reduction
IEC	TR 61311-3	Programmable Controllers – Part 3 Programming languages
IEC	TR 61311-4	Programmable Controllers – Part 4: User guidelines
IEC	TR 61311-8	Programmable Controllers – Part 8: Guidelines for the application and implementation of programming languages

1.5. 참고 문헌

1. 지은희, 최무이, 예영선, "2017 소프트웨어산업 전망", 소프트웨어정책연구소, 2017년 2월.
2. 이민창, 김태윤, 김성준, "산업안전보건의 규제제도에 관한 연구", 안전보건공단, 산업안전보건연구원, 2016년 10월.
3. 정보통신기술진흥센터, "2017년도 글로벌 상용SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017년 9월.
4. 안전보건공단, 중대재해사례집, 2013년 10월.
5. Wikipedia, 엑슨발데즈 원유 유출사고, 2018년.
6. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems in IEC 61508 : 2010(E). : International Electrotechnical Commission, (2010)
7. Safety of machinery — General principles for design — Risk assessment and risk reduction in IEC/ISO 12100:2010(E).
8. 방위사업청, 시스템엔지니어링 가이드북 Version 1.0, 2007 년, 10 월.
9. 한국산업안전보건공단, KOSHA GUIDE-안전무결성등급(SIL)의 산정에 관한 지침, 2012 년 6 월.
10. 한국산업안전보건공단, KOSHA GUIDE-방호계층분석(LOPA) 기법에 관한 기술지침, 2012 년 7 월.
11. 한국산업안전보건공단, 현장적용이 용이한 화학공장의 위험성 평가 기법 개발, 2005 년 12 월.
12. Norskoilje&gass, Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, 2018
13. 정소연, "위험사건발생빈도를 이용한 해저방폭장치 안전계장시스템의 안전무결성등급 평가", 학위논문(공학박사), 서울대학교 산업/조선공학과, 2016 년 7 월.
14. Industrial Text & Video Company, Introduction to PLC Programming and Implementation – from Relay Logic to PLC Logic, 1999 년
15. MITSUBISHI, 마이크로 PLC 교육교재 – 알기 쉬운 PLC 기초편, 2000 년

16. SafeProd, Application software design Guideline, 2006
17. SafeProd, Safety Requirements Specification Guideline, 2005
18. James A. Regh, Structured PLC Programming with Sequential Function Charts, Pennsylvania State University, 2001
19. ITER, PLC Software Engineering Handbook, 2013
20. LS 산전, 프로그래머블 로직 컨트롤러 – 위치 결정 모듈 사용설명서, 2014 년 7 월
21. SIEMENS, Safety with of without Standard PLC, 2016
22. Unitywater, Pr9833 – SCADA and PLC Architecture, 2018
23. Rockwell Automation, Safety Function: Emergency Stop with a Configurable Safety Relay, 2008
24. Rockwell Automation, Safety related control systems for machinery – principles, standards and implementation, 2016
25. Tim Roback, Introduction to Functional Safety for Machinery, Rockwell Automation, 2014

제 2 장. 제조 산업 현황

현황 조사

2.1. 산업현황

2.1.1. 국내 제조산업 현황

[1] 제조산업 트렌드

제조업을 고부가가치 산업으로 변화시키기 위해서 생산설비의 기계화, 자동화, 집중화가 성공적으로 이루어졌다. 최근에는 제조업이 ICT 인프라 결합하여 제품 생산과정의 서비스화 디지털화와 같은 새로운 방향으로 진화할 것으로 기대한다.

미국, 유럽, 일본 등과 같은 선진국들은 ICT 인프라와 제조 공장을 결합하여 해외에 있는 제조 공장들을 자국 내로 복귀시키는 리쇼어링(Reshoring)을 강화하고 있다. 이러한 영향으로 선진국들의 제조업 경기가 회복되고 있으며, 특히, 일본의 장기간 지속되었던 경기침체가 회복 조짐을 보이고 있다.

글로벌 경제위기 전까지 제조 산업 비중이 줄어들고, 서비스 산업 비중이 높아지면서 탈공업화가 진행되었다. 하지만 글로벌 경제위기를 겪은 국가들 중에서 제조업이 강한 독일, 오스트리아, 핀란드 등의 국가들이 빠르게 경기를 회복하였고, 제조업 비중이 상대적으로 낮은 나라들인 그리스, 포르투갈, 스페인 등은 마이너스 성장을 기록하였다. 따라서 글로벌 경제위기 이후 제조업 지원 정책을 기반으로 국가 성장 전략을 재편하는 등 제조업의 중요성이 재조명되고 있다.

[2] 제조업 PMI 동향

PMI (Purchasing Management Index)는 제조업체에서 물건구매를 담당하는 직원이 현재 혹은 향후 경기를 좋게 보는지 나쁘게 보는지를 의미한다. 미국은 2009년 이후 제조업 경기가 지속적으로 좋아지는 추세이다. 2010년 이후 PMI가 최고 수준을 유지하고 있다. [그림 1 미국 연간 PMI 추이는 2007년부터 2010년까지 미국 연간 PMI 추이를 나타낸다.

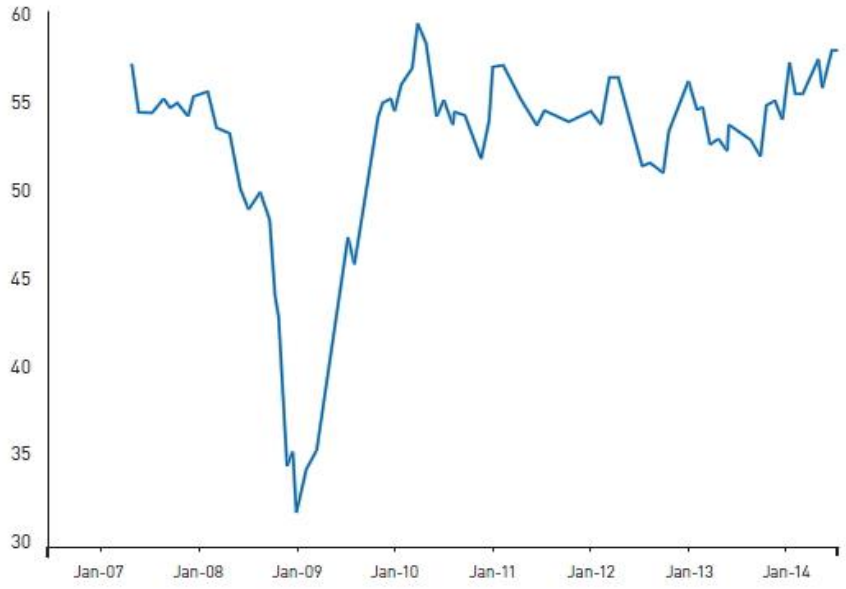


그림 1 미국 연간 PMI 추이

출처: Markit (영국 금융정보서비스 기업)

유럽은 글로벌 금융위기 직후 PMI 지수가 급격하게 하락하였고, 잠시 회복세에 접어들었으나 2011년 하반기부터 하락세를 보였다. 하지만 2013년 하반기부터 50 이상을 기록하여 경기가 확장되는 추세에 있다. [그림 2]는 1998년부터 2014년까지 EU 연간 PMI 추이를 나타낸다.

그림 2 EU 연간 PMI 추이

출처: Markit (영국 금융정보서비스 기업)

한국 제조업 경기는 글로벌 경제위기 이후 PMI가 50을 넘으며, 회복 추이에 있었지만 신규 주문 수주 감소와 생산활동 보류 및 고용의 감소로 인하여 PMI가 감소하는 추세이다. 하지만 2018년 6월 지표는 5월의 48.9보다 상승한 49.8을 기록하면서 3월 이후 지속되었던 제조업 경기 약세 흐름을 마감하였다. [그림 3는 2004년부터 2018년 6월까지의 Nikkei 한국 PMI한국 제조업 연간 추이를 나타낸다.

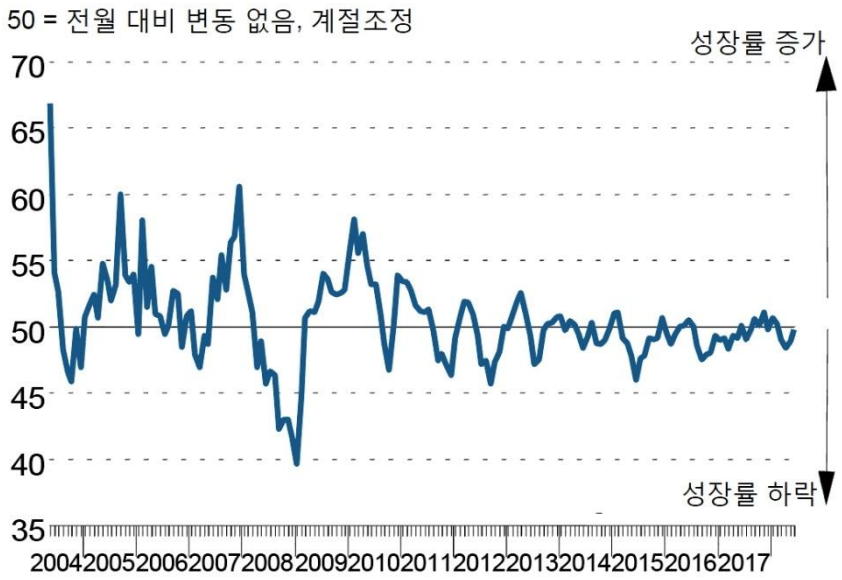


그림 3 한국 연간 PMI 추이

출처: HIS Markit

[3] 일반 기계산업 동향

기계산업은 생산기술 축적을 위해 지속적이고, 대규모의 투자가 필요한 산업이다. 이러한 투자가 지속되어 경쟁력이 확보되면 장기 성장동력이 된다. 2013년도 부가가치유발계수는 기계 (0.65), 화학 (0.48), 전기전자 (0.52), 자동차 (0.620 로 기계산업의 부가가치유발계수가 다른 산업에 비해 높은 것을 확인할 수 있다. 또한, 2013년도 고용유발계수는 기계 (6.65), 화학 (4.31), 전기전자 (3.96), 자동차 (6.19)이다. 따라서 기계 산업은 자본 집약적이며, 기술인력 의존도와 부가가치가 높은 고용창출 산업이다.

일반 기계 산업의 수급구조는 중소기업에서 기계 부품을 제작하고, 이 부품들을 완제품의 형태로 대기업 또는 중기업에서 제작하여 대기업에서 최종 소비하는 3단계로 구분된다. 국내 제조업에서 기계류 수요가 차지하는 비중은 평균적으로 전자선업이 45%, 기계 산업이 24%, 자동차 19%, 조선 포함 기타 운송장비 4%, 기타 8% 등이다.

기계 산업은 표준산업분류와 산업통상자원부의 MTI 분류가 있다. 표준산업분류에 따르면 일반 기계 산업은 일반 목적용 기계와 특수 목적용 기계로 분류되며, 하위 18개의 세분류가 있다. [표 2는 표준산업분류 상의 일반기계를 정리한 것이다. MTI 분류에 따른 일반 기계 산업은 기초 산업 기계, 산업 기계, 기계 요소 공구 및 금형, 기타 기계류로 분류되며, 하위 18개의 세분류가 존재한다. [표 3]은 MTI 상의 일반기계를 정리한 것이다.

표 2 표준산업분류 상의 일반 기계

중분류	소분류	세분류
일반 산업 기계	일반 목적용 기계 제조업	내연기관 및 터빈 제조업; 항공기용 및 차량용 제외
		유압기기 제조업
		펌프 및 압축기 제조업; 탭, 밸브 및 유사장치 제조 포함
		베어링, 기어 및 동력전달장치 제조업
		산업용 오븐, 노 및 노용 버너 제조업
		산업용 트럭, 승강기 및 물품취급장비 제조업
		냉각, 공기조화, 여과, 증류 및 가스발생기 제조업
		사무용 기계 및 장비 제조업
		기타 일반 목적용 기계 제조업
	특수 목적용 기계 제조업	농업 및 임업용 기계 제조업
		가공공작기계 제조업
		금속주조 및 기타 야금용 기계 제조업
		건설 및 광산용 기계장비 제조업
		음, 식료품 및 담배 가공기계 제조업
		섬유, 의복 및 가죽 가공기계 제조업
		반도체 및 평판 디스플레이 제조용 기계 제조업
		산업용 로봇 제조업
		기타 특수목적용 기계 제조업

표 3 MTI 상의 일반기계

중분류	소분류	세분류
MTI 일반 기계	기초 산업 기계	원동기 및 펌프
		운반하역 기계
		공기조절기 및 냉난방기
		사무 기기
		광학 기기
	산업 기계	섬유 및 화학 기계
		목재광물 및 유리 가공 기계
		금속공작 기계
		식품가공포장 기계
		건설 광산 기계
		압연기 용접기 및 주조 설비
		제지 인쇄 기계
		농기계
		기타 산업 기계
	기계요소 공구 및 금형	기계 요소
		공구
		금형
	기타 기계류	기타 기계류

2.1.2. 해외 제조산업 현황

[1] 미국 제조산업 동향

미국은 글로벌 금융위기 이후에 제조업을 발전시키고, 경쟁력을 강화하기 위하여 국가 협의체와 과학기술 단체 등을 통해서 대규모 연구개발 투자를 실시하고 있다. 특히, 제조업 르네상스 정책의 일환으로 차세대 제조업 11대 기술분야를 선정하여 집중 육성할 계획을 갖고 있다. [표 4]는 미국의 차세대 제조업 11대 기술분야와 주요 내용이다.

표 4 차세대 제조업 11 대 신기술 분야

11 대 신기술	주요 내용
첨단 센서, 측정, 공정 컨트롤 기술	- 거의 모든 산업분야에 적용 - 제품의 공급망 효율화 제고를 위해 중요한 역할을 할 것으로 전망
첨단소재의 설계, 합성, 가공 기술	- 초소형 분자와 나노물질의 설계 및 합성, 코팅, 통합부품제조에 적용 - 첨단소재를 통한 수십억 달러 규모의 신규산업 창출 효과
지속가능성을 높인 제조 기술	- 원자재, 에너지, 자원 활용의 최적화가 필요한 모든 분야 - 에너지 소모가 많은 제조업 부분에서 부품재활용 기술 등을 통해 에너지소비를 줄이고 수익성을 제고
나노 제조 기술	- 태양전지, 의료, 차세대 전자 및 컴퓨팅 등 여러 분야에 적용되어 업계의 판도를 바꿔 놓을 대변혁을 야기 - 공정 및 품질관리 시스템 개발이 선결 조건
플렉서블 전자 제조 기술	- 차세대 가전 및 컴퓨팅 기기의 차별화를 뒷받침할 기술 - 향후 10 년간 가장 빠르게 성장하는 제품영역이 될 전망
바이오제조 및 바이오 정보 기술	- 헬스케어, 식품안전, 에너지 효율적 제조과정을 위해 적용 - 바이오나노 인터페이스의 혁신으로 나노제조 기술의 비용이 저렴해지면서 시장 확산도 가속화될 것으로 기대
첨삭가공 기술	- 개인화 및 맞춤화 추세에 따라 제조업

11 대 신기술	주요 내용
	부문에서 첨삭가공 기술의 적용범위도 점차 확대 - 제조 과정에서 원료의 손실을 최소화하는 효과
첨단제조 및 검사장비 기술	- 전세계 다양한 지역에서 활발하게 개발되고 적용되는 기술 - 이 분야 장비공급자가 될 경우 경제적 이익과 더불어 혁신과 첨단엔지니어링 부분에서도 유리한 위치를 확보
산업용 로봇 기술	- 노동 집약적 제조과정에서 자동화 및 로봇 기술 적용 확대 - 작업장에서의 안전과 생산성 향상 및 저비용 생산구조 정착에 기여할 전망
첨단금형 및 접합 기술	- 기존의 제조과정에서 사용되는 전통적인 주물, 용접, 단조, 기계가공 기술을 보완 및 대체 - 미래 제품가공방식의 혁신과 효율성 재고에 기여할 전망
시각화, 인포매틱스, 디지털 제조 기술	- 부식 및 고온처리를 위한 임베디드 센서, 측정, 컨트롤 시스템 부문 등에 적용 - 제품의 설계, 제조, 출시 속도를 높여 차별화 요소로 부각

출처: 한국정보화진흥원, 2014 년 6 월.

[2] 독일 제조산업 동향

독일은 ICT와 제조업을 결합하여 스마트팩토리로 진화하는 인더스트리 4.0 전략을 추진하고 한다. 이를 통해서 제조업의 비중을 증가시키고, 노동생산성을 높이려는 목표를 갖고 있다. 특히, 인더스트리 4.0 구현을 위하여 2억 유로를 투자

하고 있으며, 스마트팩토리 구축, 사이버물리 시스템 및 인공지능 시스템 구현, 기술개발 확산, 통신 및 네트워크 기술 개발 등의 연구를 추진하고 있다. [표 5]는 인더스트리 4.0의 주요 연구개발 프로젝트와 주요 내용이다.

표 5 인더스트리 4.0 의 주요 R&D 프로젝트

프로젝트	주요 내용	기간	예산 (€)	참여기관 수
CyProS	스마트 공장의 CPS 운용방식과 도구 개발	12. 09 ~ 15. 09	약 560 만	21 개
KapaflexCy	CPS 를 활용한 유연한 생산시스템 구축	12. 09 ~ 15. 09	약 270 만	10 개
ProSense	인공지능 시스템과 지능형센서 기반의 생산관리 실현	12. 09 ~ 15. 09	약 308 만	9 개
Autonomik	통신 (인터넷) 기능, 상황감지 및 적응 기능, 기기 간 상호작용이 가능한 스마트 툴 개발	2013 ~ 2017	약 4,000 만	미정

출처: 현대경제연구원 재인용, 2014 년 2 월 27 일.

[3] 일본 제조산업 동향

일본은 2013년도에 산업재행플랜을 제시하였다. 산업재행플랜은 제조업의 경쟁력 강화를 위하여 6대 전략과 27개 과제로 구성되었다. 일 총무성에서 제시한 산업재행플랜의 주요 과제는 긴급구조개혁 프로그램, 고용제도 개혁 및 인재역량 강화, 과학기술 이노베이션 추진, 세계 최고수준의 IT 사회 실현, 입지경쟁력 강화, 중소기업 및 소규모 사업자 혁신이다. [표 6]는 국토연구원에서 정리한 일본 제조업 혁신을 위한 주요과제이다.

표 6 일본 산업재행플랜 주요 과제

프로젝트	주요 내용
긴급구조개혁 프로그램 (산업신진대사 촉진)	민간투자 활성화, 규제개혁, 벤처 및 신사업 창출기반 정비, 경영개혁, 과잉공급, 과당경쟁 구조개선, 해외사업 등

프로젝트	주요 내용
고용제도 개혁 및 인재역량 강화	노동이동 지원, 노동수급 매칭 기능 강화, 최저임금 인상, 여성, 청년, 고령자 취업 확대, 대학개혁, 외국인재 활용 등
과학기술 이노베이션 추진	종합과학기술회의 기능 강화, 전략적 이노베이션 창조프로그램 창설, 연구개발 투자 확대 등
세계 최고수준의 IT 사회 실현	규제개혁, 공공데이터 민간개방, IT 활용의 생활환경 개선, 통신인프라정비, 사이버 안전대책, 인재양성 등
입지경쟁력 강화	국가전략특구 창설, 공공시설운영권 민간개방, 공항 및 항만 정비, 도시경쟁력 향상, 환경 및 에너지 제약 극복 등
중소기업 및 소규모 사업자 혁신	지역자원 활용 창업촉진, 지방산업경쟁력협의회 설치, 일관된 자금지원, 성장분야 진입지원, 해외진출지원 등

출처: 국토연구원, 2014 년 7 월 22 일.

2.1.3. SW 산업 동향

[1] 국내 SW 산업 실적

2016년 SW 시장은 3.9%의 성장률을 기록하고, 113억 달러의 시장을 형성하였다. 특히, 패키지 SW는 7.0% 성장하였고, 42억 달러의 시장을 형성하였다. 또한 IT 서비스는 2.1% 성장하였고, 71억 달러 시장을 형성하였다.

2016년 SW의 생산은 2015년에 비해서 4.2% 성장한 41.1조원을 기록하였다. 특히, 패키지 SW는 2015년도 대비 7.2% 성장한 9조원을 기록하였고, IT 서비스는 3.3% 성장한 21.1조원을 기록하였다.

2016년도에는 패키지 SW 수출에서 성장이 지속되어서 2015년도 대비 6.0% 성장한 63.8억 달러를 기록하였다. [그림 4]는 2016년도 SW 산업 실적을 시장, 생산, 수출에 따라서 정리한 것이다.

그림 4 2016 년 SW 산업 실적

출처: 지은희, 최무이, 예영선, "2017 소프트웨어산업 전망", 소프트웨어정책연구소, 2017 년 2 월 28 일.

[2] 주요 SW 기업 활동

[표 7] 패키지 SW, IT 서비스, 인터넷 SW, 게임 SW의 각 부문에서 주요 기업들의 활동을 정리한 것이다.

표 7 주요 SW 기업 활동

분야	주요 기업	주요 활동
패키지 SW	더존비즈온, 영림원소프트랩, 엑셈 등	클라우드 기반의 서비스 개발 및 시장 진출
	한글과컴퓨터, 티맥스소프트 등	중국, 인도, 미국 등에 맞춤형 SW 제공
	더존비즈온, 와이즈넛 등	빅데이터와 인공지능 기술을 자사 제품에 적용하여 데이터 분석 서비스 제공
IT 서비스	삼성 SDS, SK㈜ C&C 등	IoT 플랫폼 기반의 물류 솔루션 개발 및 보급
	롯데정보통신, 코오롱베니트 등	계열사의 물류 IT 솔루션 서비스 시작
	삼성 SDS, LG CNS, SK㈜ C&C	현기 기업들과 합작회사 설립 및 협력을 통한 신산업 분야의 해외진출 추진
	LG CNS, SK㈜ C&C	인공지능, 빅데이터, IoT 기술 확보를 통한 다양한 산업 분야에 특화된 플랫폼 제공
인터넷 SW	네이버	- 지도 기반의 택시 및 네비게이션 서비스 제공 - 인공지능 대화시스템, 통번역 및 커넥티드카 등의 기술 확보
	다음카카오	'O2O for kakao' 플랫폼 구축 추진
	인터파크	빅데이터 기술을 통한 개인 맞춤형 쇼핑 지원
게임 SW	한빛소프트, 드래곤플라이 등	가상현실, 증강현실 게임 개발

출처: 지은희, 최무이, 예영선, "2017 소프트웨어산업 전망", 소프트웨어정책연구소, 2017 년 2 월 28 일.

[3] 주요 SW 기업 실적

2016년도 국내 SW 기업의 매출액은 2015년에 비해서 4.1% 증가하였다. 패키지 SW는 IoT, 클라우드 등의 영역에서 보안 솔루션을 제공하여 2.2% 성장을 이루었다. IT 서비스는 해외 수출 증가와 신사업 진출로 인하여 2015년에 비해서 2.0% 성장이 이루어졌다. 게임 SW는 2015년에 비해서 19.8% 매출규모가 증가하였다. 인터넷 SW는 지속적으로 고성장을 유지하고 있으며, 2016년도 매출증가율은 전년도에 비해 14.7% 증가하였다. 임베디드 SW는 국내 제조업의 전반적인 경기하락으로 2015년에 비해서 5.2% 감소하였다. [그림 5]은 2016년 SW 기업 매출 추이이다.

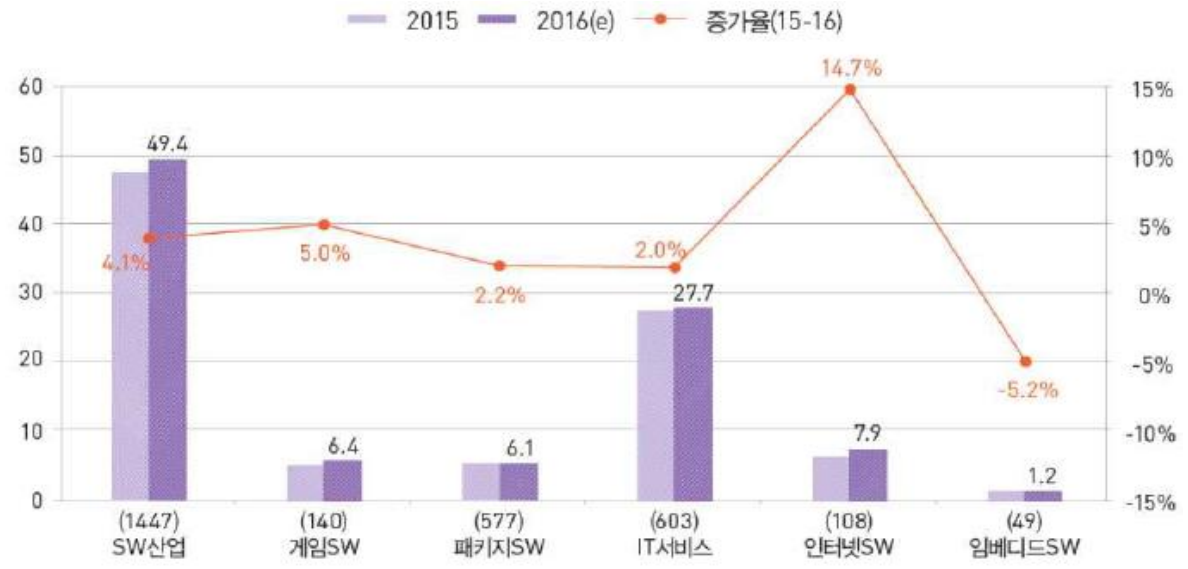


그림 5 2016 년 SW 기업 매출 증가 추이

출처: 지은희, 최무이, 예영선, "2017 소프트웨어산업 전망", 소프트웨어정책연구소, 2017 년 2 월 28 일.

2.2. 국내 안전 체계

2.2.1. 국내 안전관련 법 체계

우리나라의 안전관련 법은 1946년 '최고노동시간과 미성년보호법'으로 출발하였다. 이후, 1953년 노동법으로서는 최초로 '근로기준법'이 제정되었고, 설비 및 환경에 대한 일정 기준이 설정되었다. 1960년부터 1973년까지 산업재해예방을 위한 체제가 구축되었다. 1961년 '근로보건관리규칙', 1962년 '근로안전관리규칙', 1963년 '광산보안법', '산재보상법'이 제정되었고, 1973년에는 '대한산업안전협회'가 발족되었다.

1981년에는 법률 제3532호 '산업안전보건법'이 제정되었으며, 노동부 '산업안전과'가 신설되었다. 1989년에는 '한국산업안전공단'이 설립되었고, 2009년에 '한국산업안전보건공단'으로 명칭이 변경되었다.

[1] 산업안전보건법령 계층 구조

산업안전보건 법령은 산업안전보건법, 산업안전보건법 시행령, 산업안전보건법 시행규칙, 산업안전보건 기준에 관한 규칙, 유해, 위험 작업의 규칙 등으로 구성되어 있다. 이 중 산업안전보건 기준에 관한 규칙은 총 조문이 670조항 이상이며, 사업주가 지켜야 할 안전 및 보건조치에 대하여 상세하게 규정되어 있다. [그림 6]은 산업안전보건법령의 계층 구조를 정리한 것이다.

<table>
<tr><td>제・개정권자</td><td colspan="4">법령 및 행정규칙</td><td>법적 성격</td></tr>
<tr><td>국민투표</td><td colspan="4">기본법 (헌법)</td><td rowspan="3">법령</td></tr>
<tr><td>국회</td><td colspan="4">산업안전보건법 (법률)</td></tr>
<tr><td>대통령</td><td colspan="4">산업안전보건법 시행령 (대통령령)</td></tr>
<tr><td rowspan="3">노동부 장관</td><td colspan="4">노동부령</td><td rowspan="3">행정규칙</td></tr>
<tr><td>산업안전보건법 시행규칙</td><td>산업안전기준에 관한 규칙</td><td>산업보건기준에 관한 규칙</td><td>유해・위험작업의 취업제한에 관한 규칙</td></tr>
<tr><td colspan="4">기술상의 지침 및 작업환경의 표준(고시), 예규, 훈령</td></tr>
</table>

그림 6 산업안전보건법령 계층 구조도

산업안전보건은 제1장 총칙을 비롯하여, 제2장 안전보건관리체계, 제3장 안전보건관리규정 등 총 제9장으로 구성되어 있다. [표 8]에 산업안전보건법의 구성과 내용을 정리하였다.

표 8 산업안전보건법의 구성

구성	구분	내용	조항
제 1 장	총칙	산업안전보건법의 목적, 정의, 적용범위, 사업주 등	1~12 조
제 2 장	안전・보건관리체계	안전보건관리책임자, 관리감독자, 안전관리자, 안전보건총괄책임자 등	13 ~19 조
제 3 장	안전보건관리규정	안전보건관리규정의 작성, 변경절차, 준수의무 등	20 ~ 22 조
제 4 장	유해・위험 예방조치	안전조치, 보건조치, 작업중지, 도급사업시 안전보건 조치 등	23 ~ 41 조
제 5 장	근로자의 보건관리	작업환경의 측정, 건강진단, 질병자의 근로금지 등	42 ~ 47 조
제 6 장	감독과 명령	유해・위험방지계획서의 제출, 안전・보건진단, 감독상 조치 등	48 ~ 52 조
제 7 장	산업안전지도사 등	산업안전지도사, 산업위생지도사 등의 직무, 자격 및 시험 등	52 조의 2 ~ 52 조의 9
제 8 장	보칙	산업재해 예방시설, 명예안전감독관, 서류보존 등	61 ~ 66 조
제 9 장	별칙	각종 안전조치 위반, 양벌규정 등	66 ~ 72 조

[2] 산업안전보건법의 주요 내용

산업안전보건법의 목적 및 적용범위

산업안전보건법의 목적은 산업안전 및 보건에 관한 기준 확립, 그 책임의 소재를 명확하게 하여 산업 재해를 예방하고, 쾌적한 작업환경을 조성함으로써 근로자의 안전과 보건을 유지 및 증진하는 것이다. 산업안전보건법은 모든 사업 또는 사업장, 국가, 지방자치 단체, 정부투자 기관 및 대통령령이 정하는 사업장에 적용된다. [표 9]는 산업안전보건법의 적용 대상을 정리한 것이다.

표 9 산업안전보건법 적용 대상 사업

대상 사업	적용 규정
기계장비 및 소비용품 임대업 정보처리 및 기타 컴퓨터 과학 및 기술 서비스업	- 23 조, 안전조치 - 24 조, 보건조치 - 25 조, 근로자 준수사항 - 28 조, 유해작업 도급금지 - 33 조, 유해위험기계기구등의 방호조치 - 34 조, 안전인증 - 35 조, 자율안전확인의 신고 - 37 조, 제조 등의 금지 - 41 조, MSDS 비치 - 법 5 장 ~법 9 장
농업, 어업 봉제의복 제조업 가발, 장신품 제조업	- 14 조, 관리 감독자 - 23 조 ~ 28 조 - 31 조, 안전보건교육 - 33 조 ~ 35 조, 37 조 - 38 조, 제조 등의 허가 - 39 조 유해인자 관리
광산보안법 적용사업	- 16 조, 보건관리자

<table>
<tr><th>대상 사업</th><th>적용 규정</th></tr>
<tr><td>원자력법 적용사업</td><td rowspan="3">- 17 조, 산업보건의
- 24 조, 보건조치
- 25 조, 근로자 준수사항
- 26 조, 작업중지등
- 31 조, 안전보건 교육
- 32 조, 관리자책임자 교육
- 33 조, 유해위험기계기구등의 방호조치
- 34 조, 안전인증
- 41 조, MSDS
- 법 5 장 ~ 법 9 장</td></tr>
<tr><td>항공법 적용사업</td></tr>
<tr><td>선박안전법 적용사업</td></tr>
<tr><td>도매 및 소매업</td><td rowspan="7">- 23 조 ~ 28 조, 33 조 ~35 조
- 36 조, 안전검사
- 37 조, 제조금지
- 38 조, 제조허가
- 39 조, 유해인자 관리
- 41 조, MSDS
- 법 5 장 ~ 법 9 장</td></tr>
<tr><td>숙박 및 음식점</td></tr>
<tr><td>부동산업</td></tr>
<tr><td>연구 및 개발업</td></tr>
<tr><td>금융 및 보험업</td></tr>
<tr><td>보건 및 사회 복지사업</td></tr>
<tr><td>사무직 근로자만 사용하는 사업</td></tr>
<tr><td>상시 근로자 5 인 미만 사업</td><td>- 23 조 ~ 27 조
- 30 조, 산업안전보건관리비
- 33 조 ~ 35 조, 41 조
- 51 조, 감독상의 조치
- 52 조, 신고
- 법 8 장 ~ 법 9 장</td></tr>
</table>

정부의 책무 (제4조)

- 산업안전보건정책의 수립・집행・조정 및 통제
- 재해다발사업장에 대한 재해예방의 지원 및 지도
- 기계・기구・설비 등의 안전성 확보 및 개선
- 유해 또는 위험한 기계・기구・설비 및 물질 등에 대한 안전 보건상의 조치 기준의 작성 및 지도감독
- 안전의식을 고취하기 위한 홍보・교육 및 무재해운동 추진
- 안전보건을 위한 기술의 연구・개발 및 시설의 설치・운영
- 산업재해조사 및 통계의 유지 관리
- 안전・보건관련단체 등에 대한 지원 및 지도 감독
- 기타 근로자의 안전 및 건강의 보호・증진

사업주의 일반적 의무사항 (제5조 1항)

- 산업재해예방 기준 준수
- 안전보건에 대한 정보 제공
- 근로조건 개선으로 적절한 작업환경 조성
- 근로자의 신체적 피로와 정신적 스트레스로 인한 건강장해 예방

근로자 의무 (제6조)

- 산업재해 예방 기준 준수
- 사업주 또는 기타 단체에서 실시하는 산업재해 방지조치 준수

2.2.2. 공정안전관리 (PSM) 제도

[1] 공정안전관리 프로세스

산업안전보건법 제49조의2에 의하면, 공정안전관리는 화학공장 등의 화재·폭발·누출 등 중대산업사고를 예방하기 위해 유해·위험설비의 설치·이전 시 사업주로 하여금 공정안전보고서를 작성하도록 하여 심사·확인을 받고, 그 내용을 이행하는 제도이다.

공정안전관리는 12개 요소로 구성되어 있다. 공정을 안전하게 운전하고 사고를 예방하기 위해서 [그림 7]에 공정안전관리 프로세스를 정리하였다.

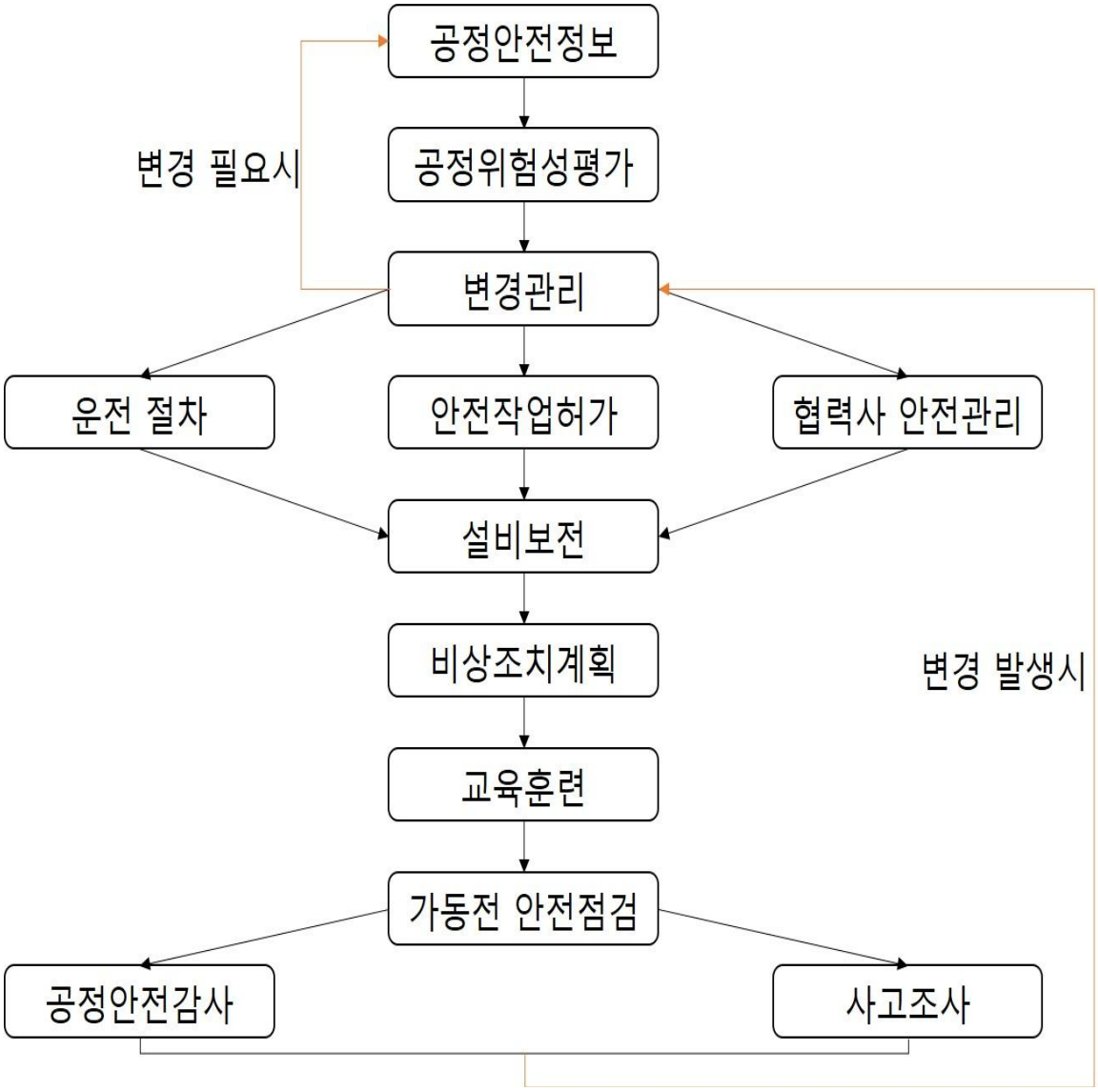


그림 7 공정안전관리 프로세스

[표 10]은 공정안전관리 프로세스의 각 요소의 목적과 활동을 정리하였다.

표 10 공정안전관리 프로세스의 활동

요소	목적	주요 활동
공정안전정보	운전원이 공정을 안전하게 운전하기 위한 자료	- 보완대상, 책임과 권한, 보완주기, 제·개정 절차, 자료관리 방법 등 사내 규정 제정 - 자료관리시스템 구축 (공정안전자료 전산화) - 변경사유 발생시 즉시 보완
공정위험성평가	공정 안전성 확보	- 신규공정 및 기존공정의 잠재적인 위험성 및 운전 상의 문제점 식별 - 문제점 식별을 위한 정성적·정량적 위험성평가 기법 활용 (HAZOP, 피해범위 모델링 등) - 위험요소 제거 및 감소를 위한 개선대책 제시 - 개선대책의 수립 및 이행
운전절차	안전한 공정 운전을 위한 절차 수립 및 준수	- 운전절차서의 작성대상, 내용, 방법 등 제·개정 절차 표준화 - 운전절차에 대한 흐름도 (block diagram) 작성 - 운전절차서에 대한 신뢰성 검증 및 보완 (1 년 주기 권장) - 운전절차서 준수여부 점검체계 구축
교육훈련	공정운전, 설계, 정비	- 연간교육 계획 수립 및 실행

요소	목적	주요 활동
	등의 각 분야별 업무를 안전하게 수행하기 위한 기초 교육 및 훈련	- 근로자에 대한 주기적인 PSM 교육 - 자체 PSM 강사양성 - PSM 교육 교재 및 자료 작성
협력사 안전관리	협력사 안전관리 능력의 지속적 향상 및 협력사와의 동시 안전 확보	- 객관적인 평가체계 구축 - 협력회사 선정 시 안전환경보건 분야 관리수준 반영 - 협력사에 대한 안전환경보건 교육 - 협력사에 대한 안전환경보건 점검 - 협력회사 포상 및 징계
가동 전 안전점검	가동 전 잠재위험요소 확인 및 제거를 통한 사고 예방	- 유해 및 위험 설비의 가동 전 안전 점검 - 가동 전 점검표의 주기적 보완 - 가동 전 안전점검 결과 개선요구사항 이행계획 수립 및 실행 - 개선요구사항 조치완료 후 구성원 교육 실시
설비보전	안전성 유지 및 신뢰성 확보를 통한 설비 결함으로 인한 사고 예방	- 제조 설비의 등록 및 관리 - 일상정비작업 관리, 정기보수작업 관리, 정비용기자재 관리 - 설비 종류별 위험등급 분류체계 수립 및 절차서 유지・관리 - 설비점검 종합계획 수립 후 검사,

요소	목적	주요 활동
		점검 및 설비이력관리 - 장치, 설비의 유지보수 시스템 구축 - 주요설비에 대한 예비품 관리대장 작성・관리
안전작업허가	불안전 행동 및 상태로 인한 안전 사고 발생 방지	- 사업장 내 수행하는 모든 작업에 대한 위험요소를 사전에 관리 - 안전작업, 전기작업, 일반작업 허가 - 주기적 작업허가절차 개선 및 보완 - 작업 전 작업위험성 및 비상대피요령 교육
변경관리	변경으로 인한 위험요소를 사전에 방지하여 사고 예방	- 설비 등 변경 시 변경관리절차 준수 - 변경관리 사항에 대한 목록작성 및 진행현황 지속관리 - 상세변경에 대한 위험성평가수행 - 변경관리 수행 후 자료 수정 및 보완
사고조사	사고 발생시 근본적인 사고원인을 규명하여 동종 사고 및 유사 사고의 재발 방지	- 사고발생시 신속한 보고 - 사고전문가로 구성된 사고조사팀을 구성하여 사고 조사 - 동종 및 유사 사고 재발방지대책 수립 - 사고조사 결과에 대한 관계자 교육실시

요소	목적	주요 활동
		- 사고조사결과 기록유지 (5 년 이상)
비상조치계획	사업장의 비상사태 발생시 주어진 물적, 인적 자원을 활용하여 사고로 인한 피해를 최소화하기 위함	- 비상대응 시나리오 작성 및 주기적 훈련 - 비상사태에 대한 비상대응 조직, 절차 및 계획 수립 - 비상대응 관련 개인별 임무 숙지 - 비상대응 설치 및 장비의 확보, 작동검사 및 유지관리
공정안전감사	지속적인 공정안전관리 수준 유지 및 향상	- PSM 12 개 구성요소가 규정대로 실행되고 있는지에 대하여 객관적인 자체감사 실시 및 사후조치 - 년간 자체감사계획 수립 (조직 별 1 회 이상) - 자체 감사팀 구성 - 자체감사 체크리스트 작성 및 감사 실시 - 자체감사 결과 분석 및 결과 기록 유지 (3 년 이상)

[2] 공정안전관리 적용대상

공정안전관리 적용 사업장은 아래의 7개 업종이다.

- 원유정체 처리업
- 기타 석유정제물 재처리업
- 석유화학계 기초화학물 또는 합성수지 및 기타 플라스틱 제조업
- 질소, 인산 및 칼리질 비료제조업
- 복합비료 제조업

- 농약 제조업
- 화약 및 불꽃 제조업

또한, 유해・위험물질을 규정량 이상 제조・취급・저장하는 설비 및 그 설비의 운영과 관련된 모든 공정설비도 공정안전관리 적용대상이다. 유해・위험물질은 인화성 가스, 인화성 액체, 메틸 이소시아네이트, 포스겐 등 총 51종이 존재한다.

표 11 공정안전관리 적용대상인 유해・위험물질 목록 및 규정량

번호	유해・위험물질	규정량(kg)
1	인화성 가스	제조・취급: 5,000, 저장: 200,000
2	인화성 액체	제조・취급: 5,000, 저장: 200,000
3	메틸 이소시아네이트	제조・취급・저장: 150
4	포스겐	제조・취급・저장: 750
5	아크릴로니트릴	제조・취급・저장: 20,000
6	암모니아	제조・취급・저장: 200,000
7	염소	제조・취급・저장: 20,000
8	이산화황	제조・취급・저장: 250,000
9	삼산화황	제조・취급・저장: 75,000
10	이황화탄소	제조・취급・저장: 5,000
11	시안화수소	제조・취급・저장: 1,000
12	불화수소	제조・취급・저장: 1,000
13	염화수소	제조・취급・저장: 20,000
14	황화수소	제조・취급・저장: 1,000
15	질산암모늄	제조・취급・저장: 500,000
16	니트로글리세린	제조・취급・저장: 10,000
17	트리니트로톨루엔	제조・취급・저장: 50,000
18	수소	제조・취급・저장: 50,000
19	산화에틸렌	제조・취급・저장: 10,000
20	포스핀	제조・취급・저장: 50
21	실란 (Silane)	제조・취급・저장: 50
22	질산 (중량 94.5% 이상)	제조・취급・저장: 250
23	발연황산 (삼산화황 중량 65% 이상 80% 미만)	제조・취급・저장: 500,000
24	과산화수소 (중량 52% 이상)	제조・취급・저장: 3,500
25	톨루엔디이소시아네이트	제조・취급・저장: 100,000
26	클로로술폰 산	제조・취급・저장: 500,000

번호	유해・위험물질	규정량(kg)
27	브롬화수소	제조・취급・저장: 2,500
28	삼염화인	제조・취급・저장: 750,000
29	염화 벤질	제조・취급・저장: 750,000
30	이산화 염소	제조・취급・저장: 500
31	염화 티오닐	제조・취급・저장: 150
32	브롬	제조・취급・저장: 100,000
33	일산화질소	제조・취급・저장: 1,000
34	붕소 트리염화물	제조・취급・저장: 1,500
35	메틸에틸케톤과산화물	제조・취급・저장: 2,500
36	삼불화 붕소	제조・취급・저장: 150
37	니트로아닐린	제조・취급・저장: 2,500
38	염소 트리플루오르화	제조・취급・저장: 500
39	불소	제조・취급・저장: 20,000
40	시아누르 플루오르화물	제조・취급・저장: 50
41	질소 트리플루오르화물	제조・취급・저장: 2,500
42	니트로 셀롤로오스 (질소 함유량 12.6% 이상)	제조・취급・저장: 100,000
43	과산화벤조일	제조・취급・저장: 3,500
44	과염소산 암모늄	제조・취급・저장: 3,500
45	디클로로실란	제조・취급・저장: 1,500
46	디에틸 알루미늄 염화물	제조・취급・저장: 2,500
47	디이소프로필 퍼옥시디카보네이트	제조・취급・저장: 3,500
48	불산 (중량 1% 이상)	제조・취급・저장: 1,000
49	염산 (중량 10% 이상)	제조・취급・저장: 20,000
50	황산 (중량 10% 이상)	제조・취급・저장: 20,000
51	암모니아수 (중량 10% 이상)	제조・취급・저장: 20,000

[3] 공정안전관리 보고서 내용

공정안전 보고서에는 공정안전자료, 공정위험성 평가서, 안전운전계획, 비상조치계획 등을 포함하여야 한다.

공정안전자료

- 취급・저장하는 유해·위험물질의 종류 및 수량
- 유해・위험물질에 대한 물질안전보건자료

- 유해・위험설비의 목록 및 사양
- 유해・위험설비의 운전방법을 알 수 있는 공정도면
- 건물・설비의 배치도, 폭발위험장소 구분도 등

공정위험성 평가서 및 잠재위험에 대한 사고예방 피해 최소화 대책

- 공정에 잠재한 사고 위험 요인 식별
- 사고 발생 빈도 및 강도를 기준으로 위험 등급 결정
- 위험등급 감소를 위한 대책 마련

안전운전계획

- 안전운전지침서
- 설비점검 검사 및 보수계획, 유지계획 및 지침서
- 안전작업허가
- 도급업체 안전관리계획
- 근로자 등 교육계획
- 가동 전 점검지침
- 변경요소 관리계획
- 자체감사 계획
- 공정 사고조사계획

비상조치계획

- 비상조치를 위한 장비, 인력 보유현황
- 사고 발생시 각 부서 및 관련 기관과의 비상연락체계
- 비상조치를 위한 조직의 임무 및 수행 절차
- 비상조치계획에 따른 교육 계획
- 주민홍보계획 및 그 밖에 비상조치 관련 사항

2.3. 해외 안전 체계

2.3.1. 미국의 산업재해 예방 정책

미국은 산재를 예방하기 위한 6개의 정책을 구상하고 있다. 6개의 정책은 범칙금 부과 강화, 중소규모 사업장 안전보건 프로그램 개발, 근로자의 이의제기 기제 마련, 재해예방 자율 거버넌스의 강화, 차별적 재해감소 전략, 사전 예방 강화이다. 이러한 정책은 다시 하위 8개의 사업이나 프로그램으로 세분화된다. [표 12]는 미국의 산재예방 정책과 프로그램 목록이다.

표 12 미국의 산재예방 프로그램

구분	프로그램
범칙금 부과 강화	중대위반 단속 프로그램 (Severe Violation Enforcement Program; SVEP)
중소규모 사업장 안전보건 프로그램 개발	중소기업 현장컨설팅 프로그램 (On-site Consultation Program)
근로자의 이의제기 기제 마련	내부고발자 보호제도 (Whistle-blower Protection Program; WPP) 마련
재해예방 자율 거버넌스의 강화	각 지역 및 주별 사무소 간의 협력을 통한 재해 예방 프로그램 (Local Emphasis Programs)
	자율 보호 프로그램 (Voluntary Protection Program) 강화
차별적 재해감소 전략	특정 고위험 사업장에 대한 감독 강화 (Site Specific Targeting; SST)
	특정 유해요인에 대한 조사감독 프로그램 (National Emphasis Program; NEP)
사전 예방 강화	설계 단계부터 안전추구 (Prevention trough Design; PtD)

출처: 이민창, 김태윤, 김성준, "산업안전보건의 규제제도에 관한 연구", 안전보건공단, 산업안전보건연구원, 2016 년 10 월 31 일.

2.3.2. 영국의 산업재해예방 정책

영국은 산재를 예방하기 위한 5개의 정책을 구상하고 있다. 5개의 정책은 사업주의 책임 강화, 산재예방 거버넌스 구축, 규제합리화 (규제 순응 및 완화 장치)의 마련, 규제업무의 위임, 잠재적 위험산업에 대한 규제강화이다. 이러한 정책은 다시 하위 8개의 사업이나 프로그램으로 세분화된다. [표 13]은 영국의 산재예방 정책과 프로그램 목록이다.

표 13 영국의 산재예방 프로그램

구분	프로그램
사업주의 책임 강화	상해, 질병 및 위험사고에 대한 보고 강화 (Reporting of Injuries Disease and Dangerous Occurrences Regulation)
	사망을 야기한 보건안전위법행위와 기업살인법의 최종지침서 (Corporate Manslaughter & Health and Safety Offences Causing Death)
	안전보건근로감독비 제도 (Fee For Intervention; FFI)
산재예방 거버넌스 구축	산업안전보건 컨설턴트 등록 (Occupational Safety and Health Consultants Register; OSHCR)
규제합리화 (규제 순응 및 완화) 장치의 마련	잠재적 위해위험성의 촉발자에 대한 규제 면제
	중복, 불필요 규제 철폐 (Simplifying the regulatory framework)
규제업무의 위임	보건안전규정에 대한 지도단속의 위임 (The enforcement of health and safety regulations)
잠재적 위험 산업에 대한 규제 강화	다 지역 기업에 대한 HSE 의 지도단속권한

출처: 이민창, 김태윤, 김성준, "산업안전보건의 규제제도에 관한 연구", 안전보건공단, 산업안전보건연구원, 2016 년 10 월 31 일.

2.3.3. 일본의 산업재해예방 정책

일본은 산재를 예방하기 위한 8개의 정책을 구상하고 있다. 8개의 정책은 정신 건강 대책과 과로 대책, 산업 보건 활동의 촉진, 특정산업 중심의 산재예방 대책, 자발적 산재예방 도모, 위험물질관리, 근로조건과 산재의 연계성 강화, 규제강화 범부처적 정책연계 강화이다. 이러한 정책은 다시 하위 21개의 프로그램으로 세분화된다. [표 14]은 영국의 산재예방 정책과 프로그램 목록이다.

표 14 일본의 산재예방 프로그램

구분	프로그램
정신 건강 대책과 과로 대책	건강 장해 방지 대책
	'과로사' 등과 정신 장애의 인정
산업 보건 활동의 촉진	과중한 노동에 대응
	위생위원회 활동의 활성화
	50 인 미만의 작업장에 대한 '지역 산업보건센터' 지원
특정산업 중심의 산재예방 대책	육상화물 운송 사업에서의 노동 재해 방지 대책
	제 3 차 산업 (소매업, 사회 복지 시설)의 노동 재해 방지 대책
	추가, 전락 재해 방지
	기계 재해 예방
	직업성 질병 등의 예방 대책
자발적 산재예방 도모	자주적인 노동재해 방지 활동 추진
위험물질관리	석면에 의한 건강 장해 예방
	직장에서의 화학 물질 관리
	나노 물질에 대한 노출 방지
	위험 평가에 근거 화학 물질 관리
근로조건과 산재의 연계성 강화	노동 조건의 준수
	최저 임금의 적정한 운영과 인상
	직장 내 권력적 괴롭힘 문제 관리
규제 강화	사법적 처분의 강화
	'산재 은폐' 대책 추진
범부처적 정책연계 강화	산재예방의 범부처적 연계성 강화조치

출처: 이민창, 김태윤, 김성준, "산업안전보건의 규제제도에 관한 연구", 안전보건공단, 산업안전보건연구원, 2016 년 10 월 31 일.

2.4. 제조 및 기계 공정 SW 사례

제조 소프트웨어의 개념

- 제품을 제조하는 대표적인 산업에 내재되어 해당 산업의 경쟁력을 높이고, 제품의 편의성, 활용성, 안전 등을 담보하여, 전반적인 제조 활동 및 제품의 운영단계에서 필요한 특화된 소프트웨어.
- 제품 자체에 소프트웨어가 결합되어 작동, 운영되거나, 제품의 개발, 설계, 생산, 판매, 유지관리, 운영 서비스 등 제조 활동의 과정에 사용되면서 해당 산업에 특화되어 있는 소프트웨어.

(출처: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.)

각 산업별 제조 소프트웨어 범위

- 조선: 조선 산업을 위한 설계; 시뮬레이션; 건조; 항해; 운항; 서비스; 운영 등을 실행하는 소프트웨어
  - ◆ 선박 및 해양플랜트 등을 설계, 개발, 제작
  - ◆ 항해, 운항하거나 해양플랜트 및 해양 구조물의 운영

- 항공: 비행운용 지원; 항공기내 디바이스 제어 및 운영; 무인 비행 및 제어; 항공 시뮬레이션 및 통합시험 등을 실행하는 소프트웨어
  - ◆ 임무수행 등의 비행운용에 필요한 소프트웨어
  - ◆ 항공기를 구성하는 부품의 동작을 담당하는 운영체제 (OS)
  - ◆ 미들웨어 등의 항공시스템에 필요한 소프트웨어
  - ◆ 무인 비행체에 필요한 소프트웨어

- 패션/의류: 소재관리; 의복 제조를 위한 디자인, 패턴, 커팅; 가상 피팅; 생산관리; 제품관리; 판매관리 등을 실행하는 소프트웨어
  - ◆ 소재를 다루는데 필요한 소프트웨어
  - ◆ 디자인 단계에서부터 제품의 생산 과정까지 커버하는 소프트웨어
  - ◆ 가상 피팅, PLM, 판매관리 등의 매니지먼트 소프트웨어

- 로봇: 로봇 설계 및 제작; 로봇 운영; 로봇의 움직임 제어; HRI (Human Robot Interaction) 기능
  - ◆ 로봇을 설계, 개발, 제작하고 운영하기 위한 로봇 동역학 및 시뮬레이션 소프트웨어
  - ◆ 머니퓰레이션 및 네비게이션 등의 동작 제어 소프트웨어
  - ◆ 운영체제 (OS)와 미들웨어 등의 로봇 시스템용 소프트웨어
  - ◆ 사람과의 교감을 위한HRI 소프트웨어

2.4.1. 조선 SW 사례

조선 SW는 설계・건조 SW, 선박 SW, 해양플랜트 SW와 같은 3종류로 구분할 수 있으며, 이러한 분류는 설계/건조, 선박 (항해/운항), 선박 (해사서비스), 해양플랜트 (운영), 해양플랜트 (안전)와 같이 5개로 세분화된다.

[1] 설계/건조 SW

[표 15]는 설계・건조 SW 분야의 사례를 정리한 것이다.

표 15 조선 SW 분야 – 설계/건조

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	GS CAD	삼성중공업	한국	자동설계시스템	- 투입물량 자동산출 - 설계안 조기 확정	조선, 해양
2	DACOS-G	대우조선해양	한국	설계 프로그램	- 설계 지원	조선, 해양
3	DaView	대우조선해양	한국	CAD viewer	- 선박 및 해양 설계 검토 - 최적화 및 검증	조선, 해양
4	midas Design+	마이다스 아이티	한국	자동화 프로그램	- 데이터 연동, 도면, 보고서 기능 - 철근콘크리트, 철골, 철골 철근 콘크리트 부재설계	구조물 설계, 해석
5	AVEVA Marine	AVEVA	영국	설계 및 구성을 위한 통합 소프트웨어	- 해양구조물 설계, 관리, 측정	의장설계, 조선, 해양
6	PDMS	AVEVA	영국	공학 기술 설계 소프트웨어 패키지	- 해양구조물 설계, 관리, 측정	조선, 해양, 플랜트

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
7	TRIBON M3	AVEVA	영국	- 통합 디자인 정보 및 생산 시스템 - 설계 프로그램	- 3D 모델 표현 - 해양구조물 설계, 관리, 측정	조선, 해양
8	AUTO CAD	오토데스크	미국	CAD 응용 소프트웨어	- 2, 3 차원 디자인 및 제도	조선, 항공, 기계, 엔지니어링
9	Smart Marine 3D	인터그래프	미국	설계 소프트웨어	- 자동화 설계 - 디자인의 일관성 보호를 위한 규칙 제공 - 모델 데이터 재사용 및 안전 중심의 규칙 지원	조선, 해양, 플랜트
10	PDS	인터그래프	미국	설계 및 엔지니어링 (CAD/CAE) 어플리케이션	- CAD, CAE - 동시 공학	조선, 해양, 플랜트
11	Siemens PLM Software	Siemens	독일	PLM	- 제품 라이프사이클 관리	자동차, 제품, 산업로봇, 엔지니어링
12	3D Symbol Designer	CAXperts	독일	3D 그래픽 작성 프로그램	- 장비, 배관 및 부품에 대한 파라메트릭 제작 - Visual Basic 프로젝트 및 Microsoft Excel 시트 템플릿 자동 생성	엔지니어링
13	CATIA	다쏘시스템	프랑스	PLM 관리 통합 툴	- 3D 모델링 및 시뮬레이션 - 실시간 동시 설계	자동차, 항공, 조선, 엔지니어링
14	Creo Advanced	PTC	미국	PLM	- 다양한 응용프로그램 (건물 구조, 기계 프레임워크, 어셈블리 라인 등)	설계, 제조, 공업기계, 해양구조물

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
	Framework Extension				을 위한 도구 지원	
15	MultiSteel	MultiSuite Software	미국	3D 설계 자동화 솔루션	- 철골 및 R/C 구조물의 설계 및 제작 - 도면 물량 보고서 등의 보고서 자동 생성	플랜트, 건축
16	OrthoGen for PDS/SP3D /PDMS/CADWorx	3DS	미국	도면 자동 생산 솔루션	- 프로젝트의 설계 및 문서화 보조 - 도면 생산 자동화	정유, 플랜트, 해양, 광산, 조선, 석유화학
17	Ship Constructor	SSI	캐나다	CAD/CAM 솔루션	- 해양 정보 모델의 Associative DWG	조선, 해양
18	SP3D to Navisworks	UNITEC	독일	포맷 변환 소프트웨어	- SP3D 데이터를 내비스워스 포맷으로 변환 - Neutral 포맷 데이터 들여오기	조선, 해양, 플랜트, 토목, 엔지니어링
19	조선해양 생산 시뮬레이션 통합 솔루션 v1.0	KIOST 부설 선박해양 플랜트연구소	한국	생산/실행 계획 시뮬레이션 프로그램	- 블록의 크레인 리프팅 및 탑재 시뮬레이션 - GIS 정보 기반의 설비 시뮬레이션 - 블록 및 물류관제 시뮬레이션	조선, 해양
20	선박운항 시뮬레이션	세이프텍 리서치	한국	시뮬레이터 설계 소프트웨어	- 선박운항 시뮬레이터 개발	선박운항
21	EcoBlock	삼인정보 시스템	한국	3 차원 설계 모델기반 정밀 형상 품질관리 소프트웨어	- 구조물 변형 분석 - 보고서 자동 생성 - 서버 기반 운영 가능	조선, 해양, 플랜트

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
22	EcoOTS	삼인정보 시스템	한국	3 차원 설계 모델 기반 조선 블록/플랜트 모듈 사전 조립 예측 소프트웨어	- 구조물 간의 간격, 중첩 분석 - 보고서 자동 생성 - 서버 기반 운영 가능	조선, 해양, 플랜트
23	Viking Navigation	CT System	네덜란드	해양 정박 및 항해용 소프트웨어	- 백터 차트 편집, DXF 지원, 네비게이션 시뮬레이터, NMEA 탐색 장치 지원 - 해양 정박을 위한 3 차원 데이터 처리	조선, 해양
24	Simsci	Schneider-Electric	프랑스	프로세스 디자인 및 시뮬레이션 소프트웨어	- 공정 설계 지원 - 공정분석 및 사용자 교육을 위한 시뮬레이션 - 프로세스 최적화 및 제어 솔루션	석유/화학, 플랜트, 엔지니어링
25	DELMIA	다쏘시스템	프랑스	가상 디지털 공정 솔루션	- 생산 및 유지관리 계획, 설계, 관리 - 가장 프로세스, 시스템 정의 및 최적화, 일정관리 - 시뮬레이션	제조, 우주항공, 산업장비, 자동차, 로봇
26	STAR-CCM+	Siemens	독일	설계 시뮬레이션 플랫폼	- 공기 역학, 유체 역학, 열전달, 고체 역학 등 산업용 시뮬레이션	항공, 우주, 자동차, 조선, 플랜트, 제조
27	risk and compliance management	Integrum	호주	통합관리시스템 솔루션	- 문서 관리 제어 - 교육 및 eLearning 관리 - 자산 관리	안전, 환경, 품질, 자산

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
	system					
28	McLaren Software	McLaren Software	미국	문서 제어 및 관리 시스템	- 수명주기 관리	건설, 석유/가스, 생명과학, 에너지
29	Bluebeam Studio	Bluebeam	미국	프로젝트 관리 플랫폼	- 데이터 실시간 공유 - 프로젝트 관리 및 모니터링	비즈니스, 엔지니어링, 디자인
30	ENOVIA	다쏘시스템	프랑스	PLM	- 요구사항 관리 - 환경 규제에 적합한 관리 환경 제공	조선, 해양, 우주항공, 자동차, 제조, 건축
31	Progress Xpert	CAXperts	독일	프로젝트 관리 플랫폼	- 마일스톤 추적 및 관리 - 프로젝트 진행 상황 공유	엔지니어링
32	SmartPlant Foundation R4 Purchase (1-49)	Intergraph	미국	플랜트 정보 관리 통합 솔루션	- 기업과 공급망 간의 액세스 및 업데이트, 제어, 알림 기능	플랜트
33	Windchill	PTC	미국	PLM	- 제품 설계 데이터 수집, 제어 및 관리 - 하드웨어 및 소프트웨어 산출물 동시 관리 - 서로 다른 유형의 소프트웨어 개발 환경 지원	제조, 자동차, 항공, 엔지니어링

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[2] 선박 SW

[표 16]는 선박 (항해/운항) SW 분야의 사례를 정리한 것이다.

표 16 조선 SW 분야 – 선박 (항해/운항)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	MESIM Indigo PMP v1.0	메타빌드㈜	한국	플랜트 운영관제 지원 미들웨어	- 제조 플랜트 및 공정에 대한 데이터 수집 및 분석 - 이벤트 관리 및 탐색, 데이터 용량 관리	공공, 국방, 금융, 제조, 플랜트
2	Meridian Enterprise	BlueCielo ECM Solutions	네덜란드	자산관리 및 엔지니어링 콘텐츠 관리 시스템	- 프로젝트를 통한 자산관리 - 폐기된 태그 및 문서 보관 처리	해양, 플랜트, 금속, 화학, 제약
3	NaviPac	EIVA	덴마크	해양 탐사용 소프트웨어	- LiDAR 네비게이션 - 3D 시각화 - 실시간측량 및 품질 관리	조선, 해양, 석유/가스
4	VISIONMASTER	Sperry Marine	독일	레이더, 통합 브릿지 및 제어 시스템, 네비게이션 솔루션	- 전자 차트 디스플레이 - 선박 운영 중 수행되는 작업에 액세스 기능	항해통신
5	FMD-3200/3300	FURUNO	일본	항해통신장비	- 다기능 디스플레이 - 항해 경로 계획, 모니터링 및 네비게이션 데이터 관리	항해통신
6	JAN-901B	JRC	일본	항해통신장비	- 다기능 ECDIS - 지속적인 위치 및 항법 안전 정보	항해통신

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					제공	
7	NAVIC-ECDIS	산엔지니어링	한국	네비게이션 정보 시스템	- Vector & Raster Chart 표현 - Real-time Automatic Check Chart 기능	항해통신
8	PM3D (ECDIS)	마린전자	한국	무선통신항해용장비	- 해도 정보, 위치 정보, 선박의 침로, 속력, 수심 자료 등을 컴퓨터 스크린에 도식	항해통신
9	ECDIS	이마린	한국	항해통신장비	- 항해 연동장비 정보 표시 - 차트 관리, 항로 계획	항해통신
10	ECS (Electro-CleanTM System)	테크로스	한국	선박 평형수 처리 장치	- 선박 평형수 처리	조선, 해양
11	GloEn-Patrol	파나시아	한국	선박 평형수 처리 장치	- 선박 평형수 처리 - 수질에 따라 전력 소모량 3 단계 자동 조절	조선, 해양
12	Synapsis	Raytheon Anschutz GmbH	독일	통합 항해 시스템	- 레이더, ECDIS 기능 - 항로 계획, 충돌 회피, 자동 루트 계획, 갯벌 예측 모드 기능	항해통신
13	Engine Monitoring System	KONGSBERG	노르웨이	엔진 모니터링 시스템	- 엔진 상태 및 진단 기능 - 운영 최적화 및 연료 소비 감소 활성화 기능	엔진
14	ACONIS	현대중공업	한국	선박 기관감시제어 장치	- 발전기 병렬 운전 제어 - 선박 항해 기록	조선, 해양

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					- 선교 감시 및 경보	
15	HMS 100/200	KONGSBERG	노르웨이	헬리콥터 착륙 유도 시스템	- 기상 데이터 수집 및 표현 - 사용 가능한 실제 선박 데이터 확인	조선, 해양, 항공
16	HMS System	Automasjon og Data	노르웨이	헬리콥터 착륙 유도 시스템	- 앵커 라인 모니터링 - 스트레스 모니터링	조선, 해양, 항공
17	HMS	VAISALA	핀란드	헬리콥터 착륙 유도 시스템	- 실시간 기상 정보 제공	조선, 해양, 항공
18	Telecommunication Management System	ABB	스위스	통신 관리 시스템	- 네트워크 관리 - 물리적 보안 정보 관리 - 시스템 상태 모니터링	석유, 가스, 화학, 조선, 해양 등
19	Telecommunication Management System	Intelecom	노르웨이	제어 시스템	- 다양한 인터페이스와 통합 기능 - 모든 종류의 통신장비 모니터링	석유, 가스, 화학, 조선, 해양 등
20	VRC (Valve Remote Control)	WOODWARD	미국	제어 시스템	- 산업, 우주 항공 및 국방 관련 원격 밸브 제어	석유, 가스, 항공, 국방, 자동화
21	Hull stress monitoring system	Automasjon og Data	노르웨이	선체 응력 (피로) 모니터링 시스템	- 가속도계, 모션 데이터 및 환경 센서 확장 기능 - 다른 모니터링 시스템과 통합 가	조선, 해양

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					능	
22	Oil Spill Detection	Automasjon og Data	노르웨이	해양환경모니터링 시스템	- 오일 유출 조기 예측	조선, 해양, 환경
23	Miros OSDTM	Miros	노르웨이	해양환경모니터링 시스템	- 오일 유출 조기 예측 - 오일 유출 모니터링	조선, 해양, 환경
24	OIL SPILL DETECTION and Monitoring System	Rutter	캐나다	해양환경모니터링 시스템	- 오일 유출 탐지	조선, 해양
25	EMS (Environ-mental Monitoring System)	Automasjon og Data	노르웨이	해양환경모니터링 시스템	- 기상 관측 - 기상 및 기상 예측 통계 데이터 제공	조선, 해양
26	iSEMS	LG CNS	한국	선박 에너지 통합 관리 솔루션	- 운항시의 선박 상태 및 성능 모니터링 - 운항 결과 분석	조선, 해양
27	ECOSOS (Energy Consumption Optimization	뉴월드 마리타임	한국	선박 에너지 최적화 시스템	- 최적의 RPM 산출 - 운항정보 보고서 생성	조선, 해양

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
	System On Ship)					

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[표 17]는 선박 (해사서비스) SW 분야의 사례를 정리한 것이다.

표 17 조선 SW 분야 – 선박 (해사서비스)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Vessel Traffic Management Solutions	TRANSAS	아일랜드	선박 교통 관리 솔루션	- VTS Radio Water-side VHF Communication 기능 - 3D VTS 기능 - 선박 통행 관리	조선, 해양
2	NOR CONTROL	KONGSBERG	노르웨이	해상 감시 솔루션	- 해안 감시 - VTS & VTMIS 기능	조선, 해양
3	ASCA	ATLAS EMS	독일	해상 및 해안 보안 시스템	- 민간 및 군사용 애플리케이션 기능 - 분류된 데이터 처리	조선, 해양, 국방
4	선박 관리시스템	현대유앤아이	한국	U& Vessel 솔루션	- 업무 관리 프로세스 제공 - 선-육간 데이터 동기화 및 유지보수 기능	조선, 해양
5	Marine Office PMS	띵크마린	한국	선박관리시스템	- 선박관리 상황 모니터링 - 방선점검, PSC 점검 관리 및 분석	조선, 해양

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
6	MARINER	마린소프트	한국	인사/급여 프로그램	- 선원 관리, 선박 관리, 급여 관리 - 경영자원 최적화	조선, 해양
7	SEA-ONE	KT	한국	트랙킹 서비스	- 선박 위치 정보를 기관이나 단체에 자동 전달 - 전 세계 주요 Port 정보와 ETA 시뮬레이션	조선, 해양
8	DANAOS ENTERPRISE	Danaos	그리스	Miritime ERP Software	- Onboard Ship Management 기능	조선, 해양
9	TSB SUPER-CARGO	토탈 소프트뱅크	한국	선박 탑제용 로딩컴퓨터	- 선박 안정성 및 강도 계산	조선, 항만, 물류
10	SHIPMANAGER-88	TECHMARINE	한국	선적 계산 시스템	- 선박 내 다양한 자원 모니터링 및 계측치 계산 - 안정성 계산	조선, 항만, 물류
11	BRIDGE	Weathernews INC	일본	선박운항경로 지원 서비스	- 선박의 최적 항로 제공	조선, 해양
12	BVS7 (Bon Voyage System)	StormGeo	미국	기상정보 제공 서비스	- 최적항로 및 최적속도 제공	조선, 해양
13	DUKC	OMC International	호주	안전 운항 지원 시스템	- 선박 모니터링 및 항해 계획	조선, 해양, 항만
14	Port Cost Management System	DA-DESK	UAE	항만비용관리 시스템	- Cash Management 기능 - Port Cost Solutions 기능	조선, 해양, 항만

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
15	PortMIS	NGL	한국	항만운영정보 시스템	- 항만 운영 업무 및 민원 업무 처리	조선, 해양, 항만

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[3] 해양플랜트 SW

[표 18]는 해양플랜트 (운영) SW 분야의 사례를 정리한 것이다.

표 18 조선 SW 분야 – 해양플랜트 (운영)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Miros OSDTM	Miros	노르웨이	Oil Spill Detection 솔루션	- 오일 유출 조기 예측	조선, 해양, 환경
2	OIL SPILL DETECTION and Monitoring System	Rutter	캐나다	오일 유출 감지 시스템	- 오일 유출 탐지	조선, 해양
3	Process Simulation	Aspen Technology Inc	미국	공정 제조 시뮬레이션 소프트웨어	- 석유 및 가스 운영 최적화	석유, 가스, 화학, 플랜트
4	Process Simulation	Schneider-Electric	프랑스	산업/기계 제어 및 솔루션	- 제조실행 및 생산 제어 기능 - 설비 제어 기능	플랜트, 원자력, 석유/화학, 제조
5	Process Simulation	Bryan Research & Engineering Inc	미국	프로세스 시뮬레이션 소프트웨어 패키지	- ProMax, 가스 처리, 정유 및 석유화학 설비 설계 및 최적화	석유, 가스, 플랜트

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
6	Process Hazards Analysis	Det Norske Veritas (DNV GL)	미국	공정 위험 분석 시뮬레이션 소프트웨어	- 공정 위험원 분석	석유, 가스, 플랜트, 화학
7	HYSIS	Hyprotech	캐나다	공정 제조 시뮬레이션 소프트웨어	- 석유 및 가스 운영 최적화	석유, 가스, 화학, 플랜트
8	Project Execution Merge	Mustang Development (Wood Group Mustang)	미국	프로젝트 실행 계획 (PEP) 지원 서비스	- 프로젝트 관리 계획 (PEP) 기능 - 프로젝트 요구사항 관리 기능	엔지니어링

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[표 19]는 해양플랜트 (안전) SW 분야의 사례를 정리한 것이다.

표 19 조선 SW 분야 – 해양플랜트 (안전)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Flare Network Analysis	Aspen Technology, Inc	캐나다	공정 안전 최적화 시뮬레이션 소프트웨어	- 플레어 시스템 설계	석유, 가스, 정제, 화학, 플랜트
2	Hazop Analysis	Primatech, Inc	미국	공정 안전 관련 소프트웨어	- 프로세스 안전 및 위험 관리를 위함 교육 과정 지원	석유, 가스, 화학, 제약, 플랜트
3	Hazop Analysis	Dyadem	미국	운영 리스크 관리 (ORM) 및 품질 리스크 관리 (QRM) 솔루션	- 운영 리스크 관리 - 품질 리스크 관리	석유, 가스, 화학, 광업, 제약, 의료, 자동차
4	Risk and Decision Analysis	Palisade Corporation	미국	리스크 분석 소프트웨어	- 몬테카를로 시뮬레이션을 활용한 리스크 분석	재무/증권, 6 시그마/품질분석, 제조, 석유/가스, 의료, 환경, 우주항공
5	Heat Transfer-General	Heat Transfer Research, Inc.	미국	설계 프로그램	- 열 전달 장비의 설계, 평가 및 시뮬레이션	에너지, 열교환기, 엔지니어링
6	Heat Transfer-General	PFR Engineering System, Inc.	미국	열 엔지니어링 서비스	- 히트 공정 안전 시뮬레이션 - 모든 유형의 보일러 및 터빈의 열 회수 섹션 시뮬레이션	석유, 화학, 열 엔지니어링, 에너지

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

2.4.2. 항공 SW 사례

항공 SW는 유인항공 SW, 무인 항공 (드론) SW, 시스템 운용/관리 SW, 시뮬레이션 SW와 같은 4종류로 구분할 수 있으며, 이러한 분류는 유인항공 (임무제어), 유인항공 (조종석 시현), 유인항공 (비행제어), 유인항공 (비행관리), 무인 항공 (비행체 탑재), 무인 항공 (지상제어), 시스템 운용/관리 (항공 표준 실시간 운영체제), 시스템 운용/관리 (항공 표준 기능 지원 미들웨어), 시스템 운용/관리 (항공소프트웨어 개발 환경), 시스템 운용/관리 (프로젝트 운용 관리), 시뮬레이션 (항공 시뮬레이터), 시뮬레이션 (비행계획 및 분석), 시뮬레이션 (통합시험장치)와 같이 13개로 세분화된다.

[1] 유인항공 SW

[표 20]는 유인항공 SW 분야의 사례를 정리한 것이다.

표 20 항공 SW 분야 – 유인항공

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	KA-1 OFP	국방과학 연구소	한국	비행운용 프로그램	- 시스템/소프트웨어 관리 - 서브시스템 통제 - 비행/항법 정보 계산	군용 항공기
2	T-50 FC OFP	한국 항공우주산업 /Lockheed Martin	한국/미국	비행운용 프로그램	- 시스템/소프트웨어 관리 - 서브시스템 통제 - 비행/항법 정보 계산	군용 항공기
3	KF-16 FCC OFP	Lockheed Martin	미국	비행운용 프로그램	- 시스템/소프트웨어 관리 - 서브시스템 통제	군용 항공기

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					- 비행/항법 정보 계산	
4	P-3 DMS (Data Management System)	L-3MID	미국	비행운용 프로그램	- 서브시스템 통제 - 시스템 데이터 관리 - 시험/임무분석 지원	해상 항공기
5	FA-50 HUD OFP	한국 항공우주산업 /Lockheed Martin	한국/미국	비행운용 프로그램	- HUD 상에 Cursive Graphic Symbol 을 시현 - 공대공 기총 탄도 및 관련 심벌의 시현을 위한 알고리즘 수행	군용 항공기
6	FA-50 IUFC OFP	한국 항공우주산업 /Lockheed Martin	한국/미국	비행운용 프로그램	- 신호 해석을 통하여 비행에 필요한 자료 입력 기능 - 비행에 필요한 데이터를 디스플레이 장비에 시현하기 위한 기능	군용 항공기
7	FA-50 MFDS OFP	한국 항공우주산업 /Lockheed Martin	한국/미국	비행운용 프로그램	- 무기류 및 센서의 동영상 및 관련 심벌/문자를 LCD 디스플레이에 시현 - 조종사 항공기 연동 (PVI, Pilot-Vehicle Interface) 제공	군용 항공기
8	MFD-268C6 OFP	Rockwell Collins Inc.	미국	장치 소프트웨어	- 임무장비 정보를 조종사에게 시현	군용/민간 항공기
9	FA-50 비행제어 OFP	한국 항공우주산업 /Lockheed	한국/미국	비행제어 및 비행운용 프로그램	- 비행 제어 및 운용	군용 항공기

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
		Martin				
10	KUH 비행제어 OFP	Airbus Helicopters	다국적	비행제어 및 비행운용 프로그램	- 비행 제어 및 운용	조선, 해양
11	A380 비행제어 OFP	Airbus Helicopters	다국적	비행제어 및 비행운용 프로그램	- 비행 제어 및 운용	군용/민간 항공기
12	Entegra Release 9	Avidyne	미국	비행관리 시스템	- 비행경로 계획 - 항공기 위치 결정 - 자동 비행	군용/민간 항공기
13	G5000	Garmin	미국	비행관리 시스템	- 비행경로 계획 - 항공기 위치 결정 - 자동 비행	군용/민간 항공기
14	CMA-9000 FMS	CMC	캐나다	디스플레이 장치	- 항공기 상태 및 항법 정보 표시	소형 민수 항공기에 탑재
15	CDU-7000	Rockwell Collins Inc.	미국	디스플레이 장치	- 항공기 상태 및 항법 정보 표시	민수/군용 항공기에 탑재
16	Multi-Function Control Display Unit	Universal Avionics	미국	디스플레이 장치	- 항공기 상태 및 항법 정보 표시	민수/군용 항공기에 탑재
17	H-TAWS (Helicopter Terrain Avoidance	탈레스	프랑스	지형 경고 시스템	- 자동비행조정장치 (AFCS)와 연동된 지형 경고 및 회피 기동 제공	민군 헬리콥터 항법

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
	Warning System)					
18	통합전자지도 컴퓨터 (IDMC, Integrated Digital Map Computer) 탑재 소프트웨어	LIG Nex 1	한국	항법 정보 소프트웨어	- 주변의 지도/지형, 전술/항법 정보들을 2 차원 및 3 차원으로 시각화하여 제공	항공기 항법
19	AV-NAV (인공시계기반 항법 시스템, Artificial Vision based Navigation System)	대한항공 항공우주사업본부	한국	항법시스템	- 3 차원 인공시계 제공 - DGPS/INS 통합항법 운용 기능	민군 항공기

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[2] 무인 항공 SW

[표 21]는 무인 항공 SW 분야의 사례를 정리한 것이다.

표 21 항공 SW 분야 – 무인 항공

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Mobile SDK	DJI	중국	소프트웨어 개발 키트	- 비행 제어, 영상 처리, 미션 수행 기능	민수용 드론 소프트웨어 개발
2	Onboard SDK	DJI	중국	소프트웨어 개발 키트	- 비행 제어, 영상 처리, 미션 수행 기능 - 드론과의 통신 및 모니터링 Onboard API functions 제공	민수용 드론 소프트웨어 개발
3	Guidance SDK	DJI	중국	소프트웨어 개발 키트	- 영상 기반 애플리케이션 제작용 SDK 제공	민수용 드론 소프트웨어 개발
4	Aerial Information Platform	Airware	미국	운영체제	- Fleet management, Data management	민간 상용 드론 플랫폼
5	큐플러스 에어	한국전자통신연구소	한국	운영체제	- 영상처리, 무선통신, 미션처리, 자동 항법 제어 운영체제 - 비행제어, 비상착륙, 출발점 복귀를 제어하는 실시간 운영체제	민군 드론 운영체제
6	틸트로터 무인기 탑재 소프트웨어	항공우주연구원/대한항공	한국	탑재 소프트웨어	- 틸팅 제어 - 수직 이착륙 제어 기능	민군 적용

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
7	UAV GCS (UAV Ground Control Solution) (Version 1.0)	메타빌드㈜	한국	무인항공기 조종 및 운용 솔루션	- 비행조종, 임무계획, 영상처리 기능 - 다 기종 무인항공기 동시 관제	군용 및 민간용 무인항공기 지상통제시스템 적용
8	UAV GCS (UAV Ground Control Solution)	유콘시스템㈜	한국	무인항공기 조종 및 운용 솔루션	- 무인항공기의 이착륙과 비행임무 전반 조종 및 통제 - 비행체로부터 획득된 자료의 수신/처리	군용 및 민간용 무인항공기 지상통제시스템 적용

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[3] 시스템 운용관리 SW

[표 22]는 시스템 운용관리 SW 분야의 사례를 정리한 것이다.

표 22 항공 SW 분야 – 시스템 운용관리

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	NEOS	㈜MDS 테크놀로지	한국	실시간 운영체제	- 컴포넌트 구조, 유연한 동적 확장, 계층화 된 포팅 구조 응용 구현	군용 및 민간용 항공기 적용
2	VxWorks-653	Wind River	미국	실시간 운영체제	- 모든 코어를 동기화하여 관리 - 멀티 DAL OFP 통합 가능	군용 및 민간용 항공기 적용
3	Integrity-178B	Green Hills	영국	실시간 운영체제	- AMP, SMP 혼합 형태의 멀티코어 지원 - 모든 코어를 동기화하여 관리 - 멀티 DAL OFP 통합 가능	군용 및 민간용 항공기 적용
4	NeoDDS	㈜MDS 테크놀로지	한국	미들웨어	- 자동 디스커버리 기능 - 일정 시간 내 데이터 전송 기능	군용 및 민간용 항공기 적용
5	NeoDDS	RTI	미국	실시간 데이터 분배 미들웨어	- 주요 범용 플랫폼과 실시간 플랫폼 지원 기능	군용 및 민간용 항공기 적용
6	OpenSplice DDS	PrismTech	미국	실시간 데이터 분배 미들웨어	- 정보 모델링, 객체 모델링, 애플리케이션 모델링 - DLRL 과 DCPS 코드 생성 및 실행 중 모니터링	군용 및 민간용 항공기 적용
7	CodeScroll	Suresoft	한국	소프트웨어 개발 환경 패키지	- 소프트웨어 품질 측정을 위한 주요 Metrics 정보 제공	군용 및 민간용 항공기 적용

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					- 무기체계의 다양한 개발 환경 제공	
8	VectorCast	Vector Software Inc	미국	소프트웨어 검증 도구	- 소프트웨어 동적시험을 위한 코드 실행율 검증	군용 및 민간용 항공기 적용
9	CodeSonar	Gramma Tech	미국	소프트웨어 정적 분석 도구	- 실생시간 오류 검증 - 소스 코드의 구조 파악	군용 및 민간용 항공기 적용
10	IBM ALM 솔루션	IBM	미국	ALM 솔루션	- 임베디드 시스템 개발 - 요구사항관리, 소프트웨어 아키텍처모델링, 형상/변경관리의 일원화된 통합개발/관리	국방, 항공, 자동차
11	Polarion ALM 솔루션	Vector Software Inc	미국	ALM 솔루션	- 무기체계내장형 소프트웨어 프로세스 관리 지원 - 요구사항부터 테스트까지 양방향 추적성 관리	국방, 항공, 자동차
12	실크로드	NSE	한국	ALM 솔루션	- 소프트웨어 개발 전체 단계에 대한 통합관리	국방, 항공, 원자력, 자동차
13	HP ALM 솔루션	HP	미국	ALM 솔루션	- 다양한 도구와 표준 운용환경 제공	국방, 항공, 자동차 등 제조 산업, IT 산업
14	Visual Studio Team Services	Microsoft	미국	클라우드 ALM 플랫폼	- 개인 레파지토리, 소셜 코드 검토 - 자동화된 구축, 테스트, 배포 프로세스 구축	국방, 항공, 자동차 등 제조 산업, IT 산업

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[4] 시뮬레이션 SW

[표 23]는 시뮬레이션 SW 분야의 사례를 정리한 것이다.

표 23 항공 SW 분야 – 시뮬레이션

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	항공 시뮬레이터 솔루션	CAE Inc.	캐나다	항공 시뮬레이터	- 모의조종훈련	군용/민항/무인기 시뮬레이터, 훈련 센터
2	항공 시뮬레이터 솔루션	L-3 Communica-tions Link Simulation & Training	미국	항공 시뮬레이터	-모의조종훈련	군용/민항/무인기 시뮬레이터, 훈련 센터
3	Flight Simulator X	마이크로 소프트	미국	비행 시뮬레이션 게임	- 비행 게임	게임, 소규모 시뮬레이터
4	Flight Animation System	CEFA Aviation	프랑스	비행 분석 소프트웨어	- 2 대 비행기와 궤적 동시 표시 - 지형에 이미지 파일 오버레이	민군 항공기 비행 데이터 분석
5	비행데이터 분석 및 시현 시스템 (FDAS, Flight Data	대한항공	한국	비행 분석 소프트웨어	- 비행 상황을 3 차원 영상, 계기, 차트, 음향으로 재현	민군 항공기 비행 데이터 분석

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
	Analysis & Animation)					
6	AHB SW (815 station)	㈜한국 항공우주	한국	시스템 검증 장비	- 항공전자 시스템의 기능 및 임무 컴퓨터 OFP (Operation Flight Program) 검증 - 항공전자 장비 모의 시뮬레이션	군용 항공기
7	FA-50 AHB	Lockheed Martin	미국	시스템 검증 장비	- 항공전자 시스템의 기능 및 임무 컴퓨터 OFP (Operation Flight Program) 검증	군용 항공기
8	KT-1T SIL	esternline CMC	캐나다	시스템 검증 장비	- 항공전자 시스템의 기능 및 임무 컴퓨터 OFP (Operation Flight Program) 검증 - 항공전자 장비 모의 시뮬레이션	군용 항공기
9	동적 시험도구 (Dynamic Test Suite)	대한항공	한국	시스템 소프트웨어 개발 및 검증 도구	- 시나리오 기반 항전 OFP 검증 - 레이더, EO/IR, 무장 등 임무장비 10 종에 대한 시뮬레이션	군용 항공기

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

2.4.3. 패션/의류 SW 사례

패션/의류 SW는 소재 SW, 의복제조 SW, 마케팅/매니지먼트 SW와 같은 3종류로 구분할 수 있으며, 이러한 분류는 자수, 텍스타일, 디자인, 패턴, 3D 시뮬레이션, 생산, 비주얼라이징, 관리와 같이 8개로 세분화된다.

[1] 소재 SW

[표 24]는 소재 SW 분야의 사례를 정리한 것이다.

표 24 패션/의류 SW 분야 – 소재

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	자수펀칭 v850	수메이트	한국	자수 프로그램	- 자수 디자인	자수 디자인 분야
2	PE-Design	brother	일본	자수 프로그램	- 자수 디자인 - 디자인 축소판 미리보기, 디자인 레이아웃 및 편집	자수 디자인 분야
3	EmbroideryStudio	Wilcom	호주	자수 프로그램	- 자수 디자인	자수 디자인 분야
4	DecoStudio	Wilcom	호주	자수 프로그램	- 자수, 인쇄, 레이저 커팅, 라인 디자인	의류장식 디자인 분야
5	TrueSizer	Wilcom	호주	자수 프로그램	- 여러 가지 색상 생성 및 저장 - 인쇄 기능	자수 디자인 분야
6	Quilt Design Software	Eletric Quilt Company	미국	퀼드 디자인 소프트웨어	- 퀼트와 블록 패턴 디자인 - 누비이불 퀼트 디자인	자수 디자인 분야

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
7	Raschel Magic	티엔에스	한국	디자인 프로그램	- 좁은 내부 레이스, 올 오버 레이스, 내부 커튼 레이스 편직 - 고품질의 Fabric Simulation 생성	편직물 디자인 분야
8	Texprint	영우씨앤아이	한국	디자인 프로그램	- 다양한 색상의 표현 및 생산 - Full Color 디자인 및 대량생산용 날염디자인 기능	디지털 텍스타일 프린트 분야
9	Texpro	영우씨앤아이	한국	디자인 프로그램	- 패션 디자인, 컬러웨이 작업과 선염직물, 편직물, 날염물의 디자인 - 패션전문 장비 및 일반 그래픽 디자인 프로그램과 자료호환 가능	텍스트일 디자인 분야
10	Textricot	영우씨앤아이	한국	디자인 프로그램	- 트리코프 경편물의 조직분석, 설계, 디자인 개발	편직물 디자인 분야
11	Texweave	영우씨앤아이	한국	디자인 프로그램	- 원사 디자인과 조직의 설계 및 기획된 제품의 시뮬레이션 - 원사의 소요량 및 생산에 필요한 데이터 자동 산출 및 관리	직물 디자인 분야
12	Texknit	영우씨앤아이	한국	Knit 전문 디자인 시스템	- Knit 조직, 스타일 디자인 및 생산 관리 - 원사 소요량 산출	편직물 디자인 분야
13	SHIMASEIKI-Textile	SHIMASEIKI	일본	디자인 프로그램	- 평면 뜨개질, 원형 뜨개질, 직조, 파일 직조 및 인쇄를 위한 시뮬레이션 및 기타 기능	도비 디자인 분야
14	Design Dobby	Textronics	인도	디자인 프로그램	- 특정 지역에 자동화된 직조 구조 삽입 기능	도비 디자인 분야

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					- 직물 디자인에 날실 및 위사 구조 추가 기능	
15	Design Jacquard	Textronics	인도	디자인 프로그램	- 다양한 워프 및 위트 밀도를 원근감있게 유지하면서 아트웍 편집 - CAM 에서 제공되는 다양한 그리기, 페인팅 및 편집 도구를 사용하여 그리드 모드로 디자인 편집	자카드 디자인 분야

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[2] 의복제조 SW

[표 25]는 의복제조 SW 분야의 사례를 정리한 것이다.

표 25 패션/의류 SW 분야 – 의복제조

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Texstylist	영우씨앤아이	한국	디자인 프로그램	- 각종 디자인 tools 제공 - 아이템 별 디자인과 스타일 도식화	패션 디자인 분야
2	Fashion Studio Suite – STORY BOARD AND Cataloging PRO	NedGraphics	네덜란드	디자인 프로그램	- 패브릭 이미지를 탐색 한 다음 드래그 앤 드롭, 위치 지정, 크기 조절, 자르기, 스택, 레이어 및 구성 조합 기능	패션 디자인 분야
3	Lectra Kaledo	Lectra	프랑스	디자인 프로그램	- 의류 관련 도구 지원	패션 디자인 분야
4	Smart Designer	모던하이테크	대만/한국	디자인 프로그램	- 일반 이미지 디자인, 니트 웨어 디자인, 선염 디자인, 3D 드레핑 디자인 - 일반 그래픽 디자인 프로그램과 데이터 연동 가능	패션 디자인 분야
5	DC Suite	physan	한국	통합 소프트웨어	- 작업한 패턴데이터를 동일 소프트웨어 내의 시뮬레이터에 직접 전송	패턴 소프트웨어 분야
6	Lectra Modaris	Lectra	프랑스	디자인 프로그램	- 패턴 제작, 그레이딩 기능	패턴 소프트웨어 분야

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
7	Lectra Diamino	Lectra	프랑스	디자인 프로그램	- 다양한 의류 및 직물의 마커 생성	패턴 소프트웨어 분야
8	AccuMark Pattern Design Software	Gerber Technology	미국	디자인 프로그램	- ERP 시스템과 연동하여 자동 주문 - 패턴 CAD 디자인에서 재단까지 모든 과정의 기능	패턴 소프트웨어 분야
9	O/DEV-Pattern making suite	Optitex Ltd.	미국	디자인 프로그램	- 마킹, 커팅 플랜, 네스팅, 매칭 기능	패턴 소프트웨어 분야
10	O/PRO-Marker making suite, Cut Plan, Automatic Nesting	Optitex Ltd.	미국	디자인 프로그램	- 마킹, 커팅 플랜, 네스팅, 매칭 기능	패턴 소프트웨어 분야
11	PAD PATTERN	PAD System International	캐나다	디자인 프로그램	- 의류 자동 마커 최적화 - 플로터, 커터로 출력	패턴 소프트웨어 분야
12	Aceapparel CAD - DGS	ACE	한국	디자인 프로그램	- 패턴 입출력, 수정, 패턴제작, 그레이딩, 마킹, 자동 패턴 기능 - 원격지원서비스 기능	패턴 소프트웨어 분야
13	CLO 3D	CLO Virtual Fashion Inc	한국	3D 시뮬레이션 프로그램	- 3D 에서 디자인 수정 (3D 가상 피팅) - 패턴 메이킹과 동시에 3D 드레이핑 시뮬레이션	3D 패션 시뮬레이션

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
14	O/DEV 3D PRODUCT CREATION SUITE	Optitex Ltd.	미국	3D 시뮬레이션 프로그램	- 플랫 패턴을 3D 디자인으로 변환 - 패턴 변경 결과 즉시 확인	3D 패션 시뮬레이션
15	TexWork	영우씨앤아이	한국	생산관리시스템	- 모든 공장에서 발생되는 커뮤니케이션을 제품에 반영 - 소비자가 요구하는 디자인 기획툴 제공	패션/의류 생산 분야
16	OPTIPLAN V3	Lectra	프랑스	생산관리시스템	- 최적의 폭으로 패브릭 주문 - 예상 주문을 만족시키기 위한 수량 계산 및 과잉재고 최소화	패션/의류 생산 분야
17	ASM	SortWear	미국	생산관리시스템	- 의복이나 신발 생산	패션/의류 생산 분야

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[3] 마케팅/매니지먼트 SW

[표 26]는 마케팅/매니지먼트 SW 분야의 사례를 정리한 것이다.

표 26 패션/의류 SW 분야 – 마케팅/매니지먼트

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	FXMirror	FXGear	한국	가상 피팅 솔루션	- 실시간 가상 피팅 및 코디네이션 - 실시간 신체 측정 - 안면 인식 로그인	가상 피팅
2	PIO	Physan	한국	가상 피팅 솔루션	- 실시간 가상 피팅 및 코디네이션 - 3D 의상 뷰어	가상 피팅
3	O/Sel	Optitex Ltd.	미국	온라인 플랫폼	- 판매, 마케팅 및 상품화 기능	가상 피팅
4	멀티상인 (알자나 TM)	알자나 솔루션		생산관리 솔루션	- 공지 관리, 입출고 관리, 물류 관리	패션/의류 관리 분야
5	Lectra Fashion PLM	Lectra	프랑스	PLM	- 전체 패션 개발 프로세스 최적화 - 기본 의류 프로세스 지원 기능	패션/의류 관리 분야
6	섬유 POP 자동화 시스템	㈜ 아이씨엔 아이티	한국	생산관리 및 품질관리 시스템	- 공정계획의 작성 및 변경 - 설비의 가동, 수명, 공구 관리	패션/의류 관리 분야

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

2.4.4. 로봇 SW 사례

로봇 SW는 로봇 제조/제어 SW, 로봇 운영 SW와 같은 2종류로 구분할 수 있으며, 이러한 분류는 동역학 및 시뮬레이션, 머니퓰레이션, 네비게이션, HRI, 운영 및 시스템과 같이 5개로 세분화된다.

[1] 로봇 제조/제어 SW

[표 27]는 로봇 제조 (시뮬레이션 동역학) SW 분야의 사례를 정리한 것이다.

표 27 로봇 SW 분야 – 로봇 제조 (시뮬레이션 동역학)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	Robotics LAB	원익로보틱스	한국	소프트웨어 개발 환경	- 실시간 로봇 제어 - 로보틱스 알고리즘을 프로토타이핑, 커스터마이징, 테스팅	로봇 설계, 제어 알고리즘 개발
2	Eureka	Roboris	이탈리아	프로세스 구현 소프트웨어	- 밀링, 선반, 프로파일링 및 로봇 장비의 분석 및 최적화 - 3D 시뮬레이션	로봇 및 머시닝 자동화 시스템 개발
3	DM Works	이지로보틱스	한국	시뮬레이션 툴	- 가상 작업장 생성 및 가상생산 - 생산 시나리오 결정 - 필요한 로봇 등 생산설비의 수량, 배치 및 설계 검증	로봇, 공정 및 생산 자동화 설계
4	iRoDi	큐빅테크	한국	범용적 로봇 소프트웨어	- 산업용 로봇 및 모바일 로봇을 레이아웃 설계 - 모바일 로봇 및 산업용 로봇 라이	로봇, 공정 및 생산 자동화 설계

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					브러리, Lua 스크립트, C 언어이용 로봇제어 기능, 물리 환경에서의 시뮬레이션 기능	
5	RoboCAD	siemens	독일	작업 셀 설계 및 시뮬레이션 도구	- 다중 장치 로봇 및 자동화된 제조 프로세스를 구성된 제품 및 자원 데이터 컨텍스트 내에서 모두 개발, 시뮬레이션, 최적화, 검증 및 오프라인 프로그래밍	로봇 제조 자동화 설계
6	Sim Pro	KUKA	독일	프로그래밍 및 시뮬레이션 소프트웨어	- KUKA 로봇의 오프라인 프로그래밍 및 시뮬레이션	로봇 오프라인 프로그래밍 및 시뮬레이션
7	K-ROSET	KAWASAKI ROBOTICS	일본	시뮬레이션 소프트웨어	- 가상 로봇 시뮬레이션, 정확한 동작 궤적, 택타임, 가골 결과 표시	로봇 교시 및 시뮬레이션
8	Roboguide	FANUC	일본	애니메이션 툴	- FANUC 로봇 및 이를 이용한 자동화 시스템의 적용 검토 - 고정도의 사이클 타임 시뮬레이션	로봇 교시 및 시뮬레이션
9	Vitual Robotics	Cogmation Robotics	캐나다	시뮬레이션 소프트웨어	- 레고 및 마인즈 스톰의 구성, 동작을 시뮬레이션	레고 로봇 시뮬레이션
10	Visual Components	Visual Components	핀란드	시뮬레이션 툴	- 로봇의 오프라인 프로그래밍 - 소프트한 모션과 충동 방지 로봇 수명 및 에너지 효율의 시뮬레이션	산업용 로봇 및 자동화 시뮬레이션
11	RoboDK	RoboDK	캐나다	제조용 로봇 특화 소프트웨어	- 제조용 로봇에 가상 제조 또는 생산 환경 구축 - 오프라인 프로그래밍을 통한 시뮬레이션	제조 및 산업용 로봇 시뮬레이션

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
12	MRDS 4	MicroSoft	미국	로봇 개발 도구	- 로봇 개발 및 시뮬레이션을 통한 로봇의 구현	지능형 로봇 시뮬레이션
13	V-REP	Coppelia Robotics	스위스	시뮬레이션 소프트웨어	- 다양한 환경에서 로봇의 동작 시뮬레이션	멀티 로봇, 팩토리 시뮬레이션
14	Webbot	Cyber Robotics	스위스	시뮬레이터	- 지능형 로봇 시뮬레이션 - C/C++, Java, Python, URBI, MATLAB 과 같은 소프트웨어 인터페이스 가능	멀티 로봇, 팩토리 시뮬레이션
15	RoboStudio	ABB	스웨덴	시뮬레이터	- 오프라인 프로그래밍 - 다양한 로봇의 센서, 그리퍼, 액츄에이터의 연계 시뮬레이션	델타, 수평/수직 다관절 로봇 및 공장 자동화 시뮬레이션
16	Gazebo	S.California Univ.	미국	시뮬레이션 소프트웨어	- 물체에 대한 조작, 다양한 인식, 위치보정 등 다양한 종류의 로봇 액션 시뮬레이션	휴머노이드와 같은 복잡한 로봇 시뮬레이션
17	Actin Simulation	Energid Technologies	미국	시스템 통합 제어 소프트웨어	- 로보틱 시스템에 대한 다양한 통합 컨트롤 알고리즘 및 어플리케이션에 대한 시뮬레이션	인티그레이티드 로봇 제어 시스템용 시뮬레이션
18	Workspace	WorkspaceLT	캐나다	시뮬레이션 소프트웨어	- 3 차원 시뮬레이션 환경 제공	다양한 제조용 로봇 시뮬레이션

참고: 정보통신기술진흥센터, "2017년도 글로벌 상용SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017년 9월.

[표 28]는 로봇 제조 (머니퓰레이션/네비게이션) SW 분야의 사례를 정리한 것이다.

표 28 로봇 SW 분야 – 로봇 제조 (머니퓰레이션/네비게이션)

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	ROS Industrial	오픈소스	미국	라이브러리	- 메이저 로봇 머니퓰레이터 및 각종 컴포넌트 제어	로봇 머니퓰레이터 제어
2	OROCOS	오픈소스	유럽연합	라이브러리	- 로봇 개발 - 로봇 머니퓰레이터 제어에 필요한 툴 제공	로봇 머니퓰레이터, 다양한 로봇 제어
3	Robomaster	Robomaster	독일	제어 프로그램 개발 툴	- CAD/CAM 기반 로봇 경로 생성 - 로봇의 경로 생성 및 최적화	산업용 로봇 머니퓰레이션 제어
4	I.R.S (Industrial Robot Software)	FANUC	일본	제어 소프트웨어 패키지	- 다양한 어플리케이션에 로봇 머니퓰레이션 제어 - 기본적인 모션, 패스생성, 에러감지, 충돌감지	산업용 로봇 머니퓰레이션 제어
5	WINCAPS	DENSO	일본	프로그래밍 및 시뮬레이션 소프트웨어	- 덴소 로봇의 프로그래밍 및 시뮬레이션	산업용 로봇 머니퓰레이션 제어
6	WorkVisual	KUKA	독일(중국)	제어 소프트웨어	- 전용 프로그래밍, 컨피규레이션, 로딩, 테스트, 진단, 변경, 압축 보관	산업용 로봇 머니퓰레이션 제어
7	MXR2	Softservo Inc.	미국	제어 소프트웨어	- 소프트서버의 윈도우 기반 모션 제어기 업그레이드 - 실시간 OS 환경에서 동작 가능한 모션 제어	산업용 다축장비 및 로봇 머니퓰레이션 제어
8	SPiiPlus	ACS Motion	이스라엘	제어 소프트웨어	- 동시에 다축을 중앙집중식 혹은	산업용 다축장비 및 로

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
					분산 제어	봇 머니퓰레이션 제어
9	ArtMinds	ArtMinds	독일	제어 소프트웨어	- 오프라인 모션 제어 프로그래밍 - 힘토크 기반 피드백 제어	산업용 로봇 머니퓰레이션 제어
10	motocalV EG	Yaskawa Motoman Robotics	일본	제어 소프트웨어	- 로봇 및 관련 장비를 동시에 캘리브레이션 할 수 있는 툴 제공	산업용 로봇 머니퓰레이션 제어
11	KeMotion	KEBA	오스트리아	제어 소프트웨어 패키지	- 로봇 모션 컨트롤 - 다양한 패키지와 연동할 수 있는 기능	산업용 로봇 및 자동화 시스템 제어
12	Kcong	Kawasaki	일본	제어 소프트웨어	- 로봇의 동작 데이터 작성 - 3D CAD 데이터를 사용한 로봇의 동작 데이터 자동 생성	산업용 로봇 머니퓰레이션 제어
13	uRON	ETRI	한국	라이브러리	- 위치 추정, 경로 계획, 경로 추종, 장애물 회피	지능형 로봇 네비게이션
14	SceneLib	Oxford Univ.	영국	라이브러리	- 자기위치 추정 및 환경지도 동시 작성	지능형 로봇 네비게이션
15	Carmen	Carnegie Mellon Univ.	미국	라이브러리	- 자기위치 추정 및 환경지도 동시 작성	지능형 로봇 네비게이션
16	KARTO	SRI International	미국	네비게이션 소프트웨어	- 매핑, 자기위치 추정, 경로계획, 탐사	지능형 로봇 네비게이션
17	Carmen	Malaga Univ.	스페인	오픈소스 소프트웨어	- 모바일 로봇의 모션 및 네비게이션에 필요한 프로그래밍 수행	모바일 로봇 제어

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

[2] 로봇 운영 SW

[표 29]는 로봇 운영 SW 분야의 사례를 정리한 것이다.

표 29 로봇 SW 분야 – 로봇 운영

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
1	센서기반 차량용 제스처 인식 시스템	전자부품 연구원	한국	HRI 소프트웨어	- 차량 주행정보와 운전자가 착용하고 있는 웨어러블 디바이스의 움직임 분석 - 차량 내 AVN 제어 및 프로그램 실행	스마트카, 웨어러블 디바이스
2	Hand Detection & Image Descriptors	Willow Garage	미국	HRI 소프트웨어	- 로봇 PR2 제어	로봇
3	Glove 형태의 Multi Sensor	Fraunhofer Institute	독일	신호 분석 시스템	- 근위 및 원위 손가락 관절 운동 뿐만 아니라 관성 측정 장치로 위치 방향 탐지	웨어러블, 로봇제어
4	EPOC	EMOTIV	미국	HRI 소프트웨어	- 얼굴 표정 인식 - 가상 공간에서 다른 사용자들과 의사소통	웨어러블, 로봇제어
5	KnowRob	TUM 대학	독일	지식 처리 시스템	- 백과사전 지식, 상식 지식, 작업 설명, 환경 모델 및 다양한 소스에서 획득한 작업에 대한 정보 결합	물리적 시스템

No	SW 명	개발사	국가	SW 유형	주요 기능	적용 분야
6	OPRoS	오픈소스	한국	오픈소스 플랫폼	- 로봇의 컴포넌트 실행 관리와 결함 관리	다양한 로봇 제어
7	OpenRTM	오픈소스	일본	소프트웨어 플랫폼	- 확장된 일부 RTC 기능 - 많은 프로그래밍 언어를 사용 가능	다양한 로봇 제어

참고: 정보통신기술진흥센터, "2017 년도 글로벌 상용 SW 백서 [제조 SW]", 과학기술정보통신부, 백서, 2017 년 9 월.

2.5. 사고사례

2.5.1. 국내 사고사례

LP가스를 이용한 건조 작업중 폭발 사고

(출처: 중대재해사례집, 안전보건공단, 2013 년 10 월)

- 사고개요

2012년 9월 17일 철제분전반 10시 20분경 1차 건조작업을 완료하고, 2차 건조작업을 수행하기 위하여 12시 30분경 건조실에 철제분전반을 적재하였다. 이 상태에서 LPG 버너에 불을 붙인 후, 작업자는 점심식사를 위하여 작업장을 떠났다. 13시 30분경 건조설비 가동 확인을 위하여 가동실의 온도계를 측정하니 60℃ 정도 되어서 건조작업 책임자에게 연락하고 대기하였다. 건조작업 책임자가 건조실 온도 확인후 가스버너에 불을 붙이기 위하여 라이터를 켜는 순간 폭발하였다.

표 30 가연물의 물리, 화학적 특성

구분	함유량 (%)	인화점 (℃)	폭발한계 (Vol. %)		최소점화 에너지 (MIE)
			하한 (LEL)	상한 (UEL)	
프로판	95	-105℃	2.0%	9.5%	0.26mJ (5%, Vol)
부탄	5	-60℃	1.5%	8.5%	0.25mJ (4.7%, Vol)

(출처: 중대재해사례집, 안전보건공단, 2013년 10월)

- 사고원인 분석
  - ◆ 가스 검지 및 경보설비가 부착되지 않음.
  - ◆ LP 가스의 지속적 누설 인지 못함.
  - ◆ 화재 3요소 (산소, 가연물, 점화원) 중 하나인 라이터(점화원)을 켬.

프레스 가공 작업중 상부금형 파손

(출처: 안전보건공단, 2017 년 8 월)

- 사고개요

2017년 7월 인천광역시 소재한 사업장내에서 프레스 가공 작업 도중 상부금형에 고정된 피어싱이 파손되면서 튕겨진 파편에 흉부를 맞아 사망하였다.

그림 8 사고발생 프레스와 피어싱

(출처: 안전보건공단, 2017 년 8 월)

- 사고원인 분석
  - ◆ 일반적으로 안전점검은 관리감독자가 실시하여야 하지만 작업시작 전 프레스 금형 설치 상태에 대한 안전점검 미실시
  - ◆ 프레스 작업 경험이 미숙한 작업자가 금형 교체작업 수행
  - ◆ 안전 교육 미실시

컨베이어 이물질 제거 중 렉과 철제 기둥사이에 끼임

(출처: 안전보건공단, 2017 년 4 월)

- 사고개요

2017년 4월 경기도 양주시 소재 보강토 블록 생산 작업장에서 에어건을 이용하여 체인 컨베이어의 이물질을 제거하던 근로자가 컨베이어를 통해 이송되고 있던 렉과 철제 기둥 사이에 머리가 끼어 사망.

- 사고내용

작업자가 컨베이어에 떨어진 불순물을 제거하기 위해 렉과 기둥 사이에 신체를 넣고 에어건을 이용하여 청소작업을 하였다. 이 때, 언로딩렉의 세

난중 두 번째 칸까지 블록의 언로딩이 완료되고, 세번째 칸 언로딩 위치로 렉이 이동할 때, 렉과 기둥사이에 머리가 끼임.

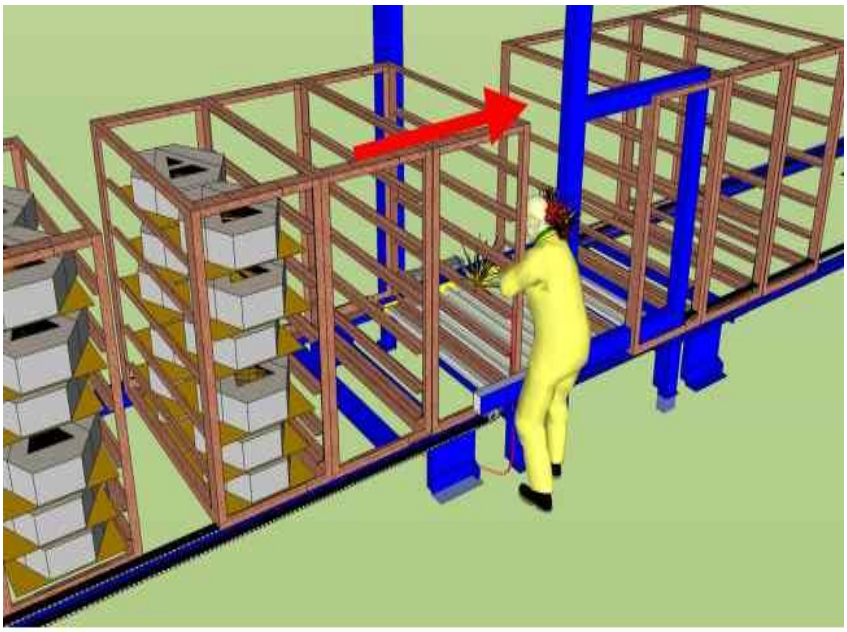


그림 9 추정된 사고 상황

(출처: 안전보건공단, 2017 년 8 월)

2.5.2. 해외 사고사례

[1] 플릭스보로 폭발 사고

(출처: Wikipedia, 2018.)

- 사고개요

영국 플릭스보로 사이클로헥산 폭발 사고는 1974년 6월 1일 토요일, 영국 북 링컨셔에 있는 플릭스보로 마을에 가까운 화학 공장에서 발생하였다. 당시 현장에 있던 72명의 인원 중 28명이 사망했고, 36명이 부상을 입었다.

- 사고내용

화학공장의 사이클로헥산 제조 반응기 6개 중 하나에서 누출 현상을 감지하였고, 공장은 정상 가동하면서 이 누출을 수리하기 위하여 제조 반응기 2개를 연결하는 임시배관을 설치하였다. 하지만 기존의 급송 파이프 28인치 보다 작은 20인치 직경의 임시배관을 사용하였다. 결국, 반응기 내압을 견디지 못하고, 임시배관이 파괴되면서 사이클로헥산이 대량 누출되었다. 30톤 가량의 사이클로헥산이 기화되어 거대한 증기운이 형성되었고, 알 수 없는 점화원에 의해 45초 후에 폭발하였다. 이 사고로 공장설비, 행정동 건물이 완전히 파괴되고, 극심한 인명피해를 주었다. 또한, 이 폭발로 인해 주위의 1821채의 주택, 167개의 상점과 공장들까지 피해를 입었다.

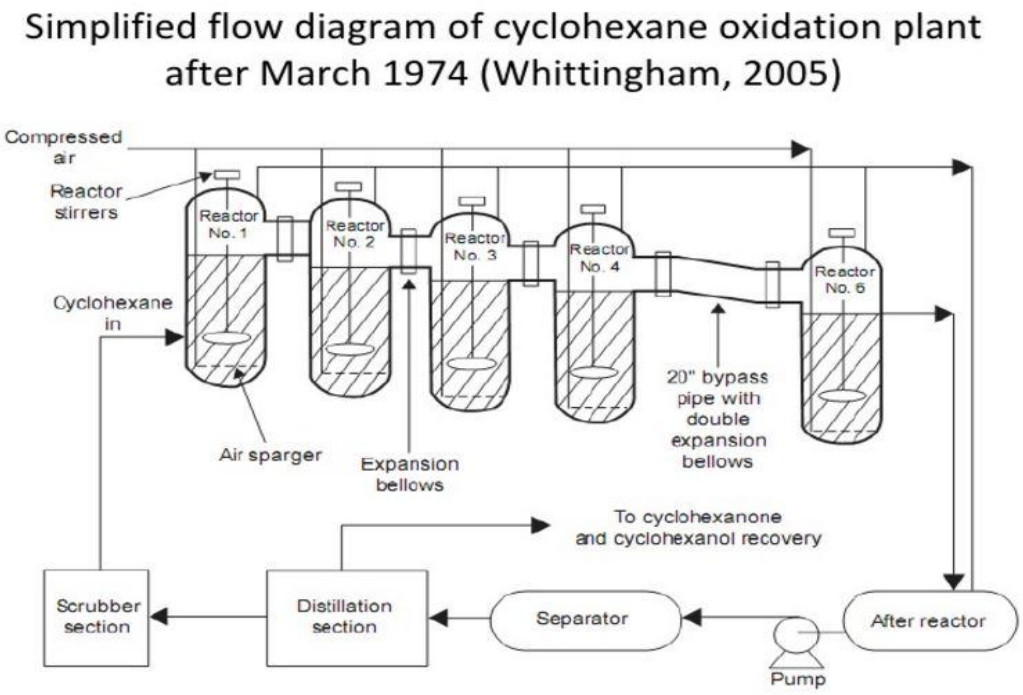


그림 10 플릭스보로 화재 사고

- 사고원인
  - ◆ 무리하게 공장 정상가동을 고집
  - ◆ 고온, 고압을 감안하지 않은 임시배관 설계 및 시공
  - ◆ 지나치게 많은 공장내 가연물

[2] 엑슨발데즈 원유 유출 사고

(출처: Wikipedia, 2018.)

- 사고개요

엑슨발데즈 원유 유출 사고는 유조선 엑슨발데즈가 좌초되면서 적하되어 있던 원유가 유출된 사고이다. 이 사고는 헬기, 비행기와 보트로만 접근할 수 있는 프린스 윌리엄 만의 원격지에서 발생하였다. 또한 이 곳은 연어, 해달, 물개 바다새의 서식지이기 때문에 해양 생태계에 커다란 피해를 주었다.

- 사고내용

엑슨발데즈호는 1989년 3월 23일 오후 9시 12분에 출발해 5,300만 갤런의 원유를 싣고 캘리포니아 주로 향했다. 오후 11시 이후에 선장이 3등 항해사에게 사전에 협의한 지점에서 항로에 돌아가도록 지시하고, 자리를 떠났다. 그러나 엑슨발데즈 호는 항로에 돌아가지 못하고, 3월 24일 오전 0시 4분경에 블라이 암초에 부딪혀 좌초하였다. 이 사고로 총 적재량의 20%인 1,100만 갤런의 기름이 바다에 유출되었다.

그림 11 원유 유출로 인한 해양 오염

- 사고원인 분석

  미국교통안전위원회의 분석에 따르면, 사고원인은 다음과 같다.

  - ◆ 3등 항해사가 올바른 조타를 하지 않았고, 당시 엑슨발데즈 호는 자동 조종 장치가 작동되고 있었다.
  - ◆ 선장이 항로 확인을 게을리 하였다.
  - ◆ Exxon Shipping Company는 선장을 감독하는 것과 적절한 인원 배치에 대한 책임을 다하지 못하였다.
  - ◆ 연안 경비대가 유효한 선박 교통 시스템을 제공하지 못하였다.

2.6. 제조 SW 현황조사 결론

2.6.1. 현황조사 정리

본 현황 조사는 제조 및 기계 소프트웨어의 안전성 확보를 위한 가이드 개발을 위해 국내와 해외 제조산업 분야의 현황 및 국내와 해외 안전 체계를 조사하고, 분석하였다. 또한 제조산업의 사고사례를 조사함으로써 안전 사고의 발생과정, 원인, 결과 등을 파악하였다.

제조 분야는 기존의 제조업을 고부가가치 산업으로 변화시키기 위한 노력을 하고 있다. 제조업은 기계화, 자동화, 집중화되고 있으며, ICT 인프라와 결합한 디지털화가 진행되고 있다. 또한, Industry 4.0의 영향으로 스마트팩토리에 대한 연구개발이 활발하게 이루어 지고 있다. 또한 최근 미국과 유럽을 중심으로 PMI가 상승 추이를 보이면서, 세계 제조업 경기가 회복세에 있음을 확인하였다.

이러한 제조업의 상승세와 맞물려서, 소프트웨어 시장의 성장세가 가속화되고 있다. 특히, 국내 소프트웨어 시장은 지속적으로 성장하고 있다. 2014년 103억 달러, 2015년 109억 달러, 2016년 113억 달러의 시장을 형성하고 있다. 소프트웨어 생산과 수출 역시 지속적인 성장세이다. 제조업이 디지털화되고, 스마트팩토리에 대한 연구개발이 활발해 지면서 자연스럽게 제조업에서 소프트웨어를 활용하는 빈도와 중요성이 높아지고 있는 추세이다.

기존의 기업들은 제조업에 ICT를 적용하기 위한 움직임을 보이고 있다. 여러 기업들이 빅데이터와 인공지능 기술을 자사 제품에 적용하여 데이터 분석을 할 수 있는 패키지 소프트웨어를 개발하고 있다. 또한, 인공지능, 빅데이터, IoT 기술을 확보하여 다양한 산업분야에 특화된 플랫폼을 제공하는 추세이다.

전반적으로 세계 제조산업 경기가 회복되고, 제조업의 다양한 도메인에서 소프트웨어를 활용하고 있지만 아직까지 제조업 분야와 소프트웨어가 안전하게 융합

되지 못하였고, 관련된 안전 사고들이 많이 발생하였다. 따라서 제조 소프트웨어 분야의 안전성을 확보하기 위한 안전 가이드의 필요성이 대두되고 있다.

2.6.2. 현황조사 결론

국내 및 해외 사고사례 분석을 통해서 사고발생 원인들을 식별하였다. 그 원인 중의 하나는 작업 환경이 열악하여 위험물질이 작업장 내에 다수 존재하였고, 기계의 고장이 발생하였음에도 무리하게 공장운영을 지속하면서 기계를 수리하였다. 두번째는 공정이나 작업 특성을 반영하지 못하여서 시스템 설계의 오류가 발생하였고, 결과적으로 안전 사고를 일으켰다. 세번째는 안전 조치 (가스 누출 감지, 위험상황 알림, 비상정지 시스템 등)이 미흡하였고, 안전 관련 시스템이나 장치가 존재하더라도 성능이 좋지 못하였다. 마지막으로 안전관련 표준이나 가이드를 숙지하지 못하였거나 부족하여서 인간이 실수한 경우이다.

안전 사고들은 사고 발생을 미연에 방지하여야 한다. 이를 위해서 공정 및 기계 분야의 시스템 설계를 수행할 때, 발생하는 Random failure와 Systematic failure에 대한 대처가 필요하다. 또한, 소프트웨어 기반의 안전 조치를 통하여 인간의 작동 미숙, 오류, 피로도 등에 의한 사고를 예방하여야 한다.

IEC 61508, IEC 61511, IEC 62061 등과 같은 안전관련 국제 표준이 존재하고, 이를 따르면 안전 설계가 가능하다. 하지만 중소기업들은 안전관련 국제 표준의 이해와 이를 이행하기 위한 역량이 부족하다. 또한, 소프트웨어 공학과 소프트웨어 안전성 확보의 중요성에 대한 인식이 부족하다. 따라서 안전사고를 예방하고, 안전한 소프트웨어 개발을 지원할 수 있는 제조분야의 소프트웨어 안전 가이드가 필요하다.

제 3 장. 안전 시스템 분석

안전 시스템 분석

3.0. 개요

안전 시스템은 시스템을 구성하는 구성요소의 의도된 기능을 수행하지 못하거나, 결함 발생시 이를 통해 유발하는 사건(Event)으로 부터, 발생되는 인적/물적 상당한 피해를 유발 가능한 시스템을 안전 시스템이라고 칭한다. '안전 시스템 분석' 활동이란, 대상 시스템의 정의 및 정의된 대상으로부터 발생 가능한 위험요소를 식별하고 설계적으로 대응 방안을 마련하는 활동이다. 안전분석이 수행되기 위해서는 대상 시스템으로부터 발생 가능한 위험요인이 식별되고 식별된 요인으로부터 발생 가능한 영향에 대한 분석이 수행되어야 한다. 이러한 분석이 충실히 이루어 지기 위해서는 안전분석 대상 자체에 대한 분석 및 정의활동이 수행되어야 한다. 대상 시스템의 분석 및 정의 과정을 통해, 시스템의 개념(System Concept Definition) 단계의 수행을 통한, 대상의 개념과 적용범위에 대한 정의를 수행하게 된다. 정의된 개념 및 범위를 대상으로 시스템 안전분석 활동이 수행되어야 한다. 특히, 시스템 개념정의 활동은 시스템공학(Systems Engineering) 활동을 기반으로 시스템 정의 및 분석 단계가 수행된다.

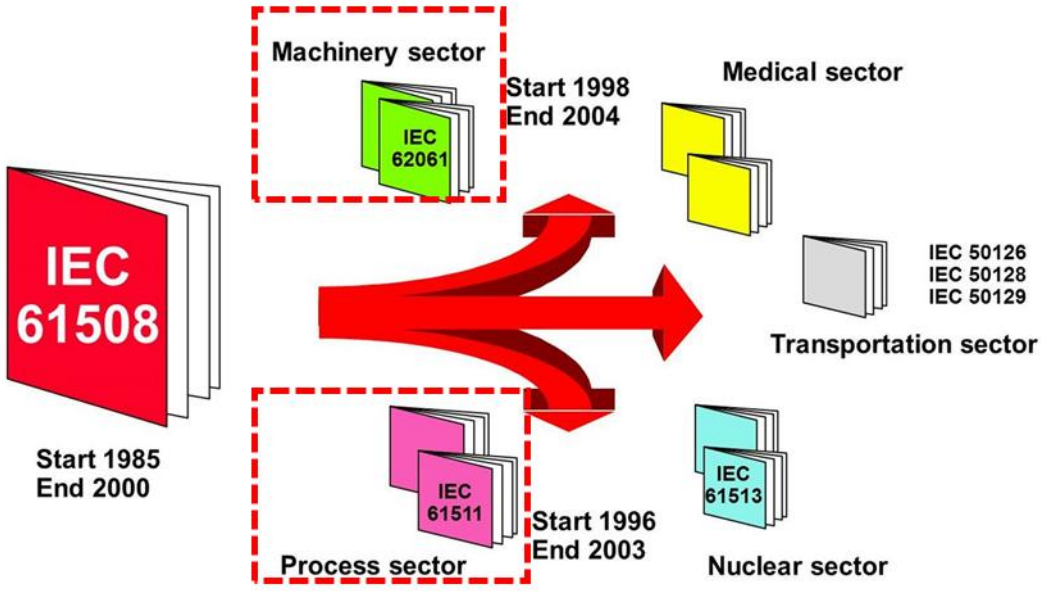


그림 12 IEC 61508 파생기반 IEC 62061/61511 표준

본 가이드에서는 초기 시스템공학 기반의 시스템 정의 및 분석 과정을 기반한 산출물을 바탕으로 제조 장치의 측면과 제조공정이라는 두 관점에 대해서 안전 시스템 분석을 위한 수행활동 대한 내용들이 가이드 되어진다. 따라서, 기계류 제어 대한 사항은 IEC 62061을 준수하도록 가이드 하였으며, 공정 제어의 경우 IEC 61511의 준수를 기반한 활동에 대한 가이드 정보를 따라 준수해야 한다. 특히, 안전 시스템에 대해 IEC 62061 및 IEC 61511의 두 표준에서 다루는 대상의 의도된 기능이 된다.

참고 1: 이하 가이드에서 사용하는 '안전 시스템' 은 IEC 62061 의 SRECS(Safety-Related Electrical Control System)와 IEC 61511 의 SIS(Safety Instrumented System)를 통칭하여 이야기 할 때 사용한다.

참고 2: 이하 가이드에서 사용하는 '안전 기능' 은 IEC 62061 의 SRCF(Safety-Related Control Function)와 IEC 61511 의 SIF(Safety Instrumented Function)를 통칭하여 이야기 할 때 사용한다.

IEC 62061 표준 개요

IEC 62061은 IEC 61508의 하부의 특정 영역인 기계류 제어에 대한 표준으로서 기계의 안전에 관련해 전기/제어 시스템의 설계와 실행을 위한 요구사항을 규정하고 있다. 최근 기계의 고장 등으로 인해 인명 피해나 경제적 손실이 발생하는 사례가 늘어나기 때문에 기계류 시스템에 대한 안전 무결성 수준(SIL, Safety Integrity Level 이하 SIL로 표기)이 요구되고 있다. 이러한 기계류 제어 시스템의 안전에 요구되는 개별 안전 무결성을 준수하기 위한 평가 및 설계적 방안에 관해 다루고 있다.

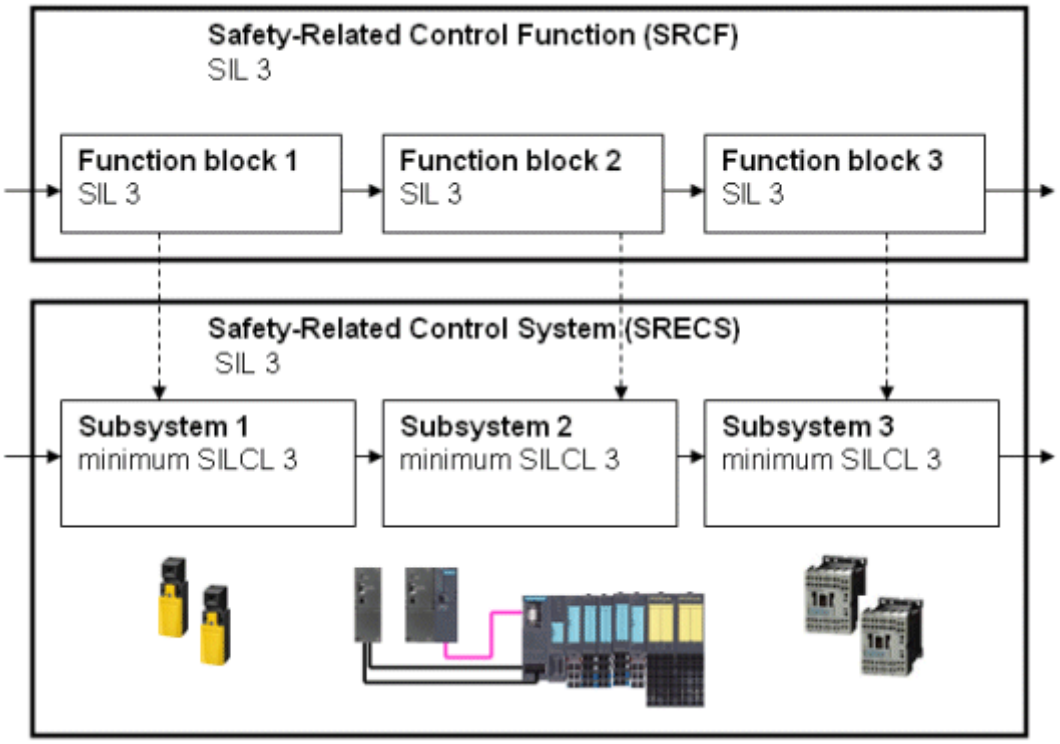


그림 13 IEC 62061 의 SRCF 및 SRCES 관계

특히, SRCF(Safety-Related Control Function 이하 SRCF로 표기) 요구사항 명세는 위험분석 및 위험 감소 단계에서 위험평가 수행의 결과에 따라, 안전 기능에 대한 필요성이 결정되고 위험 저감을 위한 SRCF가 SRECS(Safety-Related Electrical Control System 이하 SRECS로 표기)에 의해 전체적 또는 부분적으로 구현되는 과정을 통해 SRECS의 SRCF 반영을 통한 안전성을 확보하게 된다.

IEC 61511 표준 개요

국제 표준 IEC 61511은 석유화학 공정과 같은 공정 산업 제어 장치의 안전성 확보를 위한 일관성을 유지목적으로 만들어진 표준이다. 특히, IEC 61511 표준의 특징은, 안전관련 기능을 구현한 SIS(Safety Instrumented system 이하 SIS로 표기)에 있다. SIS는 대상 시스템에 대하여 안전한 상태로 유지하거나 비정상 상황에서 안전한 상태로 만들게 하는 일련의 자동화 기능을 갖춘 시스템이다. 따라서, 공정 산업에서 발생할 수 있는 대형참사가 발생하지 않도록 위험요소를 사전에 감지하여, 공정을 안전한 상태로 되돌리는 SIF(Safety Instrumented System 이하

SIF로 표기)를 포함한 SIS를 일컫는다. 또한, 다양한 공정 위험들로 부터 보호될 수 있도록 단일 혹은 복수의 기능을 실행한다. IEC 61511 표준에서는 SIS의 정의, 실행 및 관리에 대한 전 생명주기 관점에서 접근하는 방식을 사용한다. 해당 표준의 주목적은 공정위험요인 분석 및 위험성 평가를 수행한다. 또한, SIS에 의하여 도달하여야 할 위험 감소에 대한 요구사항을 명세하며, 전 수명주기적 관리 및 안전무결성 수준에 대한 의 설계, 제조 및 운영은 일반산업 표준 IEC 61508에 따라 적용되며, 프로세스 산업 부분에 특정된 표준인 IEC 61511이 적용되어 진다. 표준의 대상 시스템인, 안전계장시스템은 센서부터 액츄에이터의 이르기 까지 SIF를 수행하는데 필요한 모든 구성품 및 서브 시스템으로 구성된다.

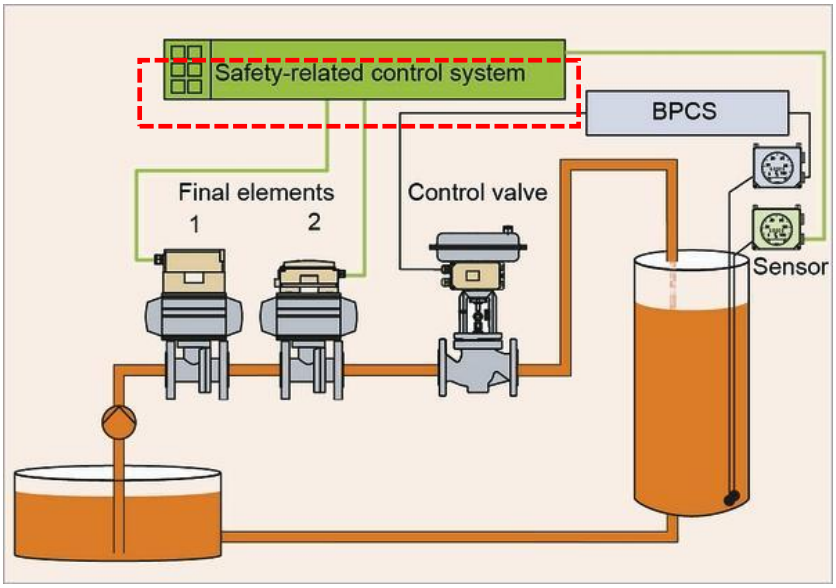


그림 14 IEC 61511 표준 개념

- 센서 : 혼란이나 비정상 상태를 탐지하기 위하여 공정을 감시하는 감지기(예: 압력센서)

- 논리장치 : 센서에서 신호를 받아 상태가 위험한지 결정하고, 위험한 경우에 작동을 취하도록 신호를 보내는 논리장치
- 최종 제어 장치 : 논리 장치에서 신호를 받아 대상 시스템의 적절한 작동이 되도록 하는 마지막 제어장치(예: 밸브 개폐 밸브, 펌프가동 정지)

이러한, SIS는 공정 위험에 노출되는 위험에 근거하여 SIL에 따라 설계되어야 한다. 기본공정제어시스템(BPCS; Basic process control system)으로 알려진 제어시스템은 온도, 단계, 압력 및 흐름과 같은 변수들을 제어한다. 따라서, 이러한 제어 및 안전시스템들은 상호 발생 가능한 위험을 모니터링 하고 위험한 상황에서 안전한 상태(Safety state)에 이르기 위해 상호 통신 정보를 공유해야 한다. 이러한 점을 반영한 인터페이스, 통합 관점에서 설계/구축/운용 되어야 한다.

안전 생명 주기 (Safety Life Cycle)

제조 소프트웨어 안전 가이드는 [그림 15]의 안전 생명 주기를 기반으로 한다. 제조 분야 안전 관련 시스템은 "분석", "구현", "운영"의 3개 파트로 구분 된 시스템 개발 생명 주기를 가지며, 이를 지원하기 위한 "기능 안전 관리" 활동과 안전 관련 시스템 개발 각 단계별 활동과 산출물에 대한 확인 및 검증 활동을 수행하는 "Validation & Verification" 활동이 개발 생명 주기를 지원한다. 단, 본 가이드에서는 "운영" 파트는 다루지 않는다.

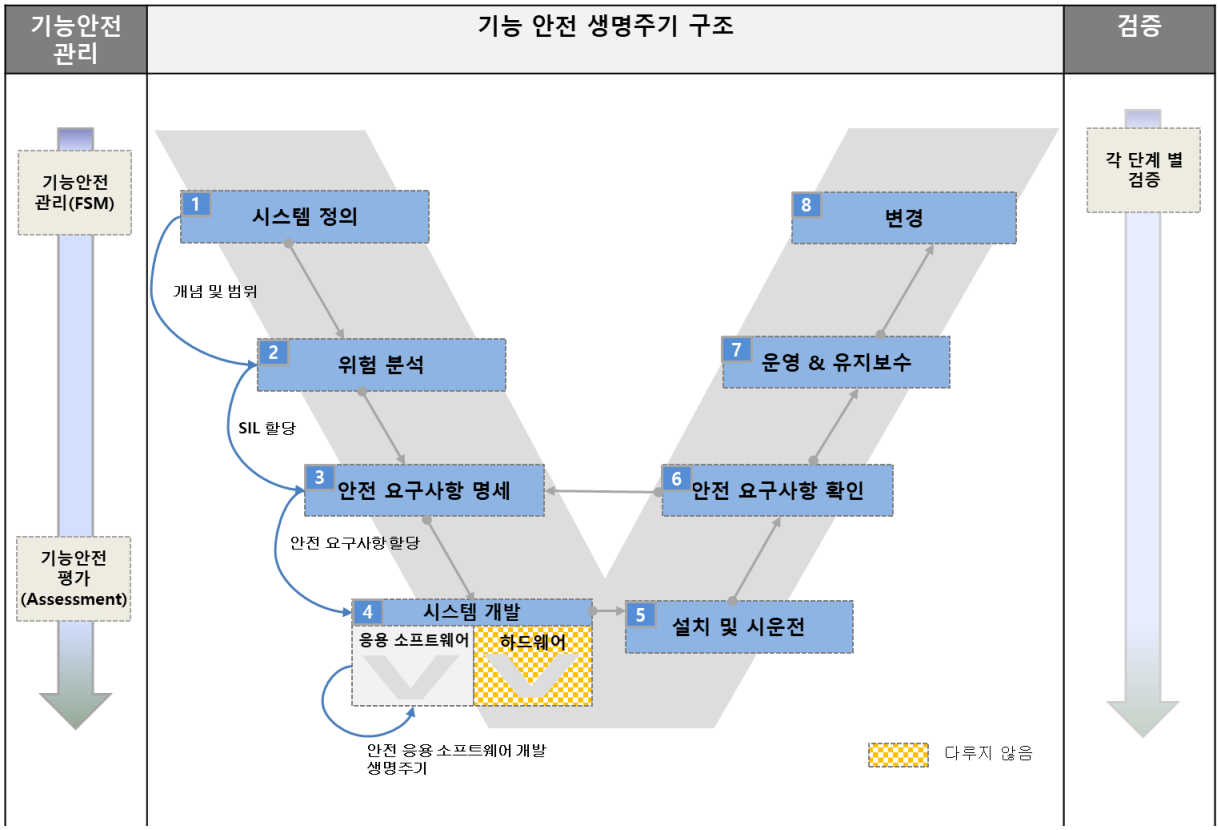
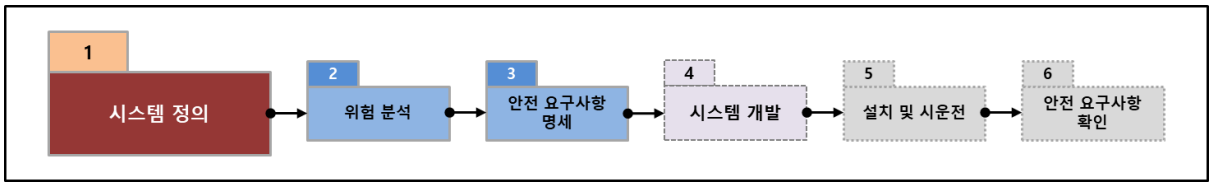


그림 15 기능 안전 생명주기 구조



3.1. 시스템 정의 및 분석

목적

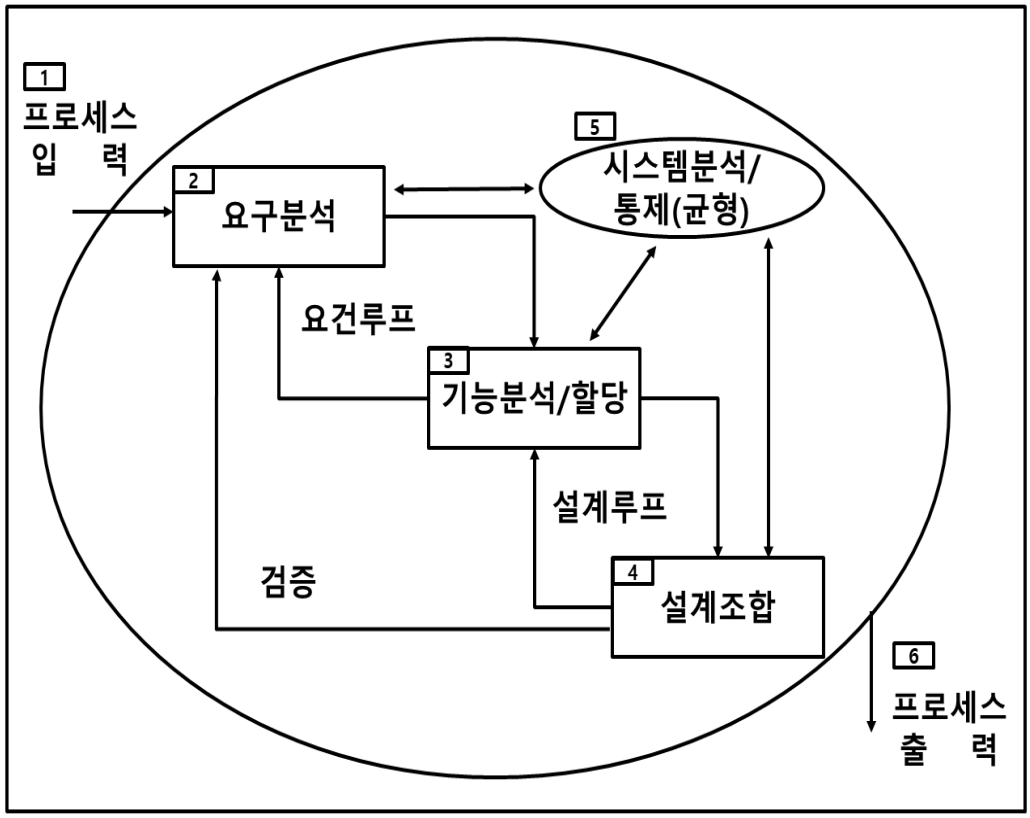
시스템 정의(System Definition) 단계는 대상 시스템에 대한 정보를 식별하여 대상 시스템에 대한 개념(Concept)를 이해하고 설계, 운용 및 관리되어야 할 범위를 정의하는 단계이다. 해당 단계의 수행을 통해, 물리적, 기능적, 제약사항(인터페이스, 성능, 안전, 운용/사용환경)등 개념적 아키텍처 정보를 포함한 사항에 대한 식별 및 정의를 수행하는 단계이다. 시스템 정의 단계를 통해 식별된 정보는『시스템 위험분석』단계에서 안전분석 수행을 위한 입력자료로서 활용되어진다. 특히, 시스템 정의 및 분석 활동은 시스템공학(Systems Engineering)을 근간으로 수행되어진다. 시스템공학 설계 프로세스를 따라, 기능적/물리적/제약사항/아키텍처 정보에 대해서 식별이 가능하다. 이러한 식별된 정보는 요구사항 명세 단계를 통해 식별된 시스템의 안전 요구사항 중 응용 소프트웨어에 할당 된 요구사항을 구현하기 위해 응용 소프트웨어에 대한 안전 요구사항을 식별하고 명세하는 단계로『시스템 정의 』단계의 입력 단계에 해당하는 에서 작성된 산출물을 기반으로 세부 단계 활동을 수행한다.

활동 단계 개요

『시스템 정의 』단계가 수행되기 위해서는 입력이 되는 정보 및 문서가 필요로 한다 시스템공학 프로세스의 입력에는 고객요구사항과 프로젝트 제약사항이 포함된다. 요구사항은 설계될 시스템의 성능 특성과 직접적으로 관계된다. 또한, 요구 사항은 수명주기중의 고객요구를 기술한 것으로 시스템의 목적이며, 운용환경에서 그 시스템이 '얼마나 잘 작동할 것인가'와 관련이 있다. 제약사항은 외

부 인터페이스, 프로젝트 지원, 기술 또는 수명주기 지원 시스템 등에 의한 제약 때문에 존재하는 조건이다. 시스템공학 프로세스의 주목적이 요구사항을 설계사항으로 변환시키는 것 이기 때문에 요구사항은 프로세스의 중요한 초점이 된다. 특히, 이러한 산출물은 다음 단계인 시스템 위험분석 활동의 기본 자료로 활용되기 때문에 시스템공학 프로세스의 입력단계에 대한 충분한 검토 및 수행되어야 한다.

구 분	설 명
선행기준	1. 개발 대상 정의 완료 2. 이해 당사자 정의 완료
입력문서	• 시스템 범위 • 이해당사자 요건(Stakeholder Needs) • 운영개념 및 운용모드 • 인터페이스 • 환경요소 • 제약조건 • 주요성과 파라미터(KPPs) • 수명주기 기반 프로세스 • 기능 및 성능, 물리 특성

수행흐름	
산 출 물	• 시스템 사양서 문서 • 시스템 기능요구사항 및 Safety Related Function 식별 • 시스템 아키텍처 문서 • 베이스라인 확립
완료기준	1. 요구사항 분석 완료 2. 요구사항 검증 완료 3. 요구사항 추적표 작성 완료

세부 수행 활동

[1] 프로세스 입력 단계

『프로세스 입력』 단계에서는 시스템 정의 및 분석 수행을 위한 시작 단계로 시스템의 근간을 마련하는 단계이다. 해당 단계에서는 개발 대상(기계 또는 공정 제어 안전 시스템)에 대한 선정이 되어야 하며, 개발과 관련한 이해당사자가 명확하게 식별되어야 한다.

수행 절차

(1) 개발 또는 관리되어야 할 대상에 대한 정의가 되어야 한다.

개발 또는 관리 되어야 할 대상에 대한 명확한 정의가 되기 위해서 다음의 사항이 고려되어 정의 되어야 한다.

- ✓ 운용환경 및 운용개념
- ✓ 대상 시스템 및 공정에 대한 기능적 관점
- ✓ 대상 시스템 및 공정에 대한 구조적 관점
- ✓ 대상 시스템 및 공정에 대한 총 수명주기적 관점
- ✓ 대상 시스템 및 공정에 대한 개발/운용상 제약사항
- ✓ 대상 시스템 및 공정에 대한 비기능적 관점(인터페이스, 성능, 안전, 법규 등)

(2) 개발 또는 관리되어야 할 대상과 관련한 이해당사자를 식별하여 리스트화 한다.

이해당사자를 식별하기 위해 다음사항을 고려 하여 식별될 수 있다. 시스템 및 공정에 관한 명확한 이해당사자 식별을 통해, 분야별 책임에 대한 명확히 할 수 있다.

- ✓ 운용개념서를 기반으로 식별되는 기능에 대한 분석을 통한 리스트가 확보되어야 한다.
- ✓ 식별된 기능과 관련해, 수행의 주체를 식별하여야 한다.
- ✓ 식별된 기능 및 수행주체간 상호 정보 교류가 있는 이해당사자는 주의 관리되어야 한다.
- ✓ 유스케이스(Usecase) 다이어그램을 활용해 개발 및 운영간 이해당사자 식별이 가능하다.

수행 절차

(1)『시스템 정의』를 위한 입력 산출물 리스트를 확인한다.

시스템에 대한 명확한 정의가 수행되기 위해서 다음의 입력정보 문서가 식별되었는지 우선 확인 되어야 한다.

- ✓ 이해당사자 요구사항
- ✓ 운용환경 및 요구사항
- ✓ 기능적 요구
- ✓ 비기능적 요구(인터페이스, 성능, 제약)

(2) 각 입력 정보를 분석 및 정의하여 문서화 한다.

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시 까지 분석을 진행한다.

(4) 필요한 필수 식별 정보를 모두 확인 후 다음 단계인『요구사항 분석』단계로 진행한다.

식별 항목

입력정보는 필수 식별 정보에 해당되며, 대상 시스템의 범위와 구현 수준과 하부 장비에 따라 상이하게 적용할 수 있으며 시스템 계획 단계나 인증 준비 단계에서 조절이 가능하다.

구 분	식별 대상
시스템 구성	• 시스템 수준별 구성(시스템-하드웨어-소프트웨어)
시스템 기능	• 시스템 내부 기능 • 시스템 외부 연동 기능 • 인터페이스 기능
시스템 제약 사항	• 성능 요구사항 • 시스템 안전 고려사항 • 시스템 내부 인터페이스 요구사항

요구분석 단계

『요구분석』은 대상 시스템에 대한 계획된 사용자, 환경요소 그리고 시스템 기능에 대한 요구사항을 결정하기 위해 식별된 시스템 특성을 배경으로 고객 요구와 목적을 정의하는 것을 포함한다. 요구분석은 식별된 기능의 성능요구사항을 최적화 시키고, 조합된 해결책이 고객 요구사항을 만족시키는지 검증하기 위해 기능분석과 함께 반복적으로 수행된다.

수행 절차

(1) 『요구분석 단계』의 입력 산출물 리스트를 확인한다.

(2) 각 입력 정보를 분석 및 정의하여 문서화 한다.

요구분석을 통해 다음의 정보를 담은 문서가 개발되어야 한다.

- ✓ 기능 요구서
- ✓ 성능 요구서
- ✓ 인터페이스 요구서

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시까지 분석을 진행한다.

(4) 필요한 필수 식별 정보(항목)를 모두 확인 후 다음 단계인『기능분석 및 할당』단계로 진행한다.

식별 항목

요구분석은 다음 사항의 명확한 이해를 통해 얻어진다.

- ✓ 기능: 시스템이 무엇을 해야 하는가.
- ✓ 성능: 기능이 얼마나 잘 수행되어야 하는가.
- ✓ 인터페이스: 시스템이 운용될 환경을 고려한 연동하는가.
- ✓ 다른 요구사항과 제약사항들

요구분석으로부터 도출된 이해는 수행을 위한 기능 및 물리적 설계의 기본을 이룬다.

기능 분석 및 할당 단계

『기능 분석 및 할당』은 어느 시스템 레벨의 기능과 성능요구사항은 상위 레벨 요구사항으로부터 개발된 다. 기능분석 및 할당은 연속적으로 하위 레벨의 기능과 성능요구사항을 정의하기 위해 반복된다. 그러므로 전보다 증가된 세부 레벨에서 아키텍처가 정의된다. 시스템 요구사항은 통합시스템 설계를 지원하기 위한 설계 및 검증 기준을 제공할 수 있도록 충분히 세부적으로 할당되고 정의되어야 한다

수행 절차

(1)『기능분석 및 할당 단계』의 입력 산출물 리스트를 확인한다.

(2) 각 입력 정보를 분석 및 정의하여 문서화 한다.

기능분석을 수행하는데 있어서, 운용개념서(Concept of Operations)는 중요한 초석의 역할을 담당하는 문서이다.

- **기능분석을 통해서, 기능간 계층(Layer)이가 분리되어야 하고, 그 결과를 바탕으로 기능 아키텍처 산출물도 산출되어 기능요구사항 간의 아키텍처 구조를 유지 및 관리 되어야 한다.**
- **분석/도출되어 산출된 기능요구사항은 이와 연관된 성능지표 및 성능요구상과 연계되었는지 분석을 통해, 개발/관리 되어야 한다.**
  - ✓ 기능 분석 및 할당을 지원하는 연계 다이어그램으로는 FFBD(Function Flow Block Diagram), Sequence Diagram, Activity Diagram 등이 있다.

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시 까지 분석을 진행한다.

(4) 필요한 필수 식별 정보(항목)를 모두 확인 후 다음 단계인『설계조합』단계로 진행한다.

식별 항목

- ✓ 기능적 관점에서 시스템을 정의하고, 최상위 레벨 기능을 하위 기능으로 분해한다.
- ✓ 연속적으로 하위 레벨에서 어떤 활동을 해야 하는지 식별한다.
- ✓ 상위 레벨의 성능요구사항을 상세 기능 및 성능 설계기준 또는 제약사항으로 변환시킨다. 즉 얼마나 잘 기능이 잘 수행되어야 하는지 식별한다.
- ✓ 모든 내부 및 외부 기능 인터페이스를 식별한다.
- ✓ 인터페이스(기능 분할)를 통제하고 최소화하기 위하여 기능적 그룹화를 식별한다.
- ✓ 시스템의 기존 또는 도출된 컴포넌트의 기능적 특성을 결정하고 분석 및 할당에 컴포넌트를 포함시킨다

설계조합 단계

『설계조합(design synthesis)』은 기능 분석 및 할당의 결과물인 기능 설명을 기반으로 개발되는 개념과 설계에 의해 이루어지는 프로세스이다. 설계조합은 사전에 설명 된 성능 파라미터의 제한된 범위 내에서 요구된 역할을 수행할 수 있는 물리적 아키텍처(제품, 시스템 및 소프트웨어 요소의 집합)를 개발하는 창조적인 활동이다. 주어진 기능 및 성능요구사항의 집합을 충족시키기 위해 개발된 몇몇 하드웨어 또는 소프트웨어 아키텍처가 있을 수 있기 때문에 설계조합은 제시된 아키텍처 중 에서 가장 최적의 대안을 선택하기 위한 절충연구의 단계를 설정하는 것이다. 설계 조합의 목적은 서술된 요구사항을 충족시킬 수 있는 설계 해결책을 성취할 수 있는 방법으로 하드웨어와 소프트웨어의 컴포넌트를 결합하거나 재구성하는 것이다. 개념개발 동안, 조합은 시스템 개념을 생성하고, 하부 시스템 간의 기본적 관계를 규정한다. 예비 설계와 상세 설계 동안, 하부 시스템과 컴포넌트의 설명서가 만들어 지고, 모든 시스템 컴포넌트 사이의 상세한 인터페이스가 정의된다.

수행 절차

(1) 『설계조합 단계』의 입력 산출물 리스트를 확인한다.

(2) 각 입력 정보(기능 아키텍처 정보)를 분석 및 정의하여 문서화 한다.

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시 까지 분석을 진행한다.

(4) 필요한 필수 식별 정보를 모두 확인 후 다음 단계인 『프로세스 출력』 단계로 진행한다.

식별 항목

(1) 물리 아키텍처(대상 요소, 소프트웨어 코드 등)

- ✓ 기능과 제약사항을 시스템 요소에 할당
- ✓ 시스템 요소 대안의 조합 .
- ✓ 대안 기술 평가

- ✓ 물리적 인터페이스 정의.
- ✓ 수명주기 기법과 절차 개발
- ✓ 시스템 요소 통합

시스템 분석 및 통제 단계

『시스템 분석 및 통제』 단계의 기능 및 목적은 균형유지이다. 따라서, 해당 단계에서는 사용자 요구사항, 기술적 목적, 설계, 사업 일정, 기능 및 성능 요구 사항 및 수명주기 비용 간에 바람직하고 실제적인 절충연구가를 식별하고 수행하여야 한다. 절충연구(Trade-off study)는 기능 또는 성능 아키텍처의 다 양한 수준에서 의사결정을 지원하기에 충분할 정도로 정의, 수행 및 문서화 되어야 한다. 각 절충연구의 상세 정도는 비용, 일정, 성능 및 위험 영향에 비례해야 한다

수행 절차

(1) 『모든 단계』의 입력/출력 산출물 리스트를 확인한다.

(2) 각 입력 정보를 분석 및 정의하여 문서화 한다.

> **입력 문서는 모든 프로세스 수행을 통해 작성되는 모든 문서를 칭한다.**
> ✓ 여러 산출물을 통해서, 대상 시스템 및 공정에 대한 목적에 부합하는 요건을 주어진 제약 범주 내에서 도출하기 위한 절충과정의 단계이다.

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시 까지 분석을 진행한다.

(4) 필요한 필수 식별 정보를 모두 확인 후 다음 단계로 진행 및 종료를 진행한다.

식별 항목

(1) 요구분석 절충연구

(2) 기능분석/할당 절충연구

(3) 조합 절충연구

(4) 시스템 비용/효과도 분석

(5) 위험관리

(6) 형상관리

(7) 인터페이스 관리

프로세스 출력 단계

『프로세스 출력』은 시스템공학 프로세스의 출력물은 시스템 요구사항과 설계 해결책을 정의하는 문서로 구성된다. 조합 프로세스를 통해 개발된 물리적 아키텍처는 연관 시스템을 포함하고 시스템 아키텍처를 완성하기 위한 활동을 포함하기 위해 확장된다. 이러한 시스템 레벨의 아키텍처는 시스템 요구사항과 문서를 보다 더 발전시키기 위한 참고 모델이 된다. 시스템공학 프로세스 출력은 시스템과 형상품목(Configuration Item) 아키텍처, 규격서, 베이스라인 및 의사결정 데이터베이스를 포함한다.

수행 절차

(1)『프로세스 출력 단계』의 입력 산출물 리스트를 확인한다.

(2) 각 입력 정보를 분석 및 정의하여 문서화 한다.

시스템공학 프로세스의 수행을 통해, 총체적 산출물을 도출하는 단계이다.

- ✓ 시스템 요구사항 사양서(Systems Requirements Documents)
- ✓ 시스템 아키텍처 문서(Systems Architecture Documents)
- ✓ 시스템 개발 프로세스 정의서(Systems Developments Process Definition Documents)

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료 시 까지 분석을 진행한다.

(4) 필요한 필수 식별 정보(항목)를 모두 확인 후 프로세스 종료를 진행한다.

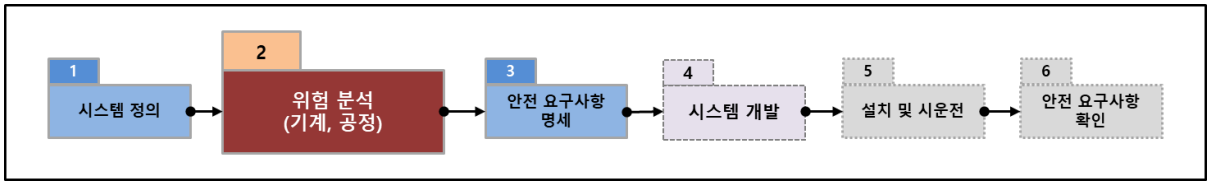
식별 항목

(1) 시스템 아키텍처 : 시스템/형상품목.

(2) 시스템 사양서.

(3) 프로그램 고유 규격서(program-unique specifications)

(4) 베이스라인(Baseline)



3.2. 위험 분석

목적

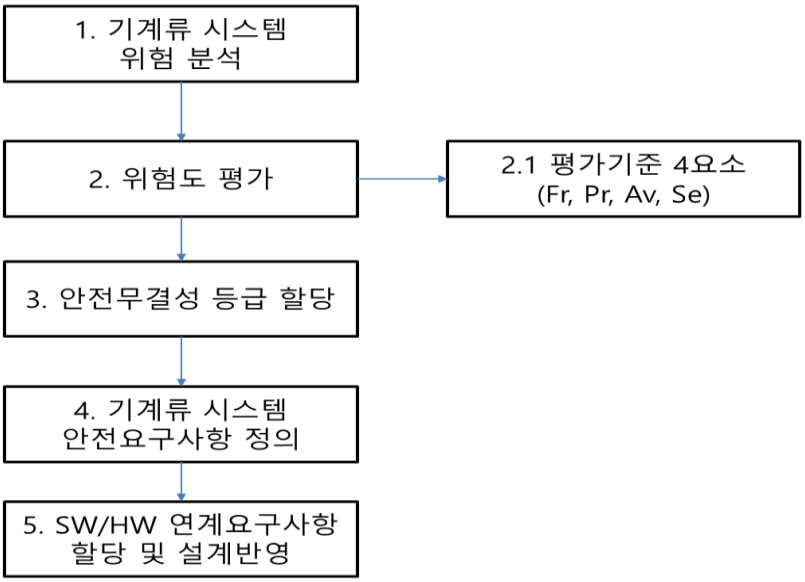
시스템 위험 분석(System Risk Analysis) 단계는 안전 요구사항을 도출하기 위한 활동이다. 안전 요구사항을 도출하기 위해서는 시스템을 구성하는 구성요소로부터 안전분석 활동이 수행되어야 한다. 명세를 위한 통해 식별된 시스템의 안전 요구사항 중 응용 소프트웨어에 할당 된 요구사항을 구현하기 위해 응용 소프트웨어에 대한 안전 요구사항을 식별하고 명세하는 단계로『시스템 분석』단계에서 작성된 산출물을 기반으로 세부 단계 활동을 수행한다.

비고: 대상 안전 시스템에 대한 "위험 분석"과 "안전 요구사항 명세" 단계는 기계류 제어 분야와 공정 제어 분야가 상이하기 때문에 각각 별도 항목으로 활동단계와 세부 절차를 다룬다.

(기계류 제어 분야)활동단계 개요

기계류 제어 분야 IEC 62061 의 위험 분석 세부수행 활동에는 위험원 식별, 위험도평가 및 안전요구사항 도출 절차로 구성된다. 식별된 개별 위험원을 바탕으로 개별 요소가 지닌 잠재적 위험도를 평가하여 안전 무결도 레벨(SIL: Safety Integrity Level)을 산정하여 설계적 저감방안을 갖추기 위한 안전요구사항(SRCF)을 도출하여 설계적 결함을 방지하는 접근 방법의 순환으로 수행되어진다.

구 분	설 명
선행기준	1. 시스템 아키텍처 설계 완료 2. 시스템 안전 기능 식별 완료 3. 시스템 사양서 정의 완료

입력문서	• 시스템 사양서 • 시스템 아키텍처 설계서 • 시스템 아키텍처 설계 제약사항 • 안전 시스템 사용자 매뉴얼 • 시스템 사양서 요구사항 추적표
수행흐름	
산 출 물	• 시스템 안전 요구사항 사양서 • 시스템 위험원 분석 보고서 • 시스템 위험도 평가 분석 보고서 • 시스템 연계 하부 요구사항 분석서
완료기준	1. 시스템 아키텍처 및 기능 기반 안전요구사항 정의 완료 2. 시스템 안전 요구사항 작성 완료 2. 시스템 기능 및 안전요구사항 추적표 작성 완료 3. 평가기준에 의한 안전기능의 위험도 평가결과 결과서 작성 완료

(기계류 제어 분야)세부수행 활동

본 가이드의 IEC 62061의 세부수행 활동에는 위험원 식별, 위험도평가 및 안전 요구사항 도출 절차로 구성된다. 식별된 개별 위험원을 바탕으로 개별 요소가 지

닌 잠재적 위험도를 평가하여 안전 무결도 레벨(SIL: Safety Integrity Level)을 산정하여 설계적 저감방안을 갖추기 위한 안전요구사항(SRCF)을 도출하여 설계적 결함을 방지하는 접근 방법의 순환으로 수행되어진다.

기계류 제어 분야 위험분석 단계

기계류 제어 분야 시스템 위험분석 단계는 앞서, 시스템 개념 및 범위정의 단계의 산출물로부터 입력정보로 받아, 제조 기계류 시스템 위험분석이 수행되어야 한다. 위험분석 단계를 통해, 제조 기계류의 운용 및 환경 조건으로부터 발생 가능한 위협요소에 대한 식별을 통해 위험원 분석 활동이 수행되어야 한다.

수행 절차

(1) 기계의 한계를 결정해야 한다. 여기에는 의도된 사용과 예측 가능한 모든 오류들이 포함되어야 한다.

(2) 위험원 및 관련 위험상황을 파악 및 식별해야 한다.

위험이 발생할 수 있는 상황(Situation)에 대한 정보는 설계적 정보를 바탕으로 식별되며

다음과 같이, 수행되어야 한다.

- ✓ 운용개념 기반의 운용상황(Situation or Event)에 대한 케이스(Case)를 정의하여야 한다.
- ✓ 정의된 케이스 상황 별, 수행되어야 하는 의도된 기능(Function)에 대한 정의가 되어야 한다.
- ✓ 발생할 수 있는 상황(Situation) 및 기능기반 발생할 수 있는 위해 상황에 대한 분석/정의가 되어야 한다.

(3) 위험상황(조건)에 발생 가능한 위험원은 파악/식별되어야 추적 정보를 확보한다.

발생 가능한 위험상황(or 조건)과 의도된 기능(Function)에 대한 조합을 통해 발생할 수 있는 위험요인에 대한 가능조합을 도출하여 위험원에 대해 식별 및 정의 되어야 한다.

(4) 식별된 위험원에 대한 발생 가능한 결과에 대한 평가를 통해, 제조 기계류에 미치는 영향에 대한 위험감소 여부를 결정한다.

- **식별된 위험원에 대한 평가는 [2] 위험도 평가 단계의 수행을 통해, 평가 매개변수 4가지(Fr, Pr, Av, Se)에 대한 결과에 대해 위험도 평가 결과를 통해, 위험감소 여부가 결정되어야 한다.**

(5) 위험감소 여부에 대한 감소결정이 정해지면, 해당 위험원에 보호조치를 반영하여 위험성을 낮춘다.

(6) 기계의 한계를 결정해야 한다. 여기에는 의도된 사용과 예측 가능한 모든 오류들이 포함되어야 한다.

위험분석 시 고려사항

(1) 안전기능(SRCF)은 의도된 기능의 실패로 인해 발생 가능한 위험이 즉각적으로 증가할 수 있는 기계의 기능으로 원치 않은 이벤트에 대한 충분한 검토를 통해 식별되어야 한다.

(2) 안전기능은 기능의 실패가 발생하여도 기계는 정상적 작동이 될 수 있지만, 작동으로 인한 부상에 대한 위험도는 증가한다.

(3) 위험원 분석 및 위험제거 또는 최소화 방법을 수행하여 위험을 제거하거나 허용 수준까지 줄이기 위해 어떤 안전기능(SRCF)와 성능이 필요한지에 대해 정의 되어야 한다

기계류 제어 분야 위험도 평가 단계

IEC 62061은 식별된 위험원을 바탕으로 발생 가능한 위험도를 산정한다. 따라서, SIL 측면에서 위험을 감소시킬 수 있도록 감소시킬 위험의 양과 제어 시스템이 성능을 설명한다. 이때, 특히, 4가지의 위험 매개변수(Fr, Pr, Av, Se)로 부터, 위험요소의 심각도 경중을 나타내는 위험도 평가 산정을 수행하게 된다. 특히, IEC 62061은 제조 기계류의 SRCF에 대한 위험도 평가를 통해 SIL 할당을 수행하기 위해 정성적 평가를 수행하게 된다. SRECS에 의해 구현될 SRCF에 의해 감소되어야 하는 각 위험에 대해 수행하며, 위험 산정은 반복적인 과정이므로 이 과정을 두 번 이상 수행해야 한다. SRCF를 구현하기 위한 특정 보호 수단을 제공하는 것이 위험 매개 변수에 영향을 미칠 수 있기 때문에 동일한 방법으로 개정된 위험 매개 변수를 사용하여 위험 산정 절차를 반복해야 하며, SIL은 SRCF에 대한 SIL 요구 사항을 산정한다.

평가 요소

(1) 위험도 평가 산정 요소.

A. 위험원에 노출 빈도와 기간 (Fr: frequency and duration)
B. - 위험한 사건의 발생 확률 (Pr: probability of hazardous event)
C. - 위해를 피하거나 제한할 수 있는 가능성 (Av: avoidance)
D. - 위해의 심각성(Se: Severity of harm)

평가 기준

위험도 평가 변수 (즉, Fr, Pr, Av Se)는 서로 독립적으로 추정되어야 한다. SRCF에 필요한 것보다 낮은 SIL을 잘못 할당하지 않도록 각 매개 변수에 최악의 가정을 사용해야 한다. 일반적으로 해를 입을 확률에 대한 적절한 고려가 이루어 지도록 작업 기반 분석을 사용하는 것이 강력하게 권장된다. 별된 위험원에 대해 위험 산정 요소변수에 대해서 개별적으로 기준이 존재한다. 개별 항목에 대한 요소와 기준은 다음과 같다.

Probability of occurrence of harm					
Frequency of exposure (Fr)		**Probability of occurrence (Pr)**		**Probabilities of avoiding or limiting harm (Av)**	
≥ 1 per h	5	Very high	5		
< 1 per h to ≥ 1 per day	5	Likely	4		
< 1 per day to ≥ 1 per 2 weeks	4	Possible	3	Impossible	5
< 1 per 2 weeks to ≥ 1 per year	3	Rarely	2	Rarely	3
< 1 per year	2	Negligible	1	Probable	1
SIL Class (Cl) = Fr + Pr + Av					

그림 16 평가요소별 기준표

(1) 노출 빈도 및 기간 (Fr)

노출 수준을 결정하기 위해 다음 측면을 고려해야 한다.

A. 모든 작동 모드 (예: 정상 작동, 유지 보수)에 따라 위험 지대에 대한 접근이 필요
B. 접근의 성격, 예를 들면 재료의 수동 공급, 설정
C. 노출과 평균 접근 빈도 간의 평균 간격을 예측할 수 있어야 한다.
D. 또한 10분 이상 지속될 경우 지속 시간을 예측할 수 있어야 한다. 지속 시간이 10분보다 짧은 경우, 값은 하향될 수 있다. 이는 h당 1회 이상의 노출 빈도에는 적용되지 않으며 절대로 값을 줄여서는 안된다.

(2) 위험 사건 발생 확률(Pr)

위해 발생 확률은 다른 관련 매개 변수 Fr 및 Av와는 독립적으로 산정되어야 한다. SRCF에 필요한 것보다 낮은 SIL을 잘못 할당하지 않도록 각 매개 변수에 최악의 가정을 사용해야 한다. 이러한 일이 발생하지 않도록 하려면 작업 기반 분석 양식을 사용하여 위해 발생 확률을 산정하는 데 적절한 고려가 이루어 지도록 해야 한다. 위험 사건 발생 확률은 다음을 고려하여 산정할 수 있다.

A. 다양한 사용 모드에서 위험 요소와 관련된 기계 부품의 동작 예측 (예: 정상 작동, 유지 보수, 고장 발견)
B. 특히 예기치 않은 시동 위험과 관련하여 제어 시스템을 신중하게 고려해야 한다. SRECS의 보호 효과를 고려하지 않는다. 이는 SRECS가 실패할 경우 노출될 위험의 양을 추정하기 위해 필요하다. 일반적으로 처리되는 기계 또는 재료가 예상치 못한 방식으로 작동하는 경향이 있는지 고려해야 한다.
C. 기계 동작은 예측이 매우 쉽거나 어려울 수도 있지만 예기치 못한 이벤트를 무시해서는 안된다. 예측 가능성은 종종 기계 기능의 복잡성과 관련이 있다.
D. 위험원과 관련된 기계 부품과의 상호 작용에 관한 인간 행동의 특정 또는 예측 가능한 특성
E. 스트레스 (예: 시간 제약, 작업 과제, 지각된 손상 제한)
F. 위험원과 관련된 정보에 대한 인식 부족
G. 위험한 사건의 "매우 높은"확률은 정상적인 생산 제약과 최악의 고려 사항을 반영하여 선택되어야 한다. 낮은 값을 사용하려면 긍정적인 이유 (예: 잘 정의된 애플리케이션 및 높은 수준의 사용자 역량에 대한 지식)가 필요하다. 필수 또는 숙련된 기술, 지식 등은 사용을 위한 정보에 명시되어야 한다.

(3) 위해 회피 또는 제한 확률(Av)

위험을 회피하거나 제한하는데 도움이 될 수 있는 기계 설계 및 의도된 응용 측면을 고려하여 산정할 수 있다.

이러한 측면에는 예를 들어

A. 위험 사건의 갑작스럽거나 빠르거나 느린 출현 속도
B. 위험에서 대피할 수 있는 공간적 가능성
C. 구성 요소 또는 시스템의 특성
D. 위험원에 대한 인식 가능성

(4) 위해 확률 등급(Cl)

각 위험원에 대해 적용 가능한 경우 각 심각도 수준에 대해 Fr, Pr 및 Av 열의 점을 합산하여 Cl값을 계산한다.

(5) 심각도(Se)

각 위험원에 대해 적용 가능한 경우 각 심각도 수준에 대해 Fr, Pr 및 Av 열의 점을 합산하여Cl값을 계산한다. 가역적 상해, 돌이킬 수 없는 상해 및 사망을 고려하여 상해 또는 건강 손상의 정도를 추정할 수 있다. 부상으로 인한 결과에 따라 적절한 심각성 값을 선택한다.

표 31. 심각도 기준 표

정도	피해 내용
4	치명적이거나 중대한 돌이킬 수 없는 상처를 의미하므로 치유 후 동일한 작업을 계속하는 것은 매우 어려움
3	치유 후 동일한 작업을 계속할 수 있는 방식으로 중대하거나 돌이킬 수 없는 손상을 의미. 부러진 팔다리 같은 가혹한 주요하지만 뒤집을 수 있는 부상도 포함될 수 있음
2	심한 열상, 찌르는 듯한 수술, 의료 종사자의주의가 필요한 심각한 타박상을 포함한 뒤집을 수 있는 부상을 의미
1	응급 처치가 필요한 찰과상 및 경미한 타박상을 포함하는 가벼운 부상을 의미

평가절차

SRECS는 안전 무결성은 일반적으로 리스크 매트릭스를 사용하여 필요한 SIL을 결정하기 위한 평가가 수행된다.

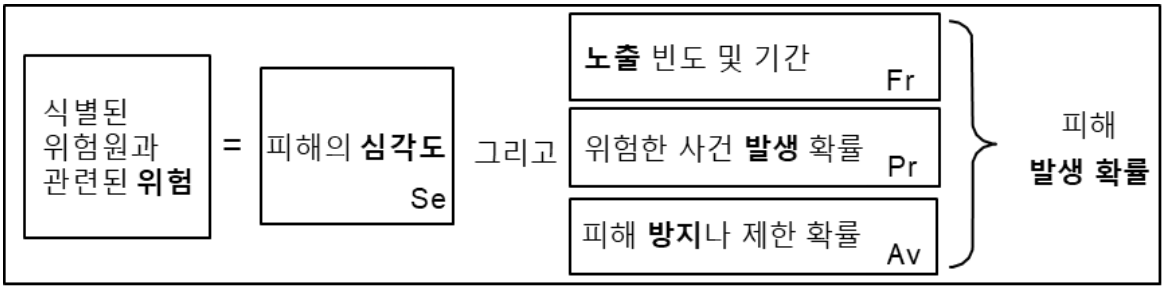


그림 17. 위험 산정 평가

위 그림(위험 산정 평가)과 같이, 위험산정 평가는 특정 위험상황에서 식별된 연계 위험원에 대해 위험평가 산정요소에 대해 평가된다. 평가를 통해, 위험분석 및 위험감소 전력단계의 위험평가에서 SRCF이 필요한 경우, 각 안전 기능에 대한 안전 요구사항 평가와 제안된 시스템이 요구사항을 충족하는지에 대한 평가가 수행된다.

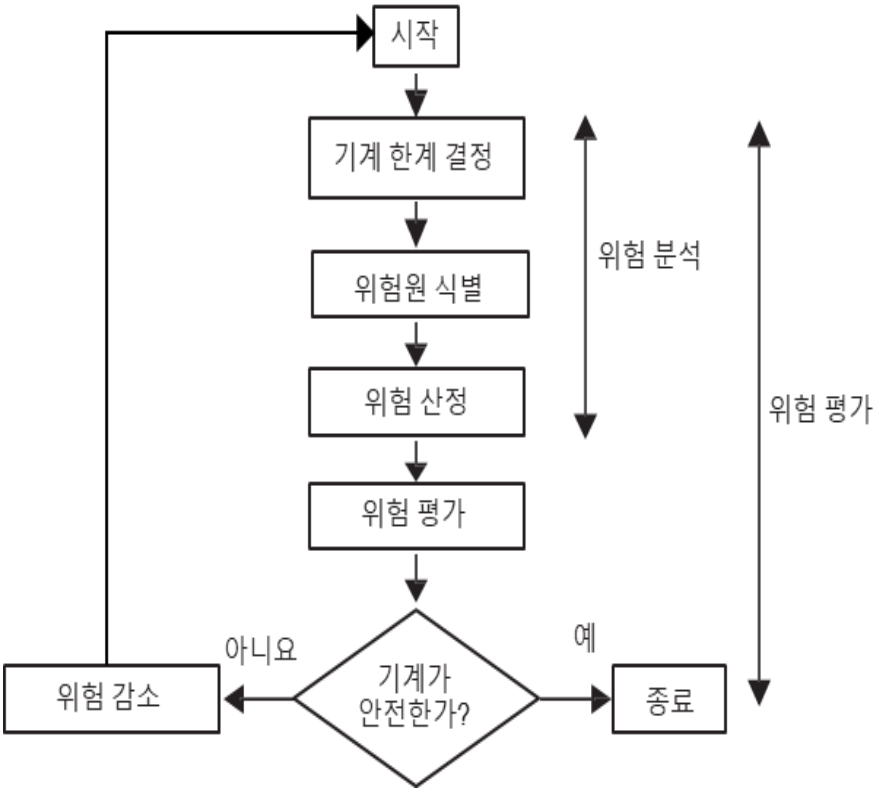


그림 3. 기계류 제어 분야 설계 중 위험 평가 접근법

SRECS 의 SRCF에 대한 위험 산정 및 SIL 할당을 위하여 정성적 위험 평가를 사용한다. SRECS에 의해 구현될 SRCF에 의해 감소되어야 하는 각 위험에 대해

수행하며, 위험 산정은 반복적인 과정이므로 이 과정을 두 번 이상 수행해야 한다.

SRCF를 구현하기 위한 특정 보호 수단을 제공하는 것이 위험 매개 변수에 영향을 미칠 수 있기 때문에 동일한 방법으로 개정된 위험 매개 변수를 사용하여 위험 산정 절차를 반복해야 하며, SIL은 SRCF에 대한 SIL 요구 사항을 산정한다.

기계류 제어 분야 위험평가 시 고려사항

(1) 기계류에 대한 고유 위험요소가 있는 경우, 각각의 특정 위험 요소에 대하여 위험평가를 수행하여 위험감소 프로세스가 필요한 것으로 결정된 모든 안전기능(SRCF)의 식별을 포함하여 기계에 대한 위험평가를 수행하여야 한다.

(2) 기계의 위험평가는 보호수단이 없다고 가정하에 기계 작동에 대한 위험평가를 수행하여 이 평가결과로 무시할 수 없는 것으로 간주되는 위험원이 있는 경우, 적절한 보호 수단(저감대책)을 수립하여 위험 감소 프로세스에 할당하여 위험요소가 기계에 미치는 영향이 무시될 때까지 위험평가에 대해 반복적 수행되어야 한다.

(3) 기계의 모든 수명주기 단계(제조, 설치, 시운전, 조립, 조정)과 관련된 위험요소의 분석 및 정의되어야 한다.

(4) 기계의 의도된 사용 모드와 오동작 발생 가능한 상황에 대해 정의되어야 한다.

(5) 기계 주변의 공간제한 및 이동 범위의 적합성이 반영되어 평가 시 고려되어야 한다.

(6) 기계 사용자에 대한 예측 가능한 훈련, 능력 및 경험수준도 위험발생 및 평가에 반영되어야 한다.

(7) 보호장치, 절차 및 간판과 같은 기존의 위험 감소 조치는 위험 요소를 식별할 때 고려하지 않으며 다양한 보호수단의 상대적 장점을 고려할 때, 특정 평가에 대해서는 가중치를 고려하여 부여하여야 한다.

기계류 제어 분야 SIL 할당 단계

IEC 62061 기반의 기계류 제어 분야 안전성평가는 위험산정 변수에 대한 평가의 결과를 조합하여 SIL 등급을 평가 산정한다. 이러한 결과를 바탕으로 해당 SIL을 충족시키기 위한 안전설계가 반영되어야 한다. 위험의 강도, 위험에의 접근 빈도, 회피 가능성을 근거로 위험성 평가를 하고 그 결과에 따라 요구되는 SIL레벨을 구한다. 따라서, 위험성 평가 결과 위험수준이 수용 가능한 범위를 넘어서면 위험성 저감 대책이 필요하게 된다.

평가 절차

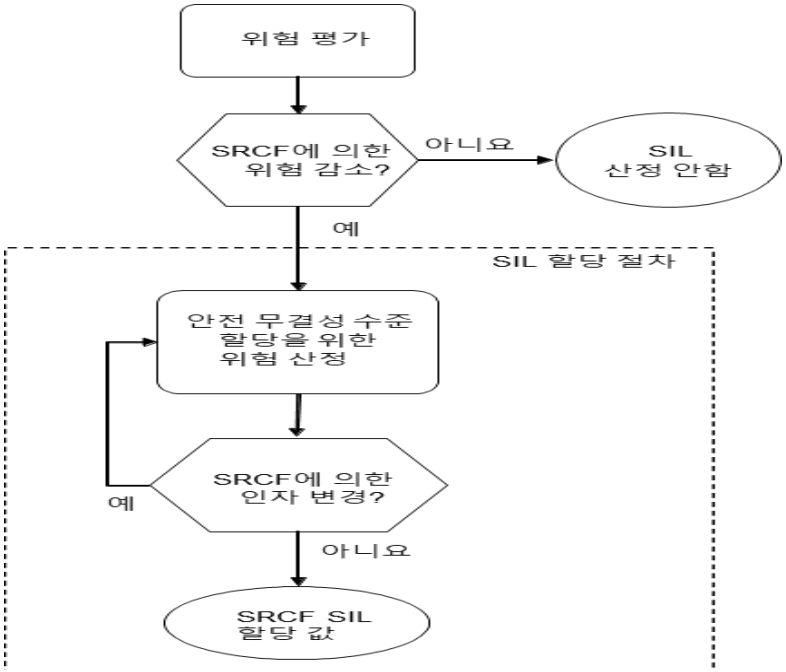
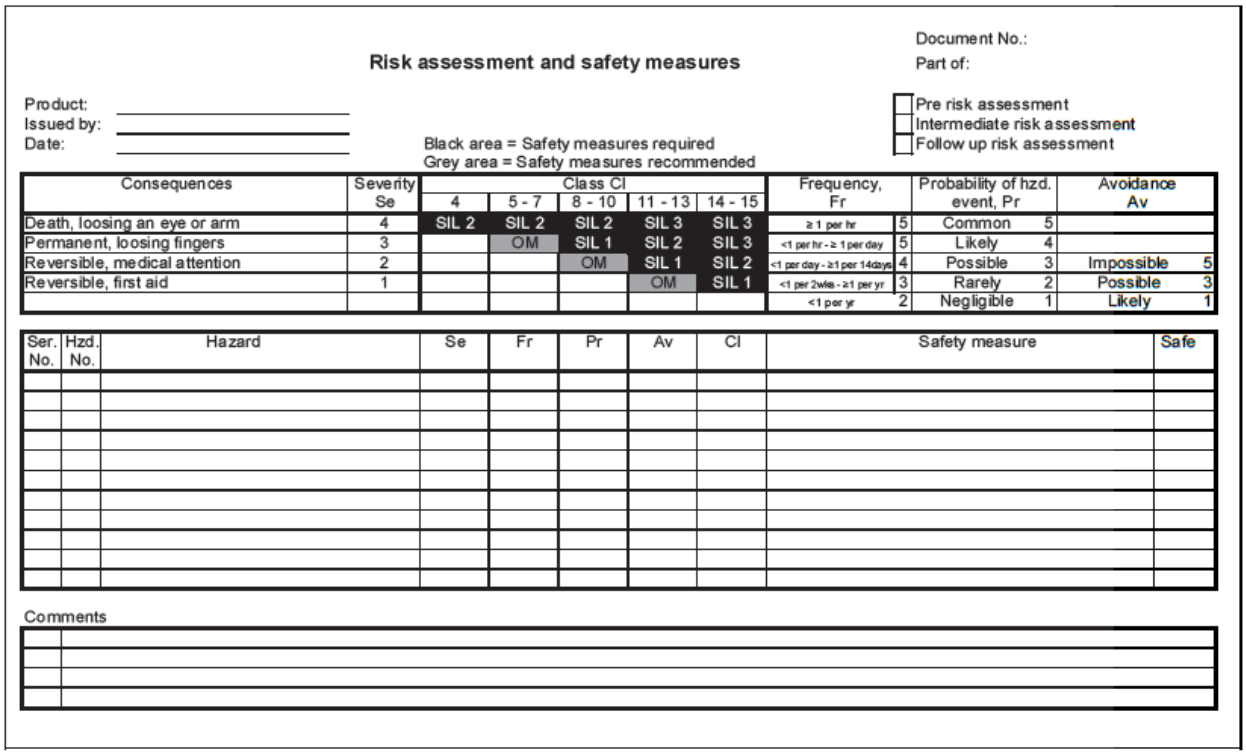


그림 18. 기계류 제어 분야 SIL 할당 절차

SRCF에 대한 위험 산정 및 SIL 할당을 위하여 정성적 위험 평가를 사용한다. SRECS에 의해 구현될 SRCF에 의해 감소되어야 하는 각 위험에 대해 수행하며, 위험 산정은 반복적인 과정이므로 이 과정을 두 번 이상 수행해야 한다.

그림 5에서 SRCF를 구현하기 위한 특정 보호 수단을 제공하는 것이 위험 매개변수에 영향을 미칠 수 있기 때문에 동일한 방법으로 개정된 위험 매개 변수를 사용하여 위험 산정 절차를 반복해야 하며, SIL은 SRCF에 대한 SIL 요구 사항을 산정한다.



Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 4	5 - 7	8 - 10	11 - 13	14 - 15
Death, loosing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, loosing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

Frequency, Fr		Probability of hzd. event, Pr		Avoidance Av	
≥ 1 per hr	5	Common	5		
<1 per hr - ≥ 1 per day	5	Likely	4		
<1 per day - ≥1 per 14days	4	Possible	3	Impossible	5
<1 per 2wks - ≥1 per yr	3	Rarely	2	Possible	3
<1 per yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

그림 19. SIL Assignment Process Example

위의 그림(SIL Assignment Process Example)은 앞서, 평가한 매개변수 4가지 요소에 대한 종합적 평가를 수행하여, 최종적으로 위험도 평가에 따른 SIL 등급을 판정 및 할당할 수 있는 테이블을 나타낸다. 개별 위험원으로부터 평가요소 4가지를 바탕으로 최종적 SIL 등급을 판정하게 된다.

(1) 개별 위험원에 대해 매개변수 요소에 대한 평가가 수행되어야 한다.

(2) 각 위험원에 대해 적용 가능한 경우 각 심각도 수준에 대해 Fr, Pr 및 Av

열의 점을 합산하여 CI값을 계산한다.

(3) 합산된 CI값과 심각도(Se)의 기준에 따라, 최종 SIL 등급을 판정하여야 한다.

SIL은 위 SIL Assignment Process Example을 활용하여 결정된다. SIL 등급 판정을 위한 (CI) 계산 공식은 다음과 같다.

$$CI = Fr + Pr + Av.$$

CI값의 계산 후, 최종적으로 심각도(Se)의 기준에 따라, SIL 할당이 최종적으로 수행되어진다.

SIL 할당에 대한 Matrix는 다음과 같다.

심각도(Se)	등급(CI) 3 - 4	등급(CI) 5 - 7	등급(CI) 8 - 10	등급(CI) 11 - 13	등급(CI) 14 - 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)*	SIL 1	SIL 2	SIL 3
2			(OM)*	SIL 1	SIL 2
1				(OM)*	SIL 1

다음은 SIL 평가 요소에 대한 평가를 통한 SIL 할당에 대한 예제 설명이다.

EXAMPLE: Se 가 3, Fr 이 4, Pr 이 5, Av 가 5 인 특정 위험에 대해서는
Cl = Fr + Pr + Av = 4 + 5 + 5 = 14
위의 표를 사용하면, SIL 3 이 SRCF 에 할당되어 특정 위험을 완화해야 한다.

개별 SRCF에 대한 안전 무결성 등급에 대한 요구조건은 다음과 같다. 이러한 요구조건이 제시되는 이유는 작동모두(High Demand Mode 또는 Low Demand Mode) 여부에 따라서, SIL 판정 기준이 달라지게 된다.

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

그림 20. Safety integrity levels: target failure values for SRCFs

요구모드에 대한 설명은 다음과 같다. 요구모드는 PFD와 PFH로 나뉘며 산업별 특성을 반영한다. IEC 62061를 통해 다루는 제조 기계류는 통상 PHD(높은 요구모드)에 해당되며, IEC 61511를 통해 다루어 지는 제조 공정 관련해서는 PFD(저 수요모드) 속한다.

- PFD(Probability of Failure on demand)
안전기능 요청 시 고장가능성, 적은 요구모드(Low Demand Mode)에서 적용

- PFH(Probability of Failure per Hour) 시간당 고장 가능성, 높은 요구 모드(High Demand Mode)에서 적용

따라서, 제조 기계류의 요구모드는 높은 요구 모드(High Demand Mode)가 적용되어 SIL 등급 판정에 따른 결과를 얻는다.

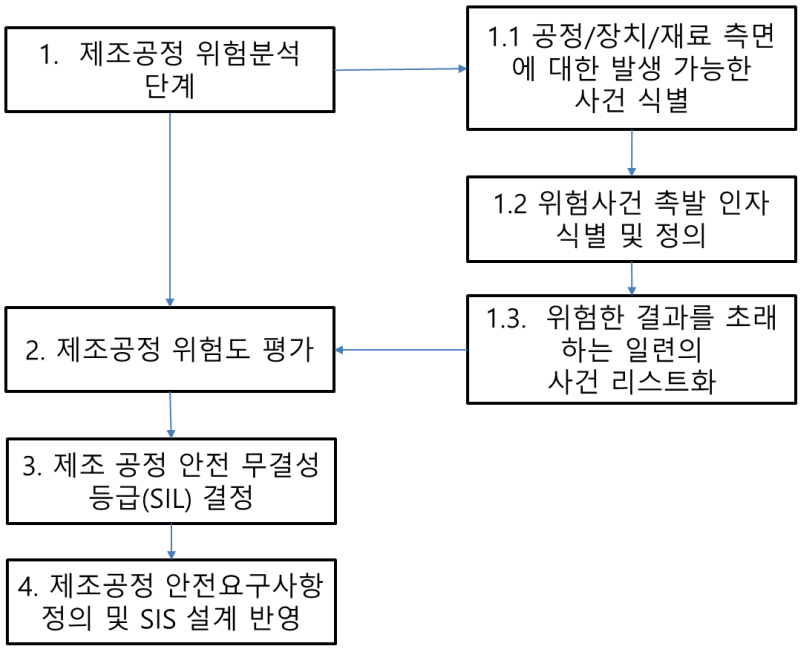
※ Mode of Operation : 작동 Mode에 따라 SIL이 틀려짐

Low Demand Mode : 작동 요구 빈도가 1년에 1회 이하 또는 작동 증명시험의 2배를 넘지 않은 경우
High Demand Mode : 작동 요구빈도가 1년에 1회 이상 또는 작동 증명시험의 2배 이상인 경우
(단, SRCF의 요구되는 안전 무결성이 SIL 1보다 작은 경우 최소한 ISO 13849-1의 범주 B 요구 사항을 충족시켜야 한다.)

(공정 제어 분야)활동단계 개요

공정 제어 분야(IEC 61511) 표준의 공정 안전성활동은 다음과 같다. 공정 및 장치 재료로 부터 발생 가능한 위험원 인자로부터 SIF 를 식별하여, 최종적으로 SIS 에 설계적 반영을 통해, 제조공정 과정에서 안전성 확보에 목적을 둔다.

구 분	설 명
선행기준	1. 제조공정 운영시나리오 정의 2. 공정 프로세스 정의 3. 시스템 아키텍처 설계 완료 4. 시스템 안전 기능 식별 완료 5. 시스템 사양서 정의 완료
입력문서	• 운용개념서(CONOPS) • 공정 프로세스 정의서 • 시스템 사양서 • 시스템 아키텍처 설계서 • 시스템 아키텍처 설계 제약사항 • 안전 시스템 사용자 매뉴얼 • 시스템 사양서 요구사항 추적표

수행흐름	
산 출 물	• 제조공정 발생가능 사건 정의서 • 제조공정 위험인자 정의서 • 제조공정 위험도 평가 분석 보고서 • 제조공정 SIS 설계 사양서
완료기준	1. 시스템 아키텍처 및 기능 기반 안전요구사항 정의 완료 2. 시스템 안전 요구사항 작성 완료 2. 시스템 기능 및 안전요구사항 추적표 작성 완료 3. 평가기준에 의한 안전기능의 위험도 평가결과 결과서 작성 완료

3.2.5. (공정 분야) 세부수행 활동

제조공정 분야의 안전표준인 IEC 6511은 SIS에 대한 정의, 실행 및 관리에 관한 전 수명주기 관점에서 접근하는 안전활동 개념을 지니고 있다. SIS의 안전 수명주기 관점에서 H&RA(Hazard and Risk assessment) 활동을 통한 위험원과 리스크에 대한 평가를 수행함으로써, 평가 결과를 바탕으로 보호층으로의 안전 기능(SIF) 할당 및 SIS의 안전요구사항 정의, 설계 순으로 진행된다.

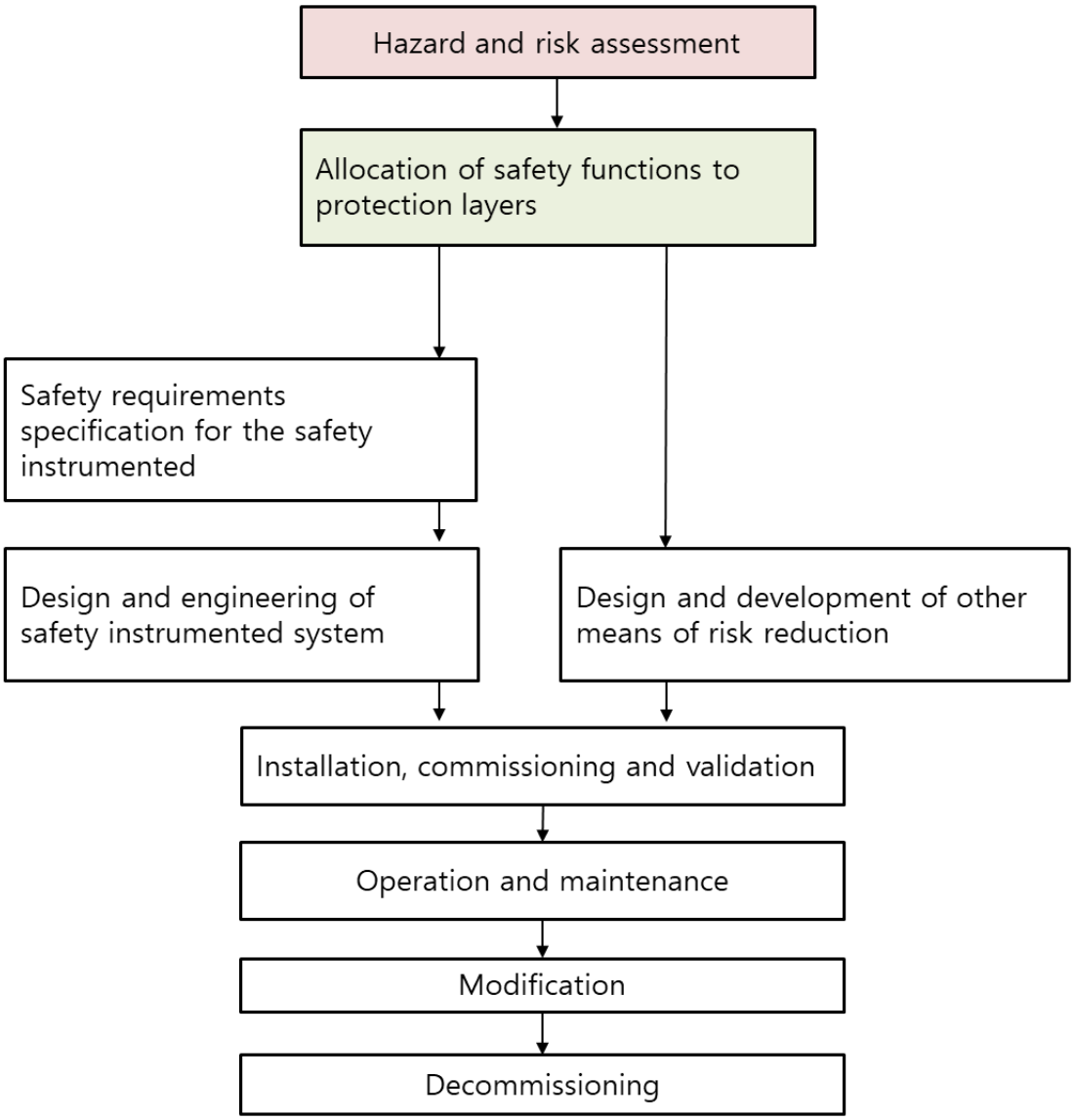


그림 21. 공정 분야 SIS safety life-cycle phases

공정 제어 분야 위험분석 단계

제조공정 안전 표준 IEC 61511에서는 제조기계류의 위험분석 단계는 H&RA(Hazard and Risk assessment)의 프로세스 이행을 통해서 위험분석 활동을 수반한 활동이 수행된다. 제조공정 위험분석을 수행하기 위해서는 아래와 같이 두 가지(프로세스 및 재료,공정, 장비)에 대한 수행활동이 진행되어야 한다.

수행절차

(1) H&RA 프로세스 수행 시 측면

A. 공정 및 관련 장비의 위험 및 발생 가능한 위험 이벤트를 식별한다.

B. 위험 이벤트를 유발 시킬 수 있는 일련의 사건을 식별하여 리스트화 한다.

C. 위험 이벤트와 관련된 프로세스적 위험요인을 정의한다.

D. 위험 감소를 위한 요구사항을 명세한다.

E. 필요한 위험 감소를 달성하기 위해 필요한 SIF를 정의한다.

F. SIF를 검토하여 최종 식별한다.

(2) H&RA의 재료, 공정, 장비에 대한 측면

A. 식별된 개별 위험 사건 및 그것에 기여하는 요인에 대한 식별이 되어야 한다.

B. 개별적 위험한 사건의 가능성 및 결과에 대한 정의 되어야 한다.

C. 정상작동, 시동, 정지, 유지보수, 공정 불균형 및 비상 정지와 같은 공정 작동 모드 고려 필요한 기능적 안전성을 달성하기 위해 필요한 추가적인 위험 감소 결정하여야 한다.

D. SIF 로 적용되는 안전 기능 여부에 대한 식별 및 정의되어야 한다.

E. H&RA 는 항목간 관계가 명확하고 추적 가능하도록 기록되어야 한다.

F. 보안 위험평가를 수행하여 SIS 의 보안 취약성을 식별활동을 수행하여야 한다

공정 제어 분야 위험도 평가 단계

제조공정과 관련한 위험도 평가 단계 역시, H&RA 단계의 수행을 통해 얻어진 입력 산출물로부터 수행되어진다. 따라서, H&RA 단계의 수행을 통한 위험도 평가를 통해 SIF 기능을 판단/결정하고 안전기능(SIF)을 보호계층으로 할당된다. 이는 특정 보호층으로 필요한 위험저감을 달성하기 위한 안전 기능이 할당되기 때문이다. 또한, 개별 SIF에 대한 위험 저감 또는 평균 위험빈도의 할당이 수행된다. 요구되는 SIL은 SIF가 제공한PFD 또는 PFH를 고려하여 유도되기 때문에 아래 위험도 평가기준에 대한 정보 식별이 선행되고 위험도 평가가 수행되어야 한다.

평가 기준

위험도 평가를 위해 위험도 허용기준(Risk Acceptance Criteria)을 먼저 결정해야 한다. 요구모드에 따라, 동작하는 개별 SIF에 대해 요구되는 SIL은 선정되어야 한다. 제조 공정상에 발생할 수 있는 위험도 평가를 위해서 위험도 평가 기준(Risk Acceptance criteria)을 먼저 결정해야 한다

표 32. . Safety Integrity Requirements: PFD avg.

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	PFDavg	Required risk reduction
4	≥ 10−5 to < 10−4	> 10 000 to ≤ 100 000
3	≥ 10−4 to < 10−3	> 1 000 to ≤ 10 000
2	≥ 10−3 to < 10−2	> 100 to ≤ 1 000
1	≥ 10−2 to < 10−1	> 10 to ≤ 100

표 33. Safety Integrity Requirements : Average frequency of dangerous failures of the SIF

CONTINUOUS MODE OR DEMAND MODE OF OPERATION	
Safety integrity level (SIL)	Average frequency of dangerous failures (failures per hour)
4	≥ 10−9 to < 10−8
3	≥ 10−8 to < 10−7
2	≥ 10−7 to < 10−6

1	≥ 10−6 to < 10−5

평가절차

제조 공정분야 위험산정 평가 절차는 다음과 같이, 크게 4단계로 구성이 된다. 첫번째, 위험성 평가 실시 계획 수립 단계, 두번째, 참고자료 수집 및 준비단계, 세번째, 공정 위험성 평가 수행 단계, 마지막, 네번째 단계로, 개선 권고사항에 대한 후속 조치 단계이다.

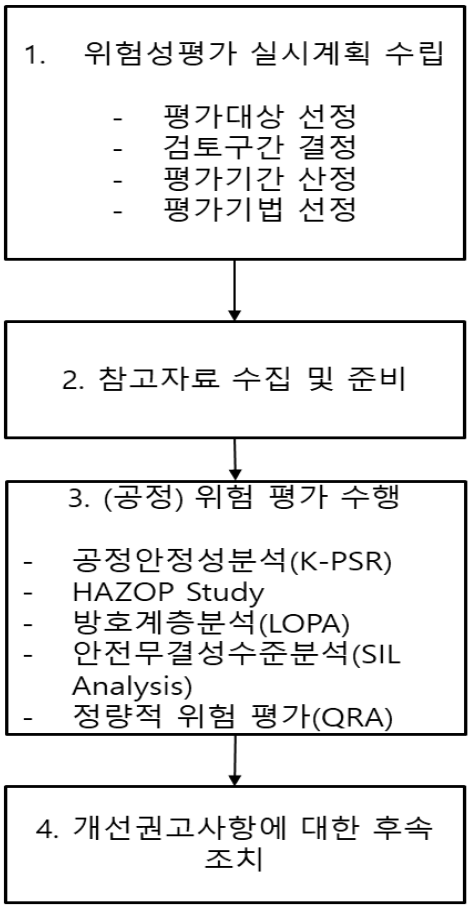


그림 22. 제조공정 위험평가 절차

위 그림(위험 산정 평가)과 같이, 위험산정 평가는 특정 위험상황에서 식별된 연계 위험원에 대해 위험평가 산정요소에 대해 평가된다. 평가를 통해, 위험분석 및 위험감소 전력단계의 위험평가에서 안전기능(SIF)이 필요한 경우, 각 안전 기

능에 대한 안전 요구사항 평가와 제안된 시스템이 요구사항을 충족하는지에 대한 평가가 수행된다..

제조 공정 프로세스 안전성 평가 기법

제조공정 프로세스의 안전성 평가 기법에는 그림 8과 같이, 다양한 기법들이 존재하며, 본 가이드를 통해서는 대표 기법인 HAZOP기법과 LOPA기법에 의한 공정 프로세스의 안전성 평가에 대해서 다룬다.

(1) HAZOP 기법

정성적 위험도 평가 방법이며, 효율성 때문에 산업계에서 널리 사용된 다. 운전과 위험분석(HAZOP) 결과는 참여한 엔지니어들의 실력에 영향을 받기 때문에 설계, 시운전, 유지보수, 위험도 등 다양한 경험을 가진 엔지니어들이 수행한다. 모든 위험요소를 식별하기 위해서는 유지보수 (Maintenance), 퍼지(Purge), 정비(Shutdown), 시동(Start-up) 등 모든 운용모드를 다룬다.

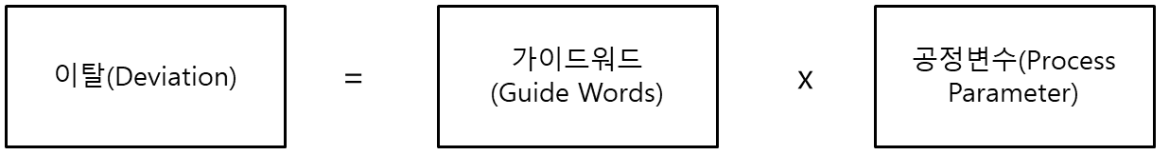


그림 23. 이탈(Deviation)의 구성

이탈(Deviation)의 구성은 가이드 워드(Guideword)와 공정변수 (Process Parameter)가 조합되어 [그림 29]과 같이 표현된다

공정변수(Process Parameter)는 설계의도에 의해 발생되며, 그 특성은 표 4과 같이, 크게 두 가지로 분류된다.

표 34. 공정 변수(Process Parameter)

특정 변수	일반 변수
유량(Flow)	첨가(Addition)
온도(Temperature)	반응(Reaction)

압력(Pressure)	유지관리(Maintenance)
액위(Level)	시험(Testing)
조성(Composition)	계장설비(Instrumentation)
상(Phase)	시료채취(Sampling)
점도(Viscosity)	완화(Relief)

가이드 워드 구성은 다음의 표와 같다.

표 35 제조공정 핵심 가이드 워드(Guide) 사례

가이드 워드	정의	예
없음 (No, Not, or None)	설계의도에 완전히 반하여 공정변수(Process Parameter)의 양이 없는 상태	유량 없음(No flow)이라고 표현할 경우 : 검토구간(Node) 내에서 유량이 없거나 흐르지 않는 상태를 뜻함
증가(More)	공정변수(Process Parameter)가 양적으로 증가되는 상태	유량증가(More flow)라고 표현할 경우 : 검토구간(Node) 내에서 유량이 설계의도보다 많이 흐르는 상태를 뜻함
감소(Less)	공정변수(Process Parameter)가 양적으로 감소되는 상태	유량감소(Less flow)라고 표현할 경우 : 누설 등으로 설계의도보다 유량이 적어진 경우를 뜻함
반대(Reverse)	설계의도와 정반대로 나타나는 상태	유량이나 반응 등에 흔히 적용되며 반대흐름(Reverse flow)이라고 표현 할 경우 : 검토구간(Node) 내에서 유체가 정반대 방향으로 흐르는 상태
부가(As well as)	설계의도 외에 다른 공정변수(Process Parameter)가 부가되는 상태, 질적 증가	오염(Contamination) 등과 같이 설계의도 외에 부가로 이루어지는 상태를 뜻함.
부분(Parts of)	설계의도대로 완전히 이루어지지 않는 상태, 질적 감소	조성 비율이 잘못된 것과 같이 설계의도대로 되지 않는 상태
기타(Other than)	설계의도가 완전히 바뀜	밸브의 잘못 조작으로 다른 원료가 공급되는 상태 등

따라서, 표4과 표5의 결합 조합을 통해서, 발생 가능한 공정 이탈현상에 대해서 분석 할 수 있다. 다음은 공정 변수의 이탈에 따른 발생 유발 가능한 원인에 대한 사례이다.

표 36. 공정 변수 이탈에 따른 발생 가능한 원인 사례

변수	이탈(Deviation)	가능한 원인(Cause)
유량(Flow)	유량 없음 (No flow)	잘못된 흐름, 배관 막힘, 맹판 설치, 반대방향으로 설치된 체크밸브, 배관파열, 계기.기기 결함, 잠김, 배관동결 등
유량(Flow)	유량증가 (More flow)	증가된 펌핑 능력, 흡입측 압력증가, 토츨측 압력 감소, 열교환기 튜브누설, 오리피스 제거, 밸브의 정렬 잘못, 제어밸브의 고장, 제어시스템의 결함, 제어밸브의 트림재질 변경, 2 대 펌프가동 등
액위(Level)	액위증가 (More)	출구 흐름차단, 유입> 유출, 액위제어 실패, 액위지시계 고장 및 오지시
액위(Level)	액위감소 (Less)	입구 흐름 차단, 유출> 유입, 액위제어 실패, 액위 지시계 고장 및 오지시, 드레인 개방
온도(Temperature)	온도증가 (More)	태양복사열, 열교환기의 튜브 막힘 또는 파열, 화재, 냉각수 차단, 반응폭주, 열매누설, 제어시스템 고장 등
혼합 (Mixing)	혼합 없음/감소(N o/Less Mixing)	교반기 고장, 전력공급중단, 체류시간 감소, 물질의 점도 증가
반응(Reaction)	반응 없음/감소(N o/Less reaction)	반응물의 조성변화, 운전조건 변화, 반응 개시제 미투입, 체류시간, 촉매이상

(2) 방호계층분석(LOPA) 기법

위험원 분석(Hazard Analysis)을 통해 위험하다 판단된 안전계장기능(SIF, Safety Instrumented Function)에 대해 정량적 분석을 실시하여 Target SIL을 결정해야 한다. Target SIL은 방호계층분석기법, Risk Graph, Risk Matrix, ALARP 등을 통해서 결정되며, 방호계층분석기법(LOPA)는 현재 가장 대표적인 분석 방법이다. LOPA는 리스크분석 방법 중에 플랜트와 관련해 리스크를 가장 정밀하게 수치화 할 수 있는 방법이며, Target SIL에 대한 가장 경제적 산정할 수 있는 방법론이다. Result SIL은 하드웨어고장허용치(HFT, Hardware Fault Tolerance), 안전고장비율(SFF, Safety Failure Fraction), 평균작동요구시 위험고장확률(PFD-avg, Average Probability of Dangerous Failure on Demand)을 모두 계산해서 결정해야 한다. Result SIL은 Target SIL 보다 반드시 같거나 높은 결과가 나와야 안전성을 확보할 수 있다.

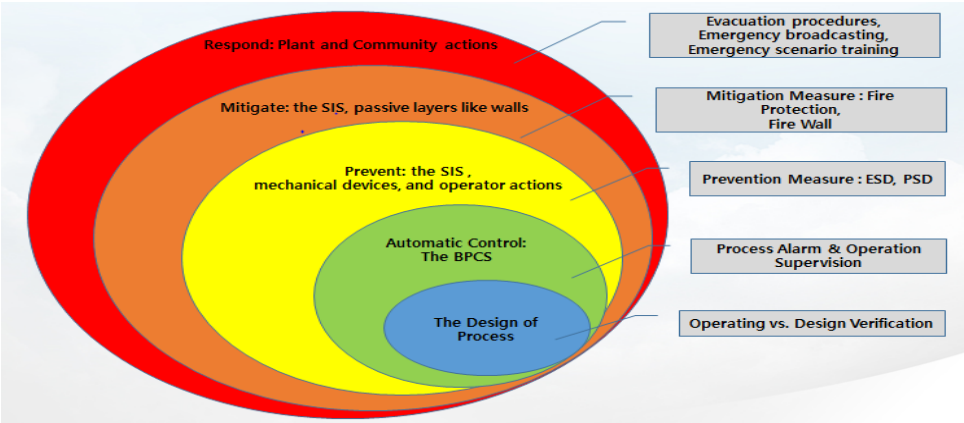


그림 24 방호계층분석 기법의 개념

LOPA 기법은 공정의 방호 계층에 대해서 양파모형의 방호 계층으로 구성되어 제어, 보호, 또는 경감에 의하여 리스크를 감소시키는 독립적인 메커니즘에 속한다.

Layers of Protection	Process	Vehicles
Basic Design	Proper specifications for the process	Proper specs for the usage (e.g., Sedan, SUV)
Process Control	BPCS (DCS, PLC's)	Accel. pedal, Transmission, Engine Control
Prevention	Alarms, Interlocks, SIF	Steering, ABS, AEB, LKAS
Mitigation	SIF, Fire walls, Fire suppression	Bumpers, Airbags, Crumple zones
Response	Evacuation, fire and emergency response, Communication	Cell phone, police, ambulance

그림 25 방호계층별 적용 예제

방호계층분석(LOPA)은 독립방호계층(IPL)이 모두 작동하지 않는 가장 심각한 사건에 대한 빈도만 구한다. 사건에 대한 발생빈도는 개시 사건 빈도(Initiating Event Frequency)와 독립방호계층(IPL)의 작동 요 구 시 고장확률(PFD)을 모두 곱해 구한다. 또한 위험도감소인자(Risk Reduction Factor, RRF) 적용해 안전 무결성 수준(SIL)을 낮춘다

#	1	2	3	4	5			6	7	8	9	10	11
					방호계층								
순서	영향 설명	강도 수준	초기 사고 원인	초기 사고 빈도	일반적인 공정 설계	기본 공정 제어 시스템	경보 등	추가적인 완화 대책, 접근 제한 등	독립 방호 계층, 추가적인 완화 대책, 다이크, 압력 방출	중간 단계의 사고 빈도	안전 계장 기능 무결 수준	완화된 사고 발생 빈도	비고
1	증류탑 파열로 인한 화재	심각	냉각수 손실	0.1	0.1	0.1	0.1	0.1	PRV 01	10^{-7}	10^{-2}	10^{-9}	고압으로 인한 증류탑 파손
2	증류탑 파열로 인한 화재	심각	스팀제어루프 고장	0.1	0.1		0.1	0.1	PRV 01	10^{-6}	10^{-2}	10^{-8}	위와 동일

그림 26 방호계층분석 결과 예시

그림 27의 LOPA의 예시에서 보이듯이, 강도수준에 따라 완화된 사고빈도가 결정되고 각 방호계층란에는 기준 테이블에 나타난 PFD를 입력하고 초기 사고빈도부터 모든 방호계층의 PFD를 곱하여 중간사고빈도를 계산한다. 그리고 최종적으로 완화된 사고 빈도를 중간사고빈도로 나눈 값이 안전계장기능(SIF) 무결성 수준을 결정하는 PFD로 결정되고 해당 PFD를 IEC 61508의 기준에 따라 SIL 등급이 환산되어야 한다. 방호계층분석(LOPA)는 인적안전(Personnel Safety), 환경, 재산에 대해 모두 실시하여야 하며, 3개의 Target SIL 중 가장 높은 SIL이 최종 Target SIL로 결정된다. Result SIL을 계산하는 방법에는 안전고장비율(SFF, Safety Failure Fraction)과 하드웨어고장허용치(HFT, Hardware Fault Tolerance)에 의한 방법 그리고 평균작동요구 시 위험고장확률(PFDavg, Average Probability of dangerous Failure on Demand)에 의한 방법을 모두 사용하여 두 가지 결과 중 더 낮은 결과를 Result SIL로 결정되어야 한다.

A. 시나리오를 선별하기 위해 사고의 결과(Consequence)를 확인한다.

- ✓ 방호계층분석(LOPA)은 이전에 실시한 위험성평가에서 개발된 시나리오를 이용하여 평가한다.
- ✓ 첫번째 단계는 시나리오를 선별(Screening)하는 것으로써 일반적으로 사고의 결과(Consequence)를 기반으로 한다.
- ✓ 사고의 결과(Consequence)는 보통 위험과 운전분석(HAZOP)과 같 은 정성적 위험성평가에서 확인한다.
- ✓ 다음으로 사고의 결과(Consequence)를 평가하고 그 크기(Magnitude)를 추정한다.
- ✓ 방호계층분석(LOPA) 대상으로는 위험과 운전분석(HAZOP)과 같은 정성적 위험성평가에서 확인한 시나리오 중 모든 안전조치(Safeguards)가 없거나 실패했다고 가정하여 추정한 위험도(Risk)가 7 이상인 시나리오와 7 미만이더라도 Interlock Logic 이 설치된 시나리오를 기반으로 해야 한다.

B. 사고 시나리오를 선택한다.

- ✓ 방호계층분석(LOPA)는 한번에 한 시나리오에만 적용되어야 한다.

- ✓ 그 시나리오는 하나의 원인과 결과 쌍(Single Cause-Consequence Pair)으로 기술하여야 한다.

C. 시나리오의 개시사건(Initiating Event)를 확인하고, 빈도를 정한다.

- ✓ 개시사건(Initiating Event)은 모든 안전조치(Safeguards)가 실패했다고 가정한 사고의 결과(Consequence)로 이어져야 한다.
- ✓ 빈도는 운전모드의 빈도 같은 시나리오의 배경적인 면을 설명할 수 있어야 한다. [작업 횟수당 실수 횟수 (Operator failure / Opportunity)]

D. 독립방호계층(IPL)을 확인하고, 작동요구 시 고장확률(PFD)을 정한다.

- ✓ 어떤 사고 시나리오는 단지 하나의 독립방호계층(IPL)을 필요로 하 는 경우도 있고, 다른 사고 시나리오는 Required PFD 를 얻기 위해 다 수의 독립방호계층(IPL)이나 작동요구 시 고장확률(PFD)이 매우 낮은 독립방호계층(IPL)을 필요로 한다.
- ✓ 주어진 사고 시나리오에 대해 독립방호계층(IPL)의 요구사항을 충족 시키는 기존의 안전조치(Safeguards)를 찾아내는 것이 방호계층분석 (LOPA)의 핵심이다.
- ✓ 사용할 독립방호계층(IPL)의 작동요구 시 고장확률(PFD)은 방호계층분석(LOPA)평가의 일관성을 유지하기 위하여 참조하여 사용하되, 적 절한 자료가 없는 경우 공신력 있는 기관 또는 협회의 자료를 사용할 수 있다.

E.사고결과(Consequence), 개시사건 빈도(Initiating Event Frequency), 작동요구 시 고장확률(PFD) 등을 토대로 수학적으로 결 합해 시나리오의 위험도(Risk)를 추정한다.

- ✓ 개시사건 빈도(Initiating Event Frequency), 작동요구 시 고장확률(PFD)를 곱하여 중간사건 빈도(IEL)를 구한다.

F. 시나리오와 관련되어 어떤 결정에 도달하기 위해 위험도(Risk) 를 평가한다.

- ✓ 위에서 계산한 시나리오의 중간사건 빈도(IEL)와 허용 가능한 완화 된 사건빈도(TMEL)를 비교하여 평가한다. 즉 요구되는 안전무결도수준 (SIL)은 허용 가능한 완화된 사건빈도(TMEL)를 중간사건 빈도(IEL) 로 나누어서 산출된 작동요구 시 고장확률(PFD)을 가지고 계산한다.
- ✓ 이러한 계산을 통해 기존에 설치된 또는 새로 설치해야 할 안전계장 기능(SIF)의 요구되는 목표 안전무결도수준(Target SIL)을 정한다.

공정 제어 분야 SIL 할당 단계

IEC 61511 기반의 제조공정 분야의 안전 무결성은 안전기능을 수행하는 안전 시스템(SIS)의 성능과 관련 된다. 안전 무결성 등급은 정해진 시간 주기 내에 모든 정해진 조건하에 필요한 안전기능(SIF)을 만족하며 수행하는 안전계장 시스템의 평균 확률이다. 목표 안전무결도 수준(Target SIL)이 구해진(SIL 1 이상) 안전기능(SIF)에 대해 안전무결도 수준 분석(SIL analysis)을 실시하여, 결과 안전무결도 수준(Result SIL)을 구한다. 안전계장기능(SIF)은 센서 (Sensor), 논리 해결기(Logic Solver), 최종조작요소(Final Element)로 구성된 것으로 안전시스템(SIS, safety instrumented system)은 하나 또는 그 이상의 안전기능(SIF, safety instrumented function)을 수행하기 위해 사용되는 계장시스템으로 센서(sensor), 논리 분석기(logic solver), 최종요소(final element)로 구성된다. 미리 결정된 어떤 특성 상황이 발생했을 때, 그 상황을 센서를 통해 인지하고 이것을 논리 분석기에서 자동적으로 최종요소에 신호를 보내 필요한 안전 기능을 수행하게 하는 시스템이다. 그 구성은 아래 그림 28 같다.

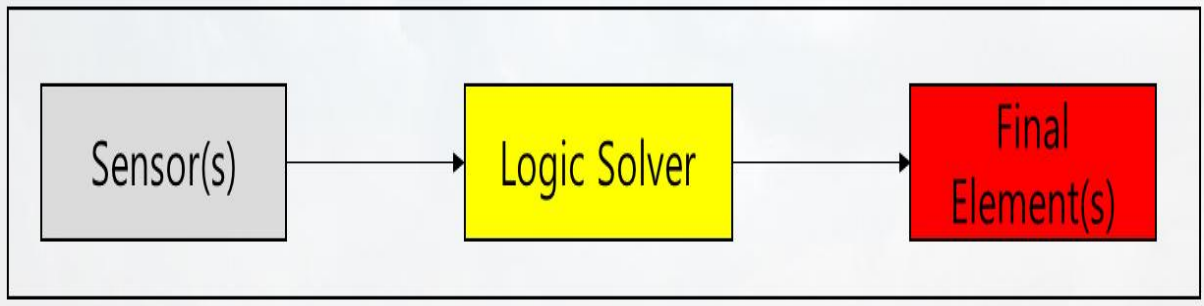


그림 27. Structure of safety instrumented system

SIL 계산 절차

IEC 61511의 대상인 제조 공정과 관련해서는 요구빈도가 낮은 안전시스템(SIS)의 경우 고장이 곧바로 위험사건과 연결되지 않을 수 있다. 작동 요구 시 고장확률(PFD)은 작동이 요구된 경우, 얼마나 고장이 나는지를 중요하게 보는 관점. 다음의 그림은 이러한 요구빈도에 따라 안전계장시스템 평가하는 기준을 선택하는 방안에 대한 모식도를 나타낸다.

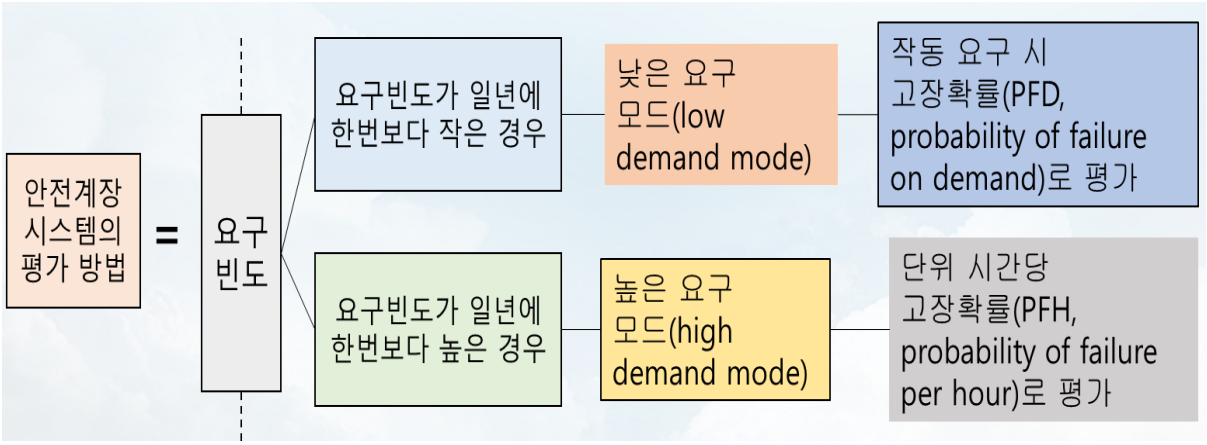


그림 28. 안전계장시스템의 Demand Mode 선택 방법

안전관련시스템(SRS, safety-related system)에 할당된 안전계장기능의 안전무결성 요구사항을 지정하는데 사용되는 4개의 이산 확률 레벨로 구성되어 있다. 낮은 요구 모드(low demand mode)의 평가 방법인 작동 요구 시 고장확률(PFD)은 작동 요구 시 설계기능을 수행하지 못할 평균 확률로 무차원 이다. 반면, 높은 요구 모드(high demand mode)의 평가 방법인 단위 시간당 고장확률(PFH)은 단위 시간당 설계기능을 수행하지 못할 확률이다. 표 18과 같이, 두 가지 작동모드의 경계 기준은 1e-4 per hour (≒ one per year 1.14e-4)이며, 작동 요구 시 고장확률(PFD)에 1e-4 per hour를 곱하면 단위 시간당 고장확률(PFH)와 오더가 같아진다.

안전시스템(SIS)의 안전무결성등급(SIL) 평가는 작동이 요구되는 빈도가 낮기 때문에 낮은 요구 모드(low demand mode)의 평가 기준인 작동 요구 시 고장확률(PFD)로 계산하는 것이 일반적이다.

$$PFD_{SIF} = PFD_{sensors} + PFD_{logic\ solver} + PFD_{final\ elements}$$

그림 29. 안전무결도 수준(SIL) 계산 방법

SIL 결정 예제

IEC 61511 기반 제조공정 분야의 위험분석 및 평가에 따른 SIL 결정의 과정은 다음과 같다.

안전무결도수준(SIL)이 결정되기 위한 계산은 방호계층분석(LOPA)에 근거하여, 위에서 언급한, 현장에 설치된 센서(Sensor), 논리해결기(Logic Solver), Final Element (Solenoid Valve, 긴급차단밸브 Body, Actuator)의 Model을 확인하고 안전무결도 수준을 결정하는 계산을 수행한다.

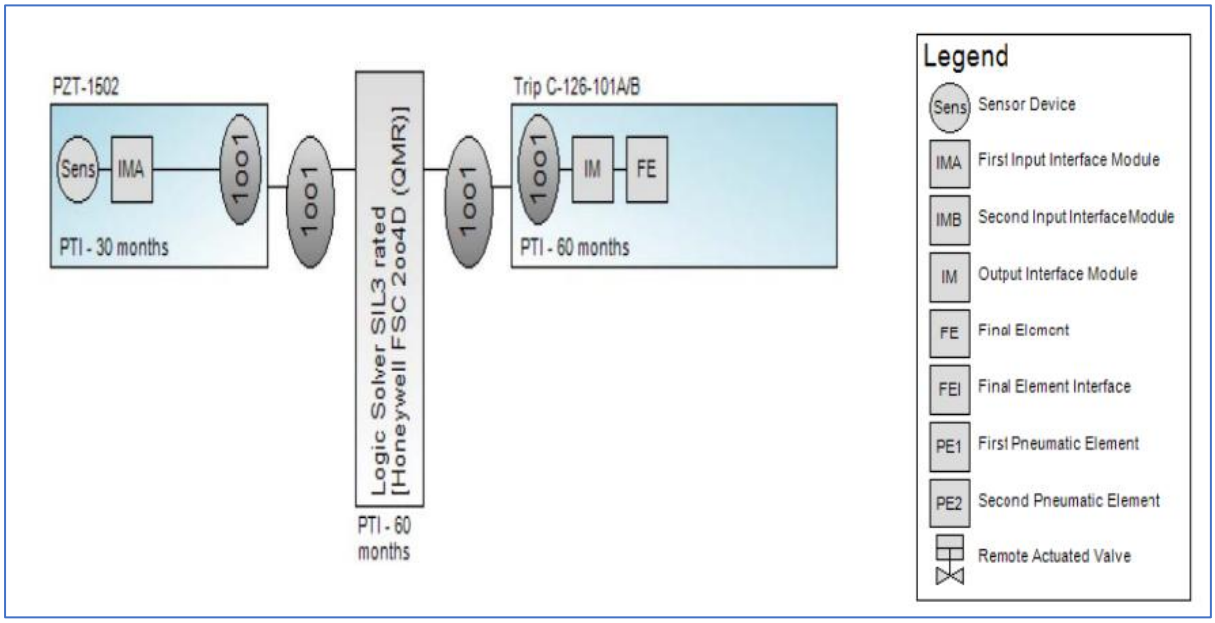


그림 30. LOPA 기법 기반의 안전계장기능(SIF)_

표 37. 센서(Sensor) 정보

Part	Description	Value
Sensor	PFD	6.15E-04
	HFT	0
	MTTFS	578.66 years

표 38. 논리해결기(Logic Solver) 정보

Part	Description	Value
Logic Solve	PFD	1.65E-06
	HFT	1
	MTTFS	613.65 years

표 39. 최종조작요소(Final Element)정보

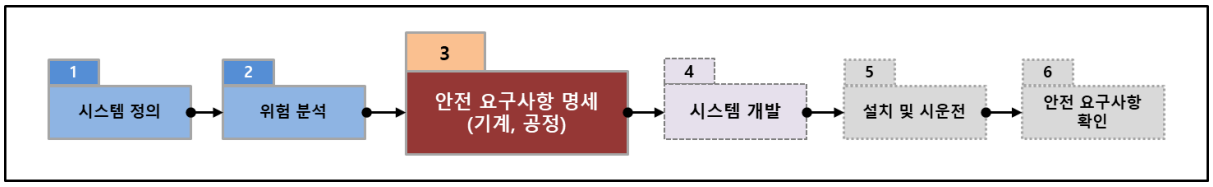
Part	Description	Value
Logic Solve	PFD	1.78E-02
	HFT	0

	MTTFS	80.93 years

결과 안전무결수준(Result SIL) 계산

$$PFD_{SIF} = PFD_{sensors} + PFD_{logic\ solver} + PFD_{final\ elements}$$

PFD_{SIF}=6.15E-04+1.65E-06+1.78E-02=1.84E-02 이며, 따라서, SIL 1.에 해당함.



3.3. 안전 요구사항 명세

목적

IEC 62061 기반의 제조 기계류의 안전 요구사항 정의 및 명세는 ISO 12100에 명시된 위험 감소 전략에 대한 필요성을 기반으로 결정된다. 제조 기계류에 대한 시스템 안전요구사항은 SRCF의 기능요구사항을 기반으로 안전 무결성 등급이 반영된 요구사항이 명세(정의)되어야 한다. SRECS에 대한 시스템 안전요구사항 명세는 SRCF와 관련한 모든 정보 분석/식별을 기반으로 수행된다.

비고: 대상 안전 시스템에 대한 "위험 분석"과 "안전 요구사항 명세" 단계는 기계류 제어 분야와 공정 제어 분야가 상이하기 때문에 각각 별도 항목으로 활동단계와 세부 절차를 다룬다.

(기계류 제어 분야) 활동단계 개요

기계류 제어 분야 위험 분석 수행활동 및 산출물을 바탕으로 시스템 안전 요구사항을 생성하게 된다. 관련해, SRECS 에 대한 안전성 활동을 통해, 안전에 중요한 영향을 미치는 기능의 경우, SRCF 로 도출되어, SRECS 설계적 반영을 위한 시스템 안전요구사항이 도출되어야 한다. 이러한 과정에 있어서, 해당 단계에서는 시스템 안전요구사항 정의 활동을 수행하기 위한 단계 및 관련 사항은 다음과 같다.

구 분	설 명
선행기준	1. 시스템 아키텍처 설계 완료 2. 시스템 안전 기능 식별 완료 3. 시스템 사양서 정의 완료
입력문서	• 시스템 사양서 • 시스템 아키텍처 설계서

	• 시스템 아키텍처 설계 제약사항 • 안전 시스템 사용자 매뉴얼 • 시스템 사양서 요구사항 추적표
수행흐름	
산 출 물	• 시스템 안전 요구사항 사양서 • 시스템 위험원 분석 보고서(SRCF 리스트) • 시스템 위험도 평가 분석 보고서 • 시스템 연계 하부 요구사항 분석서
완료기준	1. 시스템 아키텍처 및 기능 기반 안전요구사항 정의 완료 2. 시스템 안전 요구사항 작성 완료 2. 시스템 기능 및 안전요구사항 추적표 작성 완료 3. 평가기준에 의한 안전기능의 위험도 평가결과 결과서 작성 완료

(기계류 제어 분야) 세부수행 활동

IEC 62061 기반의 시스템 안전요구사항 정의 절차는 크게 시스템을 구성하는 구조정보와 기능분석 산출물을 바탕으로 수행되어 진다. 특히, IEC 62061에서 중요히 여겨지는 SRCF는 명세 시, '기능요구사항 명세'와 '안전 요구사항 명세로 구분되어 지기 때문에, 이점을 주의하여야 한다. 따라서, IEC 62061 기반의 시스템 안전 요구사항을 정의하는 수행활동은 '안전 무결성 요구사항 명세' 결과를 바탕으로 초점이 되어 수행되어 져야 한다.

수행 절차

(1) 기계 작동특성(운영모드, 사이클 시간, 응답시간 성능, 환경조건, 사람과 기계의 상호작용을 정의한다.

(2) 위(1)에서 식별 가능한 SRCF에 대한 분석결과가 충분한지 검토 후, SRCF의 리스트를 정리한다.

(3) 식별된 SRCF의 리스트를 바탕으로 위험도 평가를 수행한다.

(4) 수행된 위험도 평가 결과를 바탕으로 경감 대책이 필요한 SRCF의 경우, 설계적 안전 요구사항을 정의하여야 한다.

(5) 위 (3)에서 정의된 시스템 안전요구사항을 리스트화 하여 아키텍처 설계 및 이후 SW 설계를 위한 근원의 자료로 활용되어야 한다.

(6) SRECS에 대한 시스템 안전요구사항 명세 및 정의는 반복적인 개발방식에 따라, 설계 프로세스 수행 중에 갱신 되어야 한다.

수행 시 고려사항

(1) SRECS 설계에 영향을 미칠 수 있는 SRCF와 관련된 모든 정보를 분석한다.

(2) SRCF가 달성 가능하거나 예방하고자 하는 기계 작동에 대한 기술한다.

(3) SRCF 간 및 SRCF와 다른 기능(기계 내부 또는 외부) 간의 모든 인터페이스를 식별하여 정의 한다.

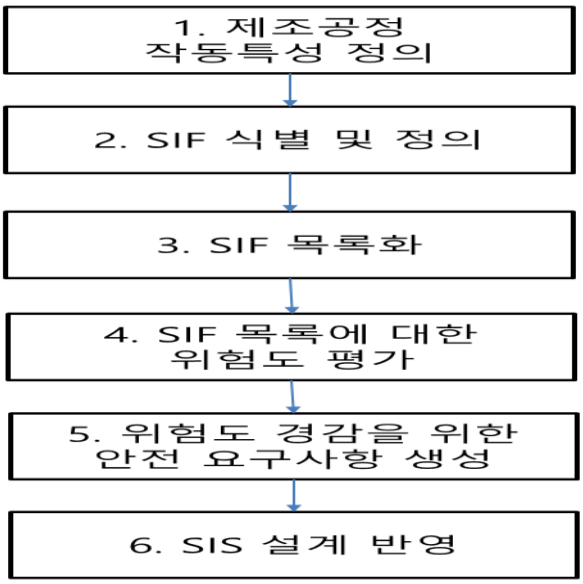
(4) 식별된 SRCF의 결함으로 부터 영향을 받는 기능 및 장치를 고려한 SRCF를 정의 및 이를 반영한 SRECS의 시스템 안전요구사항을 정의되어야 한다.

(5) 일부 정보는 SRECS의 반복적인 설계 프로세스를 시작하기 전에 충분히 정의되지 않았을 수도 있으므로, SRECS 시스템 안전 요구사항 명세는 설계 프로세스 중에 업데이트 될 수 있다.

(6) SRCF의 명세는 기능요구사항 명세와 시스템 안전 무결성 요구사항 명세로 구성된다. 따라서, 이러한 점을 활용하여, 시스템 안전요구사항이 정의되어야 한다.

(공정 제어 분야) 활동단계 개요

공정 제어 분야 위험 분석 활동을 통해 공정 제어 분야 안전 요구사항을 생성하게 된다. 관련해, 공정, 장치, 재료에 대한 안전성 활동을 통해, 제조시스템의 안전에 중요한 영향을 미치는 기능의 경우, SIF 로 도출되어, SIS 에 설계적 반영을 위한 시스템안전요구사항이 도출되어야 한다. 이러한 과정에 있어서, 해당 단계에서는 제조공정 안전요구사항 정의 활동을 수행하기 위한 단계 및 관련 사항은 다음과 같다.

구 분	설 명
선행기준	1. 공정 운영개념도 정의 완료 2. 공정간 관련 요소 정의 완료 3. 공정/장치/재료 인터페이스 식별 4. 공정 프로세스 정의 완료
입력문서	• 공정 운영개념도 정의서 • 공정 인터페이스 정의서 • 공정 프로세스 정의서 • 제조공정 사양서 • 제조공정 사양서 요구사항 추적표
수행흐름	
산 출 물	• 제조공정 안전 요구사항 사양서 • 제조공정 위험원 분석 보고서(SIS 리스트) • 제조공정 위험도 평가 분석 보고서

	• 제조공정 연계 하부 요구사항 분석서
완료기준	1. 제조공정 아키텍처 및 기능 기반 안전요구사항 정의 완료 2. 제조공정 안전 요구사항 작성 완료 2. 제조공정 기능 및 안전요구사항 추적표 작성 완료 3. 평가기준에 의한 안전기능의 위험도 평가결과 결과서 작성 완료

(공정 제어 분야) 세부수행 활동

IEC 615111 기반의 시스템 안전요구사항 정의 절차는 크게 시스템을 구성하는 공정, 구조정보와 기능분석 산출물을 바탕으로 수행되어 진다. 특히, IEC 61511 에서 중요히 여겨지는 SIF는 명세 시, '기능요구사항 명세'와 '안전 요구사항 명세'로 구분되어 지기 때문에, 이점을 주의하여야 한다. 따라서, IEC 61511 기반의 시스템 안전 요구사항을 정의하는 수행활동은 '안전 무결성 요구사항 명세' 결과를 바탕으로 초점이 되어 수행되어 져야 한다.

수행 절차

(1) 공정 및 장치, 기계 작동특성(운영모드, 사이클 시간, 응답시간 성능, 환경조건, 사람과 기계의 상호작용을 정의한다.

(2) 위(1)에서 식별 가능한 SIF에 대한 분석결과가 충분한지 검토 후, SIF의 리스트를 정리한다.

(3) 식별된 SIF의 리스트를 바탕으로 위험도 평가를 수행한다.

(4) 수행된 위험도 평가 결과를 바탕으로 경감 대책이 필요한 SIF의 경우, 설계적 안전 요구사항을 정의하여야 한다.

(5) 위 (3)에서 정의된 시스템 안전요구사항을 리스트화 하여 아키텍처 설계 및 이후 SW 설계를 위한 근원의 자료로 활용된다.

(6) SIS에 대한 시스템 안전요구사항 명세 및 정의는 반복적인 개발방식에 따라, 설계 프로세스 수행 중에 갱신 되어야 한다. .

수행 시 고려사항

(1) SIS 설계에 영향을 미칠 수 있는 SIF와 관련된 모든 정보를 분석한다.

(2) SIF가 달성 가능하거나 예방하고자 하는 기계 작동에 대한 기술한다.

(3) SIF 간 및 SIF와 다른 기능(기계 내부 또는 외부) 간의 모든 인터페이스를 식별하여 정의 한다.

(4) 식별된 SIF의 결함으로 부터 영향을 받는 기능 및 장치를 고려한 SIF를 정의 및 이를 반영한 SIS의 시스템 안전요구사항을 정의되어야 한다.

(5) 일분 정보는 SIS의 반복적인 설계 프로세스를 시작하기 전에 충분히 정의되지 않았을 수도 있으므로, SIS 시스템 안전 요구사항 명세는 설계 프로세스 중에 업데이트 될 수 있다.

(6) SIF의 명세는 기능요구사항 명세와 시스템 안전 무결성 요구사항 명세로 구성된다. 따라서, 이러한 점을 활용하여, 시스템 안전요구사항이 정의되어야 한다.

제 4 장. 응용 소프트웨어 개발

응용 소프트웨어 개발

시스템 개발은 하드웨어와 응용 소프트웨어 개발로 나누어진다. 기계류 제어나 공정 제어 시스템 등 PLC 기반 안전 시스템은 하드웨어와 소프트웨어로 구성되며, 본 가이드에서는 응용 소프트웨어의 개발만을 다루며 하드웨어의 개발은 다루지 않는다.

응용 소프트웨어의 개발은 그림과 같이 6단계로 이루어진다. 이 중 코딩 및 구현 단계는 동일한 언어를 사용하더라도 제조사별로 상이한 부분이 있고 종류가 다양하기 때문에 본 가이드에서 다루지 않고 적용할 제품의 PLC 구현 가이드를 참조하길 권장한다.

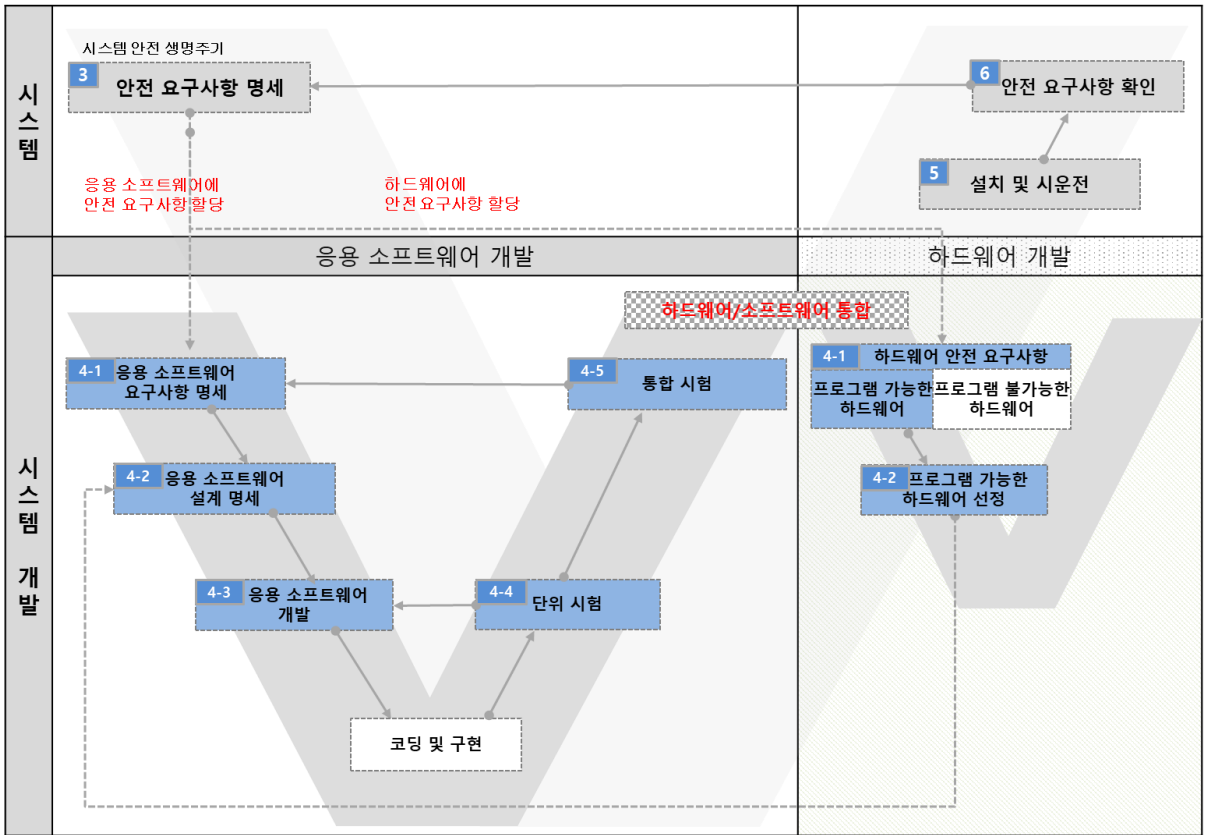
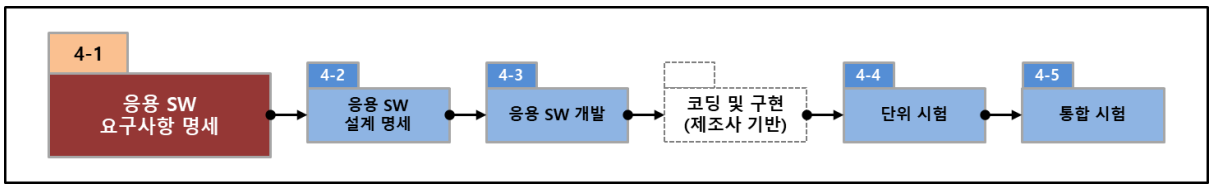


그림 31 응용 소프트웨어 개발 생명주기

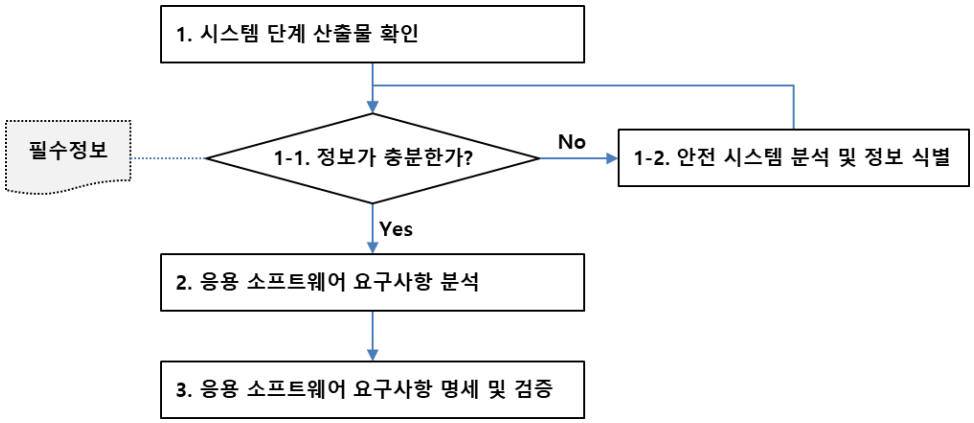


4.1. 응용 소프트웨어 요구사항 명세

4.1.1. 목적

안전 요구사항 명세 단계를 통해 식별된 시스템의 안전 요구사항 중 응용 소프트웨어에 할당 된 요구사항을 구현하기 위해 응용 소프트웨어에 대한 안전 요구사항을 식별하고 명세하는 단계로『시스템 정의 및 위험 분석』단계에서 작성된 산출물을 기반으로 세부 단계 활동을 수행한다.

4.1.2. 활동 단계 개요

구 분	설 명
선행기준	1. 안전 시스템의 안전 기능 식별 및 서브 시스템 할당 완료 2. 안전 시스템 안전 기능을 만족하는 시스템 요구사항 정의 완료 3. 안전 시스템 안전무결성 등급 할당 완료
입력문서	• 안전 시스템 아키텍처 설계서 • 안전 시스템 안전 기능 정의서 • 안전 시스템 안전 요구사항 명세서 • 안전 시스템 안전 매뉴얼 및 안전 계획서
수행흐름	
산 출 물	• 응용 소프트웨어 안전 요구사항 명세서

	• 응용 소프트웨어 안전 요구사항 검증 보고서 • 응용 소프트웨어 안전 요구사항 추적표
완료기준	1. 응용 소프트웨어 요구사항 분석 완료 2. 응용 소프트웨어 요구사항 검증 완료 3. 응용 소프트웨어 요구사항 추적표 작성 완료

4.1.3. 세부 수행 활동

[1] 시스템 단계 산출물 확인

『시스템 정의』 단계에서 『안전 요구사항 명세』 까지 진행하면서 분석된 안전 시스템 아키텍처와 안전 요구사항 명세서 등 시스템 단계 입력문서를 확인하여 응용 소프트웨어 요구사항 명세에 필요한 정보들이 식별되어 있는지를 확인한다. 기본 확인 문서는 『3.2.3. 입력문서』와 같으며 필요시 추가적인 산출물을 확인할 수 있다. (산출물 목록은 시스템 계획 단계에서 선택 가능하다.)

가. 수행 절차

(1) 『시스템 정의』 산출물 리스트를 확인한다.

(2) 각 산출물을 분석하여 응용 소프트웨어 요구사항 명세를 위한 『3.2.4.2. 식별 항목』 식별 가능 여부를 확인한다.

(3) 만약, 필요한 정보가 식별되지 않았으면, 이 단계에서 필요 정보 수집 완료시까지 분석을 진행한다.

(4) 필요한 필수 식별 정보를 모두 확인 후 다음 단계로 진행한다.

나. 식별 항목

필수 식별 정보는 대상 시스템의 범위와 구현 수준과 하부 장비에 따라 상이하게 적용할 수 있으며 시스템 계획 단계나 인증 준비 단계에서 조절이 가능하다. (본 가이드에서 제시하는 필수 식별 정보는 『1.5 참고 표준』과 관련 연구 분석 결과 일반적으로 응용 소프트웨어 요구사항 명세 시 필요한 사항을 조사하여 제공한다.)

구 분	식별 대상
(1) 안전 시스템 구성 및 범위	• 이중화 아키텍처 적용 여부 • 이중화에 따른 동기화 방법 적용 여부 • 안전 시스템 안전 기능/비-안전 기능 리스트
(2) 안전 시스템 공통 기능	• Diagnostic 기능 적용 여부 • I/O 메모리 매핑 기능 적용 여부 • 주기적 테스트 기능 적용 여부 • 외부 장치 모니터링 기능 적용 여부 • 외부 장치 통신 규격
(3) 안전 시스템 제약 사항	• 메모리 크기 및 주소 규칙 • 처리 성능 • 응답 시간
(4) 외부 장치 인터페이스	• 외부 입력 인터페이스 및 신호 • 외부 출력 인터페이스 및 신호
(5) 사용자 인터페이스	• 사용자 인터페이스 규격 및 대상 시스템 • 사용자 인터페이스 지원 대상 및 신호
(6) 운영 모드	• 안전 시스템 운영 모드 • 운영 모드 별 전환 규칙 • 운영 모드 별 제약 조건
(7) 안전 시스템 외부 장치 테스트 및 안전 기능 진단	• 외부 장치 진단 방법 및 주기 • 외부 장치 Proof 테스트 방법 및 주기 • 안전 기능 동작 가능 여부 확인 방법 • 안전 기능 동작 가능 여부 확인 주기 • 안전 기능 문제 발생 시 처리 방법

(8) 안전 시스템 리셋 (Optional)	• 안전 시스템 리셋 종류(Cold, Hot, Warm) • 안전 시스템 리셋 방법(수동, 자동) • 리셋 후 자동 정상 기능 동작 조건 • 리셋 후 수동 정상 기능 동작 조건
(9) 안전 시스템 (Optional)	• 안전 시스템의 모든 위험 상태 • 안전 시스템 위험 상태 확인 방법
(10) 알람 (Optional)	• 발생 가능한 알람 • 알람 발생 조건 • 발생 알람 제거 조건

[2] 응용 소프트웨어 요구사항 도출

『시스템 단계 산출물』 단계에서 식별한『식별 항목』을 기반으로 안전 시스템의 제어 기능을 수행하는 응용 소프트웨어의 요구사항을 분석 및 도출한다. 응용 소프트웨어는 초기 구동, 종료, 운영 중 리셋 처리 등의 운영 주기와 관련된 요구사항을 도출하고, 안전 시스템 중 응용 소프트웨어에 할당 된 안전 기능과 비-안전 기능에 대한 제어를 분석한다. 또한 안전 및 비-안전 기능이 자동 또는 수동 실행인지를 식별하여 요구사항을 도출한다. 그리고『식별 항목』을 통해 확인된 안전 시스템 항목을 만족시키기 위해 응용 소프트웨어가 수행해야 할 세부 기능 요구사항을 분석한다.

가. 수행 절차

(1) 응용 소프트웨어 초기 구동 절차 및 단계별 수행 기능을 분석한다.

A. 초기 응용 소프트웨어 구동 시 필요한 입력 신호 식별

B. 초기 구동 시 필요한 절차 식별

C. 초기 정상 구동 완료 요건 식별

D. 초기 비정상 구동 시 처리 방법 식별

A. 응용 소프트웨어 초기 구동(Start-up)을 요청하는 모든 신호나 이벤트를 식별한다.

- ✓ "전원 입력이 On 되면 응용 소프트웨어가 초기 구동을 진행한다."
- ✓ "응용 소프트웨어 초기 구동 신호 입력 확인 시 응용 소프트웨어 초기 구동을 진행한다."

B. 응용 소프트웨어 초기 구동 시 필요한 절차를 식별한다.

- ✓ (1) "전원 입력이 On 된다." Or "응용 소프트웨어 초기 구동 신호 입력을 확인한다."
- ✓ (2) "로그 또는 비-휘발성 메모리에 저장 된 고장 유무를 확인한다."

- ✓ (3) "정상 상태 시 모든 입력 및 출력 메모리를 초기화한다." (리셋 모드에 따라 다름)
- ✓ (4) "메모리 초기화 정상 완료 시 운영 모드 표시기에 "Normal"을 표시한다.
- ✓ (5) "모든 램프 신호 확인 후 모든 신호 녹색 On 한다.
- ✓ (6) "현재위치 표시 값에 "000"을 표시한다.
- ✓ (7) "정상 초기 구동 완료 비프음을 발생한다."

C. 초기 정상 구동 완료 요건을 식별한다.

- ✓ "운영 모드 표시기에 "Normal"이 표시된다."
- ✓ "모든 램프가 On 이 된다."
- ✓ "현재위치 표시 값에는 "000"이 표시된다."
- ✓ "로그 기록에 (날짜/시간)과 함께 정상 초기 구동 정보가 기록된다."
- ✓ "정상 초기 구동 완료 비프음이 발생한다."

D. 초기 비정상 구동 시 처리 방법을 식별한다.

- ✓ (2-1) 시스템에 고장 기록이 확인되고 조치 완료 기록이 없을 경우
  - ⇨ "고장 기록 확인 시 구동 절차를 중단하고 운영 모드 표시기에 "Failure"를 표시한다."
  - ⇨ "운영자가 직접 시스템을 종료하거나 고장 조치를 완료 할 때까지 대기한다."
- ✓ (3-1) 메모리 초기화 실패의 경우
  - ⇨ "메모리 초기화 실패 로그를 기록한다."
  - ⇨ "구동 절차를 중단하고 운영 모드 표시기에 "Failure"를 표시한다."
  - ⇨ "메모리 고장 알람을 발생한다."
  - ⇨ "재부팅 카운터를 동작한다."

- ✓ (5-1) 램프 신호 일부 오류 발생으로 정상 입력 신호 확인 불가의 경우
  - ⇨ "램프 입력 신호 오류 로그를 기록한다."
  - ⇨ "램프 입력 신호 확인 기능을 1회 재가동한다."
  - ⇨ "1회 재가동 후 정상 시 램프 입력 신호 오류 로그 재거 후 정상 절차를 따른다."
  - ⇨ "1회 재가동 후 여전히 비정상의 경우 알람을 발생한다."
  - ⇨ "구동 절차를 중단하고 운영 모드 표시기에 "Failure"를 표시한다."

(2) 응용 소프트웨어 종료 절차 및 단계별 수행 기능을 분석한다.

A. 종료 시 입력 신호나 이벤트 식별

B. 종료 시 필요한 절차 식별

C. 정상 종료 완료 조건 식별

D. 비정상 종료 시 처리 방법 식별

A. 응용 소프트웨어 종료 신호나 이벤트를 식별한다.

- ✓ "전원 입력 스위치 Off 감지 시 응용 소프트웨어 종료를 수행한다."
- ✓ "응용 소프트웨어 종료 신호 감지 시 응용 소프트웨어 종료를 수행한다."

B. 응용 소프트웨어 종료 시 필요한 절차를 식별한다.

- ✓ (1) "전원 입력이 Off 된다." Or "응용 소프트웨어 종료 신호 입력을 확인한다."
- ✓ (2) "로그 또는 비-휘발성 메모리에 저장 된 고장 유무를 확인한다."
- ✓ (3) "모든 입력 및 출력 메모리를 초기화한다."
- ✓ (4) "메모리 초기화 정상 완료 시 운영 모드 표시기를 Off 한다.
- ✓ (5) "모든 램프 신호 확인 후 모든 신호 표시를 Off 한다.

✓ (6) "현재위치 표시 값 표시기를 Off 한다.

✓ (7) "정상 종료 비프음을 발생한다."

C. 초기 정상 구동 완료 요건을 식별한다.

✓ "운영 모드 표시기, 램프 및 현재위치 표시기가 모드 Off 한다."

✓ "로그 기록에 (날짜/시간)과 함께 정상 종료 정보가 기록된다."

✓ "정상 종료 비프음이 발생한다."

D. 초기 비정상 구동 시 처리 방법을 식별한다.

✓ (2-1) 시스템에 고장 기록이 확인되고 조치 완료 기록이 없을 경우

⇨ "고장 기록 확인 시 로그의 종료 기록에 "Failure"를 표시한다."

✓ (3-1) 메모리 초기화 실패의 경우

⇨ "메모리 초기화 실패 로그를 기록한다."

✓ (5-1) 램프 신호 일부 오류 발생으로 정상 입력 신호 확인 불가의 경우

⇨ "램프 입력 신호 오류 로그를 기록한다."

(3) 할당 된 응용 소프트웨어 안전 및 비-안전 기능을 분석하고 요구사항을 도출한다.

A. 안전 기능의 안전 모드(Low Demand/High Demand/Continuous)에 따른 기능 동작 타이밍 식별

B. 다중화 시스템 아키텍처 구성 시 응용 소프트웨어 단계에서 다중화에 따른 신호 및 데이터의 동기화 방안 식별

C. 비-안전 기능과 안전 기능 간 데이터 및 신호 교환 여부 식별

D. 할당 된 응용 소프트웨어 안전 및 비-안전 기능의『스캔 타이밍』식별

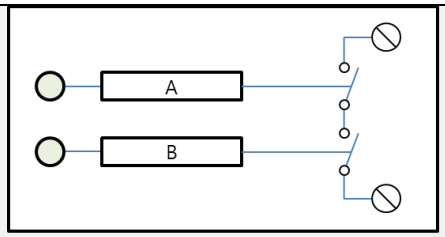
E. 할당 된 응용 소프트웨어 안전 및 비-안전 기능의 실행 절차 식별

A. 안전 기능의 안전 모드(Low Demand/High Demand/Continuous)에 따라 응용 소프트웨어의 기능 동작 타이밍을 식별하여 구체적으로 정량화 한다.

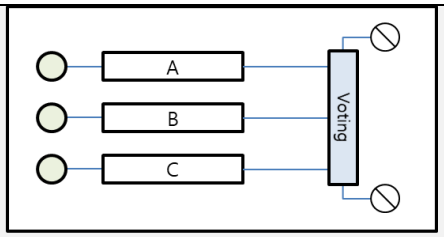
- ✓ 『시스템 정의 및 위험 분석』 단계에서 식별한 안전 기능의 요구 안전 모드의 동작 타이밍을 정량화 한다.
- ✓ 정량화 한 수치를 기반으로 안전 기능 동작 조건 만족 시 응용 소프트웨어 가 해당 안전 기능을 수행하기 위한 타이밍을 요구사항으로 식별한다.
- ✓ "압력이 기준 이상일 경우 100ms 이내에 『압력 밸브 닫힘 기능』 이 동작해야 한다."
- ✓ "『레벨 감지 모니터링 기능』 은 지속적으로 센서 감지를 통하여 유량의 레벨을 확인한다."
- ✓ "『비상 정지 기능』 은 버튼 누름 시 즉각적으로 기능을 중단해야 한다."

B. 안전 시스템의 아키텍처 다중화 구성 시 응용 소프트웨어 단계에서 다중화에 따른 신호 및 데이터의 동기화 방안을 식별해야 한다.

- ✓ "『1oo2』 이중화로 구성 된 『안전 차단』 스위치는 2개의 입력 신호로 최소 50ms 동안 동시에 『차단』 신호가 들어오면 기능을 차단한다." ← **다중화 구성 시 입력 신호의 지속 기간을 명시해야 한다.**
- ✓ "『2oo3 voting』 다중화로 구성 된 『안전 알람 발생』 스위치는 각 입력 신호마다 한번이라도 『발생』 신호가 입력되면 『Voting』 모듈에 저장되며 2개 이상 『발생』 신호 입력 시 알람을 발생하고 입력 신호를 초기화 한다."
- ✓ "『2oo3 voting』 구성은 응용 소프트웨어에서 임의로 입력 신호를 초기화 할 수 없다."



(1oo2 구성)



(2oo3 voting 구성)

C. 비-안전 기능과 안전 기능 간 데이터 및 신호 교환 여부를 식별하여 비-안전 기능이 안전 기능에 영향을 주지 않음을 확인하거나 영향을 주더라도 검증이 가능함을 확인해야 한다.

✓ "예시" 또는 상세 설명

D. 할당 된 응용 소프트웨어 안전 및 비-안전 기능의 스캔 타이밍을 확인하여 기능 실행 시간과 시스템 안전 요구사항의 요구 조건과 적합성 여부를 식별한다.

✓ "예시" 또는 상세 설명

E. 할당 된 응용 소프트웨어 안전 및 비-안전 기능의 실행 절차를 식별한다.

✓ "예시" 또는 상세 설명

(4) 할당 된 응용 소프트웨어 기능의 실행 방법(수동 또는 자동)을 분석한다.

A. 운영자에 의해 수동 실행되는 기능 동작 조건 및 순서 식별

B. 응용 소프트웨어의 제어 또는 외부 장치의 입력 조건에 따라 자동으로 실행되는 기능 동작 조건 및 순서 식별

C. 수동 실행 기능의 경우 실행 중 기능 취소 신호 입력 방법 식별

D. 자동 실행 기능의 경우 실행 중 기능 취소 신호 입력 주기 식별

A. 운영자가 수동으로 안전 기능을 수행 할 경우 이에 대한 수동 실행 조건과 종료 조건을 분석하여야 한다.

✓ "예시" 또는 상세 설명

B. 자동 실행 기능의 경우 시작 조건을 정확하게 식별해야 하며, 기능의 동작 순서도 명확하게 정리되어야 한다.

✓ "예시" 또는 상세 설명

C. 수동 실행 기능의 경우 실행 중 기능 취소 가능 여부와 가능한 경우 취소 신호 입력 방법을 명확하게 분석하고 식별해야 한다.

✓ "예시" 또는 상세 설명

D. 자동 실행 기능의 경우 실행 중 기능 취소 가능 여부와 가능한 경우 취소 신호 입력 방법을 명확하게 분석하고 식별해야 한다.

✓ "예시" 또는 상세 설명

(5) 외부 장치간 인터페이스를 분석한다.

A. 외부 입력 인터페이스 신호 타입, 주기 및 변수명 식별

B. 외부 출력 인터페이스 신호 타입, 주기 및 변수명 식별

A. 응용 소프트웨어와 연계된 외부 입력 인터페이스의 신호 타입, 송수신 주기를 식별하고 가능한 경우 변수명까지 식별한다.

✓ "외부 상위 시스템으로부터 주기적으로 입력을 받는 경우를 식별한다."

✓ "PLC에 장착된 HMI로부터 입력을 받는 경우를 식별한다."

✓ "응용 소프트웨어가 설치 된 PLC의 통신 인터페이스를 식별한다."

B. 응용 소프트웨어와 연계된 외부 출력 인터페이스의 신호 타입, 송수신 주기를 식별하고 가능한 경우 변수명까지 식별한다.

✓ "외부 상위 시스템에 주기적으로 출력을 보내는 경우가 있으면 이를 식별한다.

✓ "PLC에 장착된 HMI로 출력을 내보내는 경우 이를 식별한다."

- ✓ "응용 소프트웨어가 설치 된 PLC의 통신 인터페이스를 식별한다."
- ✓ "모터 등을 제외하고 응용 소프트웨어와 연결 된 하위 출력 장치(프린터 등)를 식별한다."

(6) 응용 소프트웨어 입력 및 출력 신호를 메모리에 할당한다.

A. 안전 시스템의 메모리 구성 식별

B. 입력 신호의 내부 메모리 주소 할당 방안 식별

C. 출력 신호의 내부 메모리 주소 할당 방안 식별

A. 안전 시스템 제품 제조사에서 제공하는 메모리 구성을 식별하고 응용 소프트웨어에서 사용하는 메모리 할당 정보를 식별한다.

- ✓ "입출력 릴레이 메모리 주소, 타이머 메모리 주소, 데이터 레지스터 주소 등 식별한다."
- ✓ "사용자 프로그램 영역 주소 식별한다."

B. 입력 신호의 경우 입력 이미지 메모리 주소의 입력 단자 할당 정보를 제조사로부터 제공 받아 입력 신호 저장 주소를 식별한다.

- ✓ "제조사 별 메모리 할당 맵 식별한다.
- ✓ "사용자 프로그램 영역 주소의 경우 입력 신호 처리 여부를 식별한다.

C. 출력 신호의 경우 출력 래치 메모리 주소의 출력 단자 할당 정보를 제조사로부터 제공 받아 출력 신호 저장 주소를 식별한다.

- ✓ "제조사 별 메모리 할당 맵 식별
- ✓ "디바이스 이미지 메모리와 출력 래치 메모리 연계 방안을 식별한다."

(7) 입/출력 신호 및 변수 범위를 분석한다.

A. 입/출력 신호 정상 범위 식별

B. 잘못된 범위의 입력 신호 처리 방법 식별

A. 식별 된 인터페이스의 입/출력 신호의 타입과 정상 범위를 식별한다.

- ✓ "**state:** BOOL 타입, True: 정상 상태, False: 비-정상 상태를 의미한다."
- ✓ "설계 시 정의 된 신호 입력 시 범위를 체크하며, 출력 시에도 정상 값인지를 확인할 수 있도록 한다."

B. 범위 이상 이나 잘못 된 타입의 신호가 입력 되었을 시 예외 처리 방법과 초기화 방법에 대해서 식별한다.

- ✓ "범위를 벗어난 입력 신호를 받으면 예외 처리를 수행하거나 정상 범위 값으로 변환하는 방법 중 시스템 정의에 잘 맞는 방법을 식별한다.
- ✓ "잘못 된 타입의 경우 예외 처리 및 알람 발생 등의 방법을 식별한다."

(8) 안전 시스템 운영 모드에 따른 응용 소프트웨어의 제어 기능을 분석한다.

A. 운영 모드의 전환이 응용 소프트웨어의 제어 기능과 관련이 있는지 식별

B. 관련이 있을 경우 운영 모드 전환 규칙 식별

C. 운영 모드 별 제약조건 식별

A. 운영 모드의 전환 시 응용 소프트웨어의 제어 기능이 변경 되는지를 확인한다.

- ✓ "PLC의 운영 모드 변경 시 응용 소프트웨어의 제어 기능이 유지되거나 변경되는지를 분석하고 이를 식별한다."
- ✓ "고장 모드일 경우 입력 값을 정상적으로 처리하면 안되기 때문에 이에 대한 응용 소프트웨어의 제어 기능 변경을 확인한다."

B. 운영 모드 전환 규칙을 식별한다.

- ✓ "입력 신호로 인해 운영 모드가 변경 되거나 내부 로직에 의해 운영 모드가 변환 되는 경우 해당 규칙을 식별한다."
- ✓ "운영 모드 전환 간 규칙에서 충돌이 발생하는지를 식별한다."

(9) 외부 장치 진단 및 안전 기능 모니터링 방법을 분석한다.

A. 외부 장치 진단 테스트 방법 식별

B. 외부 장치 Proof 테스트 방법 식별

C. 식별된 안전 기능 수행 가능 여부 모니터링 주기 식별

D. 식별된 안전 기능 수행 불가시 처리 방법 식별

A. 응용 소프트웨어가 외부 장치 진단 기능을 수행 해야 할 경우 이를 식별한다.

- ✓ "외부 장치 진단과 연관이 있을 경우 외부 장치 진단 주기와 방법을 식별한다."
- ✓ "외부 장치 진단 후 고장 발견 시 처리 방안에 대해서 분석한다."

B. 응용 소프트웨어가 외부 장치 Proof 테스트 기능을 수행 해야 할 경우 이를 식별한다.

- ✓ "외부 장치 Proof 테스트와 연관이 있을 경우 외부 장치 Proof 테스트 주기와 방법을 식별한다."
- ✓ "외부 장치 Proof 테스트 후 고장 발견 시 처리 방안에 대해서 분석한다."

C. 식별된 안전 기능 수행 가능 여부 모니터링 주기를 식별한다.

- ✓ "안전 시스템의 안전 기능 수행 가능 여부 모니터링 기능이 필요한 경우 모니터링 대상과 주기를 확인한다."

D. 안전 기능 수행 가능 여부 모니터링 불가시 처리 방법을 식별한다.

- ✓ "안전 시스템의 안전 기능 수행 여부 모니터링 기능 수행 불가시 알람 발생 등의 고장 처리 방법을 식별한다."

(10) 응용 소프트웨어 자가 진단 방법을 분석한다.

A. 응용 소프트웨어 자가진단 주기 식별

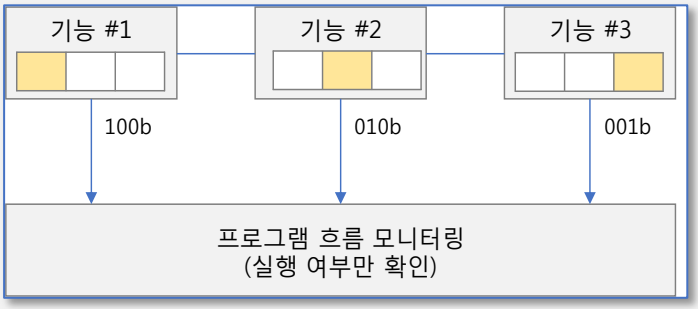
B. 응용 소프트웨어 자가진단 방법 식별

A. 응용 소프트웨어 자신의 자가 진단 주기를 식별한다.

- ✓ "5초 단위로 응용 소프트웨어 자가 진단을 수행한다."
- ✓ "예) 1회 진단 실패 시 실패 상태를 기록 후 2회 더 진단 수행 후 지속적으로 실패 발생 시 알람 발생 후 종료 절차를 수행한다."

B. 응용 소프트웨어 자신의 자가 진단 방법을 식별한다.

- ✓ "예) 응용 소프트웨어의 자가 진단을 위해 주기적으로 기능 실행 여부를 메모리에 기록한다."
- ✓ "예) 기록 된 실행 가능 여부를 자가 진단 전에 삭제하여 기능 자가



진단 시에만 새로 기록되게 한다."

나. 기본 안전 관련 요구사항 도출

안전 시스템 개발 시 제어 응용 소프트웨어가 적용되는 도메인 또는 필요에 따라 다음의 응용 소프트웨어 기본 안전 요구사항 도출 절차를 추가로 수행한다.

(1) 안전 시스템 리셋 시 응용 소프트웨어 수행 기능을 분석한다.

A. 리셋 종류(Cold, Hot, Warm)에 따른 응용 소프트웨어 처리 절차 식별

B. 리셋 방법(수동, 자동)에 따른 응용 소프트웨어 처리 방안 식별

C. 리셋 후 응용 소프트웨어 정상 동작 수행 조건 식별

D. 리셋 후 응용 소프트웨어 비-정상 상태일 경우 실행 방안 식별

A. 안전 시스템에서 제시하는 리셋 종류를 선택하고 이에 따른 응용 소프트웨어의 처리 절차를 식별한다.

✓ "안전 시스템에서 적용할 리셋 종류를 확인한다."

구분	설명
Warm Restart	재시작 전 데이터를 유지한 상태에서 초기 구동을 수행한다.
Cold Restart	모든 데이터를 삭제한 후 초기 구동을 수행한다.
Hot Restart	재시작 전 데이터를 유지한 상태에서 구동 후 재시작 중단 지점에서 시작한다.

✓ "선택한 리셋 종류에 따라 응용 소프트웨어의 리셋 처리 절차를 식별한다."

B. 리셋 방법이 수동인지 자동인지에 따라 응용 소프트웨어 처리 방안을 식별한다.

✓ "리셋의 시작 조건을 식별한다."

✓ "리셋의 처리 절차를 식별한다.

C. 리셋 완료 후 응용 소프트웨어의 정상 동작 수행 조건을 식별한다.

✓ "예) 고장 정보 존재 시 응용 소프트웨어의 기능을 정상 수행할 수 없게 하고 고장 처리 요청 신호를 출력한다."

D. 리셋 완료 후 응용 소프트웨어의 비-정상 동작 수행 조건을 식별한다.

- ✓ "비-정상 동작 조건을 식별한다."
- ✓ "비-정상 동작 시 알람 발생 등의 처리 방법을 식별한다.

(2) 알람 처리 방법을 분석한다.

A. 안전 시스템 및 할당된 응용 소프트웨어 자체 발생 알람 리스트 식별

B. 알람 별 발생 조건 식별

C. 발생 알람 제거 조건 식별

A. 안전 시스템 및 응용 소프트웨어 자체 발생 알람 리스트를 식별한다.

- ✓ "안전 시스템에서 발생 가능한 알람 리스트를 식별한다."
- ✓ "응용 소프트웨어 자체 발생 알람 리스트를 식별한다."
- ✓ "통신 불량 등의 알람을 세부적으로 식별한다."

B. 식별된 알람의 발생 조건을 확인한다.

- ✓ "응용 소프트웨어에서 발생 할 수 있는 알람의 발생 조건을 식별한다."
- ✓ "알람 발생 조건 확인 절차를 식별한다."

C. 발생 된 알람 제거 조건을 식별한다.

- ✓ "안전 시스템에서 발생한 알람의 제거 조건을 식별한다."
- ✓ "응용 소프트웨어에서 발생한 알람의 제거 조건을 식별한다."

(3) 안전 시스템 위험 상태를 분석하고 요구사항을 도출한다.

A. 안전 시스템 운영 시 발생 가능한 위험 상태 식별

B. 위험 상태 별 응용 소프트웨어의 역할 식별

C. 안전 기능 할당 영역에서 응용 소프트웨어의 역할 식별

예) 지역 또는 플랜트 영역에서의 알람 발생, 기계 위험 식별 시 알람 발생

A. 안전 시스템이 사용될 공정에서 발생 가능한 위험 상태를 모두 식별한다.

- ✓ "예) 압력 변화에 따른 밸브 상태로 인해 위험이 발생할 수 있다."
- ✓ "예) 공정 라인의 단일 흐름 센서 고장으로 인해 센서 정보 수집 불가로 인해 발생할 수 있는 위험"
- ✓ "예) 기계 긴급 정지 시 로봇 암의 위치에 따라 긴급 정지 시 별개의 라인에 영향을 미칠 수 있다."

B. 위험 상태 별 응용 소프트웨어의 역할 식별

- ✓ "예) 밸브 상태 주기적 감시 수행"
- ✓ "예) 센서 입력 값 정상 범위 확인 후 주기적 이상 발생 시 알람 발생"
- ✓ "예) 긴급 정지 시 로봇 팔의 위치가 정상 라인에 영향을 미칠 경우 이를 별도의 알람으로 발생"

C. 안전 기능 할당 영역에서의 응용 소프트웨어의 역할 식별

- ✓ "예시" 또는 상세 설명

[3] 응용 소프트웨어 요구사항 명세 및 검증

『응용 소프트웨어 요구사항 분석』 단계를 통해 안전 시스템을 제어하기 위한 응용 소프트웨어의 요구사항을 식별한 후 이를 『요구사항 명세 템플릿』에 맞게 작성한다. 작성한 『응용 소프트웨어 요구사항』은 응용 소프트웨어 검증 속성을 기반으로 하여 응용 소프트웨어의 품질을 검증하고, 안전 시스템에서 할당 받은 안전 요구사항을 기반으로 요구하는 항목을 모두 다루고 있는지를 검증하여 『응용 소프트웨어 안전 요구사항 검증 보고서』를 작성한다. 마지막으로 『응용 소프트웨어 요구사항 분석서』와 상위 문서 간의 추적 관계를 추적표로 작성한다.

가. 수행 절차

(1) 응용 소프트웨어 요구사항 분석 결과를 기반으로 요구사항 명세서를 작성한다.

A. 『요구사항 명세서 템플릿』에 분석한 내용을 명세

(2) 응용 소프트웨어 요구사항 명세서를 검증한다.

A. 안전 기능 요구사항 검증

B. 비-안전 기능 요구사항 검증

C. 『응용 소프트웨어 품질 속성』 적용 여부 확인

D. 『응용 소프트웨어 안전 요구사항 검증 보고서』 작성

(3) 시스템 단계 산출물과 응용 소프트웨어 요구사항 추적표를 작성한다.

A. 응용 소프트웨어 요구사항의 출처 작성

나. 응용 소프트웨어 안전 요구사항 명세 방법

항 목	설 명
요구사항 ID	• 안전 요구사항 ID 명세 예) ASSR_F_100_001
요구사항 명칭	• 안전 요구사항 명칭 명세

	• 요구사항 명칭은 요구사항 기능을 대표할 수 있도록 기술
요구사항 설명	• 요구사항이 수행되는 내용에 대해 설명
요구사항 명세	1) 사전조건: 기능을 수행하기 위해 사전에 충족되어야 하는 조건 명세 2) 입력정보: 기능 수행을 위해 입력되는 신호, 데이터 명세 3) 출력정보: 기능 수행 완료 후 출력되는 신호, 데이터 명세 4) 동작사양: 기능 수행을 위한 동작 및 기능 수행을 위한 인터페이스, 동작 흐름 5) 예외처리: 정상적인 동작 이외의 예외적인 상황 및 흐름 명세, 악의적인 조건이나 예외 상황 발생에 따른 처리 조건 등을 명세 6) 사후조건: 기능이 종료된 후 처리 조건 명세 7) 제약사항: 요구사항의 설계, 구현, 테스트 진행 등과 관련한 기술적 제약사항 및 고려 사항 명세
검증방법	• 요구사항을 검증할 수 있는 방법을 명세 • 테스트 케이스 도출 근거를 제시
요구사항 근거	• 해당 안전 요구사항의 근거가 되는 상위 문서 명세
관련 안전 기능	• 해당 안전 요구사항과 관련이 있는 안전 기능 명세

다. 응용 소프트웨어 요구사항 명세서 작성 예시

『응용 소프트웨어 요구사항 도출』활동을 완료한 후 도출 된 요구사항을 명세서 양식에 맞게 작성한다.작성 방법은 다음과 같다.

비고: 본 가이드에서 제시하고 있는 분석 및 작성 방법은 일반적인 작성의 예시이며 적용 환경과 활용 자원에 맞게 변형 및 수정이 가능하다.

(1) 목차 예시

1. 문서개요
- 1.1. 문서의 목적
- 1.2. 참고문헌
- 1.3. 정의 및 약어

2. 안전 표준 준수

(2) 제1장『문서 개요』항목 작성 예시

1. 문서개요

1.1. 문서의 목적

"안전 요구사항 작성 대상 시스템에 대한 설명과 문서의 작성 목적 그리고 관련 인원에 대한 내용을 작성"

1.2. 참고문헌

문서번호	문서버전	문서명
[1] IEC 62061	*2005*	*Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.*
[2] IEC 61511-1	*2016*	*Functional safety – Safety instrumented systems for the process industry sector – Part1: Framework, definitions, systems, hardware and application programming requirements.*

1.3. 용어정의 및 약어

1.3.1. 용어정의

용어	정의

1.3.2. 약어

약어	설명

(3) 제2장『안전 표준 준수』항목 작성 예시

2. 안전 표준 준수

2.1. 도메인 표준 소개

『AAA 안전 시스템 소프트웨어 개발』프로젝트는 제어 시스템 안전 표준인『IEC 61511-1』을 준수한다. 해당 표준에 대한 내용은 하기와 같다.

"표준에 대한 소개: 표준 목차와 간략한 설명"

2.2. 도메인 표준 안전 요구조건 준수

"응용 소프트웨어 안전 요구사항 도출 및 명세 시 안전 표준의 항목들을 준수하고 있는지 여부를 아래와 같이 확인한다."

2.2.1. IEC 61511-1 표준 준수

준수 항목	요구조건	적용 내용
10.3.5.a	응용 프로그램 및 해당 SIL 을 지원하는 안전 기능에 대한 설명이 있는가?	*Ref. 6. 응용 프로그램 안전 요구사항의 어디 참조*
10.3.5.b	안전 시스템의 실시간 성능 및 수신할 모든 트립 신호와 성능 매개 변수는 정의되어 있는가?	*Or 해당 내용에 대한 설명 기술*
10.3.5.c	응용 프로그램의 시퀀스와 시간 지연에 대한 설명이 있는가?	
10.3.5.d	장비 및 운영자 인터페이스에 대한 조작성이 설명되어 있는가?	
…		

(4) 제3장『입력 문서 정보』작성 예시

3. 입력 문서 정보

"입력 문서는 문서 번호, 문서 제목, 개정판 및 날짜와 함께 리스트해야 한다. 특히 입력과 출력 인터페이스 목록, 시스템 단계에서의 안전 요구사항 및 안전 기능에 대한 설명 그리고 응용 소프트웨어와 연계된 각종 신호 및 데이터 시트를 포함한 문서는 필수적으로 반영되어야 한다."

3.1. 입력 문서 리스트

문서번호	문서제목	버전	작성날짜

3.2. 입력문서 체크 항목

"가이드에 작성되어 있는『3.2.3 세부 수행 활동의 [1] 시스템 단계 산출물 확인』항목의 표에 있는 내용들이 입력문서에서 식별되고 있는지를 확인한다."

구 분	식별 대상	식별 문서
(1) 안전 시스템 구성 및 범위	• 이중화 아키텍처 적용 여부 • 이중화에 따른 동기화 방법 적용 여부 • 안전 시스템 안전 기능/비-안전 기능 리스트	*"시스템 아키텍처 설계서"*
(2) 안전 시스템 공통 기능	• Diagnostic 기능 적용 여부 • I/O 메모리 매핑 기능 적용 여부 • 주기적 테스트 기능 적용 여부 • 외부 장치 모니터링 기능 적용 여부	

	• 외부 장치 통신 규격	
(3) 안전 시스템 제약 사항	• 메모리 크기 및 주소 규칙 • 처리 성능 • 응답 시간	
(4) 외부 장치 인터페이스	• 외부 입력 인터페이스 및 신호 • 외부 출력 인터페이스 및 신호	*"시스템 인터페이스 기술서"*

(5) 제4장『안전 시스템 구성』작성 예시

4. 안전 시스템 구성

"응용 소프트웨어가 동작 할 안전 시스템에 대한 내부 외부 구성과 연동 HW 및 SW 에 대한 정보를 기술한다."

4.1. Block Diagram

"안전 시스템이 어떤 외부 장치들과 연결되어 있는지에 대한 Block Diagram 또는 연관 관계를 보이는 RBD 를 작성하거나 또는 참조한다."

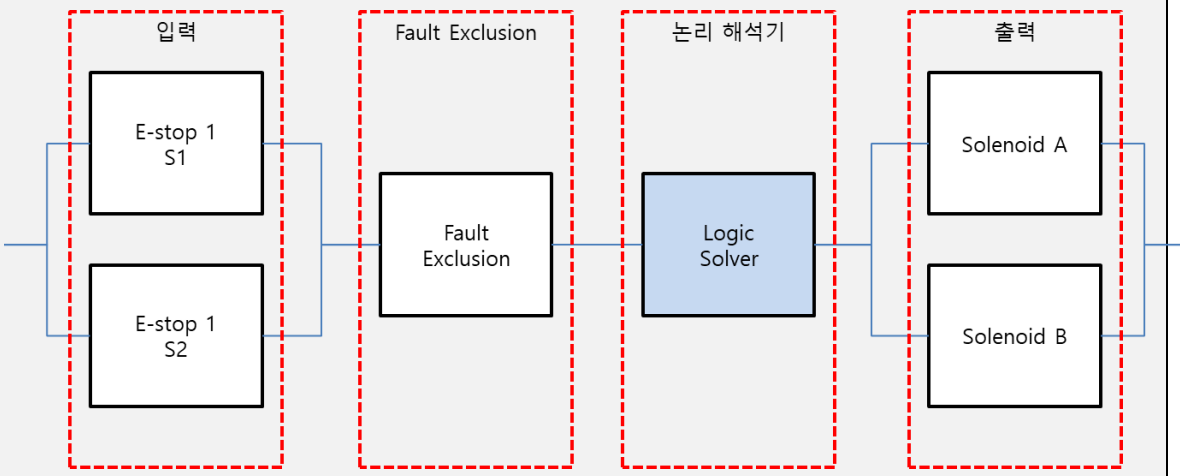


그림. 예시) 안전 시스템 Block Diagram

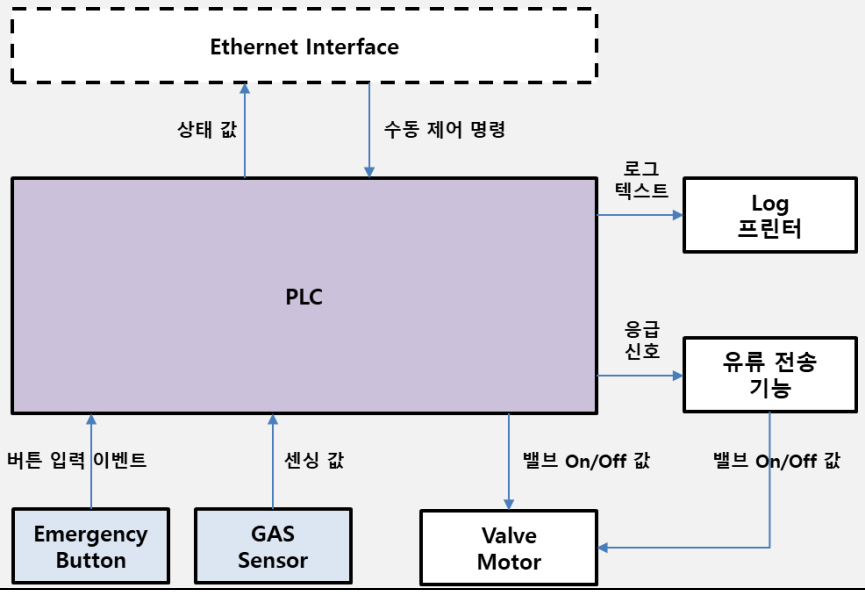


그림. 예시) 안전 시스템 Block Diagram

4.2. 연동 HW 리스트

"4.1 의 Block Diagram 으로부터 식별 된 외부 연동 HW 장치에 대한 설명을 기술한다.

연동장치	인터페이스	설명
Emergency Button	*RS-232*	*비상 상황 발생 시 버튼 이벤트 입력 사용자 인터페이스*
Log 프린터	*Ethernet*	*PLC 운영 로그를 주기적으로 출력하며 Ethernet 을 통해 로그정보를 텍스트 형태로 입력 받는다.*
…		

4.3. 연동 SW 리스트

"안전 시스템과 연계되는 임베디드 SW 에 대한 설명을 기술한다."

연동 SW	설명
상위 MES SW	*안전 시스템의 운영 정보를 확인하고 기능 수행을 제어한다.*

(6) 제5장『상세 안전기능 정보』작성 예시

5. 상세 안전기능

"안전 시스템이 수행해야 할 안전 기능들에 대한 상세 정보를 기술한다."

안전기능 명	SIL	연계 HW 정보	연계 SW 정보	기능 정의	동작 조건	종료 조건	요구 반응시간
"식별 된	*"안전*	*"4.2 에서*	*"4.3 에서*	*"안전*	*"안전*	*"안전*	*"안전*

안전 기능 명칭"	*기능 SIL 등급"*	*식별 된 HW 중 연계 된 HW"*	*식별 된 SW 중 연계 된 SW"*	*기능 설명"*	*기능 동작 조건"*	*기능 종료 조건"*	*기능 반응 시간"*

(7) 제6장『응용 소프트웨어 안전 요구사항』작성 예시

6. 응용 소프트웨어 안전 요구사항

6.1. 응용 소프트웨어 기능 리스트

"가이드의 3.2.『응용 소프트웨어 요구사항 분석 및 명세 단계의 [2] 응용 소프트웨어 요구사항 명세 및 검증의 가. 수행절차』편에서 다루고 있는 항목들을 기반으로 기능 리스트를 기술한다.

요구사항 ID	기능	설명
ASSR-F-001	*응용 소프트웨어 초기 구동*	***전원 인가 시 초기 구동을 진행한다.*** *"(1) 응용 소프트웨어 초기 구동 절차 및 단계별 수행 기능 분석에서 도출 된 내용 기술"*
ASSR-F-002	*응용 소프트웨어 초기 구동 시 고장 확인*	***초기 구동 시 고장 로그를 확인하여 초기화를 계속 수행 할 지 고장 알람을 발생할지를 식별한다.***
…		
ASSR-F-021	*압력 한계점 확인*	***압력이 100 이하일 경우 압력 밸브 닫힘 기능을 호출한다.*** *"(3) 할당 된 응용 소프트웨어 안전 및 비-안전 기능 분석 단계에서 식별 된 안전 기능의 안전 모드에 따라 응용 소프트웨어의 기능 동작 타이밍을 식별하여 구체화 한 내용을 기술"*

…		

6.2. 응용 소프트웨어 안전 요구사항

"6.1 에서 기술한 기능 리스트와 도출 단계에서 식별 된 비-기능 리스트의 개별 항목들을 대상으로 아래의 템플릿에 맞게 작성한다."

항 목	설 명
요구사항 ID	*ASSR_F_021*
요구사항 명칭	• *압력 한계점 확인*
요구사항 설명	• *압력이 100 이하일 경우 압력 밸브 닫힘 기능을 호출한다.*
요구사항 명세	*1) 사전조건* *1. 압력 센서 입력 확인 상태* *2) 입력정보: 압력 수치 (>100)* *3) 출력정보: 압력 밸브 닫힘 신호 출력* *4) 동작사양:* *1. 압력 센서로부터 압력 값 입력* *2. 압력 값이 100 이상인지 확인* *3. 100 이상인 경우 압력 밸브 닫힘 신호 출력* *3-1. 100 이하인 경우 1 번부터 3 번 까지 반복* *5) 예외처리:* *1. 압력 센서 입력 확인 상태가 아닌 경우 알람 발생* *2. 압력 값이 입력 가용 범위인 (-100 ~ 200)을 넘어가는 경우 알람 발생* *6) 사후조건: 압력 밸브 닫힘 신호 출력 후 다시 압력 센서 입력 확인 상태* *7) 제약사항: None*
검증방법	***경계 값 테스트를 통해 압력 센서 값에 따라 해당 모듈이 정상적인 결과를 출력하는지 확인한다.*** ***--(예시)--*** ***(정상 1)*** *1. 90 의 압력 수치 입력* *2. 압력 센서 입력 확인 상태 전이 확인*

	(정상 2) *1. 100 의 압력 수치 입력* *2. 압력 센서 입력 확인 상태 전이 확인* ***(정상 3)*** *1. 101 의 압력 수치 입력* *2. 밸브 닫힘 신호 출력 확인* *…* ***(비정상 1)*** *1. 201 의 압력 수치 입력* *2. 알람 발생 확인* *…*
요구사항 근거	*"3.1 의 입력문서 항목에서 요구사항이 식별된 문서 기술"*
관련 안전 기능	*"5 장의 관련 안전기능 명 기술"*

(8) 제7장『요구사항 점검 항목』작성 예시

7. 요구사항 점검 항목

"가이드의 3.2.『응용 소프트웨어 요구사항 분석 및 명세 단계의 [3] 응용 소프트웨어 요구사항 명세 및 검증의 다. 점검항목』편에서 다루고 있는 내용을 점검항목으로 두고 해당 점검 항목에 대한 준수 유무를 기술한다."

No.	Required information	Comment
01	각 안전 기능이 명확하게 정의되어 있는가?	
02	안전 기능 표준이 글로벌일인가? 로컬인가?	
03	각 안전 기능에는 고유한 식별자(identifier)가 있는가?	
04	각 안전 기능에는 해당 초기 구동 요소 및 최종 요소 태그가 식별되어 있는가?	
05	기능이 low demand 인지 high demand 인지 식별되었는가? (식별해야 하는 동일한 응용 프로그램에서 high	

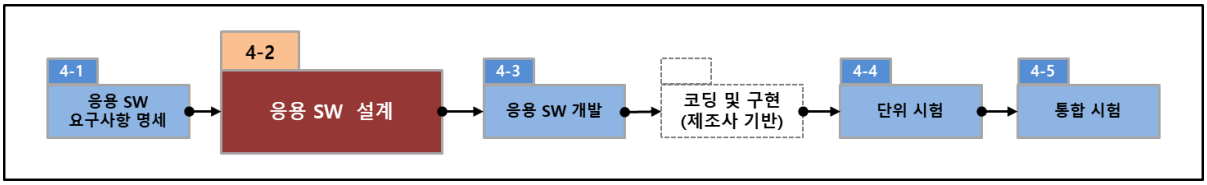
	demand 와 low demand 의 실행에 영향을 미치는 High demand 안전 기능을 식별해야 한다.)	
06	로직 솔버에 대한 PFD 가 제공되고 있는가?	
07	로직 솔버에 대한 응답 시간이 주어졌는가? (가능한 한 빨리 내부 노드간 커뮤니케이션을 식별해야 한다.)	
…		

라. 점검 항목

『응용 소프트웨어 요구사항 분석 및 명세』 활동을 완료한 후 최종 작성 된 『응용 소프트웨어 요구사항 명세서』의 내용을 대상으로 아래의 항목들이 식별되거나 포함되어 있는지를 점검한다.

No.	Required information	Comment
01	각 안전 기능이 명확하게 정의되어 있는가?	
02	안전 기능 표준이 글로벌일인가? 로컬인가?	
03	각 안전 기능에는 고유한 식별자(identifier)가 있는가?	
04	각 안전 기능에는 해당 초기 구동 요소 및 최종 요소 태그가 식별되어 있는가?	
05	기능이 low demand 인지 high demand 인지 식별되었는가? (식별해야 하는 동일한 응용 프로그램에서 high demand 와 low demand 의 실행에 영향을 미치는 High demand 안전 기능을 식별해야 한다.)	
06	로직 솔버에 대한 PFD 가 제공되고 있는가?	
07	로직 솔버에 대한 응답 시간이 주어졌는가? (가능한 한 빨리 내부 노드간 커뮤니케이션을 식별해야 한다.)	
08	트립(Trip) 전원을 차단하거나 트립(Trip)에 전원에 대한 내용이 주어졌는가?	
09	최대 허용 검증 테스트 주기가 주어졌는가?	
10	효과적인 수리 시간이 주어졌는가?	
11	트립 지점(Trip Point)이 SRS 나 다른 문서에서 제공되는가?	

12	래칭(latching, 비-휘발성) 또는 비-래칭(non-latching, 휘발성) 출력 정보가 제공되는가? (Latch 는 메모리 영역이 리셋 되도 정보가 유지되는 것을 말한다.)	
13	수동 활성화(manual activation) 요구사항이 주어졌는가?	
14	시동(Start-up) 또는 기타 운영 모드 작동 요건이 제시되어 있는가?	
15	감지된 고장(Fault)에 대한 대응 동작이 제시되어 있는가?	
16	SIS 의 고장 모드와 원하는 대응(응답)이 있는가? 예) 단일/중복 입력/출력 보드의 채널 또는 보드 고장 식별	
17	SRS 또는 기타 문서에 지정된 최대 허용 오버라이드(overrides) 수가 주어졌는가?	
18	차단(권한 관련)에 대한 제한이 식별되어 있습니까? 얘) 허용되지 않음, 키 스위치, 사용자 권한 등	
19	SRS 또는 기타 문서에서 안전 사용자의 운영에 대한 제한이 식별되어 있는가? (운영에 대한 사용자 권한이 식별되어 있는가)	



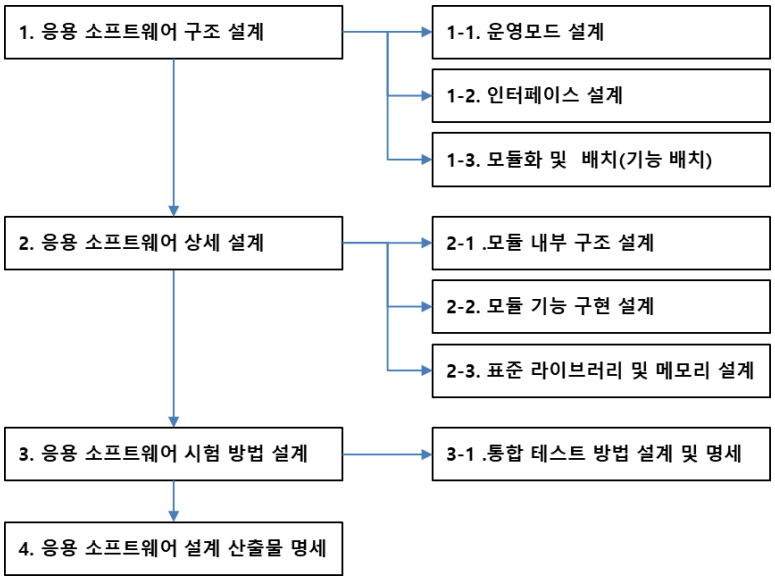
4.2. 응용 소프트웨어 설계

4.2.1. 목적

『응용 소프트웨어 분석 및 명세』 단계에서 식별 된 응용 소프트웨어의 기능 및 비-기능 요구사항을 구현하기 위해 응용 소프트웨어에 할당 된 안전 기능에 대한 구조, 상호 연결 방법, 운영 모드 그리고 세부 수행 흐름 등을 식별하고 이를 문서화 하는 단계로 『응용 소프트웨어 요구사항 분석 및 명세』 단계에서 작성된 산출물을 기반으로 세부 단계 활동을 수행한다.

4.2.2. 활동 단계 개요

구 분	설 명
선행기준	1. 안전 시스템 아키텍처 설계 완료 2. 안전 시스템 안전 기능 식별 완료 3. 응용 소프트웨어 안전 요구사항 식별 완료
입력문서	• 안전 시스템 아키텍처 설계서 • 안전 시스템 하드웨어 아키텍처 설계 제약사항 • 안전 시스템 사용자 매뉴얼 • 응용 소프트웨어 안전 요구사항 명세서 • 응용 소프트웨어 안전 요구사항 추적표

수행흐름	
산 출 물	• 응용 소프트웨어 구조 및 상세 설계서 • 응용 소프트웨어 구조 검증 보고서 • 응용 소프트웨어 요구사항 추적표 (업데이트)
완료기준	1. 응용 소프트웨어 외부 시스템 상호 연결 적용 완료 2. 응용 소프트웨어 운영 모드 및 세부 수행 흐름 적용 완료 2. 응용 소프트웨어 설계서 작성 완료 3. 응용 소프트웨어 구조 추적표 작성 완료

4.2.3. 세부 수행 활동

[1] 응용 소프트웨어 구조 설계

『응용 소프트웨어 요구사항 분석 및 명세』 단계에서 분석한 기능 및 비-기능 요구사항을 기반으로 응용소프트웨어의 운영모드, 기능 세부 모듈과 내/외부 인터페이스 등을 포함한 구조를 설계한다.

가. 수행 절차

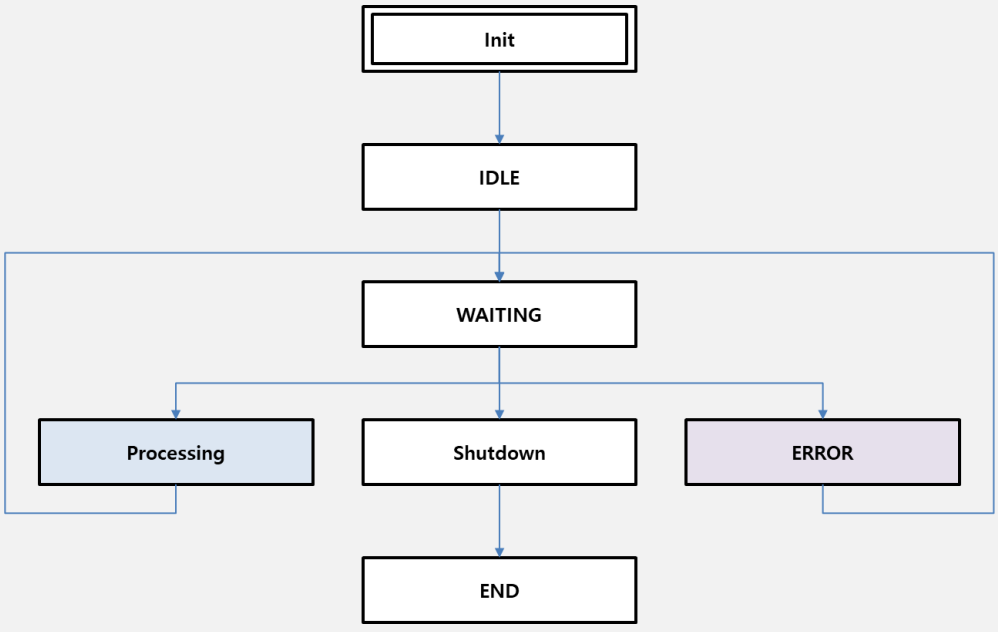
(1) 운영모드 설계

A. 응용 소프트웨어의 초기 구동부터 종료까지의 생명주기 동안 가능한 운영 모드를 식별

B. 운영모드에 따라 응용 소프트웨어의 제어 기능을 식별

A. 응용 소프트웨어 초기 구동과 종료 구동 기간 동안 발생 가능한 운영 모드를 모두 식별하고 이를 응용 소프트웨어의 생명주기 설계에 반영한다.

- ✓ "초기 구동 후 IDLE 상태로 상태가 변경된다."
- ✓ "IDLE 상태에서 200ms 경과 후 Sensor 또는 외부 제어 입력을 받아 수행하는 WAITING 상태로 변경된다.
- ✓ "정상 범위의 Sensor 입력 수집 시 해당 입력을 처리 한 후 다시 WAITING 상태로 변경된다."
- ✓ "비-정상 범위의 Sensor 입력 수집 시 ERROR 상태에서 에러 처리 후 다시 WAITING 상태로 변경된다."
- ✓ "WAITING 상태에서 종료 신호를 받으면 END 상태로 전환하면서 응용 소프트웨어를 종료한다."



B. 운영모드 변경에 따라 응용 소프트웨어가 수행해야 할 제어 기능을 식별한 후 이를 설계에 반영한다.

- ✓ "**Init:** 상태에서는 외부 입력을 받지 않으며, 식별된 초기화 절차를 수행한다."
- ✓ "**IDLE:** 상태에서는 외부 입력을 200ms 동안 외부 신호를 받지 않으며 신호 안정화를 위해 대기한다.
- ✓ "**WAITING:** 상태 진입 시부터 SENSOR 입력과 외부 제어 이벤트를 수신하며, SENSOR 정보 수신 시 값의 범위를 확인 후 Processing과 ERROR 상태로 운영모드를 변경한다."
- ✓ "**Processing:** 정상 범위의 SENSOR 입력을 수신 후 값에 따른 기능을 수행한다."
- ✓ "**ERROR**: SENSOR 입력 값이 정상 범위에 들어오지 않았을 경우 에러 처리 후 로그 파일에 기록한다. 이 후 다시 WAITING 상태로 전환한다."
- ✓ "**Shutdown**: 외부 입력으로 SHUTDOWN 명령 수신 시 모든 상태를 로그 파일에 저장 한 후 종료 절차를 수행한다."
- ✓ 필요 시 순서도를 사용하여 제어 기능 수행 절차를 명세한다.

(2) 인터페이스 설계

A. 외부 입력 및 출력 인터페이스 식별 및 설계

B. HMI 인터페이스 식별 및 설계

C. 기본 기능 및 하부 장치간 인터페이스 식별 및 설계

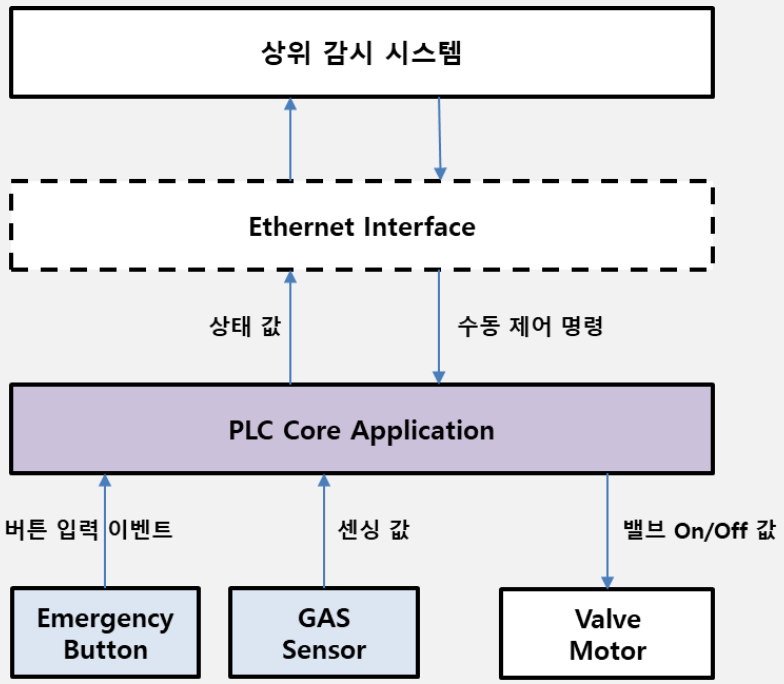
D. 인터페이스 데이터 정의

A. 식별된 외부 입력 및 출력 인터페이스를 기반으로 시스템 경계를 정의하고 이를 설계에 반영한다.

- ✓ "응용 소프트웨어는 GAS Sensor로부터 센싱 값을 입력 받아 특정 범위 이상일 경우 Valve Motor를 기동한다."
- ✓ "응용 소프트웨어는 Emergency Button으로부터 버튼 입력 이벤트를

받아 Valve Motor를 기동한다."

- ✓ "응용 소프트웨어는 Log 프린터로 로그 기록을 보내 주기적으로 출력한다."
- ✓ "응용 소프트웨어는 GAS Sensor 값을 주기적으로 Ethernet Interface를 통해 상위 감시 시스템으로 상태 값을 전달한다."
- ✓ "상위 감시 시스템은 Ethernet Interface를 통해 응용 소프트웨어로 Valve Motor 수동 제어 명령을 보낼 수 있다."
- ✓ 식별 된 사항을 기반으로 아래와 같이 응용 소프트웨어의 경계와 외부 입출력 정보를 정의하고 설계에 반영한다.

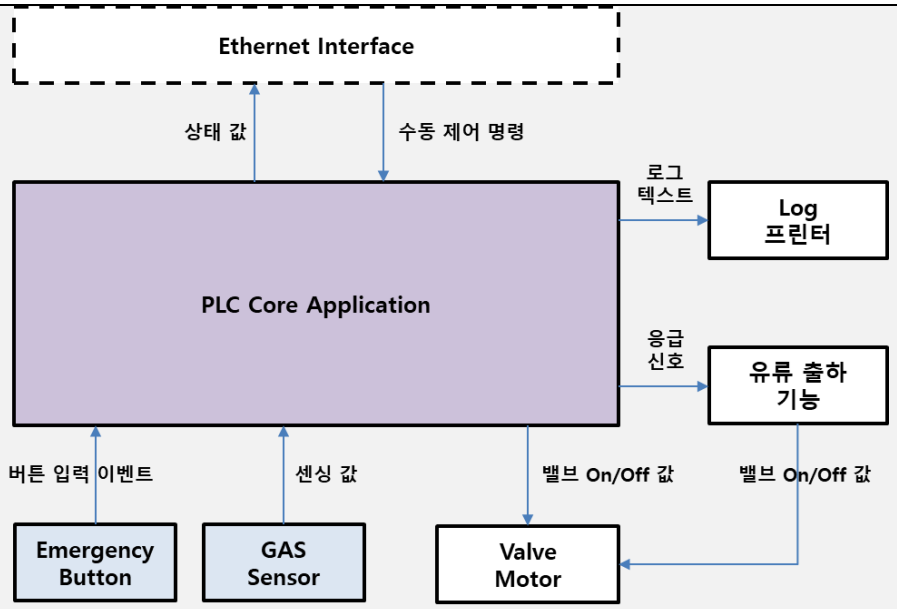


B. 외부 시스템 이외에 응용 소프트웨어가 포함된 PLC 장비 자체에 연결된 HMI에 대한 입출력 신호를 식별하고 이를 설계에 반영한다.

- ✓ "**ESC 버튼**: 설정 화면에서 빠져나온다."
- ✓ "**SET 버튼**: 측정 값을 설정하기 위한 화면으로 진입한다.
- ✓ "**ENT 버튼**: 숫자 패드로 입력한 값을 설정 값으로 입력한다."
- ✓ 사용 되는 모든 HMI에 대한 정보를 식별한다.

C. 기본 기능 및 하부 장치간 인터페이스를 식별하고 이를 설계에 반영한다.

- ✓ "유류 출하 기능: 저장 탱크로 유류를 입하 하기 위한 기능으로 기능 수행 시 Valve Motor를 On 하여 유류를 입하한다.
- ✓ Emergency Button으로부터 응급 신호 입력 시 PLC Core Application은 Valve Motor를 Off 하고 유류 전송 기능으로 응급 신호 발생 상황을 전달하여 유류 전송 기능이 정상적으로 멈추고 안정화 이후 정상 동작 할 수 있도록 한다.
- ✓ PLC Core Application은 감시 상태를 주기적으로 로그 텍스트를 Log 프린터로 전달하여 감시 상황을 출력 할 수 있도록 한다.



D. 식별된 인터페이스의 신호 및 데이터를 정의한다.

- ✓ "외부 통신 인터페이스, 하위 시스템 인터페이스, 기본 기능 인터페이스, HMI 인터페이스 등 식별 된 모든 인터페이스에서 사용될 입력/출력 신호를 식별한다."
- ✓ 신호는 식별 시 이름, 기능 및 역할, 데이터 타입, 데이터 발생지, 데이터 종착지를 명시해야 한다.
- ✓ 식별된 데이터는 상세 설계 시 변수로 변환된다.
- ✓ 필요시 이 단계에서부터 변수 네이밍 규칙에 맞게 식별하는 것도 가능하다.

I/O	기능 및 역할	타입	From	To
상태 값	PLC 에서 수집한 GAS Sensor 값을 500ms 마다 상위 시스템으로 전달한다.	INTEGER	상위 시스템	PLC
수동 제어 명령	상위 시스템에서 PLC 로 전달하는 명령으로 문자열로 구성되며, 밸브의 On/Off 와 현재 상태 값 전송 등을 수행하도록 한다.	STRING	상위 시스템	PLC
로그 텍스트	Log 프린터로 PLC 로그 정보를 전달하며, 문자열 형태로 구성되어 있으며 5 분마다 한번씩 전달	STRING	PLC	Log 프린터

	한다.			
응급 신호	유류 출하 기능으로 응급 상황 발생 여부를 전달하며, 응급 상황 발생 시 '1', 해제 시 '0', 예비위험 시 '2' 값을 전달한다.	INTEGER	PLC	유류 출하 기능
밸브 On/Off 값	밸브의 On/Off 를 전달하며 유류량 제어가 아닌 밸브의 On/Off 만을 전달하며 밸브 Open 시 On, Close 시 Off 값을 BOOL 값으로 전달한다.	BOOL	PLC 유류 출하 기능	Valve Motor
버튼 입력 이벤트	Emergency Button 입력 여부를 전달하며 BOOL 값으로 버튼 입력 시 True, 해제 시 False 값을 전달한다.	BOOL	Emergency Button	PLC
센싱 값	GAS Sensor 로부터 입력 받는 값으로 측정 된 Sensor 정보를 실수 형태로 전달한다.	FLOAT	GAS Sensor	PLC

(3) 모듈화 및 배치

A. 안전 시스템 기본 기능 모듈화 및 배치

B. 타이밍 및 메모리 처리 기능 모듈화 및 배치

C. 진단 및 결함 탐지 기능 모듈화 및 배치

D. 알람 기능 모듈화 및 배치

E. 리셋 기능 모듈화 및 배치

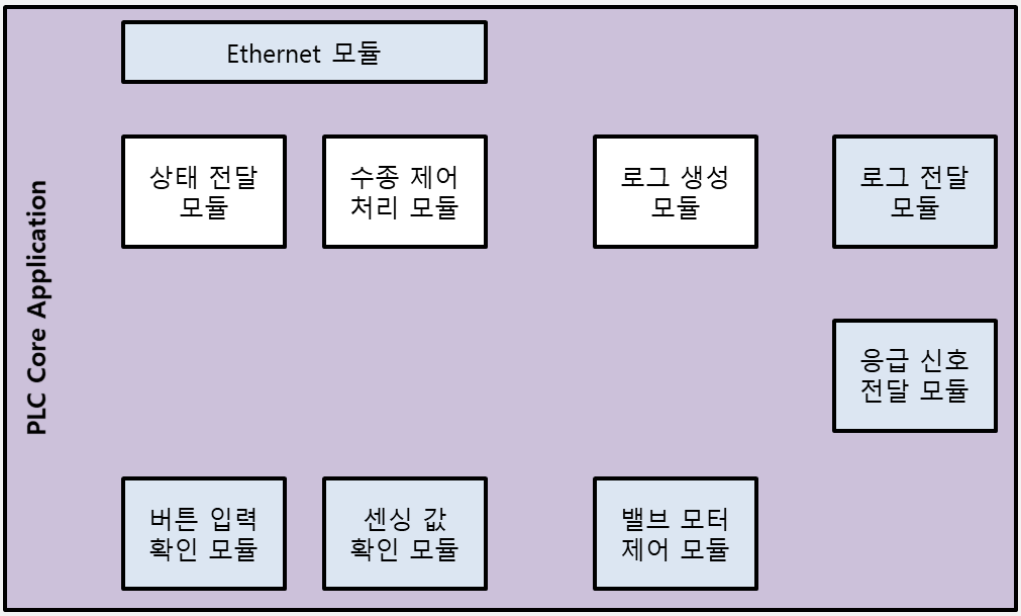
F. 온/오프라인 테스트 기능 모듈화 및 배치

G. 최종 응용 소프트웨어 배치 작성

H. 다중화 구조 적용 여부 확인 후 필요시 적용한다.

A. 안전 시스템을 구성할 기능들을 배치하고 필요시 인터페이스 처리 기능을 모듈화 하여 설계에 반영한다.

- ✓ "요구사항 명세 중 기능 요구사항을 기반으로 모듈화 한다."
- ✓ "인터페이스를 처리 할 기능을 모듈화 한다."
- ✓ "인터페이스의 경우 외부 상위 시스템, 하위 시스템, HMI, 입력 장치, 출력 장치를 모두 개별적으로 식별한 후 필요 시 처리 모듈을 통합한다."

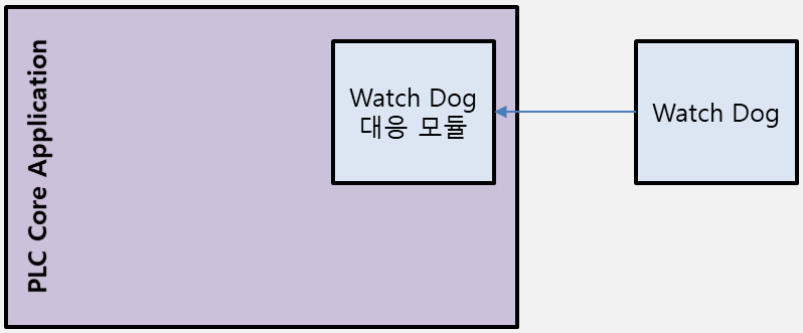


B. 기능 요구사항에서 식별되지 않은 경우 타이밍 및 메모리 관련 기능을 추가적으로 모듈화 하여 설계에 반영한다.

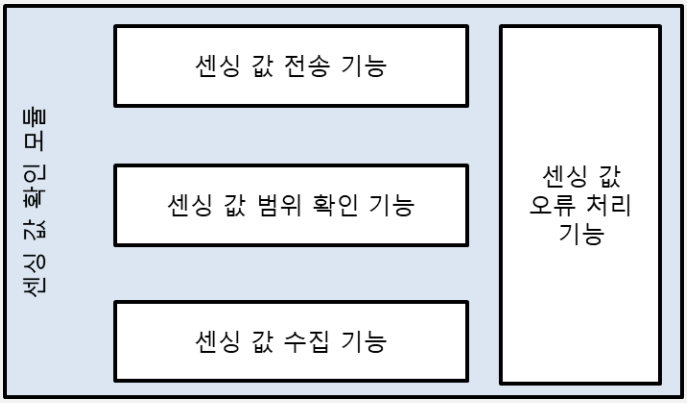
- ✓ "상태 값을 500ms 주기로 상위 시스템으로 전달해야 하므로 주기적인 타이밍 체크 모듈 이 필요하다."
- ✓ "입력과 출력에 대한 값을 메모리를 통해 전달하기 때문에 메모리 처리 모듈이 필요하다."
- ✓ "이를 설계에 반영한다."

C. 진단 기능과 하부 장치 및 인터페이스 데이터 결함 탐지 기능을 모듈화 하여 설계에 반영한다.

- ✓ "Watch Dog을 사용하여 응용 소프트웨어를 1초 단위로 진단한다."

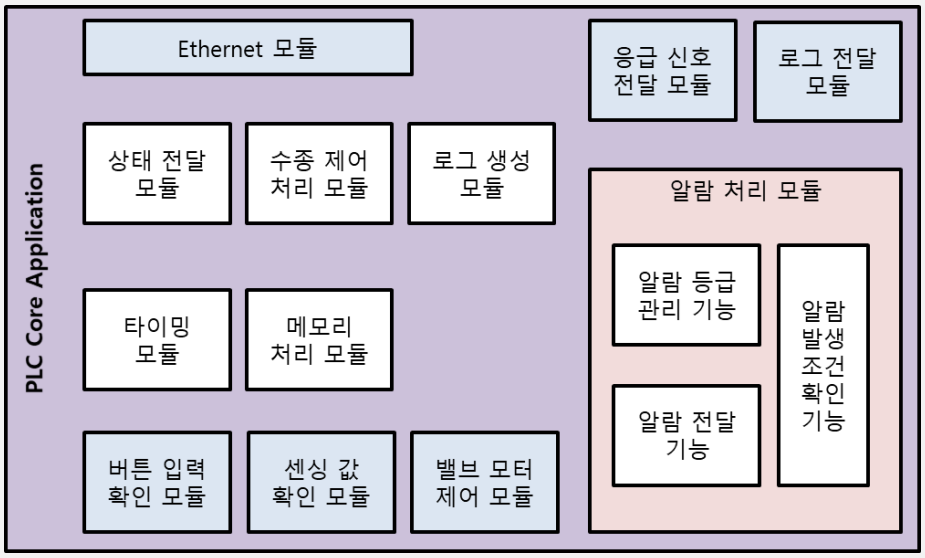


- ✓ "Ethernet 모듈과 밸브 모터 제어 모듈 등 하부 장치를 1초 단위로 진단한다."
- ✓ "GAS Sensor로부터 읽어 오는 FLOAT 값의 범위를 체크하여 가용 여부를 확인한다."
- ✓ "응급 신호 값이 정상 범위의 값인지 확인 후 전달해야 한다."
- ✓ "Emergency Button 으로부터 읽어 오는 신호가 BOOL 인지 체크하여 잘못 된 신호로 인해 오동작이 발생하지 않도록 한다."



D. 알람 기능의 경우 별도로 알람 발생 조건, 등급 등을 정의하여 설계에 반영한다.

- ✓ "알람 기능은 별도의 모듈로 관리하며, 필요한 경우 외부 시스템으로 분류한다."
- ✓ "알람 발생 조건은 검증되어야 하며, 발생 알람은 기록되어야 한다."
- ✓ "알람 발생 시 상위 시스템으로 즉각 전달되어야 한다."



E. 리셋 기능을 설계에 반영한다.

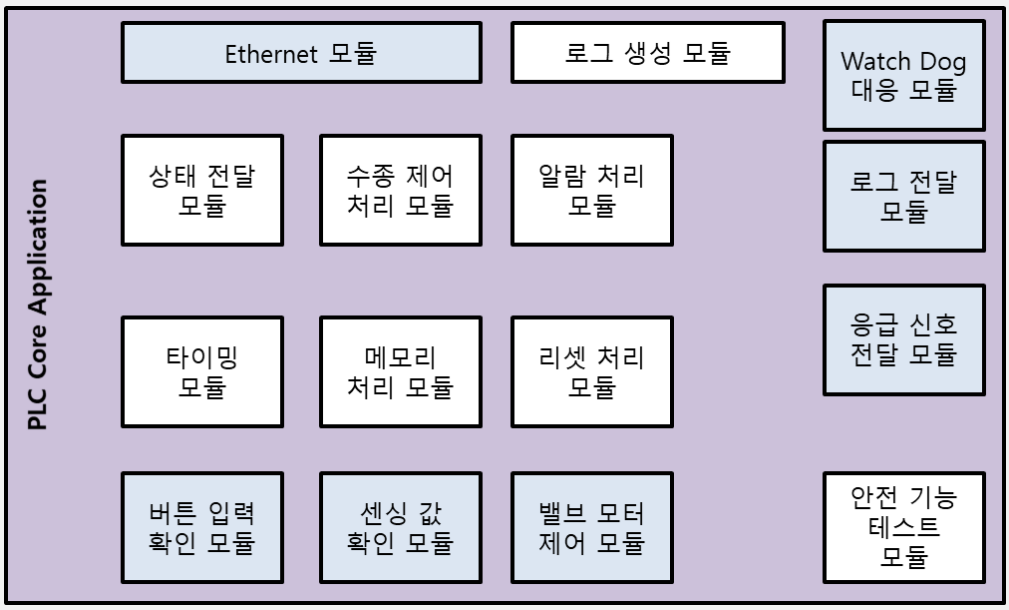
- ✓ "별도의 설계 모듈을 생성하여 초기화 기능을 수행할 수 있도록 한다."
- ✓ "리셋 후 시스템 고장 상태 확인 기능을 설계에 반영해야 한다."
- ✓ "고장으로 인한 리셋 또는 리셋 시 고장 정보 확인 시 응용 소프트웨어는 정상 기능을 수행하지 않고 고장 처리 대기 상태를 유지해야 한다."

F. 안전 기능에 대한 온/오프라인 테스트 기능을 모듈화 하여 설계에 반영한다.

- ✓ "안전 기능이 수행 가능 여부를 온라인으로 주기적 테스트 해야 한다."
- ✓ "필요한 경우 오프라인 상태에서 안전 기능의 수행 가능 여부를 확인할 수 있어야 하며 이 기능이 설계에 반영되어야 한다."

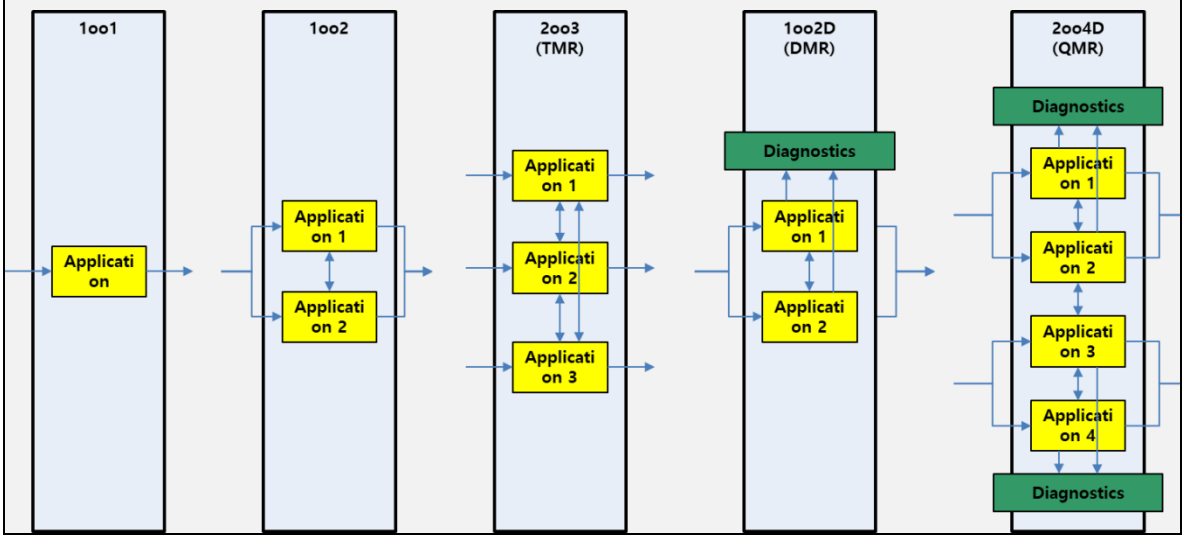
G. 모듈화 및 기능 배치를 기반으로 최종 배치도를 작성한다.

- ✓ "외부 인터페이스를 포함하여 모든 내부 모듈을 배치도로 작성한다."
- ✓ "필요한 경우 내부 데이터 및 제어 흐름을 표기한다."



H. 필요한 경우 다중화 구성을 적용한다.

- ✓ "수집 모듈과 외부 커뮤니케이션 모듈의 경우 안전성이 높은 경우 다중화 구성한다."
- ✓ "다중화의 경우 안전성을 높일 수 있지만 데이터의 동기화 절차 등에



서 오류가 발생할 가능성이 높아지므로 설계 시 주의가 필요하다.

나. 점검 항목

No.	Required information	Comment
01	설계에 필요한 입력 문서들은 식별되고 반영되었는가?	
02	운영 모드는 설계에 반영되었는가?	
03	응용 소프트웨어의 생명 주기는 운영모드와 함께 식별되었는가?	
04	운영 모드에 따른 제어 기능은 식별되었는가?	
05	외부 입력 및 출력 인터페이스는 모두 식별되었는가?	
06	HMI 인터페이스는 식별되었는가?	
07	기본 기능 및 하부 장치간 인터페이스는 식별되었는가?	
08	인터페이스에서 사용하는 데이터는 식별되었는가?	
09	인터페이스를 구분한 시스템 Boundary Diagram 은 작성되었는가?	
10	모든 기능이 모듈화 되고 식별되었는가?	
11	스캔 타임 등 타이밍 및 메모리 할당 방법이 식별되었는가?	
12	진단 및 결함 탐지 기능이 모듈화 되었는가?	
13	알람 기능이 모듈화 되었는가?	
14	리셋 기능이 모듈화 되었는가?	
15	온/오프라인 테스트 기능이 모듈화 되었는가?	

[2] 응용 소프트웨어 상세 설계

『응용 소프트웨어 구조 설계』 단계에서 설계한 응용 소프트웨어의 기능, 인터페이스와 구조를 기반으로 세부 모듈들에 대한 상세 설계를 수행한다. 상세 설계에는 스캔타임과 관련된 타이밍 제약과 스캔 타임 내에서 수행해야 할 기능 절차 등을 설계하고, 메모리 처리와 표준 라이브러리 사용에 대한 설명을 명세한다.

가. 수행 절차

(1) 모듈 내부 구조 설계

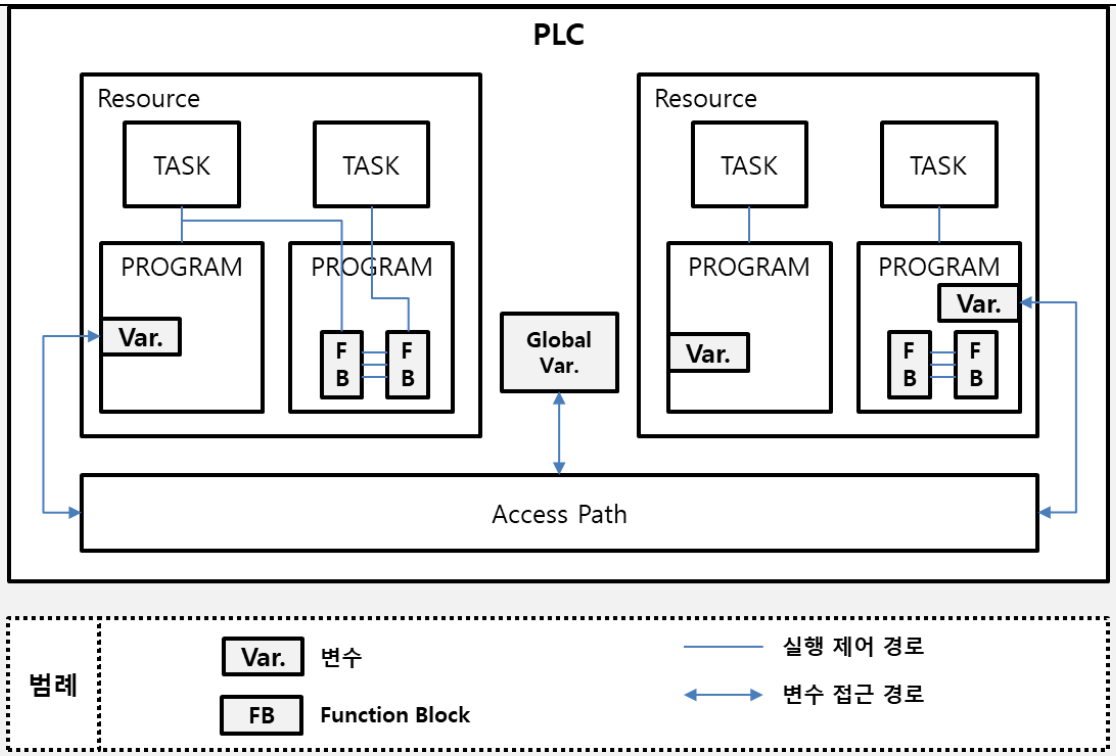
A. PLC 응용 소프트웨어 모델 기반 모듈화 및 기능 식별

B. 응용 소프트웨어 구조 설계 단계에서 식별 된 모듈의 세부 기능 단위 식별 및 설계 반영

C. 모듈 간 데이터 및 제어 흐름 식별 및 설계 반영

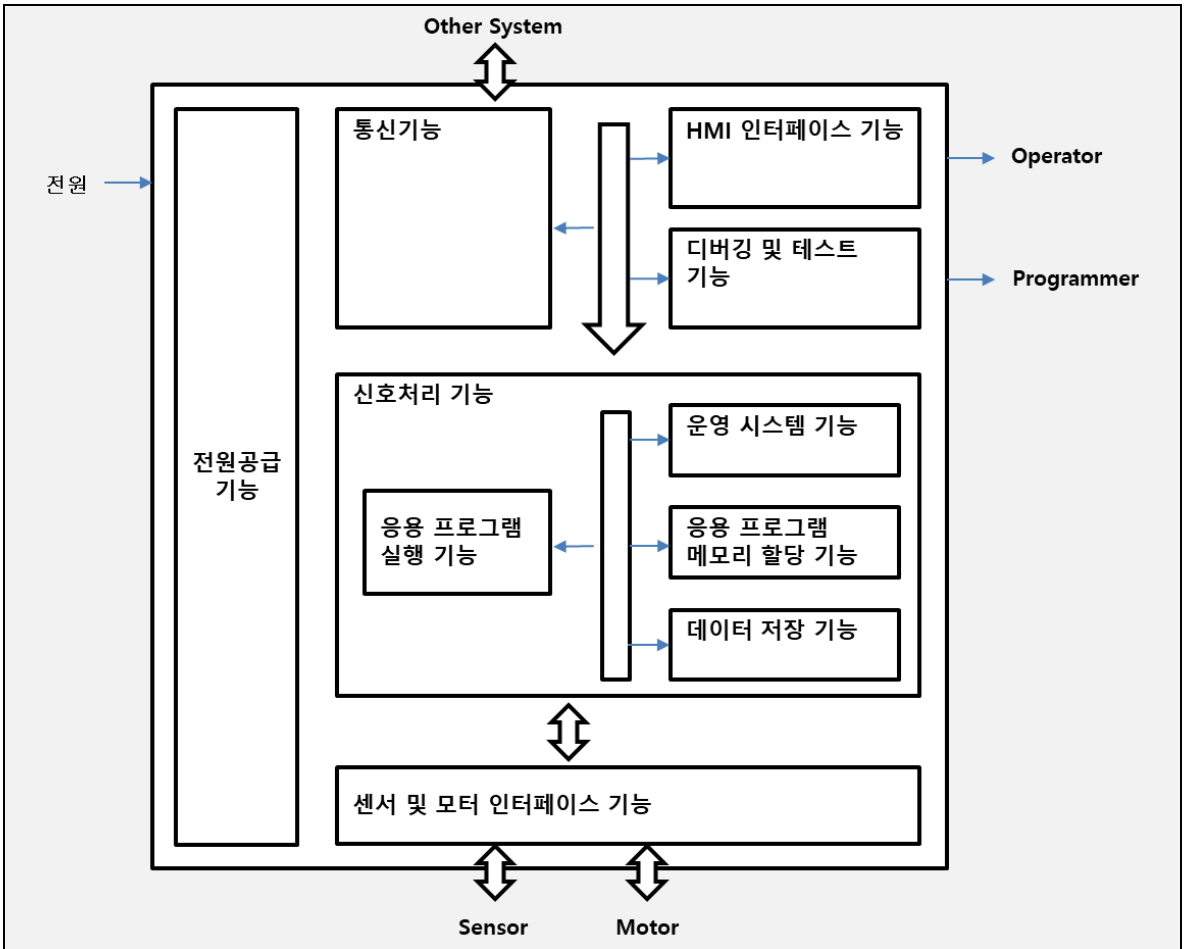
A. PLC (LVL) 기반 응용 소프트웨어의 모델에 따라 모듈을 세부 기능 단위로 식별하여 설계에 반영한다.

- ✓ "PLC 응용 소프트웨어는 다수의 프로그램으로 구성된다. (모듈)"
- ✓ "프로그램은 다수의 Function Block으로 구성된다. (기능)"
- ✓ "필요한 경우 단일 프로그램으로 기능을 수행할 수도 있다."
- ✓ "프로그램은 로컬 변수를 가질 수 있다."
- ✓ "PLC 전체의 공용 변수를 지정하여 사용할 수 있다."
- ✓ "변수는 접근 경로를 통해서만 접근이 가능하다."



B. 구조 설계 단계에서 식별 된 모듈을 세부 기능 단위로 식별하고 이를 설계에 반영한다.

- ✓ "모듈화 원칙에 따라 응집도를 높일 수 있도록 세분화 한다."
- ✓ "모듈화 원칙에 따라 결합도를 낮일 수 있도록 기능을 배분한다."
- ✓ "내부 모듈간 데이터 및 제어 흐름을 설계한다.



- ✓ "안전 기능과 비-안전 기능을 명확하게 구분하여 설계한다."
- ✓ "비-안전 기능이 안전 기능에 영향을 주지 않도록 설계하며, 만약 연결관계가 있을 경우 영향이 없음을 입증 해야 한다."
- ✓ "알람 기능은 별도의 모듈로 구성한다."
- ✓ "Watch Dog 모듈은 별도의 프로세스로 구성한다."

C. 내부 모듈간 데이터 입출력을 식별하고 세부적인 타입까지 식별하여 설계에 반영한다.

- ✓ "구조 설계에서 식별한 외부 인터페이스 뿐만 아니라 내부 모듈간 데이터의 입출력을 식별하고 가급적 타입과 범위까지 식별한다." (외부 인터페이스 식별 활동과 동일)
- ✓ "각 단위 프로그램의 상태 변화를 식별하고 이에 대한 테이블을 작성

한다."

No.	상태		설명
1	Init		프로그램 초기화 상태
2	IDLE		프로그램 초기화 중 IDLE 상태
3	WAITNG		프로그램 대기 상태
4	프로그램 상태	Processing	프로그램에 에러가 없거나 허용 가능한 고장만 발생한 상태
5		ERROR	프로그램에 에러가 발생한 상태
6	Shutdown		프로그램 종료 진행 상태
7	END		프로그램 종료 상태

✓ 응용 소프트웨어에서 사용할 공용 변수를 식별한다.

(2) 모듈 기능 상세 설계

A. 스캔 타이밍 동안 수행 해야 할 기능을 명세한다.

B. 데이터 별 타이밍을 정의한다.

C. 상세 기능을 정의한다.

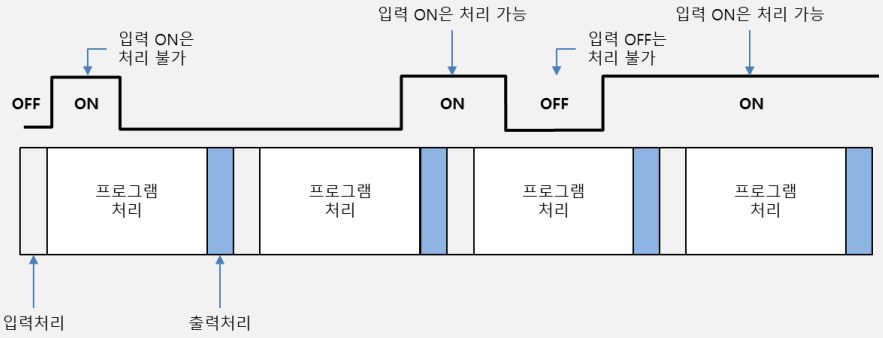
D. 알람 코드 및 알람 처리 기능 식별

A. 응용 소프트웨어에서 사용할 스캔 타이밍을 적용하여 기능 수행을 명세한다.

✓ "모듈의 기능 수행에 적합한 프로그램 스캔 방식을 식별한다."

반복 연산방식	▪ 작성된 순서대로 처음부터 마지막 스텝까지 반복적으로 프로그램을 수행 ▪ 스캔(Scan) 처리 방식이라 함 ▪ 가장 널리 사용되는 PLC 프로그램 처리방식
고정주기 연산방식	▪ 반복연산 프로그램을 정해진 시간마다 실행 ▪ 프로그램을 모두 수행한 후 대기하다가, 정해진 시간이 되면 프로그램 처리 재개 ▪ 입출력 갱신과 동기를 맞추어 프로그램 실행
인터럽트 연산방식	▪ 반복 연산방식으로 프로그램 처리 도중 우선 처리 프로그램이 있는 경우 해당 프로그램 실행 ▪ 긴급 상황을 알려주는 입력 신호를 추가 설치 (타이머 인터럽트, 외부 접점 신호) ▪ 디바이스의 상태 변화에 따라 기동하는 처리 방식도 있음

✓ "입력 신호 처리 특성을 적용한다."

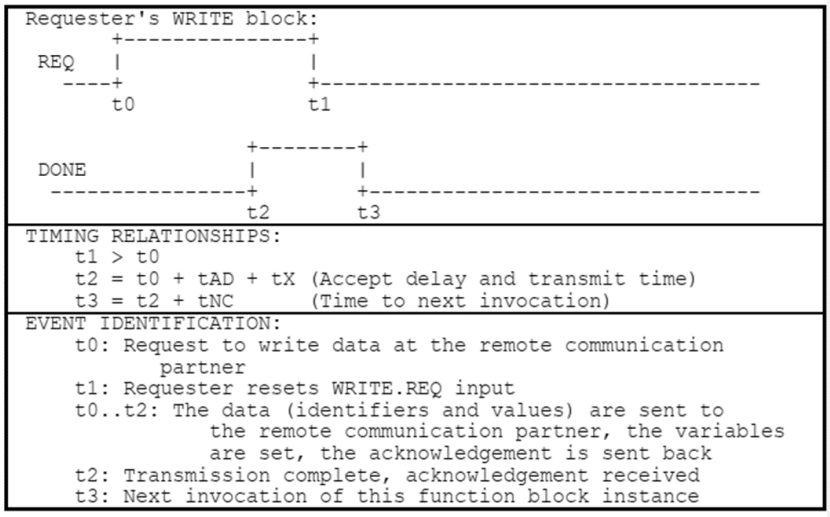


B. 모듈 별 데이터(변수)의 타이밍을 정의한다.

✓ "변수 신호에 대한 타이밍 다이어그램을 작성한다."

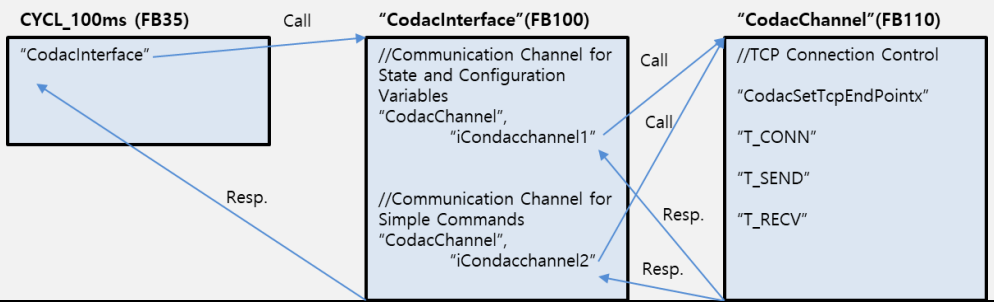
✓ "변수 타이밍 관계를 수식으로 작성한다."

✓ "타이밍 ID를 정의한다."

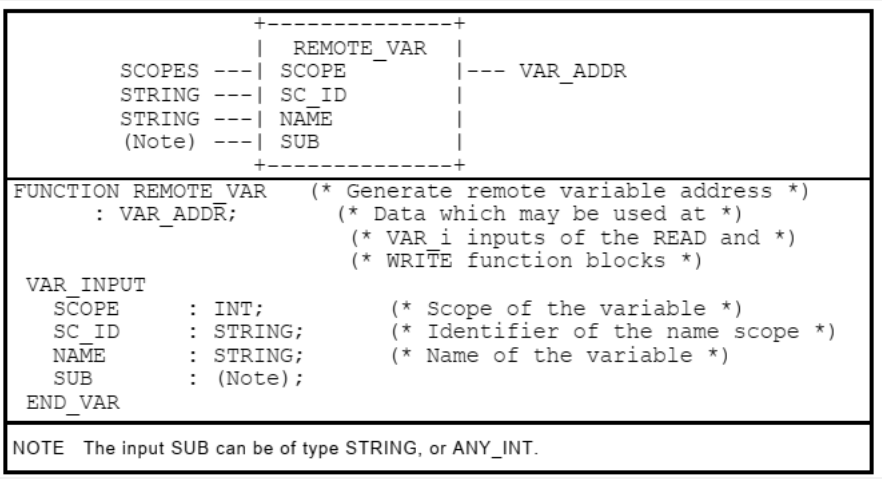


C. 상세 기능을 정의한다.

✓ "스캔 타임 동안 수행 할 세부 기능들을 정의한다."



✓ "세부 기능을 상세하게 정의한다."



```
                  +--------------+
                  |  REMOTE_VAR  |
        SCOPES ---| SCOPE        |--- VAR_ADDR
        STRING ---| SC_ID        |
        STRING ---| NAME         |
        (Note) ---| SUB          |
                  +--------------+
FUNCTION REMOTE_VAR    (* Generate remote variable address *)
      : VAR_ADDR;        (* Data which may be used at *)
                          (* VAR_i inputs of the READ and *)
                          (* WRITE function blocks *)
 VAR_INPUT
   SCOPE      : INT;          (* Scope of the variable *)
   SC_ID      : STRING;       (* Identifier of the name scope *)
   NAME       : STRING;       (* Name of the variable *)
   SUB        : (Note);
 END_VAR
NOTE  The input SUB can be of type STRING, or ANY_INT.
```

D. 알람 코드 및 알람 처리 기능 식별한다.

✓ "시스템 및 하드웨어에서 정의한 고장 및 알람 코드를 확인한다."

✓ "설계단계에서 식별한 알람 발생 조건과 종료 조건을 확인한다."

✓ "알람 발생 조건과 종료 조건에 맞는 처리 알고리즘을 정의한다."

✓ "알람 리포트 기능을 정의한다."

(3) 표준 라이브러리 및 메모리 처리 설계

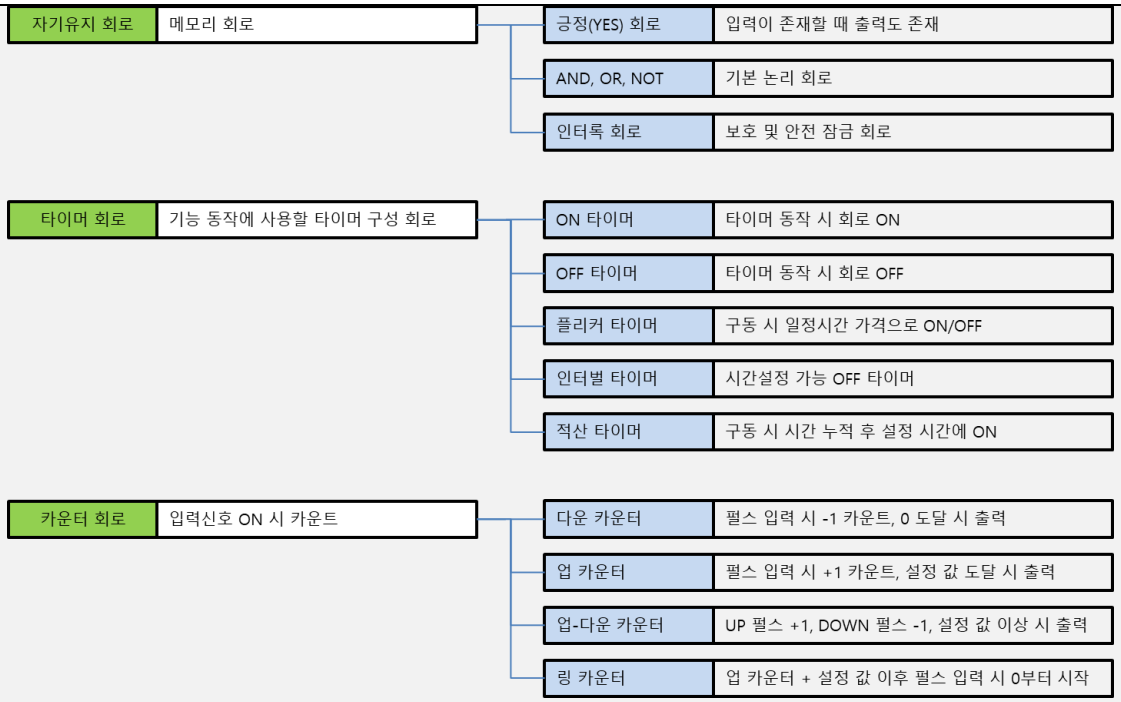
A. 표준 라이브러리 사용 명세

B. 메모리 할당 방법 명세

A. 표준 라이브러리와 데이터 타입을 사용한 경우 해당 라이브러리의와 데이터 타입의 사용 방법과 범위를 설계에 명세한다.

✓ "PLC 응용 소프트웨어 개발 시 제조사에서 제공하는 라이브러리를 사용한 경우 해당 라이브러리의 사용 방법과 범위를 명세한다."

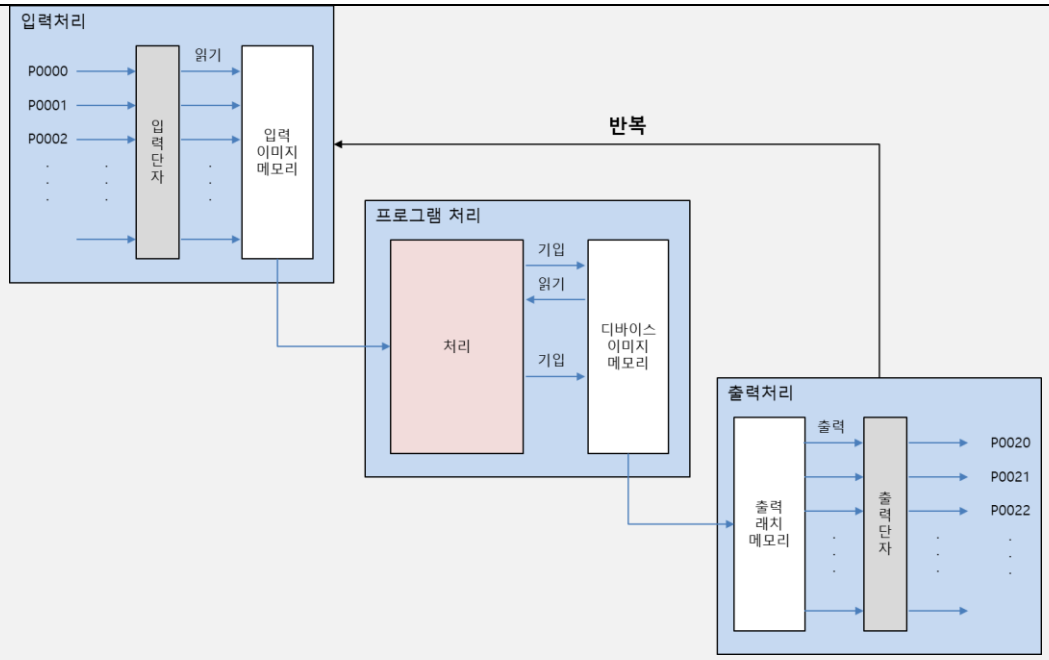
✓ "데이터 타입은 아래의 표준 라이브러리만을 사용하여 설계한다."



- ✓ "필요한 경우 단일 프로그램으로 기능을 수행할 수도 있다."
- ✓ "프로그램은 로컬 변수를 가질 수 있다."
- ✓ "PLC 전체의 공용 변수를 지정하여 사용할 수 있다."
- ✓ "변수는 접근 경로를 통해서만 접근이 가능하다."

B. 응용 소프트웨어의 메모리 할당 방법을 설계에 명세한다.

- ✓ 입력과 출력에 대한 메모리 사용 방법을 식별하여 적용한다.



✓ "데이터 범위와 무결성 검사 방법을 식별한다."

✓ "입력 데이터에 대한 데이터 범위와 출력 데이터에 대한 데이터 무결성 체크를 기능의 수행 절차로 식별해야 한다."

나. 점검 항목

No.	Required information	Comment
01	모듈 별 상태 변화는 식별되었는가?	
02	모듈 별 변수 타이밍은 식별되었는가?	
03	전역 변수는 식별되었는가?	
04	모듈 별 세부 기능에 대한 Function Block 은 식별되었는가?	
05	안전과 비-안전 기능은 모두 식별되고 모듈화 되었는가?	
06	내부 및 외부 진단 모듈 및 기능은 식별되었는가?	
07	데이터 무결성 검사 방법은 적용되었는가?	
08	내부 모듈 간 데이터 입/출력은 식별되었는가?	
09	알람 처리 기능 모듈은 식별되었는가?	
10	모든 기능이 모듈화 되고 식별되었는가?	
11	안전 기능 실패에 대한 관리 기능은 식별되었는가?	
12	안전 기능 온/오프라인 테스트 기능 모듈은 식별되었는가?	

[3] 응용 소프트웨어 시험 방법 설계

『응용 소프트웨어 구조 및 상세 설계』 단계에서 도출 된 구조와 상세 기능을 명세서 양식에 맞게 작성한다. 작성 방법은 다음과 같다.

비고: 본 가이드에서 제시하고 있는 분석 및 작성 방법은 일반적인 작성의 예시이며 적용 환경과 활용 자원에 맞게 변형 및 수정이 가능하다.

가. 수행 절차

(1) 응용 소프트웨어 구조 분석 결과를 기반으로 응용 소프트웨어의 구성도를 작성한다.

A. 『응용 소프트웨어 설계 명세서』에 응용 소프트웨어의 Boundary Diagram 명세

B. 외부 인터페이스 명세

C. 내부 모듈 구조 명세

(2) 응용 소프트웨어 모듈 별 기능을 명세한다.

A. 모듈 별 스캔 타이밍 동안 수행 해야 할 기능 명세

B. 데이터 별 타이밍을 명세

C. 상세 기능 및 처리 순서 명세

D. 알람 코드 및 알람 처리 기능을 명세

나. 응용 소프트웨어 설계 명세서 작성 예시

『응용 소프트웨어 설계』 활동을 완료한 후 도출 된 구조와 상세 기능 설계를 명세서 양식에 맞게 작성한다. 작성 방법은 다음과 같다.

(1) 목차 예시

1. 문서개요

1.1. 문서의 목적

(2) 제1장『문서 개요』항목 작성 예시

1. 문서개요

1.1. 문서의 목적

"응용 소프트웨어 설계에 대한 설명과 문서의 작성 목적 그리고 관련 인원에 대한 내용을 작성"

1.2. 참고문헌

문서번호	문서버전	문서명
[1] IEC 62061	*2005*	*Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.*
[2] IEC 61511-1	*2016*	*Functional safety – Safety instrumented systems for the process industry sector – Part1: Framework, definitions, systems, hardware and application programming requirements.*

1.3. 용어정의 및 약어

1.3.1. 용어정의

용어	정의

1.3.2. 약어

약어	설명

(3) 제2장『입력 문서 정보』작성 예시

3. 입력 문서 정보

"입력 문서는 문서 번호, 문서 제목, 개정판 및 날짜와 함께 리스트해야 한다. 특히 입력과 출력 인터페이스 목록, 시스템 단계에서의 안전 요구사항 및 안전 기능에 대한 설명 그리고 응용 소프트웨어와 연계된 각종 신호 및 데이터 시트를 포함한 문서는 필수적으로 반영되어야 한다."

3.1. 입력 문서 리스트

문서번호	문서제목	버전	작성날짜

3.2. 입력문서 체크 항목

"응용 소프트웨어 설계 단계에서 식별한 항목들의 출처 문서를 기술한다."

(4) 제3장『응용 소프트웨어 구성』작성 예시

3. 응용 소프트웨어 구성

"응용 소프트웨어의 외부 환경과 인터페이스 및 데이터를 기술하고, 내부 기능 모듈 구성도를 작성한다."

3.1. Boundary Diagram

"응용 소프트웨어 구조 분석 단계에서 식별한 외부 환경 중 연관관계가 있는 인터페이스를 식별하고 이를 도식화 하여 작성한다."

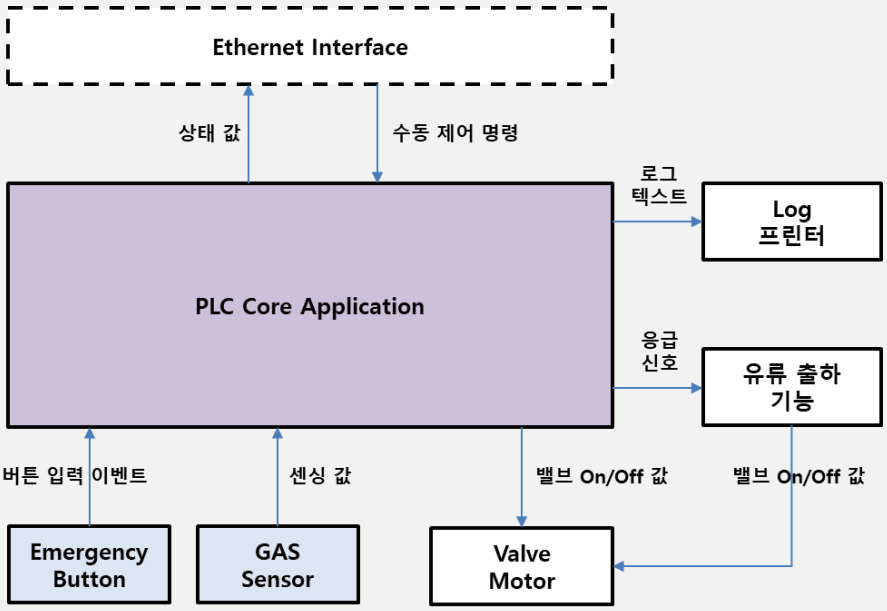


그림. 예시) 응용 소프트웨어 Boundary Diagram

3.2. 외부 인터페이스 및 데이터 정의

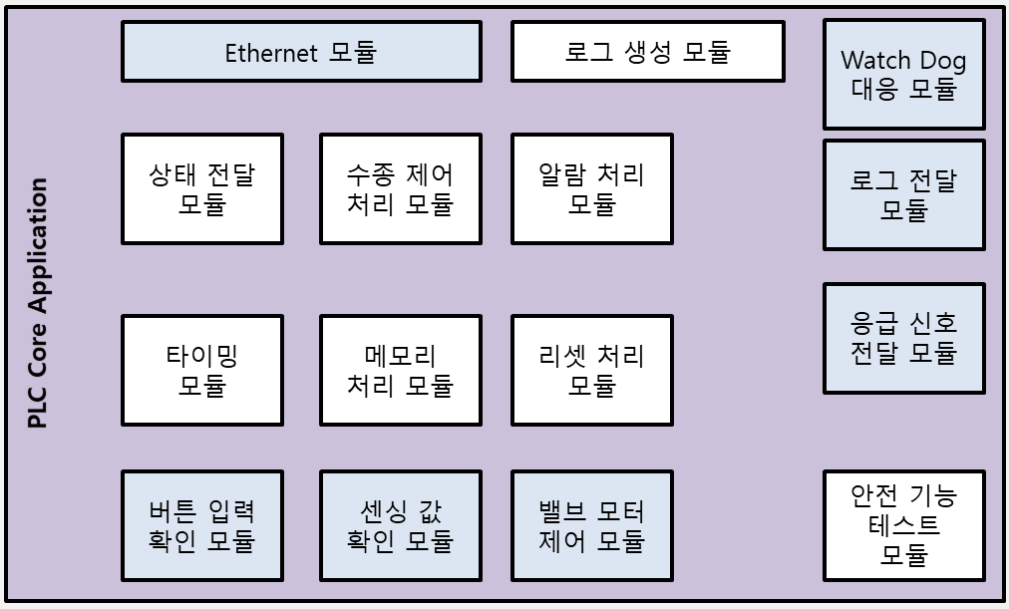
"3.1 에서 식별 된 외부 인터페이스와 데이터에 대한 설명을 기술한다.

I/O	기능 및 역할	타입	From	To
상태 값	*PLC 에서 수집한 GAS Sensor 값을 500ms 마다 상위 시스템으로 전달한다.*	*INTEGER*	*상위 시스템*	*PL*

수동 제어 명령	*상위 시스템에서 PLC로 전달하는 명령으로 문자열로 구성되며, 밸브의 On/Off와 현재 상태 값 전송 등을 수행하도록 한다.*	*STRING*	*상위 시스템*	*PLC*
로그 텍스트	*Log 프린터로 PLC 로그 정보를 전달하며, 문자열 형태로 구성되어 있으며 5분마다 한번씩 전달한다.*	*STRING*	*PLC*	*Log 프린터*
응급 신호	*유류 출하 기능으로 응급 상황 발생 여부를 전달하며, 응급 상황 발생 시 '1', 해제 시 '0', 예비위험시 '2' 값을 전달한다.*	*INTEGER*	*PLC*	*유류 출하 기능*
밸브 On/Off 값	*밸브의 On/Off를 전달하며 유류량 제어가 아닌 밸브의 On/Off 만을 전달하며 밸브 Open 시 On, Close 시 Off 값을 BOOL 값으로 전달한다.*	*BOOL*	*PLC 유류 출하 기능*	*Valve Motor*

3.3. 모듈 구성도

"응용 소프트웨어 내부 모듈 구성을 도식화 한다."



(5) 제4장『응용 소프트웨어 설계 고려사항』작성 예시

4. 응용 소프트웨어 설계 고려사항

"응용 소프트웨어 개발 시 다중화나 Voting 기법 등을 적용한 경우 이를 기술한다."

"응급 신호 전달 모듈은 안전성을 위해 2 중화 한다."

"상태 전달 모듈은 안전성과 신뢰성을 위해 2oo3 구조를 적용한다."

(6) 제5장『응용 소프트웨어 모듈 별 상세 설계』작성 예시

5. 응용 소프트웨어 모듈 별 상세 설계

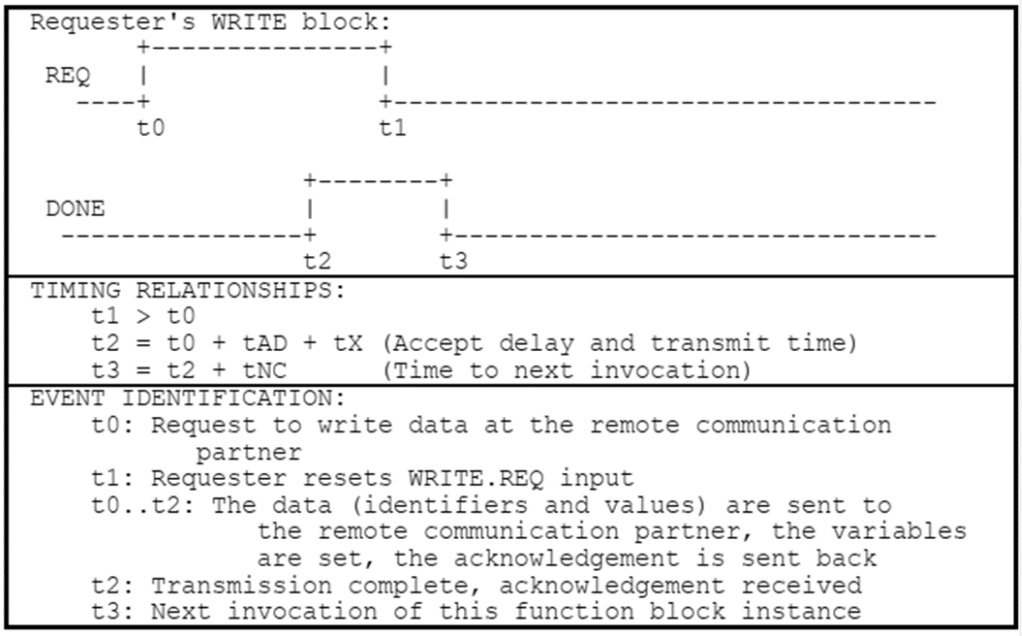
5.1. 모듈 상태

"각 단위 모듈 또는 프로그램 단계에서 해당 기능을 수행하기 위해 동작하는 모듈이나 프로그램이 가질 수 있는 상태 정보를 기술한다."

No.	상태		설명
1	*Init*		*프로그램 초기화 상태*
2	*IDLE*		*프로그램 초기화 중 IDLE 상태*
3	*WAITNG*		*프로그램 대기 상태*
4	*프로그램 상태*	*Processing*	*프로그램에 에러가 없거나 허용 가능한 고장만 발생한 상태*
5		*ERROR*	*프로그램에 에러가 발생한 상태*
6	*Shutdown*		*프로그램 종료 진행 상태*
7	*END*		*프로그램 종료 상태*

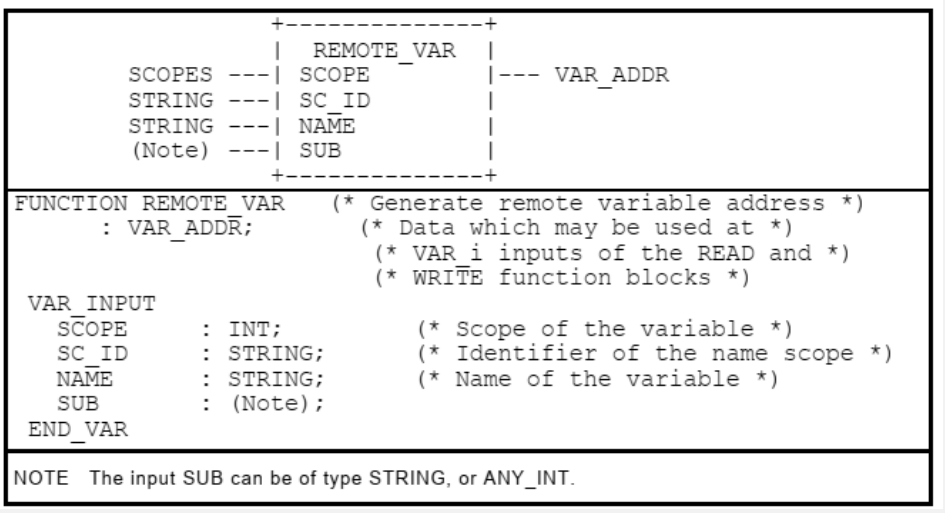
5.2. 모듈 데이터 처리 타이밍

"모듈이 데이터를 처리하기 위한 타이밍과 입력 및 출력 시 신호를 입력 받는 타이밍을 구체적으로 기술한다."
"구체적인 신호 타이밍과 타이밍에 대한 정의를 문서화 한다."



5.3. 기능 정의

"모듈 별 기능 타이밍에 처리해야 할 기능에 대해 구체적으로 기술한다."



(7) 제6장『외부 라이브러리 정의』작성 예시

6. 외부 라이브러리 정의

"가이드의 3.2.『응용 소프트웨어 요구사항 분석 및 명세 단계의 [2] 응용 소프트웨어 요구사항 명세 및 검증의 가. 수행절차』편에서 다루고 있는 항목들을 기반으로 기능 리스트를 기술한다.

(8) 제7장『설계 점검 항목』작성 예시

7. 설계 점검 항목

7.1. 구조 점검 항목

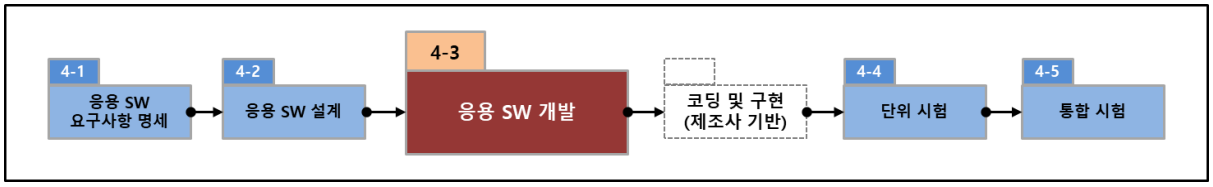
"가이드의 3.3.『응용 소프트웨어 구조 설계 단계의 [1] 응용 소프트웨어 구조 설계의 나. 점검항목』편에서 다루고 있는 내용을 점검항목으로 두고 해당 점검 항목에 대한 준수 유무를 기술한다."

No.	Required information	Comment
01	*설계에 필요한 입력 문서들은 식별되고 반영되었는가?*	
02	*운영 모드는 설계에 반영되었는가?*	
03	*응용 소프트웨어의 생명 주기는 운영모드와 함께 식별되었는가?*	
04	*운영 모드에 따른 제어 기능은 식별되었는가?*	
05	*외부 입력 및 출력 인터페이스는 모두 식별되었는가?*	
06	*HMI 인터페이스는 식별되었는가?*	
07	*기본 기능 및 하부 장치간 인터페이스는 식별되었는가?*	
...		

7.2. 기능 설계 점검 항목

"가이드의 3.3.『응용 소프트웨어 구조 설계 단계의 [2] 응용 소프트웨어 상세 설계의 나. 점검항목』 편에서 다루고 있는 내용을 점검항목으로 두고 해당 점검 항목에 대한 준수 유무를 기술한다."

No.	**Required information**	**Comment**
01	*모듈 별 상태 변화는 식별되었는가?*	
02	*모듈 별 변수 타이밍은 식별되었는가?*	
03	*전역 변수는 식별되었는가?*	
04	*모듈 별 세부 기능에 대한 Function Block 은 식별되었는가?*	
05	*안전과 비-안전 기능은 모두 식별되고 모듈화 되었는가?*	
06	*내부 및 외부 진단 모듈 및 기능은 식별되었는가?*	
07	*데이터 무결성 검사 방법은 적용되었는가?*	
...		



4.3. 응용 소프트웨어 개발

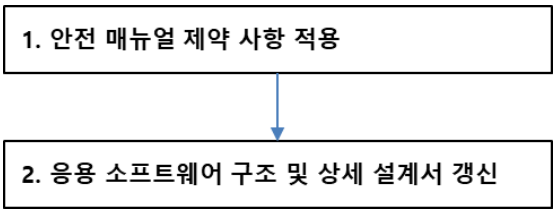
4.3.1. 목적

『응용 소프트웨어 설계』 단계에서 식별 된 응용 소프트웨어의 구조와 구성 모듈 별 상세 기능 식별 결과를 기반으로 응용 소프트웨어를 개발한다. 개발 단계에서는 안전 시스템의 하드웨어 제조사에서 제공하는 응용 소프트웨어 안전 매뉴얼의 입출력 인터페이스 정보, 메모리 할당 방법, 운전모드, 리셋 제약사항, 알람 코드 정보와 제약 사항을 식별하고, 기능 별 사용 언어를 선정하여 『응용 소프트웨어 설계』 단계에서 식별한 상세 기능 개발을 위한 구현 설명서를 작성한다. (환경에 따라 "응용 소프트웨어 설계서" 를 업데이트 하는 방법으로 문서의 수를 줄이는 것도 가능하다.)

주의: 본 가이드에서는 응용 소프트웨어 개발과 관련하여 『응용 소프트웨어 개발』 단계 까지만 다루며 『코딩 및 구현』 단계는 PLC 제조사에서 제공하는 도구와 절차를 준수하여 구현하는 것을 권장한다.

4.3.2. 활동 단계 개요

구 분	설 명
선행기준	1. 응용 소프트웨어 외부 시스템 상호 연결 적용 완료 2. 응용 소프트웨어 운영 모드 및 세부 수행 흐름 적용 완료 3. 응용 소프트웨어 설계서 작성 완료 4. 응용 소프트웨어 구조 추적표 작성 완료
입력문서	• 안전 시스템 아키텍처 설계서 • 안전 시스템 하드웨어 아키텍처 설계 제약사항 • 응용 소프트웨어 구조 및 상세 설계서

수행흐름	
산 출 물	• 기능별 응용 소프트웨어 구현 언어 선정 • 응용 소프트웨어 구조 및 상세 설계서 (갱신) • 응용 소프트웨어 단위 테스트 계획서
완료기준	1. 응용 소프트웨어 구현 언어 선택 완료 2. 응용 소프트웨어 구현 설명서 작성 완료 3. 응용 소프트웨어 단위 테스트 계획서 (갱신)

4.3.3. 세부 수행 활동

[1] 안전 매뉴얼 제약 사항 적용

안전 시스템의 하드웨어 제조 업체에서 제공하는『안전 매뉴얼』을 기반으로 안전 기능 제어를 위한 응용 소프트웨어 개발 시 고려해야 할 제약 사항을 확인한다.

가. 수행 절차

(1) 입출력 인터페이스 제약사항 확인

A. 입력 인터페이스 제약사항 식별

B. 출력 인터페이스 제약사항 식별

A. 안전 시스템 PLC 하드웨어의 입력 인터페이스 기능 및 정보를 식별한다.

✓ "입력 인터페이스 관련 기본 정보를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼

구분	명칭	부품도	기능 설명	사용 가능 개수					참조
				1유닛당				1축당	
				2축 유닛	4축 유닛	8축 유닛	16축 유닛		
입력축 모듈	서보 입력축	—	• 심플 모션 유닛으로 제어하고 있는 서보모터의 위치를 바탕으로 해, 입력축을 구동하는 경우에 사용합니다.	2	4	8	16	—	2.1절
	동기 엔코더축	—	• 동기 엔코더로부터의 입력 펄스에 의해 입력축을 구동하는 경우에 사용합니다.	4				—	2.2절

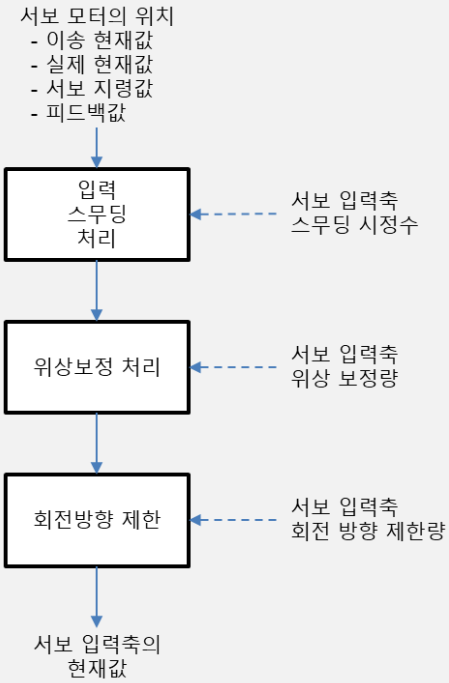
✓ "입력 인터페이스의 실제 적용 단위를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼

"[Pr.300] 서보 입력축 종류"의 설정값	"[Pr.1] 단위 설정"의 설정값	서보 입력축 위치 단위	범 위
1 : 이송 현재값 2 : 실제 현재값	0 : mm	$\times 10^{-4}$mm (10^{-1}μm)	−214748.3648~214748.3647 [mm] (−214748364.8~214748364.7 [μm])
	1 : inch	$\times 10^{-5}$inch	−21474.83648~21474.83647 [inch]
	2 : degree	$\times 10^{-5}$degree	−21474.83648~21474.83647 [degree]
	3 : PLS	PLS	−2147483648~2147483647 [PLS]
3 : 서보 지령값 4 : 피드백값	—	PLS	−2147483648~2147483647 [PLS]

✓ "입력 인터페이스의 속도 단위를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼

"[Pr.300] 서보 입력축 종류"의 설정값	"[Pr.1] 단위 설정"의 설정값	서보 입력축 속도 단위	범 위
1 : 이송 현재값 2 : 실제 현재값	0 : mm	$\times 10^{-2}$mm/min	−21474836.48~21474836.47 [mm/min]
	1 : inch	$\times 10^{-3}$inch/min	−2147483.648~2147483.647 [inch/min]
	2 : degree	$\times 10^{-3}$degree/min※1	−2147483.648~2147483.647 [degree/min] ※1
	3 : PLS	PLS/s	−2147483648~2147483647 [PLS/s]
3 : 서보 지령값 4 : 피드백값	—	PLS/s	−2147483648~2147483647 [PLS/s]

✓ "입력 인터페이스의 입력 처리 관계를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼



✓ "입력 인터페이스가 포함하고 있는 제약조건 등을 식별한다." 예) MITSUBISHI 공용 PLC 매뉴얼

0 : 회전방향 제한 없음 …… 회전방향 제한은 실시하지 않습니다.
1 : 현재값 증가 방향만 허가 …… 서보 입력축 현재값이 증가하는 방향의 입력 이동량만 허가합니다.
2 : 현재값 감소 방향만 허가 …… 서보 입력축 현재값이 감소하는 방향의 입력 이동량만 허가합니다.

✓ "입력 인터페이스의 파라미터 정보를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼

설정 항목	설정 내용	설정값	공장 출하시의 초기값	버퍼메모리 어드레스
[Pr.300] 서보 입력축 종류	• 서보 입력축의 입력값의 생성원이 되는 현재값 종류를 설정합니다. 취득주기 : 전원 투입시	■ 10진수로 설정합니다. 0 : 무효 1 : 이송 현재값 2 : 실제 현재값 3 : 서보 지령값 4 : 피드백값	0	32800+10n
[Pr.301] 서보 입력축 스무딩 시정수	• 입력값에 스무딩 처리를 하는 경우로 설정합니다. 취득주기 : 전원 투입시	■ 10진수로 설정합니다. 0~5000 [ms]	0	32801+10n
[Pr.302] 서보 입력축 위상보정 진행시간	• 위상을 진행시키는 또는 늦추는 시간을 설정합니다. 취득주기 : 연산주기	■ 10진수로 설정합니다. −2147483648~2147483647 [μs]	0	32802+10n 32803+10n
[Pr.303] 서보 입력축 위상보정 시정수	• 위상보정을 반영하는 시간을 설정합니다. 취득주기 : 전원 투입시	■ 10진수로 설정합니다. 0~65535 [ms] *1	10	32804+10n
[Pr.304] 서보 입력축 회전방향 제한	• 입력 이동량을 한방향으로만 제한하는 경우에 설정합니다. 취득주기 : 전원 투입시	■ 10진수로 설정합니다. 0 : 회전방향 제한 없음 1 : 현재값 증가 방향만 허가 2 : 현재값 감소 방향만 허가	0	32805+10n

B. 안전 시스템 PLC 하드웨어의 출력 인터페이스 기능 및 정보를 식별한다.

✓ "출력 인터페이스 관련 기본 정보를 확인한다." 예) MITSUBISHI 공용 PLC 매뉴얼

구분	명칭	부품도	기능 설명	사용 가능 개수					참조
				1유닛당				1축당	
				2축 유닛	4축 유닛	8축 유닛	16축 유닛		
주축 모듈	주축 메인 입력축		• 주축 모듈의 메인측의 입력축입니다. • 주축 위치의 기준이 됩니다.	2	4	8	16	1	4.1절
	주축 보조 입력축		• 주축 모듈의 보조측의 입력축입니다. • 주축 메인 입력축의 위치에 대해서 보정량을 입력하는 경우에 사용합니다.	2	4	8	16	1	4.1절
	주축 합성 기어		• 주축 메인 입력축과 주축 보조 입력축의 이동량을 합성해 주축 기어에 전달합니다.	2	4	8	16	1	4.1절
	주축 기어		• 주축 합성 기어 후의 이동량을 설정된 기어비로 변환해 전달합니다.	2	4	8	16	1	4.1절
	주축 클러치		• 주축의 이동량을 클러치로 ON/OFF해 전달합니다.	2	4	8	16	1	4.1절 4.3절
보조축 모듈	보조축		• 보조축 모듈의 입력축입니다.	2	4	8	16	1	4.2절
	보조축 기어		• 보조축의 이동량을 설정된 기어비로 변환해 전달합니다.	2	4	8	16	1	4.2절
	보조축 클러치		• 보조축의 이동량을 클러치로 ON/OFF해 전달합니다.	2	4	8	16	1	4.2절 4.3절
	보조축 합성 기어		• 주축과 보조축의 이동량을 합성해 전달합니다.	2	4	8	16	1	4.2절

✓ "입력 인터페이스의 실제 적용 단위를 확인한다.

✓ "출력 인터페이스의 속도 단위를 확인한다."

✓ "출력 인터페이스의 출력 처리 관계를 확인한다."

✓ "출력 인터페이스의 파라미터 정보를 확인한다."

✓ "그 외 출력 인터페이스가 포함하고 있는 제약조건 등을 식별한다."

(2) 입출력 메모리 할당 및 제약사항 확인

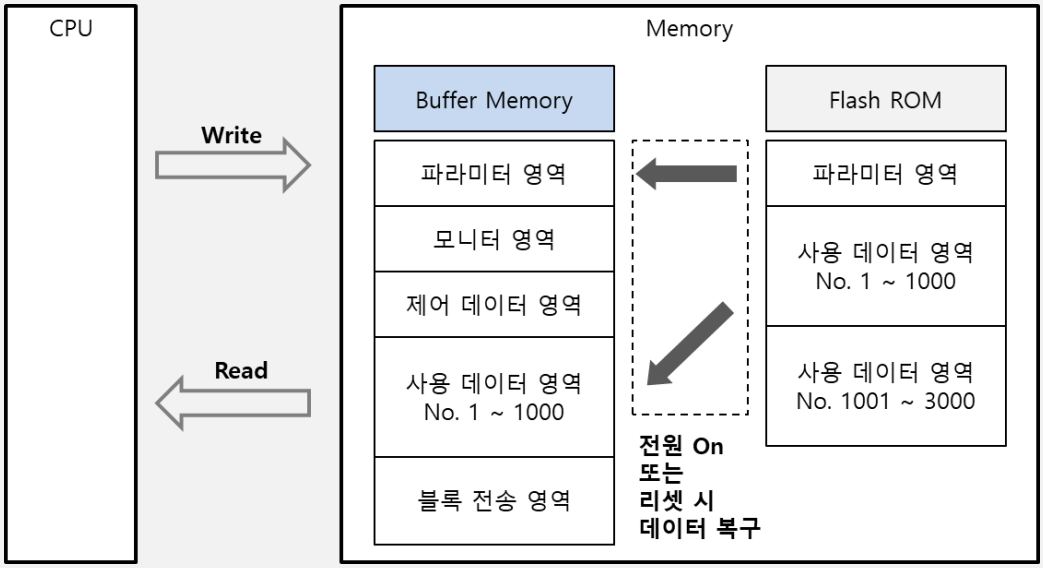
A. 안전 시스템의 하드웨어 메모리 구조를 확인

B. 입력과 출력 메모리 할당 및 제약사항 확인

C. 내부 메모리 할당 및 제약사항 확인

A. 안전 시스템 PLC 하드웨어의 메모리 구성을 확인한다.

✓ "안전 시스템 PLC 하드웨어 메모리 종류와 구성을 확인한다."



✓ "**버퍼 메모리**: PLC CPU에서 직접 읽기 / 쓰기가 가능한 메모리 영역으로 각종 파라미터, 위치 데이터, 에러 코드 등을 저장한다."

✓ "**OS메모리**: PLC 제어를 실행할 때 실제로 사용하는 데이터 저장 영역으로 각종 파라미터와 하드웨어 입출력 정보를 저장한다."

✓ "**플래시 ROM**: 파라미터 및 기능 수행 데이터의 백업용 메모리이다."

B. 입력과 출력 메모리 할당 및 메모리 사용의 제약사항을 확인한다.

✓ "입출력 메모리 표기 방법을 확인한다." 예) LG XGK PLC 메모리 표기 방법

A 제품	B 제품	C 제품	D 제품
P □□□□□ (주소 / 접점)	X □□ Y □□	IX □. □. □ QX □. □. □	I □. □ Q □. □
주소: 10진수 접점: 16진수 (0~F)	주소: 16진수 (0~F) 입력: X, 출력 Y	주소: 16진수 (0~F) 입력: IX, 출력: QX	주소: 16진수 (0~F) 입력: IX, 출력: QX

✓ "가변식 입출력 메모리 사용시 할당 정보를 확인한다." 예) LG XGK PLC 메모리 표기 방법

슬롯번호:	0	1	2	3	4	5	6	7
전원 / CPU	P0000 ~ P000F 입력 16점	P0010 ~ P002F 입력 32점	P0030 ~ P003F 출력 16점	P0040 ~ P004F 통신 모듈	P0050 ~ P005F 출력 16점	P0060 ~ P006F 출력 32점	P0080 ~ P008F A/D 모듈	P0090 ~ P009F XPM 모듈

✓ "고정식 입출력 메모리 사용시 할당 정보를 확인한다." 예) LG XGK PLC 메모리 표기 방법

슬롯번호:	0	1	2	3	4	5	6	7
전원 / CPU	P0000 ~ P003F 입력 16점	P0040 ~ P007F 입력 32점	P0080 ~ P011F 출력 16점	P0120 ~ P015F 통신 모듈	P0160 ~ P019F 출력 16점	P0200 ~ P023F 출력 32점	P0240 ~ P027F A/D 모듈	P0280 ~ P031F XPM 모듈
메모리 할당(점)	64	64	64	64	64	64	64	64

✓ "입출력 메모리 할당 방식을 확인한다." 예) LG XGK PLC 메모리 표기 방법

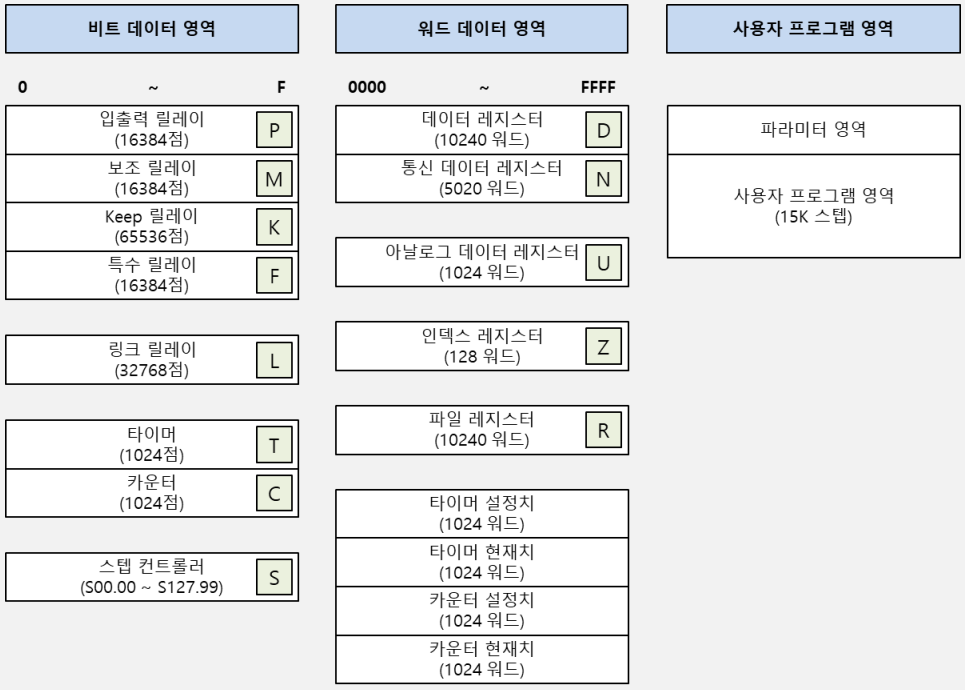
알아두기

입출력 메모리 할당 방식
(1) 입x출력 번호의 할당 방식은 기본 파라미터에서 설정 합니다.
(2) 기본베이스는 베이스 번호가 '0'으로 고정되며, 증설 베이스는 베이스 번호를 설정하는 스위치가 있습니다.
(3)I/O 파라미터로 모듈타입을 설정한 경우는 실제 장착된 모듈의 타입이 일치 되어야 운전이 개시됩니다.
(4) 증설1단의 0번슬롯에 16점 출력모듈의 입출력 번호의 할당은 고정식인 경우 P00640~P0064F가 되고 가변식인 경우에는 P00240~P0024F가 됩니다. 증설베이스의 입출력번호의 할당은XG5000의 시스템 모니터에서도 확인이 가능합니다.
(5) 자세한 내용은 CPU사용설명서의 2.3 기본 시스템의 내용을 참조하여 주십시오.
(6) 확장 또는 고장 난 경우 예비부 품목의 대체 시 I/O의 번호 변경없이 프로그램을 작성할 수 있도록 모듈 점수를 예약하는 기능을 I/O 파라미터에서 설정할 수 있습니다.(미리 설정해야 함.)

C. 내부 메모리 할당 및 메모리 사용의 제약사항을 확인한다.

✓ "입출력 메모리를 제외한 모든 메모리를 말한다."

✓ "내부 메모리 구조를 확인한다." 예) LG XGK PLC



✓ "PLC 재 기동 후에도 운전 중 발생 데이터를 유지할 필요가 있을 때에는 데이터 래치를 사용한다." 예) LG XGK PLC

디바이스	1 차 래치	2 차 래치	특 성
P	X	X	입출력 접점의 상태를 저장하는 이미지영역
M	O	O	내부 접점 영역
K	X	X	정전 시 접점 상태가 유지되는 접점
F	X	X	시스템 플래그 영역
T	O	O	타이머 관련 영역 (비트/워드 모두 해당)
C	O	O	카운터 관련 영역 (비트/워드 모두 해당)
S	O	O	스텝 제어용 릴레이
D	O	O	일반 워드 데이터 저장 영역
U	X	X	아날로그 데이터 레지스터 (래치 안 됨)
L	X	X	통신 모듈의 고속링크/P2P 서비스 상태 접점(래치 됨)
N	X	X	통신 모듈의 P2P 서비스 주소 영역(래치 됨)
Z	X	X	인덱스 전용 레지스터 (래치 안 됨)
R	X	X	플래시 메모리 전용 영역 (래치 됨)

✓ "내부 메모리 구성과 관련 제약사항을 확인한다." 예) LG XGK PLC

알아두기

1) K, L, N, R 디바이스들은 기본적으로 래치 됩니다.
2) K, L, R디바이스은 1차 래치와 같이 동작합니다. 즉, Overall 리셋 또는 CPU모듈 D.CLR 스위치 조작으로 지워집니다.
3) N디바이스는 XG5000 온라인메뉴 PLC지우기의 메모리 지우기 창에서 지울 수 있습니다.
4) 자세한 사용 방법은 XG5000 사용 설명서의 '온라인' 부를 참조 바랍니다

(3) 운전 모드 제약 사항을 확인한다.

A. 시스템 지원 운전 모드 종류 확인

B. 운전 모드 종류 별 구동 절차 확인

C. 운전 모드 변경 방법을 확인

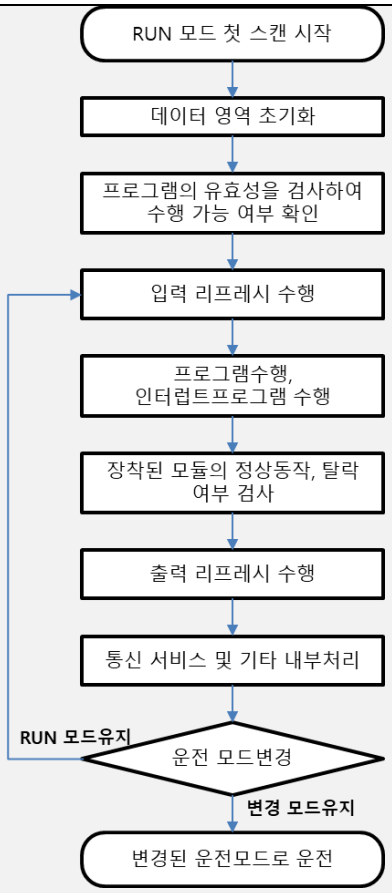
A. 안전 시스템 매뉴얼에서 제시하고 있는 운전 모드의 종류를 확인한다.

✓ "운전 모드를 확인" 예) LG XGK PLC

운전 모드	설명
RUN 모드	프로그램 연산을 정상적으로 수행하는 모드입니다.
STOP 모드	프로그램 연산을 하지 않고 정지 상태인 모드입니다. 원격 STOP 모드에서만 프로그램의 업로드가 가능합니다.
DEBUG 모드	프로그램의 오류를 찾거나, 연산 과정을 추적하기 위한 모드로 이 모드로의 전환은 STOP 모드에서만 가능합니다. 프로그램의 수행상태와 각 데이터의 내용을 확인해 보며 프로그램을 검증할 수 있는 모드입니다.

B. 운전 모드 종류 별 구동 절차 및 제약사항을 확인한다.

✓ "RUN 모드의 구동 절차와 모드 변경 타이밍을 확인한다." 예) LG XGK PLC



✓ "STOP 모드는 RUN 모드 운전 변경 상태일 때만 변경 가능하다." 예) LG XGK PLC

✓ "디버그 운전 조건은 아래와 같이 4가지가 있고 브레이크 포인터에 도달한 경우 다른 종류의 브레이크 포인터의 설정이 가능하다." 예) LG XGK PLC

운전 조건	동작 설명
한 연산 단위 실행 (스텝 오버)	운전 지령을 하면 하나의 연산 단위를 실행 후 정지한다.
브레이크 포인트 실행 (지정 포인트 실행)	프로그램에 브레이크 포인트를 지정하며 지정한 포인트에서 정지한다.
접점의 상태에 따라 실행	감시하고자 하는 접점 영역과 정지하고자 하는 상태지점(Read, Write, Value)을 하면 설정한 접점에서 지정한 동작이 발생할 때 정지한다.
스캔 횟수의 지정에 따라 실행	운전할 스캔 횟수를 지정하면 지정한 스캔 수 만큼 운전하고 정지한다.

C. 운전 모드 변경 방법과 조건을 확인한다.

✓ "안전 시스템 운전 모드와 설정 방법은 다음과 같다." 예) LG XGK PLC

운전모드 스위치	개발 시스템 명령 가능	원격 허용 스위치	운전모드
RUN	X	X	RUN
STOP	RUN	On	원격 RUN
	STOP		원격 STOP
	DEBUG		DEBUG RUN
	모드 변경 수행	Off	이전 운전 모드
RUN -> STOP	-	X	STOP

✓ "원격 모드 변환은 "**PLC 원격 허용: On**", "**모드 스위치: STOP**" 인 상태에서 가능하며, PLC-A는 키 스위치가 스톱일 때 가능하다." 예) LG XGK PLC

✓ "원격 'RUN' 상태에서 스위치에 의해 'STOP' 으로 변경하고자 할 경우는 스위치를 (STOP) -> RUN -> STOP 으로 조작하여 주십시요." 예) LG XGK PLC

(4) 명령어 제약 사항을 확인한다.

A. 시스템이 지원하는 시스템 플래그를 확인

B. 시스템 지원 기본 명령어와 타이밍 차트 확인

A. 시스템이 지원하는 시스템 플래그를 확인한다.

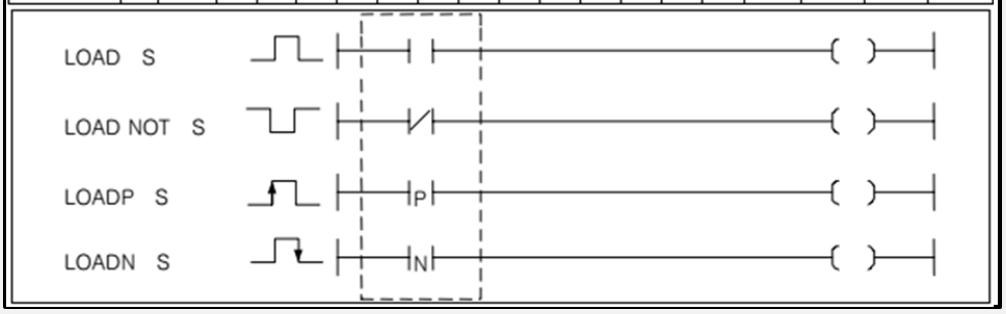
✓ "디바이스 지원 플래그 변수는 다음과 같다." 예) LG XGK PLC

디바이스	변수	설명	디바이스	변수	설명
F00000	_RUN	PLC Run 시 ON	F00096	_T20S	20 초 주기 CLOCK (10 초 ON, 10 초 OFF)
F00001	_STOP	PLC Run 시 ON	F00097	_T60S	1 분 주기 CLOCK (30 초 ON, 30 초 OFF)
F00002	_ERROR	Error 발생 시 ON	F00099	_ON	항상 ON
F00090	_T20MS	20ms 주기 CLOCK (10ms ON, 10ms OFF)	F0009A	_OFF	항상 OFF
F00091	_T100MS	100ms 주기 CLOCK (50ms ON, 50ms OFF)	F0009B	_1ON	첫 스캔 ON
F00092	_T200MS	200ms 주기 CLOCK (100ms ON, 100ms OFF)	F0009C	_1OFF	첫 스캔 OFF
F00093	_T1S	1 초 주기 CLOCK (0.5 초 ON, 0.5 초 OFF)	F0009D	_STOG	매 스캔 반전
F00094	_T2S	2 초 주기 CLOCK (1 초 ON, 1 초 OFF)	F00110	_LER	연산 에러 (1 스캔 ON)
F00095	_T10S	10 초 주기 CLOCK (5 초 ON, 5 초 OFF)	F00112	_CARRY	연산 캐리 발생 시 ON

B. 시스템이 지원하는 기본 명령어를 확인한다.

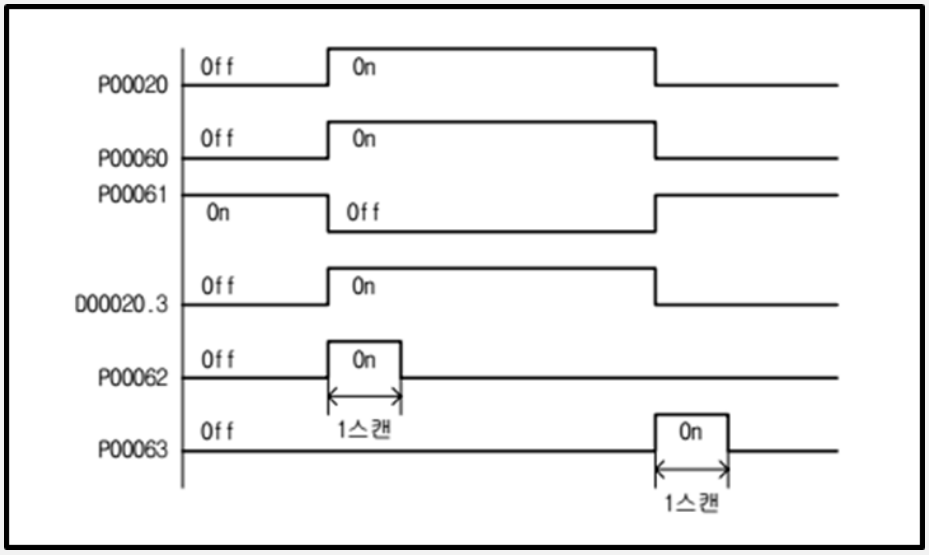
✓ "기본 명령어 LOAD, LOAD NOT, LOADP, LOADN" 예) LG XGK PLC

명 령		사용가능영역														스텝	플래그		
		PMK	F	L	T	C	S	Z	D.x	R.x	상수	U	N	D	R		에러 (F110)	제로 (F111)	캐리 (F112)
LOAD LOAD NOT	S	O	O	O	O	O	O	-	O	O	-	O	-	-	-	1~2	-	-	-
LOADP LOADN	S	O	O	O	O	O	O	-	O	O	-	O	-	-	-	2			



✓ LOAD는 한 회로의 a 접점 연산 시작을 의미하고, LOAD NOT은 b 접점 연산 시작을 의미한다. 예) LG XGK PLC

✓ "LOAD의 실행 타이밍은 아래 그림과 같다." 예) LG XGK PLC



(5) 리셋과 관련한 제약사항을 확인한다.

A. 운전 모드와 관련한 리셋 초기화 제약사항 확인

B. 구체적인 운전모드와 리셋 절차 확인

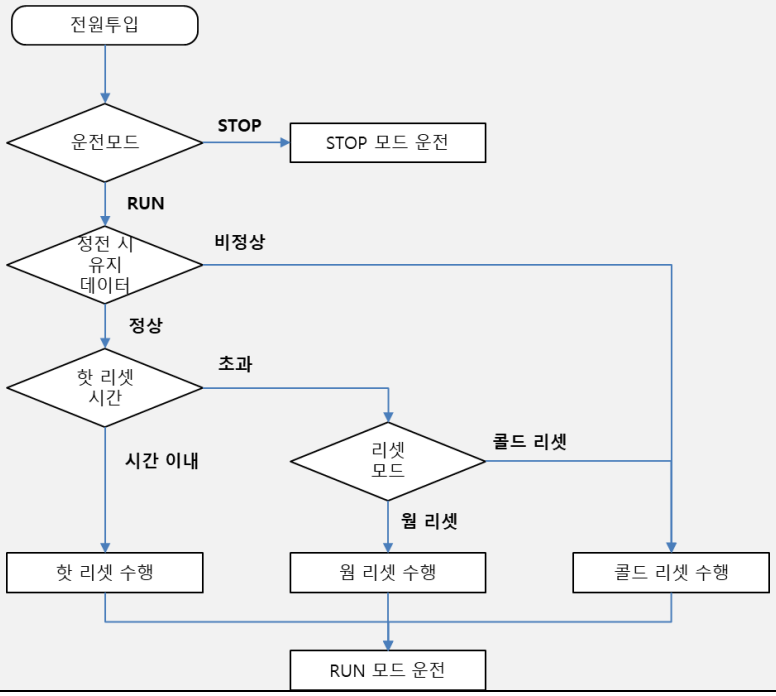
A. 안전 시스템 매뉴얼에서 제시하고 있는 운전 모드에 따른 리셋 방법을 확인한다.

✓ "해당 안전 PLC의 리셋은 운전 모드에 따라 아래 그림과 같다." 예) GLOFA-GM PLC

구분	콜드(COLD)	웜(WARM)	핫(HOT)
디폴트 모드	"0"으로 초기화	"0"으로 초기화	이전 값 유지
리테인 모드	"0"으로 초기화	이전 값 유지	이전 값 유지
초기화 모드	사용자 지정 값	사용자 지정 값	이전 값 유지

B. 구체적인 운전모드와 리셋 절차를 확인한다.

✓ "운전 중 전원 재 투입 시 리셋 절차는 다음과 같다." 예) GLOFA-GM PLC



(6) 알람과 관련한 제약사항을 확인한다.

A. 알람 리스트를 확인하다.

B. 알람 발생 조건과 종료 조건을 확인한다.

A. 제조사에서 제공하는 알람 리스트를 확인한다.

✓ 알람 코드 리스트와 에러의 구분 확인 예) MITSUBISHI MELSEC-A

에러 코드	에러의 구분
001 ~ 009	치명적 에러
010 ~ 099	시스템 기동시의 에러
100 ~ 199	공통적 에러
200 ~ 290	원점 복귀시의 에러
300 ~ 399	JOG 운전시의 에러
400 ~ 499	수동 펄서 운전시의 에러
500 ~ 599	위치 결정 운전시의 에러
900 ~ 999	파라미터 설정 범위 체크시의 에러

B. 알람 발생 조건과 종료 조건 또는 대처 방법을 확인한다.

✓ "알람 관련 명칭, 검출 타이밍, 에러 발생시 동작 상태, 대처 방법 등을 확인" 예) MITSUBISHI MELSEC-A

에러 코드	에러 명칭	검출 타이밍	에러 발생시의 동작 상태	대처 방법
000	정상 상태			
001 003 004 005	<치명적 에러> Fault 0 으로 나눔 Overflow Underflow	하드웨어 이상	시스템이 정지됨	- 노이즈등의 영향이 없는지 확인 - 하드웨어 이상을 점검
51	위치 지령 범위 초과	PLC Ready Off→On 시	AD75 준비완료 플래그 [X0]가 Off 하지 않음	파라미터의 위치 데이터를 4.23 항에 지정한 범위 이내로 수정함. 위치 결정 어드레스를 4.23 항으로 지정 범위
		위치 결정 시동시	시동하지 않음	
52	속도 지령 범위 초과	PLC Ready Off→On 시	AD75 준비완료 플래그 [X0]가 Off 하지 않음	파라미터의 속도 데이터를 4.23 항에 지정한 범위내로 수정함
		위치 결정 시동시	시동하지 않음	위치 결정 데이터의 지령 속도를 4.23 항에 지정한 범위내로 수정
100	<공통> 운전중 주변 기기 정지	운전중에 주변 기기에서의 [정지]키가 입력될 때	감속 정지 또는 급정지를 함	축 에러 리셋으로 에러를 해제함
101	운전중 PLC Ready Off	운전중에 PLC Ready 신호가 Off 될 때	감속 정지 또는 급정지를 함	축 에러 리셋으로 에러를 해제함
102	드라이브 유닛 Ready Off	운전중에 드라이브 유닛 Ready 신호가 Off 될 때	즉시 정지	축 에러 리셋으로 에러를 해제함
103	운전중 테스트 모드 이상	테스트 모드중	감속 정지	원인을 파악한 후, AD75 본체와 주변 기기의 전원을 Off→On 함

(7) 자가진단과 관련한 제약사항을 확인한다.

A. 자기진단 기능 유무와 방법을 확인

B. 외부 장치 또는 입출력 진단 방법 확인

C. 프로그램 체크 기능을 확인

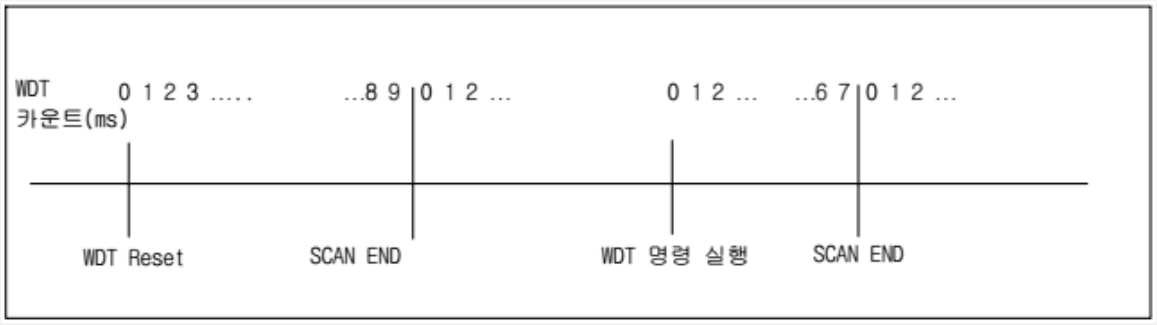
A. 해당 PLC가 자가진단 기능을 사용하는지 그렇다면 어떤 방법인지 확인한다.

✓ "해당 시스템이 가지고 있는 자가진단 방법과 제약사항을 확인한다."
예) LG XGK PLC

(1) 와치독 타이머는 사용자 프로그램 이상에 의한 연산지연을 검출하기 위하여 사용하는 타이머 입니다. 와치독 타이머의 검출시간은 XG5000 의 기본 파라미터에서 설정합니다.
(2) 와치독 타이머는 연산 중 스캔 경과 시간을 감시하다가, 설정된 검출시간의 초과를 감지하면
PLC 의 연산을 즉시 중지시키고 출력을 전부 Off 합니다.
(3) 사용자 프로그램 수행 도중 특정한 부분의 프로그램 처리(FOR ~ NEXT 명령,CALL 명령 등을 사용) 에서 연산지연 감시 검출시간 (Scan Watchdog Time)의 초과가 예상되면 WDT

명령을 사용하여 타이머를 클리어 하면 됩니다. WDT 명령은 연산지연 감시 타이머의 경과 시간을 초기화하여
0 부터 시간 측정을 다시 시작합니다.
(4) 와치독 에러 상태를 해제하기 위해서는 전원 재투입, 수동 리셋 스위치의 조작 또는 STOP 모드로의 모드전환이 있습니다.

✓ "자가진단 기능 실행 흐름도를 작성한다." 예) LG XGK PLC



B. 외부 입출력 신호나 모듈의 이상체크 기능을 확인한다.

✓ "기동 시와 운전 중 입출력 모듈의 상태 체크 기능을 확인한다." 예) LG XGK PLC

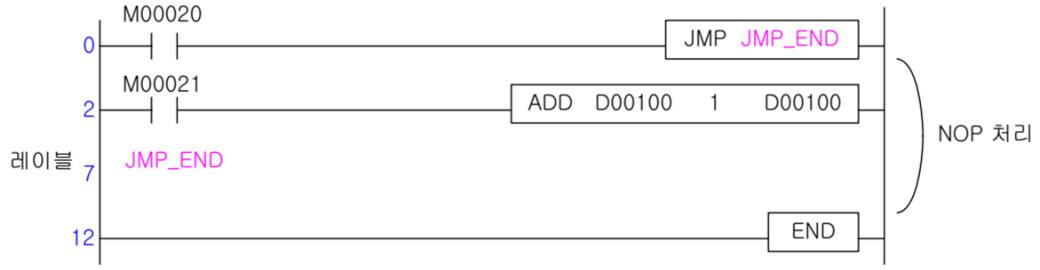
F 영역	내 용
F104[0~B]	메인 베이스에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F105[0~B]	증설 베이스 1 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F106[0~B]	증설 베이스 2 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F107[0~B]	증설 베이스 3 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F108[0~B]	증설 베이스 4 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F109[0~B]	증설 베이스 5 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F110[0~B]	증설 베이스 6 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On
F111[0~B]	증설 베이스 7 단에 장착되어 있는 모듈 착탈 에러 발생 시 해당 슬롯 비트 On

C. 외부 입출력 신호나 모듈의 이상체크 기능을 확인한다.

✓ "프로그램 전체에서 사용할 수 있는 레이블의 수의 제한으로 인한 명령 사용 중 진단 기능" 예) LG XGK PLC

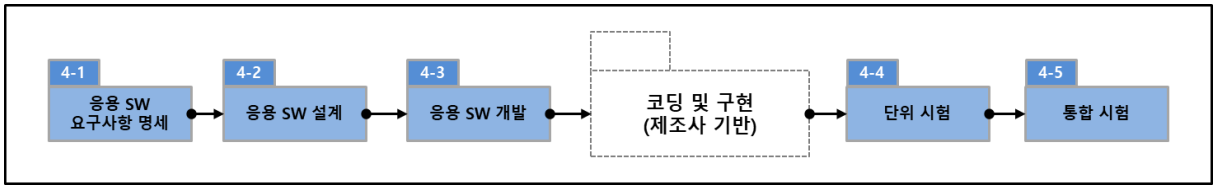
2.9.1 JMP-LABEL

1) 프로그램 전체에서 사용할 수 있는 레이블(LABEL)의 개수는 XGK 는 512 개, XGB 는 128 개입니다. 사용된 레이블의 개수가 512(XGK)/128(XGB)개를 초과시에는프로그램이 다운로드가 되지 않습니다. JMP 조건이 만족되어 해당 레이블로 점프(Jump)할 때 JMP 명령과 레이블사이의 모든 명령을 NOP 처리합니다.



나. 점검 항목

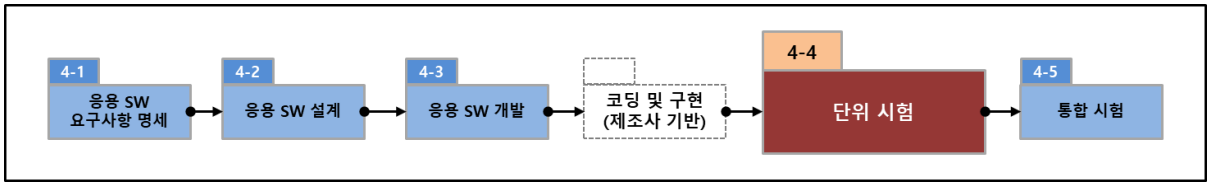
No.	Required information	Comment
01	안전 시스템 및 하위 시스템 제조업체가 제공하는 개발 도구 및 제한사항을 준수하였는가?	
02	응용 소프트웨어의 모듈 및 기능 블록, 기능, 프로그램 단위가 식별되었는가?	
03	개발에 사용한 안전 매뉴얼 버전은 식별되었는가?	
04	개발 모듈과 안전 기능 그리고 안전 시스템에 대한 추적성은 식별되었는가?	
05	개발 모듈과 응용 소프트웨어 안전 요구사항의 추적관계는 식별되었는가?	
06	논리규칙, 표준 라이브러리 기능, 응용 라이브러리 기능을 포함하여 사용된 기호는 식별되고 설명되었는가?	
07	논리 해석기의 입력 및 출력 신호는 식별되었는가?	
08	응용 소프트웨어가 통신 기능을 사용할 경우 통신 정보 흐름에 대한 설명이 되어있는가?	
09	입력과 출력 데이터의 논리적 처리 순서와 스캔 타임을 포함한 프로그램 구조의 설명이 되었는가?	
10	안전 요구사항에서 요구하는 경우 필드 데이터의 정확성 보장과 통신 데이터의 정확성 보장 방법은 식별되고 설명되어 있는가?	
11	필요한 경우 통신 데이터의 보안 기법이 적용되어 있는가?	
12	이전에 개발된 응용 프로그램이나 라이브러리 기능을 적용한 경우 적합성 근거는 명시되어 있는가?	
13	응용 소프트웨어의 알람 코드, 처리 방법 및 리포트 상세 기능이 식별되고 설명되었는가?	
14	리셋 상세 기능이 식별되고 설명되었는가?	
15	온/오프라인 테스트 상세 기능이 식별되고 설명되었는가?	



4.4. 코딩 & 구현

주의: 본 가이드에서는 응용 소프트웨어 개발과 관련하여『응용 소프트웨어 개발』단계 까지만 다루며『코딩 및 구현』단계는 PLC 제조사에서 제공하는 도구와 절차를 준수하여 구현하는 것을 권장한다.

"문법 및 구현 방법: 제조사별 제공 PLC 개발 매뉴얼 참조"



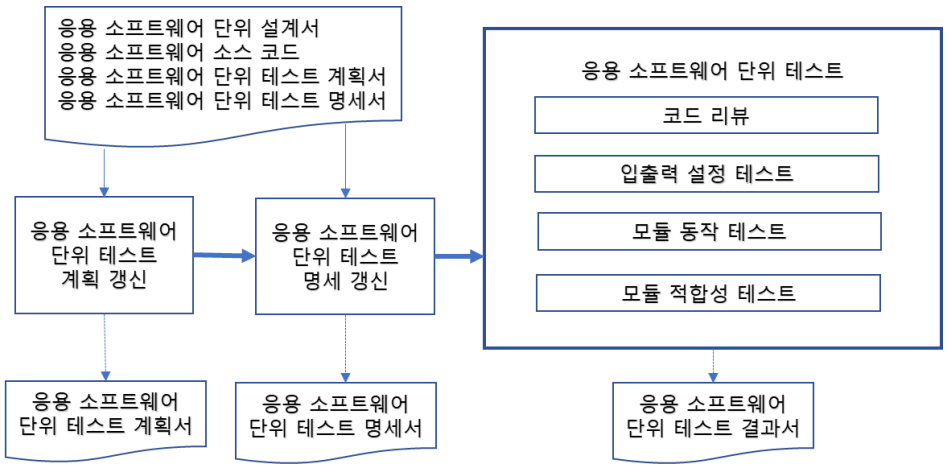
4.5. 단위 시험

4.5.1. 목적

응용 소프트웨어 단위 시험 단계에서는 응용 소프트웨어 단위 구현이 완료되면 각 소프트웨어 모듈에 대하여 응용 소프트웨어 단위 시험 계획과 명세에 따라서 소프트웨어 단위 모듈들이 상세 설계와 안전 요구사항을 준수하도록 구현되었는지 검증하기 위하여 단위 시험을 수행하는 단계이다. 이는 응용 소프트웨어 모듈이 관련 사양을 만족하는지, 즉 검증되었는지를 보증하는 코드 리뷰와 구조 테스트의 조합으로, 필요시 단위 시험 계획서 및 단위 시험 명세서를 갱신하고 단위 시험 환경 구축이 완료되면 단위 시험 명세에 따라 테스트 활동을 수행하고 결함이 발생하면 모든 결함에 대하여 해결을 완료하고 단위 시험 결과서를 작성한다

4.5.2. 활동 단계 개요

구 분	설 명
선행기준	1. 응용 소프트웨어 단위 설계 완료 2. 응용 소프트웨어 단위 시험 계획 수립 완료 3. 응용 소프트웨어 단위 시험 명세 완료 4. 응용 소프트웨어 단위 설계 리뷰 완료 5. 응용 소프트웨어 단위 시험 계획 / 명세 리뷰 완료 6. 응용 소프트웨어 구현 완료
입력문서	• 응용 소프트웨어 단위 설계서 • 응용 소프트웨어 단위 시험 계획서 • 응용 소프트웨어 단위 시험 명세서 • 응용 소프트웨어 단위 설계 리뷰 결과 • 응용 소프트웨어 단위 시험 계획 / 명세 리뷰 결과

	• 소스 코드
수행흐름	
산 출 물	• 응용 소프트웨어 단위 시험 계획서 (갱신) • 응용 소프트웨어 단위 시험 명세서 (갱신) • 응용 소프트웨어 단위 시험 결과서
완료기준	1. 응용 소프트웨어 단위 시험 계획서 갱신 완료 2. 응용 소프트웨어 단위 시험 명세서 갱신 완료 3. 소스 코드 리뷰 및 후속 치 완료 4. 응용 소프트웨어 단위 시험 및 결함 해결 완료 5. 응용 소프트웨어 단위 시험 결과서 작성 완료 6. 응용 소프트웨어 단위 설계와 테스트 결과의 추적성 확보 7. 응용 소프트웨어 단위 설계와 테스트 결과의 일관성 확보

4.5.3. 세부 수행 활동

[1] 응용 소프트웨어 단위 시험 계획 갱신

응용 소프트웨어의 단위 설계에 따라서 응용 소프트웨어 단위가 개발되었는지 검증하는 활동에 대한 계획을 수립한 응용 소프트웨어 단위 시험 계획서를 필요 시 갱신한다.

가. 수행 절차

(1) 응용 소프트웨어 단위 시험 전략을 검토 및 갱신한다.

응용 소프트웨어 단위가 응용 소프트웨어 상세 설계와 안전 요구사항에 대해

준수하는지 증거를 제공하는 방법을 정의하기 위한 단위 시험 전략을 검토하고 필요시 갱신한다. 응용 소프트웨어 단위 시험 전략에는 다음 항목을 포함한다.

A. 검증 대상물의 정의

B. 검증 및 테스트와 관련된 특정 요구사항 (예: 테스트 특정 이해 관계자 요구사항, IEC 62279, 61511, 측정 지표, 코딩 표준)을 다루는 방법의 정의.

C. 상세 설계 및 비기능 요구사항에서 도출된 테스트 케이스 및 테스트 데이터 개발 방법의 정의.

D. 정적 검증 및 검토를 위한 방법과 도구의 정의

E. 각 테스트 방법에 대한 테스트 환경의 정의

F. 프로젝트 및 릴리즈 계획과 관련된 테스트 적용 범위의 정의

G. 소프트웨어 장치 검증을 위한 시작 및 완료 기준의 정의

H. 테스트의 실패, 정적 검증의 실패 및 리뷰 결과 처리 대한 접근 방법

(2) 응용 소프트웨어 단위 시험 범위를 검토 및 갱신한다.

A. 소프트웨어 단위 평가 대상 및 제외 대상을 검토 및 갱신한다.

(3) 응용 소프트웨어 단위 시험 방법을 검토 및 갱신한다.
응용 소프트웨어 단위 시험 방법에는 다음을 참고한다.

A. 인터페이스 테스트: 소프트웨어 통합 전 컴포넌트의 인터페이스 설계 준수 여부

B. 자원 사용 평가: 적정한 자원을 사용하는지 평가

C. 모델 기반 코드 평가: 모델과 코드 구현 결과의 일치성 평가

D. 요구사항 기반 평가: 소프트웨어 기능 평가

E. 결함 주입 테스트: 소프트웨어 악의 평가

(4) 응용 소프트웨어 단위 시험 상세 활동 계획을 검토 및 갱신한다.
상세 계획에는 다음 항목을 포함한다

A. 테스트 케이스 추출방법

B. 테스트 수행 시점

C. 테스트 수행 환경

D. 테스트 수행 준비 절차

E. 테스트 수행 절차

F. 테스트 수행 결과 정리

(5) 응용 소프트웨어 회귀 테스트 계획을 검토 및 갱신한다.

A. 변경된 응용 소프트웨어 단위의 재검증을 위한 회귀 테스트 계획, 수행 여부, 절차를 검토하고 갱신한다.

[2] 응용 소프트웨어 단위 시험 명세 갱신

『응용 소프트웨어 단위 설계 및 구현』 단계에서 응용 소프트웨어의 단위 설계에 따라서 응용 소프트웨어 단위가 개발되었는지 검증하는 활동에 대한 수행을 명세한 응용 소프트웨어 단위 시험 명세서를 필요시에 갱신한다.

가. 수행 절차

(1) 응용 소프트웨어 단위 시험 케이스를 검토 및 갱신한다.

A. 요구사항 분석 기반

B. 동등 분할

C. 경계 값 분석

D. 탐사적 평가 기반

(2) 응용 소프트웨어 단위 설계와 응용 소프트웨어 단위 시험 케이스 간의 추적성을 검토 및 갱신한다.응용 소프트웨어 단위 시험 추적 매트릭스에 작성된 응용 소프트웨어 단위 설계와 단위 시험 명세서 간의 추적성을 검토 및 갱신하여 확보한다.

(3) 응용 소프트웨어 단위 시험 기준을 검토 및 갱신한다.
응용 소프트웨어 단위 시험 계획서를 기반으로 응용 소프트웨어 단위 시험 기준을 상세화하고, 테스트 패스 기준을 수립한다. 패스 기준의 예로는 다음과 같다.

A. 소프트웨어 단위 설계서 검토: 결함 수정률

B. 인터페이스 테스트: 테스트 케이스 패스율

C. 자원 사용 평가: 실행 시간, 메모리 사용량, 네트워크 부하 량

D. 모델 기반 평가: 테스트 케이스 패스율

E. 기능 평가: 테스트 케이스 패스율

F. 악의 평가: 테스트 케이스 패스율

G. 단위 소프트웨어 테스트 패스 기준

i. 구분 커버리지

ii. 분기 커버리지

(4) 응용 소프트웨어 단위 시험 자원 식별 내역을 검토 및 갱신한다.

A. 소프트웨어 단위 시험 조직

B. 소프트웨어 단위 시험 환경

C. 소프트웨어 단위 시험 측정 지표

(5) 응용 소프트웨어 단위 시험 결과 작성 절차를 검토 및 갱신한다.

A. 소프트웨어 단위 시험 결과서 작성 절차

B. 소프트웨어 단위 시험 결함 발견 및 해결 절차

[3] 응용 소프트웨어 단위 시험

응용 소프트웨어 단위 시험은 소프트웨어 모듈과 상세 설계에 대한 적합성에 중점을 두어 응용 소프트웨어 모듈을 나머지 시스템과 통합하기 전에 모듈이 제대로 작동하는지 확인하는 것이다. 단위 시험은 테스트를 작성할 때 코드 구조를 고려하기 때문에 화이트 박스 테스트의 한 형태이며, 목표는 코드의 구조를 사용하여 테스트를 최적화하여 테스트가 철저한 기준을 충족하면서 수행할 수 있는 최소 수의 테스트 케이스로 테스트를 줄이는 것이다. 단위 시험 중에 테스트되는 응용 소프트웨어의 많은 경로는 테스트의 후반 단계에서는 쉽게 테스트할 수 없다. 응용 소프트웨어 단위 시험 단계에서는 다음 유형의 오류를 탐지할 수 있다

(1) 소프트웨어 명세를 만족하지 못하는 알고리즘

(2) 부정확한 루프 연산

(3) 부정확한 논리 결정

(4) 입력 데이터의 유효한 조합을 정확하게 계산할 수 없음

(5) 누락되거나 변경된 입력 데이터에 대한 부정확한 응답

(6) 배열 경계 위반

(7) 잘못된 계산 순서

(8) 부적절한 정밀도

(9) 알고리즘의 정확도 또는 성능

가. 수행 절차

개별 응용 소프트웨어 모듈이 의도된 기능을 수행하고 제한된 테스트 데이터를 선택하여 시스템이 의도하지 않은 기능을 수행하지 않는지 확인하기 위해 테스트해야 하며, 상위 SIL의 경우 예상치 못한 오류 조건에 대한 테스트 범위를 늘려야 한다. 예를 들어, SIL 1 및 SIL 2 시스템의 경우 테스트에는 경계 값 테스트 및 파티셔닝 테스트가 포함되어야 하며 SIL 3 및 SIL 4는 특정 중요 이벤트의 원인 결과 분석에서 생성된 테스트가 포함되어야 한다.

(1) 코드 리뷰

A. 개별 응용 소프트웨어 모듈이 관련 규격과 사양을 만족하는지, 의도된 기능을 수행하고 의도하지 않은 기능을 수행하지 않는지 확인하기 위해 코드를 리뷰한다.

(2) 입출력 설정 테스트

A. 입출력 데이터가 올바른 응용 프로그램 로직에 매핑 되었는지 확인하기 위해 리뷰, 테스트 또는 시뮬레이션을 통해 각 입력 및 출력 지점의 환경 설정을 점검한다.

(3) 모듈 동작 테스트

각 소프트웨어 모듈의 리뷰, 시뮬레이션 및 테스트 과정을 거쳐 계획된 기능이 올바르게 실행되고 의도하지 않은 기능이 실행되지 않았는지를 확인한다.

A. 응용 소프트웨어 단위 설계 명세에 대한 시험의 완전성

B. 응용 소프트웨어 단위 설계 명세에 대한 시험의 정확성

C. 반복성

D. 정확하게 정의된 테스트 구성

(4) 모듈 적합성 테스트

응용 소프트웨어 단위 시험은 시험되는 특정 모듈에 적합해야 하며 다음을 수행해야한다.

A. 모든 응용 소프트웨어 모듈의 각 지점이 실행되는지 확인

B. 경계 데이터가 행사되는지 확인

C. 관련 동기화 조건을 포함하여 시퀀스가 올바르게 구현되었는지 확인

나. 점검 항목

각 응용 소프트웨어 모듈에 대하여 아래 항목을 테스트해야 하며, 특정 테스트가 모듈에 적용되지 않는 경우 이 테스트가 적용되지 않는 이유를 설명하고 점검 목록에 NA 표시한다.

No.	점검 항목	설명
01	모듈이 의도한 기능을 수행하는가?	수행된 모든 테스트에 대해 출력이 정확한지 확인
02	모듈이 의도하지 않은 기능을 수행하지 않는가?	별도로 시험하지는 않으나 다른 테스트에서 의도하지 않은 결과가 발생하는지 분석 의도하지 않은 결과의 예) - 배열 범위 밖에 쓰기 - 루프의 초과 수행 - 함수에서 지정하지 않은 위치에 쓰기
03	모듈의 모든 입력에 대하여 등가 클래스가 생성되었는가?	가능한 모든 입력의 작은 하위 집합을 제시하여 가장 많은 오류를 찾을 가능성을 높인다 등가 클래스를 만드는 과정은 각 입력을 두 개 이상의 그룹으로 나누는 것으로 구성되며, 유효한 등가 클래스와 유효하지 않은 등가 클래스를 모두 고려해야 한다.
04	각 등가 클래스에 대해 경계 값이	경계 값 분석은 등가 클래스 기법의 확장으로, 차이

No.	점검 항목	설명
	테스트되었는가?	점은 테스트할 값을 선택하는 방법에 있다. 등가 클래스 내에서 값을 선택하는 대신 등가 클래스의 가장자리가 테스트의 대상이 되도록 하나 이상의 값을 선택한다. min, max, min - 1 및 max + 1 (정수일 경우)을 명시 적으로 테스트
05	모든 입력에 0 값이 테스트되었는가?	0 은 예기치 않은 문제 (예 : 0 으로 나누기, 배열의 0 요소 등)를 나타내는 특수한 테스트 사례이다. 따라서 모든 입력에 대해 항상 테스트 포인트로 사용되어야 한다.
06	출력의 한계 값이 테스트되었는가?	출력을 최대 및 최소값으로 강제 설정하는 테스트가 생성된다.
07	가능할 경우, 출력의 한계 값 이상이 테스트되었는가?	가능하면 출력을 최소값 이하로 최대 값 이상으로 강제 설정하는 테스트가 생성된다.
08	시퀀스의 첫번째와 마지막 요소가 테스트되었는가?	배열이나 연결된 목록과 같은 시퀀스가 있는 경우 시퀀스의 첫 번째 요소와 마지막 요소를 읽고 쓰는 방법으로 테스트를 수행하는 것이 중요하다.
09	0, 1, 2 요소를 포함하는 시퀀스가 테스트되었는가?	배열이나 링크드 리스트와 같은 시퀀스가 있는 경우 배열의 요소가 0, 1, 2 인 경우를 테스트하는 것이 중요하다.
10	모든 분기를 포함하여 모듈내 모든 구문이 실행되었는가?	분기가 수행할 수 있는 모든 가능한 단계를 포함하여 모든 코드 행을 테스트하는 것이 중요하다. 코드가 처음으로 필드에서 실행되는 것은 바람직하지 않다.

다. 문서화

응용 소프트웨어 단위 시험 결과는 시간 기록 및 필요한 시정 조치로 문서화되어야 한다. 모듈 및 테스트 지침 버전 번호가 명확하게 표시되어야 하고, 예상 결과와의 불일치가 명확하게 보여야한다. 필요한 모든 재 테스트를 결정하기 위해 테스트 단계 이후에 구현된 소프트웨어 수정 또는 변경 사항을 분석해야 하고, 각 모듈에 대해 다음 설명이 있어야한다.

(1) 테스트 실행 날짜

(2) 테스트 실행 플랫폼

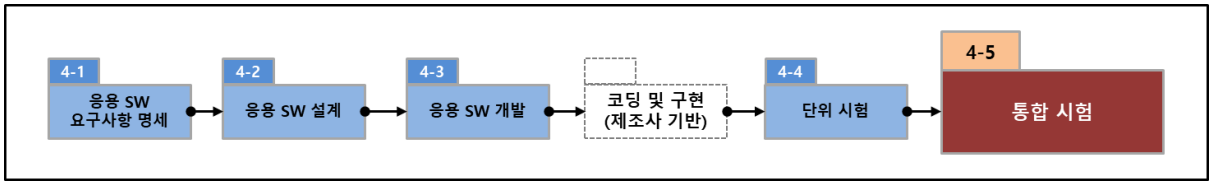
(3) 컴파일러를 포함하여 테스트에 사용된 도구의 버전

(4) 테스터 성명

(5) 테스트중인 모듈의 이름과 버전

(6) 수행된 테스트와 통과 또는 실패 여부를 나타내는 완료된 단위 시험 체크리스트.

(7) 모든 등가 클래스 및 경계 값에 사용된 실제 테스트 값



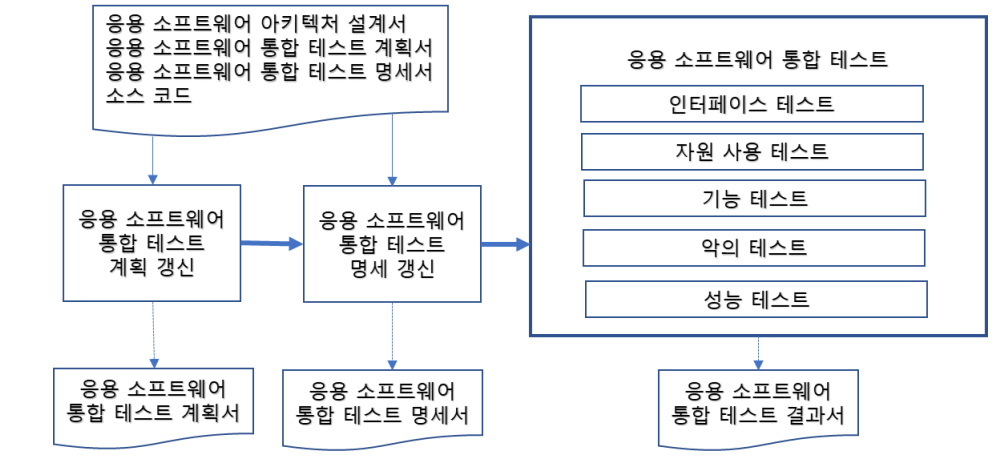
4.6. 통합 시험

4.6.1. 목적

응용 소프트웨어 통합 시험 단계에서는 모든 응용 소프트웨어 모듈과 컴포넌트 / 서브 시스템이 소프트웨어 아키텍처 설계와 안전 무결성 수준을 준수하도록 의도된 기능을 수행하기 위해 서로 및 기본 내장 소프트웨어와 정확하게 상호작용하는지 그리고 안전 기능을 위태롭게 할 수 있는 의도하지 않은 기능을 수행하지 않는지 응용 소프트웨어 통합 시험 계획과 명세에 따라 테스트 활동을 수행하고 결함이 발생하면 모든 결함에 대하여 해결을 완료하고 통합 시험 결과서를 작성한다

4.6.2. 활동 단계 개요

구 분	설 명
선행기준	1. 응용 소프트웨어 아키텍처 설계 완료 2. 응용 소프트웨어 통합 시험 계획 수립 완료 3. 응용 소프트웨어 통합 시험 명세 완료 4. 응용 소프트웨어 아키텍처 설계 리뷰 완료 5. 응용 소프트웨어 통합 시험 계획 / 명세 리뷰 완료 6. 응용 소프트웨어 단위 시험 완료
입력문서	• 응용 소프트웨어 아키텍처 설계서 • 응용 소프트웨어 통합 시험 계획서 • 응용 소프트웨어 통합 시험 명세서 • 응용 소프트웨어 아키텍처 설계 리뷰 결과 • 응용 소프트웨어 통합 시험 계획 / 명세 리뷰 결과 • 응용 소프트웨어 단위 시험 결과서 • 단위 시험 완료 소스 코드

수행흐름	
산 출 물	• 응용 소프트웨어 통합 시험 계획서 (갱신) • 응용 소프트웨어 통합 시험 명세서 (갱신) • 응용 소프트웨어 통합 시험 결과서 • 통합 바이너리 파일
완료기준	1. 응용 소프트웨어 통합 시험 계획서 갱신 완료 2. 응용 소프트웨어 통합 시험 명세서 갱신 완료 4. 응용 소프트웨어 통합 시험 및 결함 해결 완료 5. 응용 소프트웨어 통합 시험 결과서 작성 완료 6. 응용 소프트웨어 아키텍처 설계와 테스트 결과의 추적성 확보 7. 응용 소프트웨어 아키텍처 설계와 테스트 결과의 일관성 확보 8. 응용 소프트웨어 통합 바이너리 생성 완료

4.6.3. 세부 수행 활동

[1] 응용 소프트웨어 통합 시험 계획 갱신

응용 소프트웨어의 아키텍처 설계에 따라서 응용 소프트웨어가 개발되었는지 검증하는 활동에 대한 계획을 수립한 응용 소프트웨어 통합 시험 계획서를 필요 시 갱신한다.

가. 수행 절차

(1) 응용 소프트웨어 통합 시험 전략을 검토 및 갱신한다.

응용 소프트웨어가 응용 소프트웨어 아키텍처 설계와 안전 요구사항을 준수하여 개발되었는지 검증하기 위한 방법을 제공하는 응용 소프트웨어 통합 시험 전략을 검토하고 필요시 갱신한다. 응용 소프트웨어 통합 시험 전략에는 다음 항목을 포함한다.

A. 테스트 범위의 정의

B. 테스트와 관련된 특정 요구사항

C. 테스트 케이스 및 테스트 데이터 개발 방법 정의

D. 테스트 케이스 선정 기준의 정의

i. 신규 또는 변경된 요구사항의 범위

ii. 아키텍처 또는 인터페이스 사양의 변경 범위

iii. 변경 요청의 범위

iv. 항목 변경 범위

v. 변화 분석 (예: 인과 관계 분석)에 기반한 종속성 고려

vi. 기본 테스트 케이스를 포함하여 회귀 테스트에 적합한 테스트 케이스 선정.

E. 각 테스트 방법에 관한 테스트 환경의 정의

F. 프로젝트 계획 및 릴리즈 계획과 관련된 테스트 커버리지 정의.

G. 테스트 시작 / 완료 기준 정의

H. 실패한 테스트 처리 방법

(2) 응용 소프트웨어 통합 절차 및 통합 시험 대상을 검토 및 갱신한다.

소프트웨어 통합 평가 대상 및 제외 대상을 검토 및 갱신한다.

통합 절차 검토시에 다음의 고려 사항을 참고한다.

A. 응용 소프트웨어 통합과 관련된 기능상 의존성

B. 응용 소프트웨어 통합과 소프트웨어-하드웨어 통합 사이에서 의존성

(3) 응용 소프트웨어 통합 시험 방법을 검토 및 갱신한다.
응용 소프트웨어 통합 시험 방법에는 다음을 참고한다.

A. 인터페이스 테스트: 소프트웨어 통합 전 컴포넌트의 인터페이스 설계 준수 여부
B. 자원 사용 평가: 적정한 자원을 사용하는지 평가
C. 모델 기반 코드 평가: 모델과 코드 구현 결과의 일치성 평가
D. 요구사항 기반 평가: 소프트웨어 기능 평가
E. 결함 주입 테스트: 소프트웨어 악의 평가

(4) 응용 소프트웨어 통합 시험 상세 활동 계획을 검토 및 갱신한다.
상세 계획에는 다음 항목을 포함한다

A. 통합 시험 케이스 추출방법
B. 통합 시험 수행 시점
C. 통합 시험 수행 환경
D. 통합 시험 수행 준비 절차
E. 통합 시험 수행 절차
F. 통합 시험 수행 결과 정리

(5) 응용 소프트웨어 회귀 테스트 계획을 검토 및 갱신한다.

A. 변경된 응용 소프트웨어의 재검증을 위한 회귀 테스트 계획, 수행 여부, 절차를 검토하고 갱신한다.

[2] 응용 소프트웨어 통합 시험 명세 갱신

응용 소프트웨어가 아키텍처 설계에 따라서 개발되었는지 검증하는 활동에 대한 수행을 명세한 응용 소프트웨어 통합 시험 명세서를 필요시 갱신한다. 응용 소프트웨어 시스템 통합 시험 명세에는 다음의 사항이 명시되어야 한다.

소프트웨어를 관리 가능한 통합 세트로 분리
테스트 케이스 및 테스트 데이터
수행될 테스트 유형;
테스트 환경, 도구, 구성 및 프로그램
테스트 완료 판단 기준;
테스트 실패 시 시정 조치 절차

가. 수행 절차

(1) 응용 소프트웨어 통합 시험 케이스를 검토 및 갱신한다. 테스트 케이스를 추출할 때는 다음의 방법을 사용한다.

A. 요구사항 분석 기반

B. 동등 분할

C. 경계 값 분석

D. 탐사적 평가 기반

(2) 응용 소프트웨어 아키텍처 설계와 응용 소프트웨어 통합 시험 케이스 간의 추적성을 검토 및 갱신한다.응용 소프트웨어 통합 시험 추적 매트릭스에 작성된 응용 소프트웨어 아키텍처 설계와 통합 시험 명세서 간의 추적성을 검토 및 갱신하여 확보한다.

(3) 응용 소프트웨어 통합 시험 기준을 검토 및 갱신한다.응용 소프트웨어 통합 시험 계획서를 기반으로 응용 소프트웨어 통합 시험 기준을 상세화하고, 테스트 패스 기준을 수립한다. 패스 기준의 예로는 다음과 같다.

A. 소프트웨어 아키텍처 설계서 검토: 결함 수정률

B. 인터페이스 테스트: 테스트 케이스 패스율

C. 자원 사용 평가: 실행 시간, 메모리 사용량, 네트워크 부하 량

D. 모델 기반 평가: 테스트 케이스 패스율

E. 기능 평가: 테스트 케이스 패스율

F. 악의 평가: 테스트 케이스 패스율

G. 통합 소프트웨어 테스트 패스 기준

i. 함수 커버리지

ii. 호출 커버리지

(4) 응용 소프트웨어 통합 시험 자원 식별 내역을 검토 및 갱신한다.

A. 소프트웨어 통합 시험 조직

B. 소프트웨어 통합 시험 환경

C. 소프트웨어 통합 시험 측정 지표

(5) 응용 소프트웨어 통합 시험 결과 작성 절차를 검토 및 갱신한다.

A. 소프트웨어 통합 시험 결과서 작성 절차

B. 소프트웨어 통합 시험 결함 발견 및 해결 절차

[3] 응용 소프트웨어 통합 시험

응용 소프트웨어 통합 시험은 소프트웨어 모듈의 올바른 조립과 소프트웨어 컴포넌트 간의 상호 관계에 중점을 둡니다. 변수 및 상수의 잘못된 초기화, 매개변수 전송 오류, 모든 데이터 변경, 특히 전역 데이터, 잘못된 이벤트 및 작업 순서 지정과 같은 종류의 오류를 표시하는 데 사용할 수 있으며, 소프트웨어 통합 시험을 통하여 다음을 검증할 수 있어야 한다.

소프트웨어 실행의 순서가 정확함
모듈 간 데이터 교환
성능 기준 충족
글로벌 데이터의 변경이 없음

가. 수행 절차

개별 응용 소프트웨어 모듈 테스트가 완료되면 사전 정의된 통합 시험 케이스 및 테스트 데이터를 사용하여 응용 소프트웨어 통합 시험을 수행해야 한다. 이 테스트에는 기능적 "블랙 박스"및 성능 테스트가 포함되어야 한다.

(1) 인터페이스 테스트

소프트웨어 모듈을 개발하고 하고 나서 각 모듈을 통합했을 때 제대로 작동하는지를 검증하는 것이다. 즉 각 모듈의 개발이 끝나고 나면 단위 시험을 수행해서 개별 모듈에서 문재가 없다는 것을 검증하고 모듈을 통합했을 때 아키텍처 설계에서 정의한대로 각 모듈이 통신을 하는지 검증한다. 인터페이스 테스트 결과는 다음을 포함하여 작성한다.

A. 인터페이스 테스트 수행 시점
B. 인터페이스 테스트 수행 환경
C. 인터페이스 테스트 수행 절차
D. 인터페이스 테스트 수행 결과 정리

(2) 자원 사용 테스트

시스템에서 주요한 자원인 수행시간 측정, RAM/ROM 사용량, CPU 부하 등을 측정한다. 자원 사용 테스트는 각 개별 모듈, 응용 소프트웨어 전체에 대해서 수행할 수 있으며 자원 사용량을 측정하기 때문에 이런 측정이 가능한 테스트 케이스를 사용하여 수행한다. 자원 사용 테스트 결과는 다음을 포함하여 작성한다.

A. 자원 사용 테스트 수행 시점

B. 자원 사용 테스트 수행 환경

C. 자원 사용 테스트 수행 절차

D. 자원 사용 테스트 수행 결과 정리

(3) 기능 테스트

통합 소프트웨어의 기능이 제대로 동작하는지 검증하기 위해서 기능 테스트를 수행한다.

A. 기능 테스트는 요구사항 기반 테스트를 사용하여 아래 순서로 수행된다.

i. 테스트 케이스 도출

ii. 테스트 케이스 리뷰

iii. 기능 검증 수행

B. 기능 테스트 결과는 다음을 포함하여 작성한다.

i. 기능 테스트 수행 시점

ii. 기능 테스트 수행 환경

iii. 기능 테스트 수행 절차

iv. 기능 테스트 수행 결과 정리

(4) 악의 테스트

통합 소프트웨어가 악의적인 환경에서 기능이 제대로 동작하는지 검증하기 위해서 악의 테스트를 수행한다. 소프트웨어 악의 테스트에는 결함 주입 테스트를 사용하며 일반적으로 요구되는 안전고장율이 90% 이상인 경우에 수행하는데, 시

스템의 복잡도와 요구 안전 무결성 수준에 따라서 90% 이하에서도 수행해야 한다. 일반적인 테스트로는 달성할 없는 코드 영역을 테스트하기 위해서 고의적으로 결함을 주입하여 테스트하는 방법이다. 결함을 주입하는 시점에 따라서 컴파일 시 결함 주입과 런타임 시 결함 주입으로 나눌 수 있다. 컴파일 결함 주입은 컴파일 시 코드를 일부 수정하거나 결함을 삽입하는 별도 함수를 작성하여 테스트하는 방법이다. 런타임 시 결함 주입 방법은 소프트웨어 트리거를 사용해서 소프트웨어가 실행될 때 결함을 주입하는 방법으로 다음과 같은 기술들이 사용된다.

A. 메모리 영역 손상: 램, 프로세서 레지스터, I/O맵을 손상시키는 방법
B. 시스템 콜을 사용한 방법: OS 커널을 통해서 실행되는 소프트웨어에 결함을 주입하는 방법
C. 네트워크 레벨에서 결함 주입: 네트워크 패킷에 결함을 주입하는 방법
D. 악의 테스트 결과는 다음을 포함하여 작성한다.
E. 악의 테스트 수행 시점
F. 악의 테스트 수행 환경
G. 악의 테스트 수행 절차
H. 악의 테스트 수행 결과 정리

(5) 성능 테스트

A. 성능 테스트 케이스는 인터페이스 분석, 유즈케이스 분석, 사용 사례 분석 등을 통하여 추출할 수 있으며, 통합 소프트웨어의 안전 기능과 관련된 다음과 같은 성능을 측정하여 검증한다.
   i. 태스크 스케줄링
   ii. 타이밍
   iii. 입출력 시간
   iv. 결함 허용 시간
B. 성능 테스트 결과는 다음을 포함하여 작성한다.

i. 성능 테스트 수행 시점

ii. 성능 테스트 수행 환경

iii. 성능 테스트 수행 절차

iv. 성능 테스트 수행 결과 정리

나. 점검 항목

응용 소프트웨어 통합 시험 결과에 대하여 아래 항목을 점검해야 하며, 특정 테스트가 적용되지 않는 경우 이 테스트가 적용되지 않는 이유를 설명하고 점검 목록에 NA 표시한다.

No.	점검 항목	비고
01	통합된 응용 소프트웨어가 의도한 기능을 수행하는가?	
02	통합된 응용 소프트웨어가 의도하지 않은 기능을 수행하지 않는가?	
03	응용 소프트웨어 통합 시험 결과가 기준에 따라 판단되었는가?	
04	응용 소프트웨어 통합 시험 결과에 테스트 환경 구성 정보를 기술하였는가?	
05	응용 소프트웨어 통합 시험 결과가 형식에 맞도록 기술되었는가?	
06	응용 소프트웨어 통합 시험에서 발견된 결함이 분석되고 후속 조치가 완료되었는가?	
07	응용 소프트웨어 요구사항과 통합 시험 결과의 추적성이 확보되었는가?	
08	응용 소프트웨어 아키텍처 설계와 통합 시험 결과의 추적성이 확보되었는가?	
09	응용 소프트웨어 통합 시험 케이스가 모두 검증되었는가, 생략된 케이스에 대한 정당한 사유가 작성되었는가?	
10	결함에 대한 재설계, 코드 수정 및 제검증이 적절히 수행되었는가?	

다. 문서화

응용 소프트웨어 통합 시험 결과는 소프트웨어 통합 시험 보고서에 기록되어야 하며 최소한 다음 사항을 포함해야 한다.

(1) 통합 소프트웨어의 버전

(2) 수행된 시험에 대한 설명 (투입 물, 산출물, 절차)

(3) 통합 시험 결과 및 평가. 테스트 실행 플랫폼

(4) 테스트 기준 목표 충족 여부

(5) 고장이 있는 경우, 고장 이유 및 취해진 시정 조치

(6) 응용 소프트웨어 통합 시험 중에 소프트웨어 수정 또는 변경은 다음을 결정하는 안전 영향 분석의 대상이 된다.

A. 영향 받는 모든 소프트웨어 모듈

B. 필요한 모든 재검증 및 재설계 활동

제 5 장. 가이드 적용 사례

가이드 적용 사례

5.1. 기계류 제어 SRECS 개발 사례

5.1.1. 일반 사항

본 가이드에서 사용하는 IEC 62061 기반의 기계류 제어 시스템(이하 SRECS)의 설계에 대한 구조적 접근법은 안전 관련 제어 기능(이하 SRCF)에 대한 기능 및 안전 무결성 요구 사항이 여러 하위 기능으로 분해되는 방법론을 정의한다. 이 프로세스는 기능 안전을 위한 기술 프레임 워크를 기계 분야에 구현하는 데 사

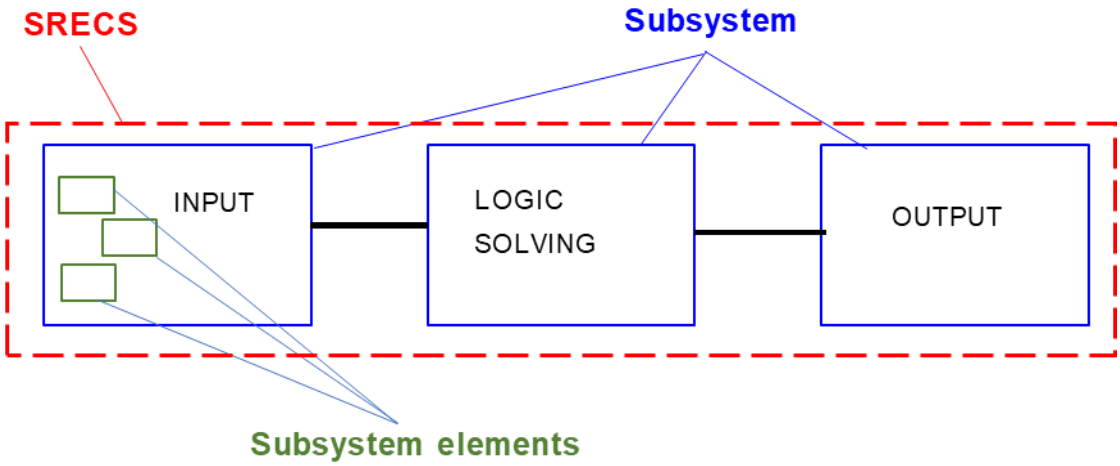


그림 32 기계 안전 기능 분해 용어

용되며, [그림 32]은 SRECS 설계를 기계 설비에 통합할 때 중요한 각 레벨에서 사용되는 용어를 설명한다.

이러한 개발 방법론은 SRECS가 안전 요구 사항 명세를 충족함을 입증하기 위해 검증 및 확인 프로세스를 사용할 수 있다. SRECS 설계의 다음 예는 SRECS 설계 및 통합 요구 사항에 따라 특정 안전 관련 제어 기능의 기능적 분해 및 실현 원리를 명확히 하기위한 것이다. 이 예시는 단순화되어 실제 실행에 필요할 수 있는 추가 수단을 고려하지 않는다.

일반적으로 위의 [그림 32]에 제시된 용어는 설계 과정을 두 가지 주요 단계로 구분하기위한 것이다.

- 기계 설계자 또는 제어 시스템 통합자가 수행할 수 있는 SRECS 설계
- 전기 장비 및 제어 장치 (예 : 전기접촉기, 연동 스위치, PLC) 및 기계 설계자 또는 제어 시스템 통합 업체 공급 업체에게 적용할 수 있는 서브 시스템 (및 서브 시스템 요소) 설계.

본 가이드에서 사용된 방법론은 안전 관련 제어 기능의 명세에 대한 구조화된 하향식 접근 방식과 이러한 기능을 구현하는 SRECS 설계를 기반으로 한다.

본 예시에서는 기계 관점에서의 위험 분석과 평가, SRECS 관점에서의 SRCF 명세 및 SRECS 아키텍처 설계 및 서브 시스템 실현 및 달성된 SIL 결정에 대하여 IEC 62061을 적용하여 실용적인 예제를 간략하게 설명한다. 응용 소프트웨어 요구사항 명세, 설계 및 개발, 통합 및 테스팅에 대하여서는 가이드와 템플릿만을 설명하고, 추가적으로 형상관리, 소프트웨어 기반 매개 변수화, 기능 안전 계획 작성 가이드를 제공한다.

5.1.2. 기계 안전 시스템 개발 예시

[1] 예시 기계의 특성

- 블레이드가 기계에서 회전
- 힌지 보호 덮개를 블레이드 보호용으로 사용
- 작업자가 정기적으로 청소할 때 보호 덮개를 열어 블레이드에 접근

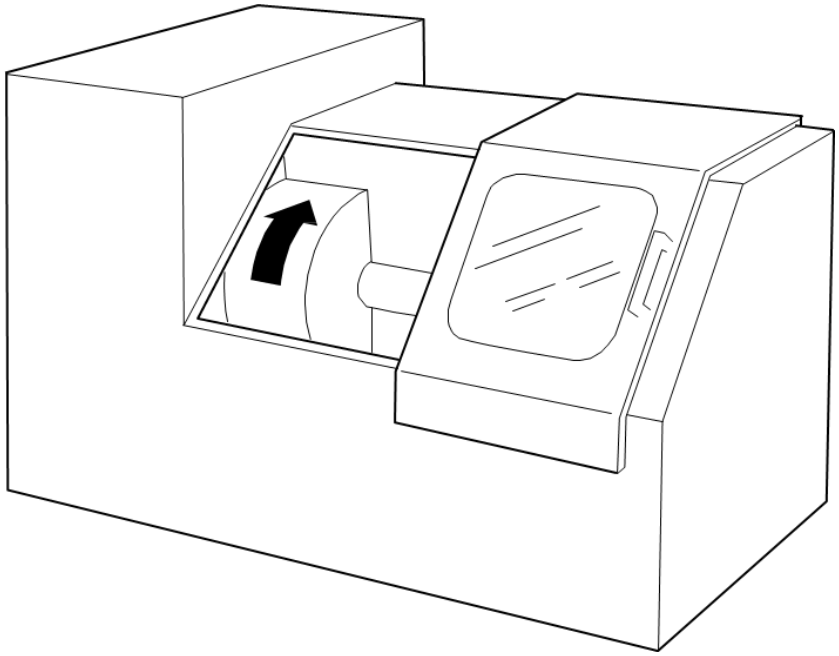


그림 33 예시용 기계

[2] SRCF 안전 기능 명세

가. 위험 분석

안전 기능은 실패로 인해 위험이 즉각적으로 증가할 수 있는 기계의 기능으로 원치 않는 이벤트가 발생할 가능성을 줄이고 위험을 노출시키기 위해 취한 조치이다. 안전 기능은 기계 작동의 일부가 아니며, 이러한 기능이 실패하면 기계는 정상적으로 작동할 수 있지만 작동으로 인해 부상을 당할 위험이 높아진다. 따라서 위험 분석 및 위험 제거 또는 최소화 방법 평가를 수행하여 위험을 제거하거나 허용 수준까지 줄이기 위해 어떤 안전 기능과 성능이 필요한지 정의해야 한다.

기계 고유의 위험이 있는 경우 각각의 특정 위험 요소에 대하여 위험 평가를 수행하여 위험 감소 프로세스가 필요한 것으로 결정된 모든 안전 기능의 식별을 포함하여 기계에 대한 위험 평가를 수행한다. 기계의 위험 평가는 보호 수단이 없다고 가정하고 기계 작동에 대한 위험 평가를 수행하며 이 평가의 결과로 무

시할 수 없는 것으로 간주되는 위험이 있는 경우, 적절한 보호 수단을 수립하여 위험 감소 프로세스에 할당하고, 위험이 무시될 때까지 위험 평가를 반복하여 수행한다

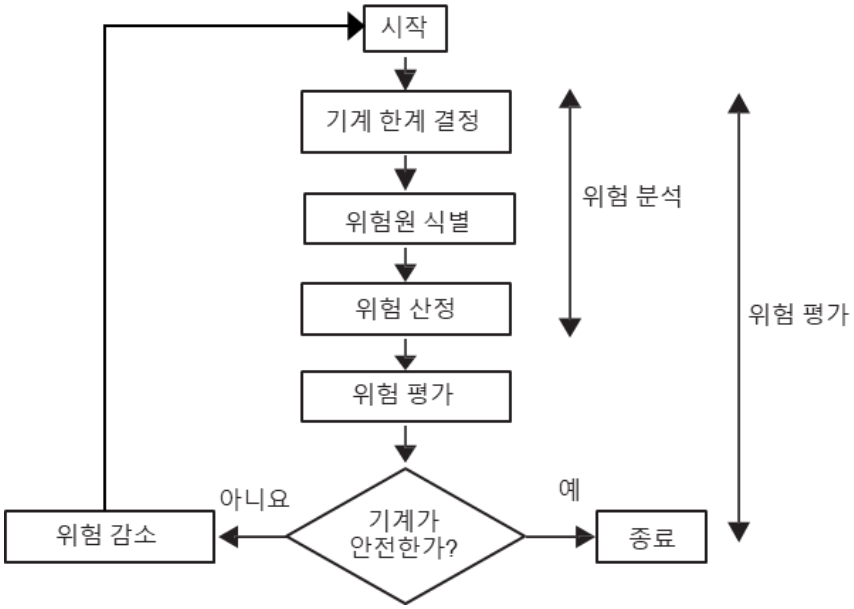


그림 34 기계 설계 중 위험 평가 접근법

기계 위험 평가는 다음 사항을 고려해야 한다.

- 기계 수명의 모든 단계 (예: 제조, 설치, 시운전, 조립, 조정)와 관련된 위험
- 기계의 의도된 사용: 올바른 사용, 비 산업/가정용, 합리적으로 예측 가능한 오용
- 기계 주변의 공간 제한 및 이동 범위의 적합성
- 기계 사용자에 대한 예측 가능한 훈련, 능력 및 경험 수준

보호 장치, 절차 및 간판과 같은 기존의 위험 감소 조치는 위험 요소를 식별할 때 고려하지 않으며, 다양한 보호 수단의 상대적인 장점을 고려할 때, 특정 평가에 대하여 다음과 같이 효과의 가중치를 고려하여 부여한다.

1) 최대 효과

본질적으로 안전한 설계 조치, 즉 안전한 설계 작성, 프로세스 변경

2) 다소 효과

보호 및 보완 조치, 즉 안전 관련 제어 기능, 기능 안전, 정적 가딩

3) 낮은 효과

사용에 대한 정보, 즉 경고 표시, 신호, 기계 장치 및 작동 지침

4) 최저 효과

추가 예방 조치, 즉 절차, 교육 훈련을 통한 사용자 보호 조치

예시 기계에 대한 위험 분석결과는 다음과 같다.

- 기계에 위험 요소가 있음
- 위험을 최소화하기 위한 SRCF가 필요함

위험원	요구되는 안전기능
보호 커버가 열리면 작업자는 회전 날에 심각한 상해를 입을 수 있다.	"회전 날 멈춤"

나. 위험 평가

위험 평가는 각 위험원에 대한 위험을 최소화하기 위해 취해야 할 조치를 분석한다. 해당 수단이 SRCF 인 경우이 SRCF에 대해 필요한 안전 무결성 수준(SIL)을 정의해야 한다. SIL은 위험 요소의 잔류 위험이 허용 가능하게 낮도록 정의된다.

위험 산정을 수행하는 방법에는 리스크 매트릭스, 리스크 그래프, 수치 스코어링 및 하이브리드 접근법이 있는데 SRECS의 안전 무결성은 일반적으로 리스크 매트릭스를 사용하여 필요한 SIL을 결정하기 위해 위험 평가를 수행한다. 위험을

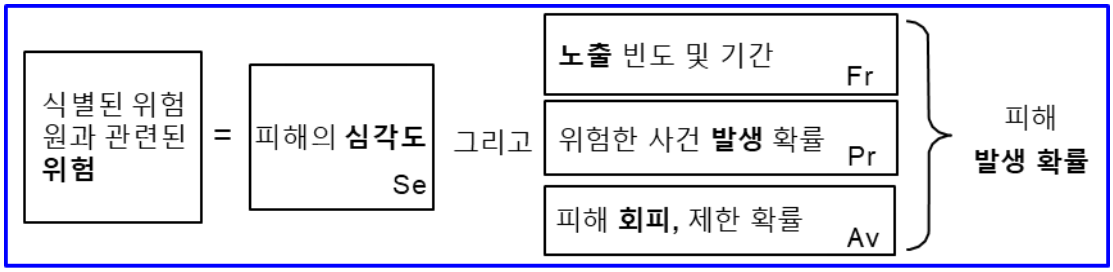


그림 35 위험 산정 및 평가

평가한 후 SRCF에 요구되는 SIL을 결정할 수 있다. 일반적으로 다음 사항이 적용되며, 결정된 위험이 높을수록 필요한 SIL이 높아진다.

피해의 심각도는 다음의 표를 적용하여 평가한다

피해의 심각성	Se
회복 불가 : 예) 사지 절단	4
회복 불가 : 예) 사지 골절	3
회복 가능 : 예) 병원 치료	2
회복 가능 : 예) 응급 처치	1

결정된 피해와 심각도(Se)는 다음과 같다.

구분	설명
입력	블레이드에 접촉하면 손가락 또는 팔이 손상될 수 있다
결과	Se = 4

아래의 표는 사람이 위험에 얼마나 자주 얼마나 노출되어 있는지를 평가하는데 사용된다.

노출		Fr
빈도	지속 시간 > 10 분(*1)	
<= 1 시간	예	5
1 시간 ~ 1 일	예	5
1 일 ~ 2 주	예	4
2 주 ~ 1 년	예	3
> 1 년	예	2

결정된 위험 노출 빈도 및 기간(Fr)은 다음과 같다.

구분	설명
입력	작업자는 운영 주기마다 적어도 한 번 보호 커버를 열어야 하며, 그러면 작업자는 약 15 분 동안 위험구역에 있게 된다.

결과	Fr = 5

아래의 표는 위험의 발생 가능성(Pr)을 평가하는 데 사용된다.

발생 확률	**Pr**
매우 높음	5
높음	4
낮음	3
매우 낮음	2
거의 없음	1

결정된 위험한 사건 발생 가능성은 다음과 같다.

구분	설명
입력	보호 커버가 열려 있으면 작업자가 블레이드의 작동 범위 안에 들어갈 가능성이 있습니다.
결과	Pr = 4

아래의 표는 작업자가 해를 피할 수 있는지 여부(Av)를 평가하는 데 사용된다.

위험 회피 또는 제한 가능성	Av
불가능	5
거의 없음	3
가능	1

결정된 피해를 피하거나 제한할 가능성 다음과 같다.

구분	설명
입력	작업자가 블레이드를 피할 가능성이 거의 없다.
결과	Av = 3

아래의 표는 SRCF 의 SIL 을 결정하는 데 사용된다.
클래스 C1 은 Fr, Pr 및 Av 에 대한 값을 더하여 결정된다.

- Cl = Fr + Pr + Av (5 + 4+ 3)

위해 심각도	**Class Cl**

Se	3 ~ 4	5 ~ 7	8 ~ 10	11 ~ 13	14 ~ 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3			SIL 1	SIL 2	SIL 3
2				SIL 1	SIL 2
1					SIL 1

결정된 SRCF 에 필요한 SIL 평가 결과는 다음과 같다.
SRCF 에 요구되는 안전 무결성 수준은 SIL3 이다.

구분	결과
입력	Se = 4
	Cl = 5 + 4 + 3 = 12
안전 무결성 수준	SIL 3

안전 무결성 요구사항은 각 SRCF의 시간당 위험한 실패 가능성에 대한 목표 실패 값으로 표시된다. 각 SRCF에 대한 안전 무결성 요구사항은 아래 표와 같이 SIL로 지정되고 관리되어야 하며, 이에 따라 결정된 시단당 위험 실패 확률은 아래의 테이블을 참고하여 10^{-7} 보다 작아야 한다.

안전 무결성 수준	시간당 위험 실패 확률 (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

다. SRCF 명세 개발

기계에서 필요한 안전 관련 제어 기능 (SRCF)을 식별한 후 이제 SRCF를 명세한다.

SRCF 안전 요구 사항 명세에서 다음 정보가 도출될 수 있다.

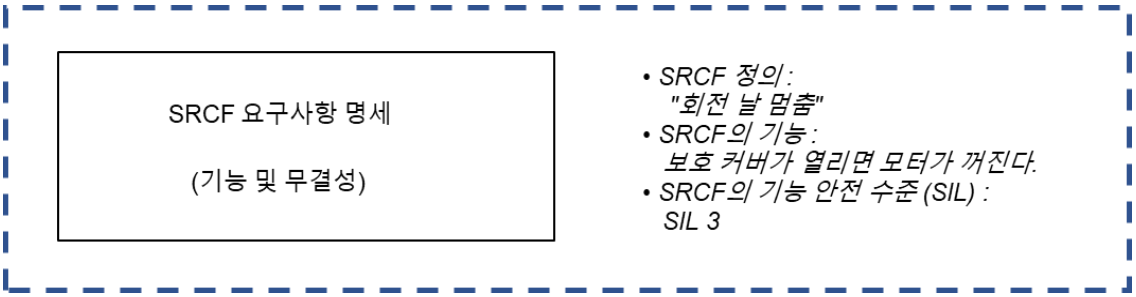


그림 36 SRCF 요구사항 명세

SRCF에 대한 모든 중요한 정보의 기술은 다음과 같다.

구분	정보
SRCF 가 예방할 수 있는 장비의 위험 요소	보호 커버가 열리면 작업자는 회전하는 블레이드로 다칠 수 있다.
기계에 접근 가능한 사람	유지보수 작업자
SRCF 가 활성화될 기계의 모드	“청소” 모드

SRCF의 기능에 대한 요구 사항 설명은 다음과 같다.

구분	요구 사항
SRCF 의 기능	보호 커버가 열리면 모터를 꺼야 한다.
SRCF 가 활성화 또는 비활성화되어야 하는 조건	SRCF 는 시스템에서 항상 활성화되어야 한다.
요구 반응 시간	보호 커버가 열리면 최소한 200ms 이내에 모터를 정지해야 한다.
결함에 대한 반응	오류가 발생하면 다음 반응을 수행해야 한다. • 모터 스위치 끄기 • “장애” 표시등 켜기

	아래의 모든 요구사항이 충족될 경우에만 모터를 다시 켤 수 있어야 한다. • 오류 수정 완료 • 보호 커버 닫힘 • 작업자가 기계의 버튼을 통해 확인 완료
전자 기계 구성요소의 작동 주기 비율	보호 커버 위치 스위치: • 주기당 1회 (매 8시간마다 1회)
	모터 접촉기: • 주기당 1회 (매 8시간마다 1회)

SRCF의 안전 무결성에 한 요구 사항 설명은 다음과 같다.

구분	요구 사항
SRCF 의 안전성 무결성 레벨 (SIL)	SIL 3
SRCF 의 PFH_D 값 (PFH_D)	$PFH_D < 10^{-7}$

[3] SRECS 설계 및 개발

가. SRECS 구조

예시 기계에 대한 SRECS 아키텍처는 아래와 같다.

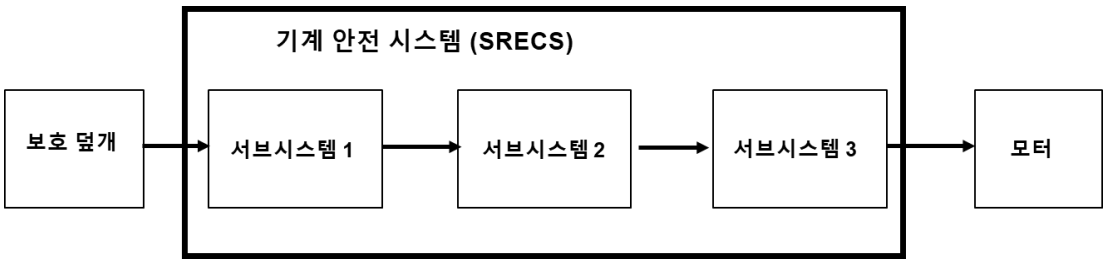


그림 37 SRECS 아키텍처

SRECS는 아래와 같이 3개의 서브시스템과 기능으로 구성된다.

서브 시스템	기능	컴포넌트
서브시스템 1	두 개의 위치 스위치를 통해 보호 커버의 위치 감지	안전 도어

서브시스템 2	PLC 로 신호 처리	로직 컨트롤러
서브시스템 3	두 개의 접촉기를 통해 모터 스위치 끄기	접촉기

나. SRCF 기능 블록 식별

예시 기계의 SRCF는 세 개의 기능 블록으로 구분된다. SRCF를 수행하려면 세 가지 기능 블록이 모두 필요하며, 기능 블록이 실패하면 전체 SRCF가 실패한다. SRCF 명세는 SRCF가 SIL 3을 준수해야한다고 정의하였다. 즉, 각 기능 블록은 최소한 SIL 3을 준수해야한다.

아래 그림과 표는 기능 블록의 분할을 보여준다.

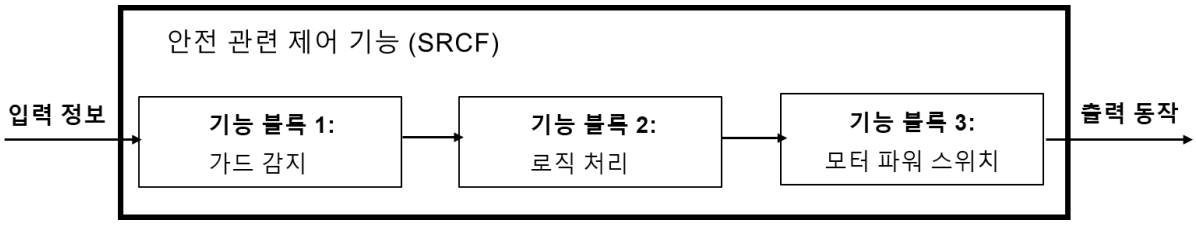


그림 38 SRCF 기능 블록 분할

예시 기계의 SRCF 기능 블록에 대한 기능은 다음과 같다.

기능 블록	기능
기능 블록 1	가드 감지: 가드 도어 위치에 대한 감지가 제공된다.
기능 블록 2	로직 처리: 가드 감지 결과를 입력으로 받아 모터 작동 중에 가드 도어가 열리면 모터 전원 차단 출력을 보낸다.
기능 블록 3	모터 파워 스위치: 모터 전원을 끈다..

다. SRCF 기능 블록 요구 명세

SRCF의 각 기능 블록에 대한 요구사항은 다음과 같은 구조의 테이블을 사용하여 작성한다.

각 기능 블록	설 명

입력	기능 블록에 필요한 입력 정보 기술
출력	기능 블록의 출력 정보 기술
기능	기능 블록의 수행 작업 기술

예시 기계의 SRCF의 기능 블록 1 "가드 감지"에 대한 요구사항은 다음과 같다

기능 블록 1	설 명
입력	보호 커버의 위치 : "열림"또는 "닫힘"
출력	보호 커버 위치 정보 : • 보호 커버가 열림 • 보호 커버가 닫힘
기능	기기의 모든 모드 : • 보호 커버 위치 감지.

예시 기계의 SRCF의 기능 블록 2 "로직 처리"에 대한 요구사항은 다음과 같다

기능 블록 2	설 명
입력	보호 커버 위치 정보 (기능 블록 1 의 출력)
출력	모터 제어 명령: • 보호 커버가 열리면 모터 전원 공급 장치 단절
기능	기계의 모든 모드: • 보호 커버 위치 및 해당 모터 제어에 대한 정보 평

예시 기계의 SRCF의 기능 블록 3 "모터 파워 스위치"에 대한 요구사항은 다음과 같다

기능 블록 3	설 명
입력	모터를 제어하는 명령 (기능 블록 2 의 출력)
출력	없음
기능	기계의 모든 모드: • 모터를 전원 공급으로부터 분리

라. 서브 시스템에의 기능 블록 할당

SRECS 안전 요구사항 명세에 명시된 각 SRCF는 아래 그림과 같이 기능 블록의 구조로 분해되어 서브 시스템에 할당된다.

분해 과정은 SRCF의 기능 및 무결성 요구사항을 완전하게 설명하는 기능 블록 구조로 이루어져야 한다. 이 프로세스는 기능 블록의 전체 기능 요구사항을 서브시스템에 할당할 수 있는 경우, 각 기능 블록에 대해 결정된 기능 및 무결성 요구사항을 서브시스템에 할당할 수 있는 수준까지 적용해야 한다.

하나 이상의 기능 블록을 단일 서브 시스템에 할당하는 것이 가능하지만, 하나의 기능 블록을 개별적인 기능 및 무결성 요구사항을 가지고 있는 여러 서브시스템에 할당할 수 없다.

각 기능 블록의 입력과 출력은 속도, 위치, 작동 모드 등과 같이 전송되는 정보이며, 기능 블록은 SRCF의 기능을 나타내며 SRECS 진단 기능은 포함하지 않는다. 진단 기능은 SRCF와는 다른 구조의 별도의 기능으로 간주된다.

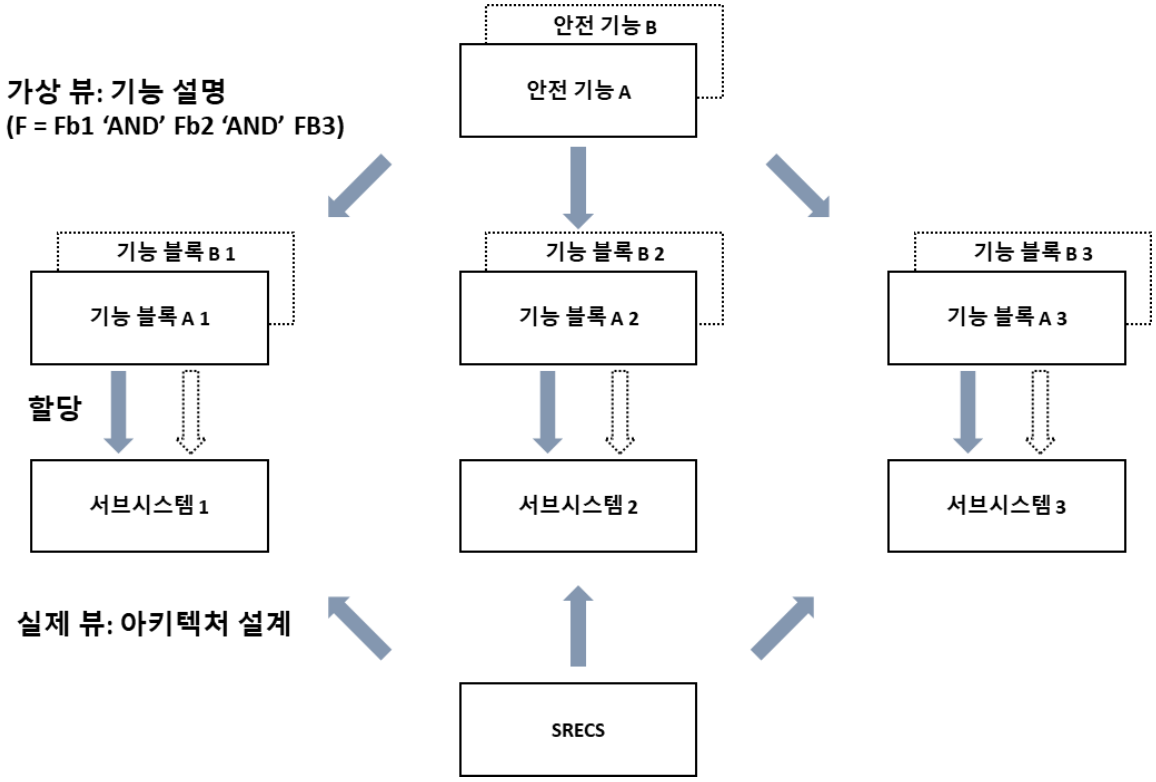


그림 39 서브 시스템에 대한 기능 블록의 안전 요구 사항 할당

각 기능 블록은 SRECS 구조 내의 서브시스템에 할당되어야 한다. 하나 이상의 서브 시스템에 하나 이상의 기능 블록이 할당될 수 있으며, 각 서브 시스템과 할당된 기능 블록은 명확하게 식별되어 아키텍처는 서브 시스템과 그 상호 관계를 설명하고 문서화되어야 한다.

하드웨어 안전 무결성과 관련하여 SRCF에 대해 제기할 수 있는 최고 안전 무결성 수준은 SRCF를 수행하는 서브시스템의 하드웨어 내결함성 및 안전 고장율

안전 고장률	하드웨어 내결함성 (비고 1)		
	0	1	2
< 60 %	허용 불가	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (비고 2)
≥ 99 %	SIL3	SIL3 (비고 2)	SIL3 (비고 2)
비고 1 N의 하드웨어 결함 허용은 N + 1 결함이 안전 관련 제어 기능의 손실을 초래할 수 있음을 의미 비고 2 SIL 4의 경우 IEC 61508-1 참조			

그림 40 서브 시스템에 대한 아키텍처 제약 사항

에 의해 제한된다. 아래 그림의 아키텍처 제약은 SRCF의 기능 블록을 구현하는 각 서브 시스템에 적용되어야 한다.

단일 서브시스템 엘리먼트만을 포함하는 서브시스템은 아래 테이블의 요구사항을 충족시켜야 한다. 특히, 하드웨어 내결함성이 0인 서브시스템의 경우, 99 % 이상의 SFF는 SRECS 진단 기능에 의해 달성되어야 한다. 이 요구사항은 SIL 3의 SILCL을 정당화하기 위해 하나의 서브시스템 엘리먼트만을 포함하는 서브시스템에 아키텍처 제약 조건의 적절한 형태가 적용되도록 보장하기 위해 필요하다

SRCF, 기능 블록, 서브 시스템은 SIL 3를 만족해야 하고, 안전 고장률(SFF)는 99% 이하 이어야 하므로, 예시 기계에 대한 SRCF 기능 블록의 서브 시스템 할당은 아래와 같다.

기능 블록		서브 시스템	
1	가드 감지: 가드 도어 위치에 대한 감지가 제공된다.	1	진단 기능을 포함하여 이중화: 열림 동작을 감지하는 두개의 위치 스위치
2	로직 처리: 가드 감지 결과를 입력으로 받아 모터 작동 중에 가드 도어가 열리면 모터 전원 차단 출력을 보낸다.	2	안전 PLC
3	모터 파워 스위치: 모터 전원을 끈다..	3	진단 기능을 포함하여 이중화: 리드 백 접점이 있는 두개의 접촉기

예시 기계의 SRECS 아키텍처 설계는 다음과 같다.

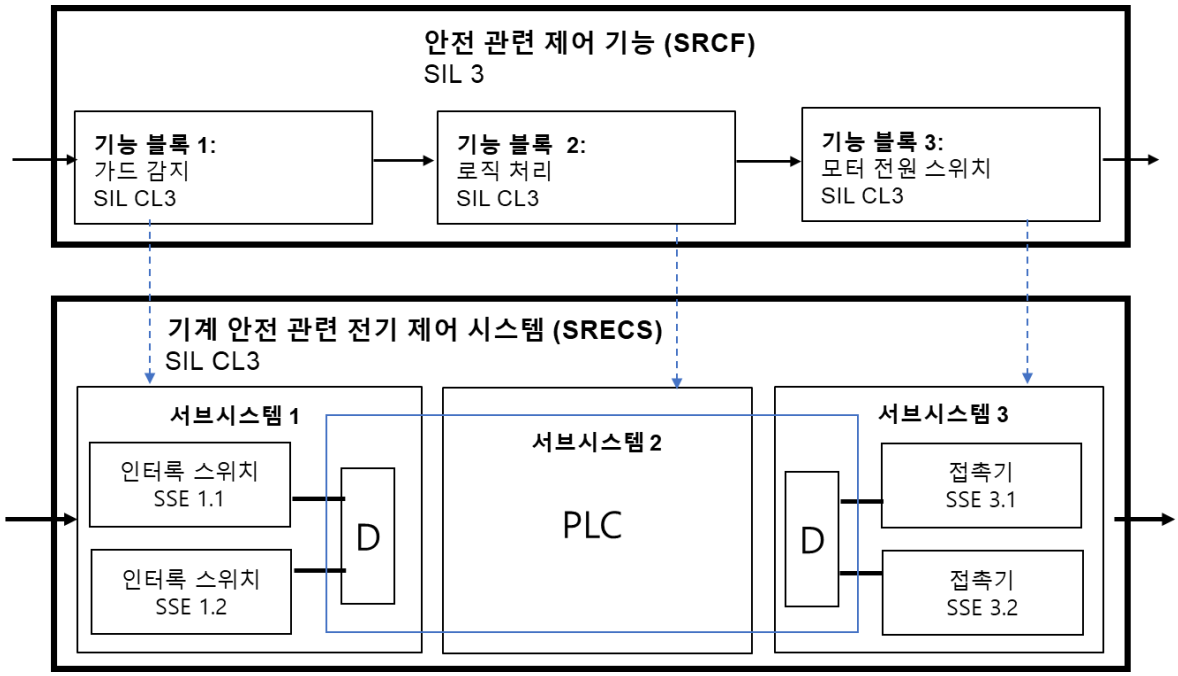


그림 41 SRECS 아키텍처

예시 기계의 각 서브 시스템은 다음과 같은 기능을 수행한다.

서브 시스템	기능
1	감지: 보호 커버 위치 감지
2	평가: 감지된 위치를 평가하고 조치를 트리거 한다
3	반응: 모터를 공급 장치에서 분리한다.

마. 서브 시스템 실현

SRECS의 아키텍처 설계가 완료된 후 SRECS의 서브 시스템이 실현된다. 할당된 기능 블록의 모든 안전 요구사항을 충족하는 서브시스템을 구현하기 위하여 다음의 두 가지 접근 방법을 고려한다.

- 해당 서브시스템에 대한 요구사항을 충족시키기에 충분한 장치의 선정
- 기능 블록 엘리먼트를 결합하고 배열 방식 및 상호 작용 방식을 명세하여

서브시스템을 설계 및 개발

서브 시스템 설계 및 개발은 아래 그림의 모든 측면을 고려하여 명확하게 정의된 프로세스를 따라야한다.

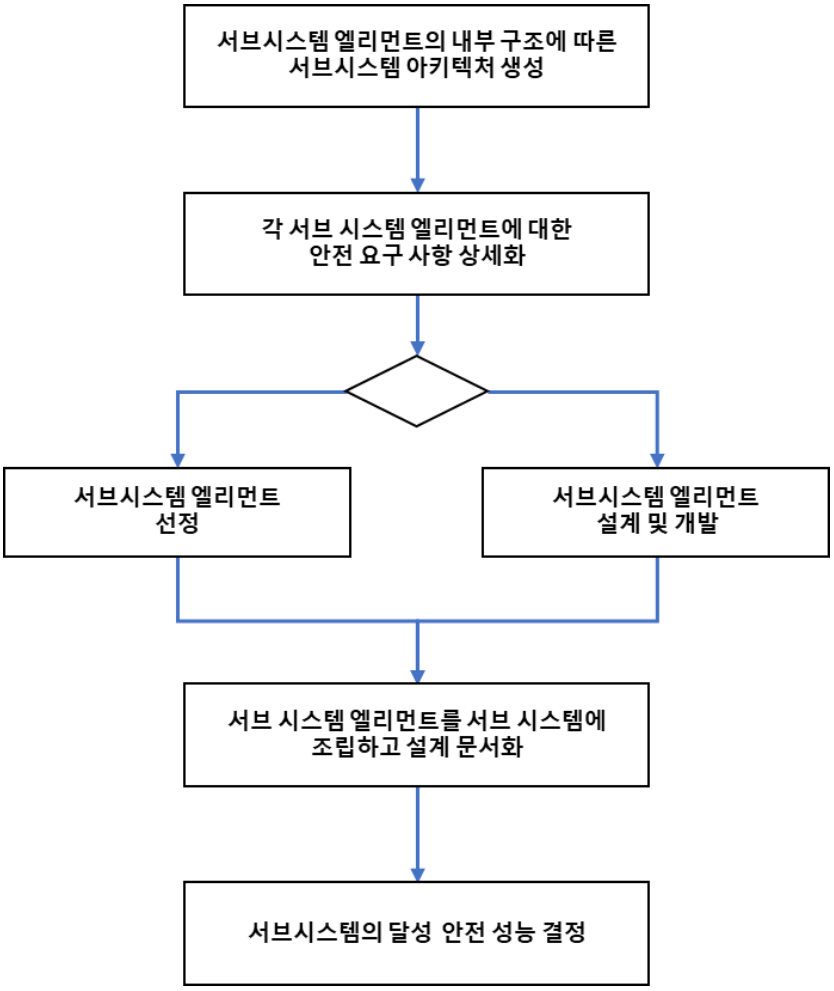


그림 42 서브시스템 설계 및 개발 작업 흐름

서브 시스템 아키텍처 설계 중에 분해 프로세스는 기능 블록의 기능적 요구사항을 완전히 나타내는 기능 블록 엘리먼트의 구조로 이어져야 한다. 이 프로세스는 각 기능 블록 엘리먼트에 대해 결정된 기능 요구사항이 서브시스템 엘리먼트에 할당되도록 허용하는 수준까지 적용해야 한다

기능 블록의 기능 블록 엘리먼트 및 관련 서브시스템 엘리먼트로 분해는 아래의 그림과 같다.

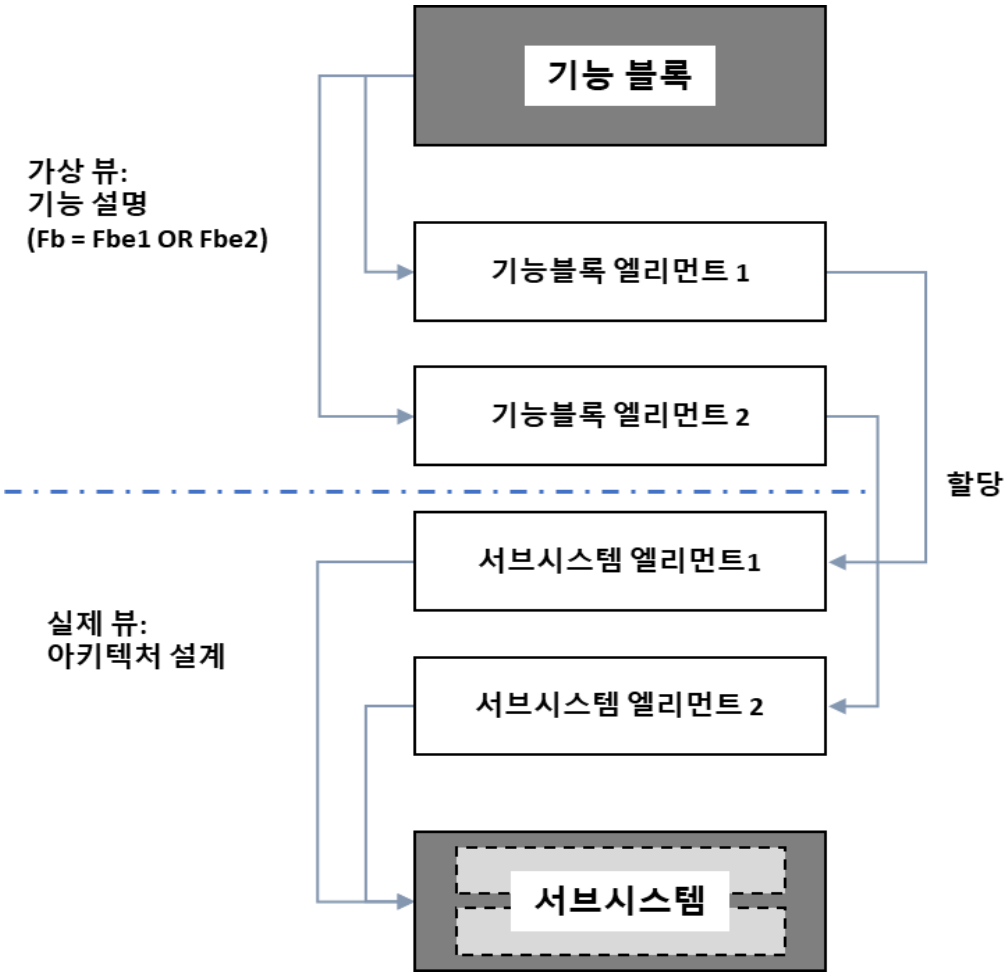


그림 43 기능블록 분해 및 할당

서브시스템 아키텍처는 엘리먼트와 엘리먼트 간의 상호 관계에 대해 문서화해야 한다. 필요시 서브시스템 엘리먼트에 할당된 기능 블록 엘리먼트와 관련된 정보도 포함해야 한다

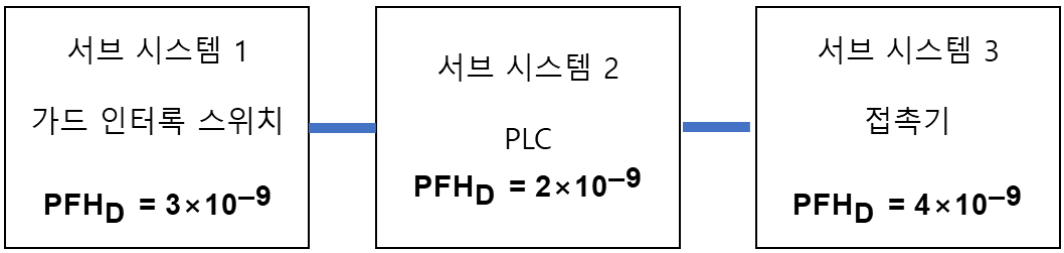
바. SRECS 에 의해 달성된 SIL 의 결정

실현된 기계 안전 시스템 (SRECS)으로 각 안전 관련 제어 기능 (SRCF)에 대해 필요한 안전 무결성 레벨 (SIL)이 달성되는지 여부가 점검된다.

예시 기계의 SRCF에 대해 서브 시스템으로 구성된 안전 시스템 (SRECS)이 실현되었으며, 속성은 아래 표에 요약되었다.

서브 시스템	SIL CL	PFH_D
서브시스템 1	3	$3 * 10^{-9}$
서브시스템 2	3	$2 * 10^{-9}$
서브시스템 3	3	$4 * 10^{-9}$

따라서 이 예시에서 SRECS의 설계는 SIL 3에서 할당된 안전 관련 제어 기능을



구현하기위한 모든 요구 사항을 충족할 수 있다.

$$PFH_{DSRECS} = (3 \times 10^{-9}) + (2 \times 10^{-9}) + (4 \times 10^{-9}) = 9 \times 10^{-9}$$

5.1.3. 기계류 제어 분야 안전 기능 적용 예시

비상 정지, 안전 가드, 접근 감지 기능 등 기계의 안전에는 센서, 입력 장치, 로직 처리 장치, 출력 장치를 포함한 여러 요소가 필요하다. 이러한 요소들은 통합되어 IEC 62061의 안전 무결성 수준을 준수하도록 성능을 제공해야 하며, 안전 기능 적용의 예로는 다음과 같다.

[1] 인터록 안전 기능

인터록 안전 기능은 무접점 인터록 스위치 및 긴급 정지 버튼(E-Stop)을 입력 장치로, PLC를 로직 제어 장치로, 안전 컨택터를 출력 장치로 구성 및 통합하여 안전 시스템을 구축한다.

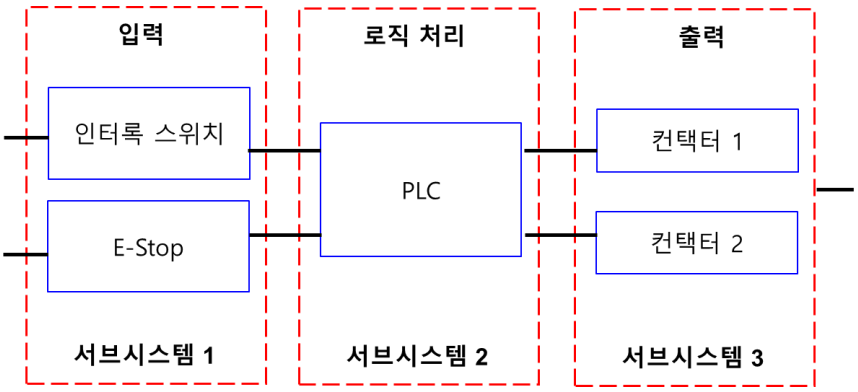
(1) 안전 기능

- 도어가 열려 있다는 것을 안전 시스템이 감지할 때 위험 요소로부터 전원을 제거하는 도어 모니터링 기능
- 안전 시스템이 E-Stop이 작동했다는 것을 감지하면 위험 요소에서 전원을 제거하는 E-Stop 기능

(2) 안전 기능 요구 조건

가드 도어가 열리면 모터에서 전원이 제거되어 위험 모션을 중단 및 방지하고, 도어를 닫으면 리셋 등의 2차 조치를 취할 때까지 위험 모션과 모터 전원 공급이 다시 시작되지 않는다.

E-Stop 버튼을 누르면 모터에서 전원이 제거되어 위험 모션을 중단 및 방지하고, 모터가 관성을 정지한다. E-Stop 버튼을 놓으면 리셋 등의 2차 조치를 취할 때까지 위험 모션과 모터 전원 공급이 다시 시작되지 않는다. 도어 인터록 스위치, 배선 단자 또는 안전 컨트롤러의 결함은 다음 안전 요청 전에 검출된다. 이 두 안전 기능은 IEC 62061 기준 SIL3 요건을 충족한다.



(3) SRECS 아키텍처 설계 예

[2] 라이트 커튼 안전 기능

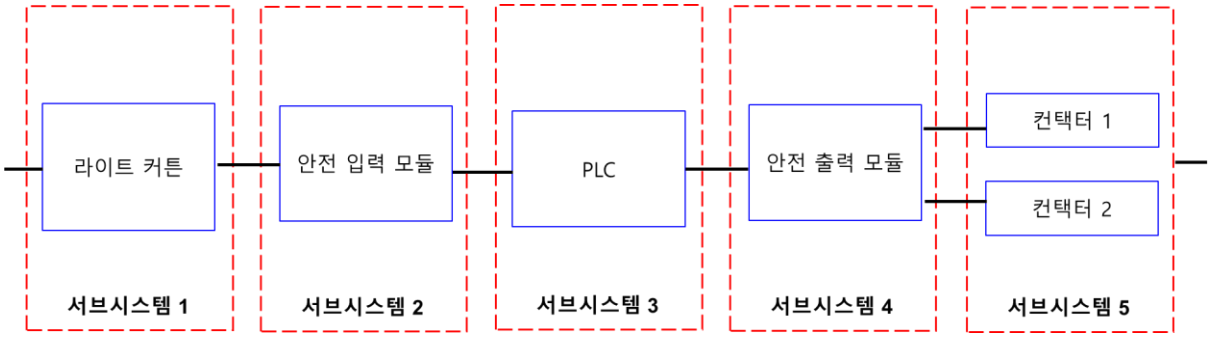
라이트 커튼을 모니터링하여 요청이 있거나 모니터링 회로에 결함이 감지되면 제어 장비의 전원을 차단한다.

(1) 안전 기능

- 라이트 커튼의 감지로부터 개시된 위험과 관련된 동작의 안전한 정지

(2) 안전 기능 요구 조건

라이트 커튼을 차단하면 모터 전원이 제거되어 위험 모션이 중단 및 방지된다. 라이트 커튼을 리셋 하면 2차 조치(시작 버튼 누름)를 취할 때까지 위험 모션과 모터 전원 공급이 다시 시작되지 않는다. 라이트 커튼의 안전거리 위치는 사용자가 위험 요소에 도달하기 전에 위험 모션을 멈출 수 있도록 설정되어야 한다.



(3) SRECS 아키텍처 설계 예

[3] 양손 조작 안전 기능

양손 조작식 안전 시스템은 작업자가 각 버튼을 한 손으로 동시에(0.5초 이내 간격) 눌러 작업자가 적절하고 안전한 위치에 있다는 것을 확인하면, 두 컨택터에 전원이 공급되어 위험 모션을 작동시키고, 한 손이나 양손을 떼면 시스템이 안전 컨택터를 끈다.

(1) 안전 기능

- 라이트 양손 조작식 모니터링 안전 기능: 작업자의 손이 양손 조작식 버튼에 동시에 놓여 있을 때만 전원이 위험 요소로 공급된다. 버튼에서 한 손이나 양손을 떼면 전원이 제거된다.
- Emergency Stop 안전 기능: 안전 시스템이 Emergency Stop이 작동했다는 것을 감지하면 위험 요소에서 전원이 제거된다.

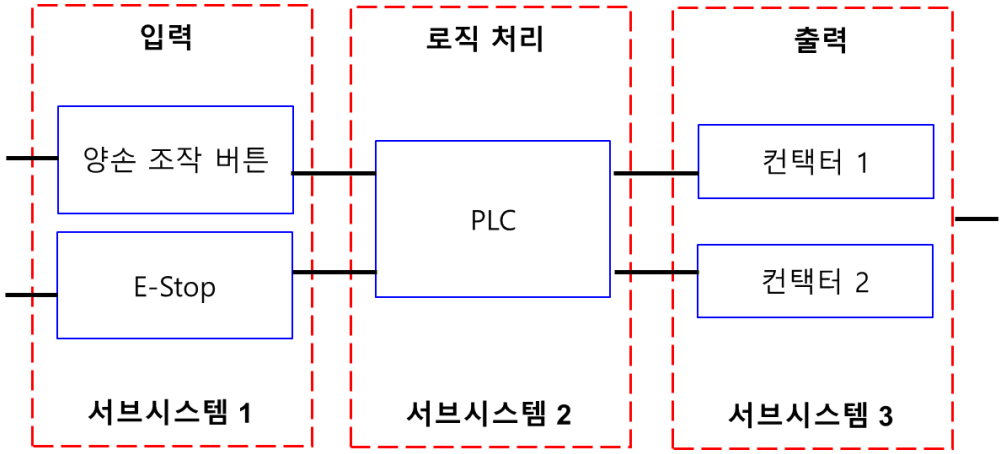
(2) 안전 기능 요구 조건

라이트 양손 조작식 모니터링 안전 기능: 모터에 전원을 공급하기 위해 양손 조작식 버튼의 연속 작동을 요구함으로써 위험 모션 중 작업자의 손 위치를 제어한다. 두 버튼의 동시 작동은

0.5초 이내에서 이루어져야 하며, 양손 조작식 버튼에서 한 손이나 양손을 떼면 모터에서 전원이 제거된다. 양손 조작식 버튼에 양손을 동시에 올려 놓으면

위험 모션이 재시작 한다. 양손 조작식 버튼, 배선 단자 또는 안전 컨트롤러의 결함은 다음 안전 요청 전에 검출된다.

비상 정지 안전 기능: 비상 정지 버튼을 누르면 모터 전원이 제거되어 위험 모션이 중단 및 방지된다. 비상 정지 푸시 버튼을 리셋 하면 2차 조치(리셋 버튼을 눌렀다 놓음)를 취할 때까지 위험 모션과 모터 전원 공급이 다시 시작되지 않는다. 이 비상 정지 기능은 장비의 다른 안전 기능을 보완하는 기능이고, 다른 안전 기능의 성능을 저해해서는 안 된다.



(3) SRECS 아키텍처 설계 예

5.2. 공정 제어 분야 SIS 개발 사례

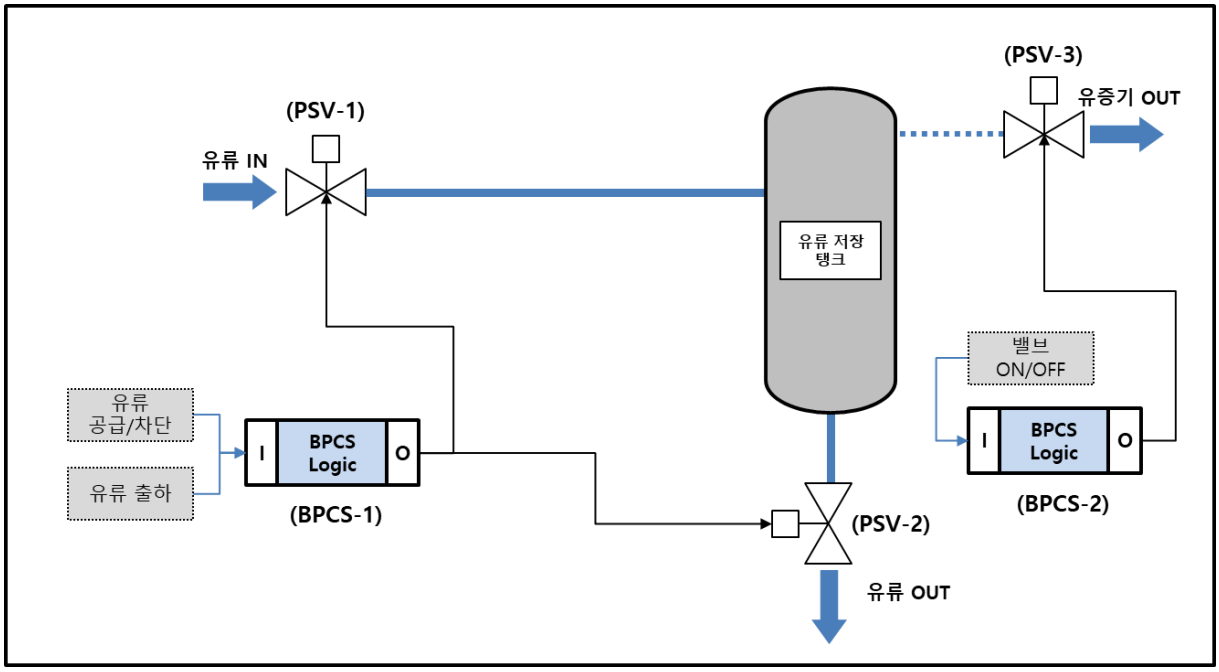
5.2.1. 대상 시스템 및 연구 목적

공정 제어 분야 SIS 개발 사례 연구 대상은 유류 탱크 저장 시스템으로 원양선이나 탱크로리 등으로부터 유류를 입하되고 필요시 다시 원양선이나 탱크로 출하하기 위해 유류를 저장하고 관리하는 공정 시스템이다. 초기 입하와 출하 및 유증기 처리를 위한 기본 시스템만 설계 및 구축된 상태에서 위험 분석을 통해 발생 가능한 위험원을 도출하고, 도출 된 위험원으로부터 유류 탱크 저장 시스템을 안전하게 보호하기 위한 저감 대책을 도출하고 SIS를 개발하는 과정을 본 가이드의 프로세스에 접목시켜 가이드의 적용 방법을 제시한다.

[1] 시스템 정의

대상 시스템의 기본 설계는 그림과 같으며, 유류 저장 탱크와 탱크로 들어오는 공정 라인을 제어하는 밸브, 출하 공정 라인을 제어하는 밸브, 유류 탱크의 유증기를 제어하는 밸브로 구성되어 있으며, 공정 라인과 밸브를 제어하는 BPCS 2기로 관리되고 있다. 모든 기능은 운영자가 BPCS를 조작하여 수행한다. 사례 연구를 위해 실제 시스템 중 범위를 한정하였다. 범위를 축소한 시스템에 대한 시스템 정의 단계 수행 후 도출한 대표 기능은 다음과 같다.

장치	기능	제어	명령
PSV-1	입하 라인 밸브 열림	BPCS-1	유류 공급
	입하 라인 밸브 닫힘	BPCS-1	유류 공급 차단
PSV-2	출하 라인 밸브 열림	BPCS-1	유류 출하
	출하 라인 밸브 닫힘	BPCS-1	유류 출하 정지
PSV-3	유증기 방출 밸브 열림	BPCS-2	밸브 ON
	유증기 방출 밸브 닫힘	BPCS-2	밸브 OFF



[2] 위험 분석

가. Top Hazard 선정

유류 저장 공정 시스템에서 발생할 수 있는 최상위 위험원을 선정한다. 최상위 위험원은 경험적인 부분이나 브레인스토밍 등을 사용하며, 초기 시스템 구축 시에 수행한다.

ID	Top Hazard	설명
TOP-HZD-01	유류 저장 탱크 파손으로 저장 시스템 폭발 위험	유류 입하나 출하 시 또는 저장 탱크 유증기로 인해 탱크에 손상이 생겨 폭발 위험성 존재

나. HAZOP 분석

(1) HAZOP Guideword 선정

변수	Guideword
유량(Flow)	High, Low
압력(Pressure)	High. Low
전기(Power)	No
제어(Control)	No

(2) HAZOP 분석

ID	대상	이상현상	결과	원인
HZD-01	유류 저장 탱크	압력 High	압력 상승으로 탱크 손상 및 폭발 발생	유증기 배출 차단 임계치 이상으로 유류 입하
HZD-02	유류 저장 탱크	압력 Low	압력 감압으로 탱크 손상 및 폭발 발생	유증기 과다 배출 유류 과다 또는 강제 출하
HZD-03	유류 저장 탱크	레벨 High	유류가 탱크 저장 임계치 이상 입하되어 탱크 손상 및 폭발 발생	유류 과다 입하
HZD-04	유류 저장 탱크	레벨 Low	유류가 압력 유지를 위한 수준 이하로 출하되어 탱크 손상 및 폭발 발생	유류 과다 출하
HZD-05	모든 라인	전기 No	유류 입하 시 순간적인 전원 차단으로 유류 입하 조절 실패 탱크 손상 및 폭발 발생	전원 차단 감지 기능 부재
HZD-06	모든 라인	제어 No	제어 불가로 유류 저장 탱크 레벨 및 압력 증가 발생	비상 정지 기능 부재

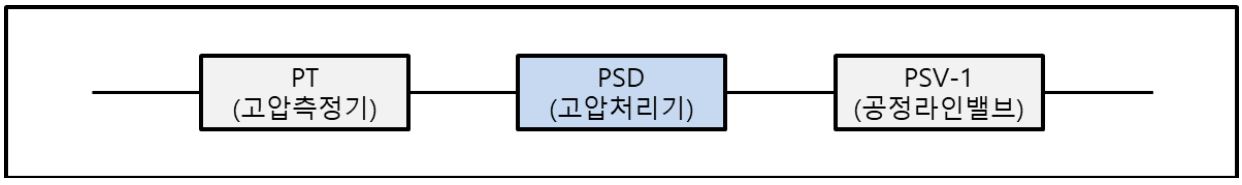
다. SIL 할당

(1) HAZOP 분석 결과 도출된 결과를 예방하기 대안 정의

ID	대상	결과	대안
HZD-01	유류 저장 탱크	압력 상승으로 탱크 손상 및 폭발 발생	High 압력 감지 센서 추가 High 압력 발생 시 처리

			제어기 추가
HZD-02	유류 저장 탱크	압력 감압으로 탱크 손상 및 폭발 발생	Low 압력 감지 센서 추가 Low 압력 발생 시 처리 제어기 추가
HZD-03	유류 저장 탱크	유류가 탱크 저장 임계치 이상 입하되어 탱크 손상 및 폭발 발생	High 레벨 감지 센서 추가 High 레벨 발생 시 처리 제어기 추가
HZD-04	유류 저장 탱크	유류가 압력 유지를 위한 수준 이하로 출하되어 탱크 손상 및 폭발 발생	Low 레벨 감지 센서 추가 Low 레벨 발생 시 처리 제어기 추가
HZD-05	모든 라인	유류 입하 시 순간적인 전원 차단으로 유류 입하 조절 실패 탱크 손상 및 폭발 발생	전원 감지기 추가 비상 발전기 추가 전원 차단 시 공정 Shutdown 제어기 추가
HZD-06	모든 라인	제어 불가로 유류 저장 탱크 레벨 및 압력 증가 발생	Emergency Stop 기능 추가 Emergency Stop Button 추가

(2) 대안에 따른 장치 구성 (HZD-01 대안 RBD)



(3) 장치 제조사에서 제공하거나 측량된 PFD 계산

장치	개별 PFD	누적 PFD

PT (고압측정기)	$1.5 \cdot 10^{-3}$	$1.5 \cdot 10^{-3}$
PSD Logic (고압처리기)	$2.6 \cdot 10^{-3}$	$1.0 \cdot 10^{-2}$
PSV-1(공정라인밸브)	$8.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-2}$
Total		$4.5 \cdot 10^{-2}$

(4) IEC 61511 기반 SIL 할당 (LOPA 계산은 제외): **SIL 1**

SIL	PFDavg	Required risk reduction
3	≥ 10−4 to < 10−3	> 1 000 to ≤ 10 000
2	≥ 10−3 to < 10−2	> 100 to ≤ 1 000
1	≥ 10−2 to < 10−1	> 10 to ≤ 100

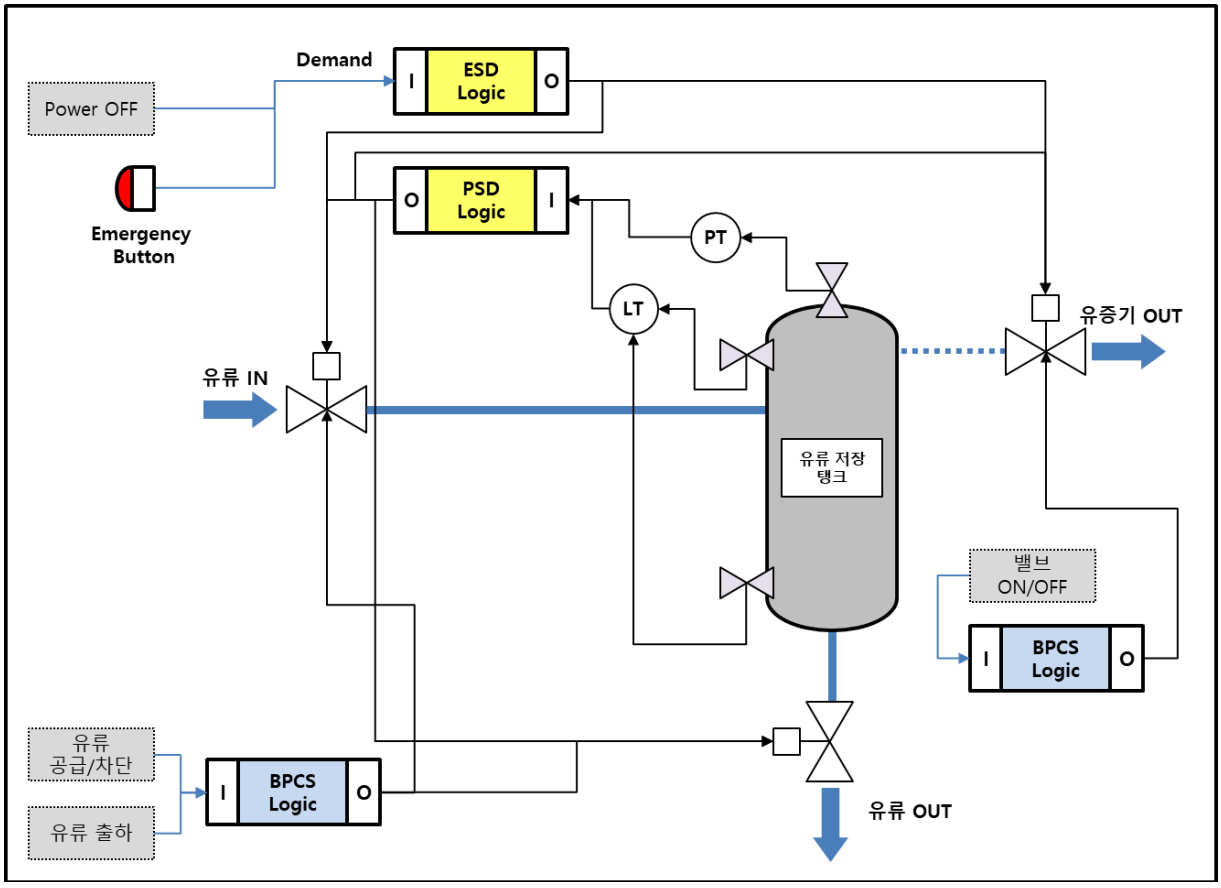
라. 안전 요구사항 명세

(1) SIF 식별

(2) 기능 요구사항 정의

ID	기능 요구사항
TZD-01	200 이상의 압력 감지 시 PSV-1을 닫아 유류 입하를 중지하고 PSV-3을 열어유증기를 방출하여 압력을 낮춘다.
…	…
TZD-10	Emergency Button이 눌리면 PSV-1을 닫아 유류 입하를 중지하고, PSV-3을 열어 유증기를 방출하여 압력을 낮추고, PSV-2를 닫아 유류 탱크의 출하를 방지한다.
…	…

(3) SIF를 반영한 SIS 구성도 작성



[3] 응용 소프트웨어 개발

가. 응용 소프트웨어 요구사항 도출

항 목	설 명
요구사항 ID	• *TZD-SW-R-F-10*
요구사항 명칭	• *공정 라인 비상 정지 기능*
요구사항 설명	• *Emergency Button 이벤트가 발생하면 유류 라인 밸브 OFF 신호를 보내고 유증기 방출 밸브는 ON 시킨다.*
요구사항 명세	*1) 사전조건: PSD 정상 기동, RUN 모드* *2) 입력정보: Emergency Button 신호 (EB-Bool)* *3) 출력정보: PSV-1-OFF, PSV-2-OFF, PSV-3-ON* *4) 동작사양:* *1. EB-Bool 신호 확인* *2. PSV-1-OFF 신호 출력* *3. PSV-2-OFF 신호 출력* *4. PSV-3-ON 신호 출력* *5) 예외처리: RUN 모드가 아닌 경우 신호 무시*

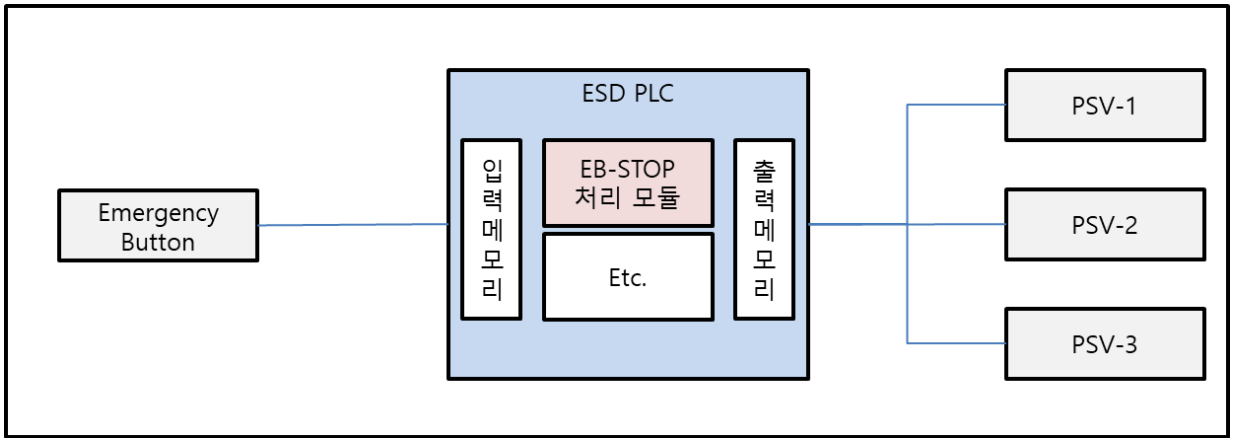
	6) 사후조건: EB-Bool 해제 시 까지 대기 *7) 제약사항: 없음*
검증방법	• *EV 테스트 수행*
요구사항 근거	• *시스템 안전 요구사항 명세서*
관련 안전 기능	• *TZD-10*

나. 응용 소프트웨어 설계

(1) 외부 인터페이스와 내부 처리 모듈 구성도를 작성

(2) 인터페이스에서 사용하는 공용 변수 정의

(3) 알람 시스템 등 기본 안전 기능 정의



다. 응용 소프트웨어 개발

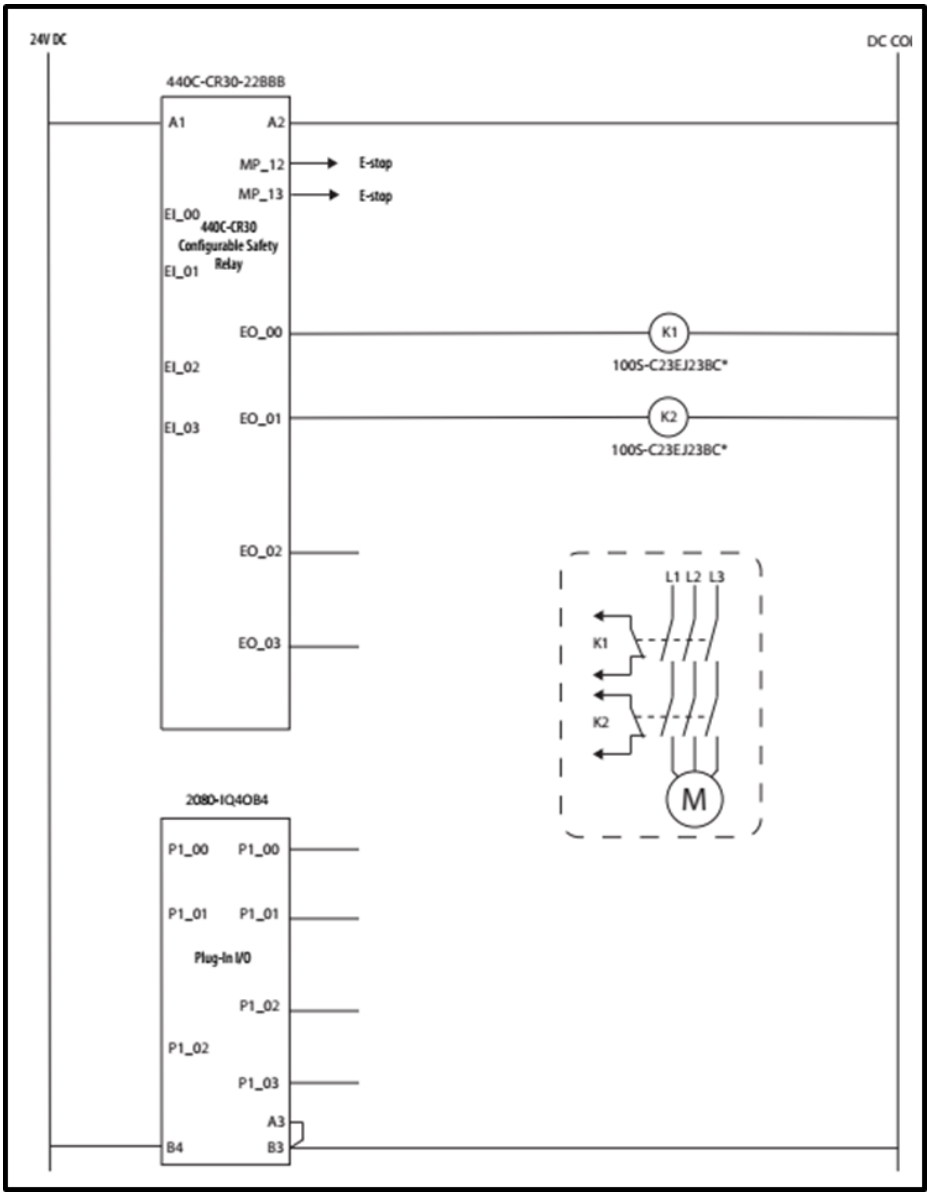
(1) 제조사 제약사항 확인 (메모리 할당 등)

(2) 제조사 제공 개발 도구 및 개발 방법 확인

라. 코딩 및 구현

(1) 개발 언어로 코딩 및 구현 예시) Rockwell 사 E-Stop

(2) 변수명 및 초기 값 확인


24V DC
DC COI
440C-CR30-22BBB
A1
A2
MP_12
E-stop
MP_13
E-stop
EI_00
440C-CR30
Configurable Safety
Relay
EI_01
EO_00
K1
100S-C23EJ23BC*
EI_02
EO_01
K2
EI_03
100S-C23EJ23BC*
EO_02
EO_03
L1 L2 L3
K1
K2
M
2080-IQ4OB4
P1_00
P1_00
P1_01
P1_01
Plug-In I/O
P1_02
P1_02
P1_03
A3
B4
B3

제 6 장. 결론

결론

6.1. 연구 요약

본 과제를 통해 제조분야 시스템의 신뢰·안전성을 확보하기 위해 국내·외 제조분야의 시스템 및 소프트웨어 현황 및 사례를 분석하고 안전관련 국제 표준인 IEC 62061, IEC 61511을 기반으로 현장에서의 사용성과 편의성을 확보하여 제조분야 시스템 개발 시 관련 중소기업의 개발자들이 실무에 적용 할 수 있는 사례를 포함해 구체적 실행 지침 및 기법을 개발하였다.

가이드 주요 항목	주요 내용
제조 SW 분야의 현황 분석	▪제조분야 소프트웨어 유형 분석 ▪제조SW 관련 국내/외 표준 현황 및 주요국 규제 관리 현황 ▪국내 제조 분야SW 시장 규모 및 구조, 표준 및 규제 강화에 대한 기업 대응 현황 등
제조분야 안전가이드	▪시스템 안전분석 생명주기 에 따른 단계 별 수행 가이드 ▪응용소프트웨어 개발 생명주기에 따른 단계 별 수행 가이드
사례 연구	▪제조 공정상의 기계 장치 안전시스템의 개발 사례 연구 ▪ 공정 장치 산업의 안전계장시스템의 개발 사례 연구
부록	▪ 용어 및 약어 ▪기능안전 생명주기 상의 필수안전관리활동 분류(매트릭스 테이블) ▪기능안전 생명주기 상의 필수안전관리활동 설명 및 상세 가이드

6.2. 연구 결론

제조업을 고부가가치 산업으로 변화시키기 위해서 생산설비의 기계화, 자동화, 집중화가 필수 적이며, 4차 산업혁명 속에서 제조업이 ICT 인프라 결합하여 제품 생산과정의 서비스화, 디지털화와 같은 새로운 방향으로 진화하고 있다.

최근 제조업 경쟁력 회복의 대안으로 부상하고 있는 스마트공장이 새로운 미래 산업으로 각광받고 있으며, 스마트공장은 전 세계적으로 매년 7%씩 성장해, 오는 2020년이면 시장규모가 3000억 달러에 이를 전망이다. 이러한 제조 공정상의 자동화 및 무인화에 따라 이를 관리, 제어, 통합하는 소프트웨어의 비중과 복잡도도 급격히 증가하고 있으며 이러한 과정에서 시스템에서 발생할 수 있는 위험요소도 다발적으로 증가하고 있다.

제조분야 시스템 안전표준의 경우, 4차 산업혁명의 핵심인 스마트공장 분야의 자동화 시스템에서 발생 가능한 위험을 식별하고 이를 저감, 회피, 예방 할 수 있는 안전 요건을 제시해 안전사고 및 인명손실의 최소화를 목적으로 하고 있는 IEC 62061 및 IEC 61511의 국제 안전표준의 적용과 준수를 요구하고 있는 추세이다.

본 과제에서는 관련 중소기업들이 실무에서 해당 표준을 적용해 제품을 개발하는데 있어, 국제 안전표준인 IEC 62061 및 IEC 61511을 기반으로 현장에서 실무차원의 수행 기법 및 목표 수준 달성을 위한 가이드라인과 현장에서 용이하게 활용 가능한 적용사례를 제시하여 제품 개발 시 신뢰성과 안전성을 확보할 수 있도록 하였다.

부록

부록

부록 A. 약어 및 용어

A.1. 약어

약어	전체
AC/DC	Alternating current/direct current
AIChE	American Institute of Chemical Engineers
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
AP	Application program
BPCS	Basic process control system
CCF	Common Cause Failure(s)
CCPS	Centre for Chemical Process Safety (AIChE)
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
EMC	Electro-magnetic compatibility
FAT	Factory acceptance test
FB	Function Block
FPL	Fixed program language
FSA	Functional safety assessment
FSMS	Functional safety management system
FTA	Fault tree analysis
FVL	Full variability language
H&RA	Hazard & risk assessment
HFT	Hardware fault tolerance
HMI	Human Machine Interface
I/O	Input/Output
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
LVL	Limited variability language
LVL	Limited Variability Language
MooN	"M" out of "N" channel architecture
MPRT	Maximum permitted repair time

약어	전체
MRT	Mean repair time
MTTF	Mean Time To Failure
MTTR	Mean time to restoration
NFPA	National Fire Protection Association(US)
NP	Non-programmable
OEM	Original Equipment Manufacturer
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of dangerous failure on demand
PFDavg	Average probability of dangerous failure on demand
PFH	Probability (average frequency of dangerous failures) of failure per hour
PFHD	Probability of dangerous Failure per Hour
pl	Plural
PLC	Programmable logic controller
PTE	Probability of dangerous Transmission Error
SAT	Site acceptance test
SC	Systematic capability
SFF	Safe Failure Fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SILCL	Safety Integrity Level (SIL) Claim Limit (for subsystems)
SIS	Safety instrumented system
S-R	Safety Related
SRCF	Safety-Related Control Function
SRECS	Safety-Related Electrical Control System
SRS	Safety requirement specification
SYS	System

A.2. 용어 상세

A.2.11 결함(Fault)

요청된 기능을 수행할 때 기능 유닛의 능력이 감소하거나, 손실이 발생하는 비정상적 조건

A.2.21 계통적 고장(Systematic Failure)

설계 또는 생산 프로세스의 수정이나 동작 프로시저, 문서 또는 기타 관련 요인에 의해 제거될 수 있는 장애

A.2.31 고장(Failure)

요청된 방법 이외의 방법으로 기능 유닛 기능 또는 동작을 정상적인 제공이 멈추는 경우

A.2.41 공통원인고장(Common Cause Failure)

멀티 채널 시스템에서 둘 또는 그 이상의 분리된 채널의 장애가 동시발생 하는 경우, 시스템 장애 발생

A.2.51 기능안전(functional safety)

제조 운전설비 또는 운전제어 시스템의 일부인 전기/전자 프로그램 가능형 안전시스템, 다른 기술로 구성된 안전시스템 또는 외부의 위험감소 설비가 올바르게 동작하도록 하는 기능과 관련 안전을 말함.

A.2.61 단위시간당 위험한 고장확율

시간당 위험한 오류 개연성
위험 고장율(PFHd: Probability of Dangerous Failure Hour)
주어진 시간 동안 특정 안전 기능을 수행하기 위한 안전 관련 시스템/서브 시스템의 시간당 위험한 고장의 평균 확률

A.2.71 무작위 하드웨어 고장

임의 하드웨어 고장(random hardware failures)
임의의 시간에 발생하는 하나 또는 그 이상의 하드웨어 오염 메커니즘을 발생시키는 장애

A.2.81 방호계층분석(LOPA; Layer of protection analysis)

정성적 판단으로는 위험의 판정이 어렵거나 사고의 결과가 심각할 경우에 적용하는 것으로 사고 시나리오에 대한 방호계층의 가치를 평가하는 전력화된 평가기법이다.

A.2.91 상해(Harm)

자산이나 환경에 대한 손상의 결과로서 직/간접적인 부상 혹은 건강에 대한 손상을 말함.

A.2.101 안전 관련 제어 기능(SRCF: Safety Related Control Function)

제조시스템의 안전성 확보를 위한 기능적 측면의 안전기능

A.2.111 안전 시스템(Safety System)

제조 운전설비의 안전상태를 유지하도록 안전기능을 수행하는 전기/전자 프로그램 가능한 시스템, 다른 기술로 구성된 시스템 또는 외부의 위험감소 설비 등을 말함.

A.2.121 안전관련 전기제어 시스템(SRECS ;Safety Related Electrical/Electronic Control System)

안전한 상태를 유지 하거나 성취하는데 필수적으로 요구되는 안전기능을 구현하도록 설계되어진 시스템을 의미한다. SRS 에서 의미하는 안전기능(Safe Function)은 명시된 위험한 사건(Specific hazardous event)에 대하여 EUC 의 안전상태(여기서는 Fail Safe)를 유지하거나 성취하도록 의도된 E/E/PES SRS 에 의해서 구현된 기능이라 할 수 있다.

A.2.131 안전기능(Safety Function)

61511: 특정 위험한 사건과 관련하여 프로세스의 안전한 상태를 달성하거나 유지하기 위한 하나 이상의 보호 계층에 의해 구현되는 기능
62061: 기능의 장애로 인해 위험이 즉각적으로 증가 할 수 있는 기계의 기능

A.2.141 안전무결성(Safety Integrity)

제조 안전관련 시스템이 주어진 시간동안 모든 운전상태에서 요구되는 안전 기능을 만족스럽게 수행할 수 있는 확률을 말함.

A.2.151 안전 무결성 등급(SIL: Safety Integrity Level)

안전 시스템의 무결성을 나타내는 통계적 기준

A.2.161 안전 무결성 등급 분석 작업표(SIL Classification worksheets)

요구수준 안전 무결성 등급을 산정하기 위하여 공정의 위험성 분석 등을 기술하는 작업양식을 말한다.

A.2.171 안전수명주기(Safety Lifecycle)

안전시스템의 구성의 개념단계에서부터 기능안전성이 더 이상 유효하지 못할 때까지의 안전시스템 이행에 필요한 모든 활동을 말한다.

A.2.181 위험(Risk)

유해 상황의 발생확률과 유해의 치명도를 조합한 위험의 정도를 말함.

A.2.191 위험 그래프 방법론(Risk Graph Methodology)

IEC 61508-5 를 기준으로 하여 인적안전, 환경피해, 재산피해의 안전 무결성 등급 값을 구한 후에 요구수준 안전 무결성 등급(Required SIL)을 결정하는 방법론을 말함.

A.2.201 위험사건(Hazardous event)

유해로 나타나는 위험한 상황을 말함.

A.2.211 위험요인(Hazard)

잠재적 유해 요소를 말하며, 화재/폭발과 같은 단기간 범위 내에서 발생하는 위험과 독성물질의 누출과 같은 근로자의 건강에 장기간 영향을 주는 위험이 있다.

A.2.221 위험한 고장(Dangerous Failure)

61511: 주어진 안전 조치를 방해하거나 불가능하게 하는 고장
62061: 위험 요소 또는 비 기능적 상태를 야기 할 가능성이 있는 SRECS, 서브 시스템 또는 서브 시스템 요소의 고장

A.2.231 전기/전자 프로그래밍전자장치(Electric/Electronic/Programmable electronic devices)

전기/전자 프로그램이 가능한 전자기술을 기반으로 한 장치를 말함.

A.2.241 전체적 변화언어(FVL: Full Variability Language)

공정 운영상에 발생할 수 있는 위험원에 대한 가이드워드 기법을 활용해 이탈현상에 대한 분석을 통해, 위험원을 식별하여 대응하는 안전분석 기법.

A.2.251 제어안전기능(SIF; Safety Instrumented Function)

기능안전에 필요한 명시된 안전 무결성 등급의 안전기능으로, 안전시스템의 안전 보호기능 또는 안전시스템의 제어기능을 말한다.

A.2.261 제어안전시스템(SIS; Safety Instrumented System)

하나 또는 그 이상의 제어안전기능을 사용하는 안전시스템을 말하며 IEC 61511 의 SIS 가 해당된다. SIS 의 구성은 센서, 논리 시스템, 최종 구성요소의 조합으로 이루어진다.

A.2.271 제한된 다양성 언어(LVL: Limited Variability Language)

61511: 관련 안전 매뉴얼에 정의 된 대로 애플리케이션에 제한된 기능 범위를 가진 상용 및 산업용 프로그래머블 전자 컨트롤러 용 프로그래밍 언어.
이 언어의 표기법은 텍스트 또는 그래픽 일 수도 있고 둘 다의 특성을 가질 수도 있음
62061: 미리 정의 된 응용 프로그램 별 라이브러리 기능을 결합하여 안전 요구 사항 사양을 구현하는 기능을 제공하는 언어 유형

A.2.281 진단범위(DC: Diagnostic Coverage)

61511: 진단에 의해 탐지 된 위험한 고장률의 일부. 진단 범위에는 교정 테스트에서 발견된 모든 결함이 포함되지 않음
62061: 자동 온라인 진단 테스트에 의해 감지 된 위험한 고장 비율

A.2.291 평균위험고장시간(MTTF: Mean Time to Dangerous Failure)

고장까지의 평균 기대 시간

부록 B. 안전관리활동

B.1. IEC-61508 T&M 과 제조 안전관리활동 매핑 목록

본 매핑 목록은 공통 표준인 IEC-61508의 SIL 별 권장 T&M (Technique/Measure: 이하 T&M) 목록에 제조 표준의 안전관리활동을 매핑한 것이다.

제조 표준의 안전관리활동이란 제조 안전을 달성하기 위한 각종 기술이나 대책, 기법들을 가리키는 활동이다.

공통 표준에서는 SIL별 권장 T&M을 가이드하고 있으나 이와 달리, 제조 표준의 경우 SIL별 권장 T&M 목록을 제시하거나 따로 단계별 T&M을 기술하지 않았다. 이에 본 가이드라인은 제조 표준의 단계 가이드라인에 언급된 안전관리를 위한 활동이나 가이드라인 내용에 따라 매핑 되는 활동들을 기준으로 매핑 목록을 작성하여 본 가이드라인의 이용자들에게 제공하고 있다. 단, 앞서 말한 바와 같이 한계가 존재하므로 이점을 고려하여 안전관리활동을 참고하기를 권장하는 바이다.

B.1.11 IEC-61508-2(System) T&M 과 제조 안전관리활동 매핑 목록

본 가이드의 안전관리활동은 각각의 SIL Level 별로 단계별 검증해야 할 것을 IEC 61511, IEC 62061, IEC 62508, IEC 62278과 SW안전가이드 공통분야를 참고하여 구성하였다. 제안하는 안전관리활동은 절대적인 것이 아니라 권장하는 것이므로 적용 시스템이나 환경에 맞춰 선택하도록 한다.

IEC-61508에서는 안전성 무결성 수준에 따라 요구 사항이 제시되는데, 첫째로 기술 또는 수단의 중요성과 두 번째로 그것이 사용될 경우 필요한 유효성이다.

다음은 IEC-61508의 T&M의 중요성과 효과에 대한 기준이다.

중요성은 다음과 같이 나타낸다.

M :이 안전 무결성 등급을 위해 기술 또는 조치가 필요하다. (필수).

HR : 이 안전 무결성 등급을 위해 기술이나 조치를 적극 권장한다. 이 기법이나 수단이 사용되지 않는다면, 그것을 사용하지 않는 이유는 상세히 설명되어야 한다.

R :이 안전 무결성 등급을 위해 기술이나 조치를 권장한다.

- : 기술 또는 조치가 사용되는 것이나 사용에 대해 권고가 없다.

NR : 이 안전 무결성 등급에서는 기법이나 조치가 적극적으로 권장되지 않는다. 이 기술이나 조치가 사용된다면 그 기술을 사용하는 근거는 상세히 기술되어야 한다.

필요한 효과는 다음과 같이 나타낸다.

낮음 (low) : 사용된다면 체계적 결함에 대해 최소한의 효과를 나타내기 위해 필요한 정도로 기술 또는 조치를 사용해야 한다.

중간 : 사용된다면 체계적 결함에 대해 적어도 중간 정도의 효과를 주는데 필요한 정도로 기술 또는 수단을 사용해야 한다.

높음 : 사용된 경우 기술 또는 조치는 체계적인 오류에 대해 높은 효과를 나타낼 정도로 필요하다.

조치가 의무적이지 않은 경우 원칙적으로 다른 조치 (개별적으로 또는 조합하여)로 대체 할 수 있다. 이것은 표에 설명된 것처럼 음영 처리된다.

여기에 제시된 모든 기술과 방법은 E/E/PE 안전 관련 시스템의 기본 기능으로 온라인에서 오류를 제어하는데 도움이 될 수 있다. E/E/PE 시스템 안전 수명주기 전반에 걸쳐 절차적,조직적 기술과 조치가 필요하며, 예상 외부 영향에 대한 E/E/PE 안전 관련 시스템의 동작을 테스트하는 검증 기술이 필요하다.

표 40 IEC-61508-2(System) T&M 과 제조 안전관리활동 매핑 목록

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
Techniques	1	Program sequence monitoring	프로그램 순서 모니터링	HR low	HR low	HR	HR	부록 B.2.17

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
and measures to control systematic failures caused by hardware design						medium	high	
	2	Failure detection by on-line monitoring (see Note 4)	온라인 모니터링에 의한 고장 탐지	R low	R low	R medium	R high	부록 B.2.18
	3	Tests by redundant hardware	중복 하드웨어에 의한 테스트	R low	R low	R medium	R high	
	4	Standard test access port and boundary-scan architecture	표준 테스트 접근 포트와 바운더리 스캔 아키텍처	R low	R low	R medium	R high	
	5	Code protection	코드 보호	R low	R low	R medium	R high	부록 B.2.19
	6	Diverse hardware	다양한 하드웨어	– low	– low	R medium	R high	
Techniques and measures to control systematic failures caused by environmental stress or influences	1	Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	전압 브레이크 다운, 전압 변동, 과전압, 저전압 및 기타 현상(위험한 고장으로 이어질 수 있는 전원 주파수 변동과 같은)에 대한 대책	M low	M medium	M medium	M high	
	2	Separation of electrical energy lines from information lines (see Note 4)	정보 통신망과 전기선의 분리 (노트 4 참조)	M	M	M	M	
	3	Increase of interference immunity	간섭 내성 증가	M low	M low	M medium	M high	
	4	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	물리적 환경 (예 : 온도, 습도, 물, 진동, 먼지, 부식성 물질)에 대한 대책	M low	M high	M high	M high	
	5	Program sequence monitoring	프로그램 순서 모니터링	HR low	HR low	HR medium	HR high	부록 B.2.17
	6	Measures against temperature increase	온도 상승 대책	HR low	HR low	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
						medium	high	
	7	Spatial separation of multiple lines	여러 줄의 공간 분리	HR low	HR low	HR medium	HR high	
	8	Idle current principle (where continuous control is not needed to achieve or maintain a safe state of the EUC)	유휴 전류 원리 (EUC 의 안전한 상태를 달성하거나 유지하기 위해 지속적인 제어가 필요하지 않은 경우)	R	R	R	R	
	9	Measure to detect breaks and shorts in signal lines	신호 라인의 단락 및 단락을 감지하기위한 측정	R	R	R	R	
	10	Failure detection by on-line monitoring (see Note 5)	온라인 모니터링에 의한 고장 탐지	R low	R low	R medium	R high	부록 B.2.18
	11	Tests by redundant hardware	중복 하드웨어에 의한 테스트	R low	R low	R medium	R high	
	12	Code protection	코드 보호	R low	R low	R medium	R high	부록 B.2.19
	13	Antivalent signal transmission	등가 신호 전송	R low	R low	R medium	R high	
	14	Diverse hardware (see Note 6)	다양한 하드웨어	– low	– low	– medium	R high	
	15	Software architecture	소프트웨어 아키텍처	See Tables A.2 and C.2 of IEC 61508-3				
Techniques and measures to control systematic operational failures	1	Modification protection	수정 보호	M low	M medium	M high	M high	
	2	Failure detection by on-line monitoring (see Note 4)	온라인 모니터링에 의한 고장 탐지	R low	R low	R medium	R high	부록 B.2.18
	3	Input acknowledgement	입력 확인	R low	R low	R medium	R high	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	4	Failure assertion programming	오류 주장 프로그래밍	See Tables A.2 and C.2 of IEC 61508-3				
Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements	1	Project management	프로젝트 관리	M low	M low	M medium	M high	
	2	Documentation	문서화	M low	M low	M medium	M high	
	3	Separation of E/E/PE system safety functions from non-safety functions	E/E/PE 시스템 안전 기능과 비 안전 기능 분리	HR low	HR low	HR medium	HR high	
	4	Structured specification	구조화 된 명세	HR low	HR low	HR medium	HR high	
	5	Inspection of the specification	명세 검사	– low	HR low	HR medium	HR high	부록 B.2.21
	6	Semi-formal methods	준 정형 방법	R low	R low	HR medium	HR high	
	7	Checklists	점검표	R low	R low	R medium	R high	
	8	Computer aided specification tools	컴퓨터 지원 명세 도구	– low	R low	R medium	R high	
	9	Formal methods	정형 방법	– low	– low	R medium	R high	
Techniques and measures to avoid introducing faults during E/E/PE system design and	1	Observance of guidelines and standards	지침 및 표준 준수	M high	M high	M high	M high	
	2	Project management	프로젝트 관리	M low	M low	M medium	M high	
	3	Documentation	문서화	M low	M low	M medium	M high	
	4	Structured design	구조적 설계	HR low	HR low	HR medium	HR high	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
development	5	Modularisation	모듈화	HR low	HR low	HR medium	HR high	
	6	Use of well-tried components	잘 사용 된 구성 요소의 사용	R low	R low	R medium	R high	
	7	Semi-formal methods	준 정형 기법	R low	R low	HR medium	HR high	
	8	Checklists	점검표	– low	R low	R medium	R high	
	9	Computer-aided design tools	컴퓨터 지원 설계 도구	– low	R low	R medium	R high	
	10	Simulation	시뮬레이션	– low	R low	R medium	R high	부록 B.2.22
	11	Inspection of the hardware or walkthrough of the hardware	하드웨어 검사 또는 하드웨어 워크 스루	– low	R low	R medium	R high	부록 B.2.23 부록 B.2.24
	12	Formal methods	정형 기법	– low	– low	R medium	R high	
Techniques and measures to avoid faults during E/E/PE system integration	1	Functional testing	기능 테스트	M high	M high	M high	M high	
	2	Project management	프로젝트 관리	M low	M low	M medium	M high	
	3	Documentation	문서화	M low	M low	M medium	M high	
	4	Black-box testing	블랙 박스 테스트	R low	R low	R medium	R high	부록 B.2.25
	5	Field experience	현장 경험	R low	R low	R medium	R high	
	6	Statistical testing	통계 테스트	– low	– low	R	R high	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
						medium		
Techniques and measures to avoid faults and failures during E/E/PE system operation and maintenance procedures	1	Operation and maintenance instructions	운영 및 유지 보수 지침	HR high	HR high	HR high	HR high	
	2	User friendliness	사용자 친근성	HR high	HR high	HR high	HR high	
	3	Maintenance friendliness	유지 보수 용이	HR high	HR high	HR high	HR high	
	4	Project management	프로젝트 관리	M low	M low	M medium	M high	
	5	Documentation	선적 서류 비치	M low	M low	M medium	M high	
	6	Limited operation possibilities	제한된 작업 가능성	– low	R low	HR medium	HR high	
	7	Protection against operator mistakes	운전자 실수 방지	– low	R low	HR medium	HR high	
	8	Operation only by skilled operators	숙련 된 운영자 만의 작업	– low	R low	R medium	HR high	
Techniques and measures to avoid faults during E/E/PE system safety validation	1	Functional testing	기능 테스트	HR high	HR high	HR high	HR high	
	2	Functional testing under environmental conditions	환경 조건에서의 기능 테스트	HR high	HR high	HR high	HR high	
	3	Interference surge immunity testing	간섭 서지 면역 테스트	HR high	HR high	HR high	HR high	
	4	Fault insertion testing (when required diagnostic coverage ≥ 90%)	결함 삽입 테스트 (필요한 진단 범위가 90 % 이상인 경우)	HR high	HR high	HR high	HR high	부록 B.2.26
	5	Project management	프로젝트 관리	M low	M low	M	M high	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
						medium		
	6	Documentation	문서화	M low	M low	M medium	M high	
	7	Static analysis, dynamic analysis and failure analysis	정적 분석, 동적 분석 및 고장 분석	– low	R low	R medium	R high	부록 B.2.27 부록 B.2.28 부록 B.2.29
	8	Simulation and failure analysis	시뮬레이션 및 고장 분석	– low	R low	R medium	R high	부록 B.2.22 부록 B.2.29
	9	Worst-case analysis, dynamic analysis and failure analysis	최악의 케이스 분석, 동적 분석 및 고장 분석	– low	– low	R medium	R high	부록 B.2.28 부록 B.2.29 부록 B.2.30
	10	Static analysis and failure analysis (see Note 4)	정적 분석 및 고장 분석 (주 4 참조)	R low	R low	NR	NR	부록 B.2.27 부록 B.2.29
	11	Expanded functional testing	확장된 기능 테스트	– low	HR low	HR medium	HR high	
	12	Black-box testing	블랙 박스 테스트	R low	R low	R medium	R high	부록 B.2.25
	13	Fault insertion testing (when required diagnostic coverage < 90%)	결함 삽입 테스트 (필요한 진단 범위 <90 %)	R low	R low	R medium	R high	부록 B.2.26
	14	Statistical testing	통계 테스트	– low	– low	R medium	R high	
	15	Worst-case testing	최악의 케이스 테스트	– low	– low	R medium	R high	
	16	Field experience	현장 경험	R low	R low	R medium	NR	

B.1.21 IEC-61508-3(SW) T&M 과 제조 안전관리활동 매핑 목록

본 가이드의 안전관리활동은 각각의 SIL Level 별로 단계별 검증해야 할 것을 IEC 61511, IEC 62061, IEC 62508, IEC 62278과 SW안전가이드 공통분야를 참고하여 구성하였다. 제안하는 안전관리활동은 절대적인 것이 아니라 권장하는 것이므로 적용 시스템이나 환경에 맞춰 선택하도록 한다.

다음은 제조 안전관리활동과 매핑한 IEC-61508의 SIL별 T&M 목록이다.

IEC-61508의 SIL 1 에서 4 에 대한 T&M의 적용은 다음을 참고한다.

- HR : Highly Recommended, 이 기법 및 수단은 안전무결성을 위해 반드시 권고되는 기법임을 나타낸다. 이 기법이나 수단이 이용되지 않는다면 안전 계획에서 그 합리적 근거가 상술 되어야 하고 평가자의 동의를 얻어야 한다.
- R : Recommended, 이 기법 및 수단은 안전무결성을 위해 HR 보다 낮은 권고 수준을 갖는다.
- --- : 이 기법 및 수단은 안전무결성을 위해 권고되는 사항이 없음을 의미한다.
- NR : Not Recommended, 이 기법 및 수단은 안전무결성을 위해 절대 권고되지 않음을 의미한다. 이 기법이나 수단을 이용한다면 그것을 이용하는 합리적 근거를 안전 계획 중에 상술 되어야 하고 평가자의 동의를 얻어야 한다.

표 41 IEC-61508-3(SW) T&M 과 제조 안전관리활동 매핑 목록

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
IEC61508-3 A.1 - Software safety requirements specification	1a	Semi-formal methods	준 정형 기법	R	R	HR	HR	
	1b	Formal methods	정형 기법	---	R	R	HR	
	2	Forward traceability between the system safety requirements and the software safety requirements	시스템 안전 요구 사항과 소프트웨어 안전 요구 사항 간의 전방 추적성	R	R	HR	HR	
	3	Backward traceability between the safety requirements and the perceived safety needs	안전 요구 사항과 인식 된 안전 요구 사항 간의 역 추적성	R	R	HR	HR	
	4	Computer-aided specification tools to support appropriate techniques/measures above	위의 적절한 기술 / 조치를 지원하는 컴퓨터 지원 사양 도구	R	R	HR	HR	
IEC61508-3 A.2 - Software design and development - software architecture design	1	Fault detection	오류 감지	---	R	HR	HR	
	2	Error detecting codes	코드 감지 오류	R	R	R	HR	
	3a	Failure assertion programming	오류 주장 프로그래밍	R	R	R	HR	부록 B.2.19
	3b	Diverse monitor techniques (with independence between the monitor and the monitored function in the same computer)	다양한 모니터 기술 (모니터와 모니터 기능이 동일한 컴퓨터에서 독립적 임)	---	R	R		
	3c	Diverse monitor techniques (with separation between the monitor computer and the monitored computer)	다양한 모니터 기술 (모니터 컴퓨터와 모니터링 되는 컴퓨터가 분리되어 있음)	---	R	R	HR	
	3d	Diverse redundancy, implementing the same software safety requirements specification	다양한 중복성, 동일한 소프트웨어 안전 요구 사항 사양 구현	---	---	---	R	부록 B.2.1

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	3e	Functionally diverse redundancy, implementing different software safety requirements specification	기능적으로 다양한 중복, 다른 소프트웨어 안전 요구 사항 사양 구현	---	---	R	HR	부록 B.2.1
	3f	Backward recovery	역방향 복구	R	R	---	NR	
	3g	Stateless software design (or limited state design)	무상태 소프트웨어 설계 (또는 제한된 상태 설계)	---	---	R	HR	
	4a	Re-try fault recovery mechanisms	장애 복구 메커니즘 다시 시도	R	R	---	---	
	4b	Graceful degradation	단계별 성능저하	R	R	HR	HR	
	5	Artificial intelligence - fault correction	인공 지능 - 오류 수정	---	NR	NR	NR	
	6	Dynamic reconfiguration	동적 재구성	---	NR	NR	NR	
	7	Modular approach	모듈 방식	HR	HR	HR	HR	부록 B.2.2
	8	Use of trusted/verified software elements (if available)	신뢰할 수 있고 검증 된 소프트웨어 요소의 사용 (있는 경우)	R	HR	HR	HR	부록 B.2.4
	9	Forward traceability between the software safety requirements specification and software architecture	소프트웨어 안전 요구 사항 사양과 소프트웨어 아키텍처 간의 포워드 추적성	R	R	HR	HR	
	10	Backward traceability between the software safety requirements specification and software architecture	소프트웨어 안전 요구 사항 사양과 소프트웨어 아키텍처 간의 역 추적성	R	R	HR	HR	
	11a	Structured diagrammatic methods **	구조 다이어그램 **	HR	HR	HR	HR	
	11b	Semi-formal methods **	준 정형 기법 **	R	R	HR	HR	
	11c	Formal design and refinement methods **	정식 디자인 및 개선 방법 **	---	R	R	HR	
	11d	Automatic software generation	자동 소프트웨어 생성	R	R	R	R	
	12	Computer-aided specification and design tools	컴퓨터 지원 사양 및 설계 도구	R	R	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	13a	Cyclic behaviour, with guaranteed maximum cycle time	최대 사이클 시간을 보장하는 주기적 동작	R	HR	HR	HR	
	13b	Time-triggered architecture	시간 트리거 아키텍처	R	HR	HR	HR	
	13c	Event-driven, with guaranteed maximum response time	이벤트 중심, 최대 응답 시간 보장	R	HR	HR	-	
	14	Static resource allocation	정적 리소스 할당	-	R	HR	HR	
	15	Static synchronisation of access to shared resources	공유 리소스에 대한 액세스의 정적 동기화	-	-	R	HR	
IEC61508-3 A.3 - Software design and development - support tools and programming language	1	Suitable programming language	적절한 프로그래밍 언어	HR	HR	HR	HR	
	2	Strongly typed programming language	강력한 형식의 프로그래밍 언어	HR	HR	HR	HR	
	3	Language subset	언어 하위 집합	---	---	HR	HR	
	4a	Certified tools and certified translators	공인 된 도구 및 공인 번역사	R	HR	HR	HR	
	4b	Tools and translators: increased confidence from use	도구 및 번역자 : 사용으로 인한 자신감 증가	HR	HR	HR	HR	
IEC61508-3 A.4 - Software design and development - detailed design	1a	Structured methods **	구조화 기법 **	HR	HR	HR	HR	
	1b	Semi-formal methods **	준 정형 기법 **	R	HR	HR	HR	
	1c	Formal design and refinement methods **	정식 디자인 및 개선 방법 **	---	R	R	HR	
	2	Computer-aided design tools	컴퓨터 지원 설계 도구	R	R	HR	HR	
	3	Defensive programming	방어 프로그래밍	---	R	HR	HR	부록 B.2.5
	4	Modular approach	모듈 방식	HR	HR	HR	HR	부록 B.2.2
	5	Design and coding standards	디자인 및 코딩 표준	R	HR	HR	HR	부록 B.2.6
	6	Structured programming	구조화 된 프로그래밍	HR	HR	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	7	Use of trusted/verified software elements (if available)	신뢰할 수 있고 검증 된 소프트웨어 요소의 사용 (있는 경우)	R	HR	HR	HR	부록 B.2.4
	8	Forward traceability between the software safety requirements specification and software design	소프트웨어 안전 요구 사항 사양과 소프트웨어 디자인 간의 포워드 추적성	R	R	HR	HR	
IEC61508-3 A.5 - Software design and development - software module testing and integration	1	Probabilistic testing	확률론적 테스트	---	R	R	R	
	2	Dynamic analysis and testing	동적 분석 및 테스트	R	HR	HR	HR	부록 B.2.28
	3	Data recording and analysis	데이터 기록 및 분석	HR	HR	HR	HR	
	4	Functional and black box testing	기능 및 블랙 박스 테스트	HR	HR	HR	HR	
	5	Performance testing	성능 테스트	R	R	HR	HR	
	6	Model based testing	모델 기반 테스트	R	R	HR	HR	
	7	Interface testing	인터페이스 테스트	R	R	HR	HR	
	8	Test management and automation tools	테스트 관리 및 자동화 도구	R	HR	HR	HR	
	9	Forward traceability between the software design specification and the module and integration test specifications	소프트웨어 설계 명세와 모듈 및 통합 테스트 명세 간의 전향적 추적성	R	R	HR	HR	
	10	Formal verification	정형 검증	---	---	R	R	
IEC61508-3 A.6 - Programmable electronics integration (hardware and software)	1	Functional and black box testing	기능 및 블랙 박스 테스트	HR	HR	HR	HR	
	2	Performance testing	성능 테스트	R	R	HR	HR	
	3	Forward traceability between the system and software design requirements for hardware/software integration and the hardware/software integration test	하드웨어 / 소프트웨어 통합 및 하드웨어 / 소프트웨어 통합 테스트 사양에 대한 시스템과 소프트웨어 설계 요구 사항 간의 전향적 추적성	R	R	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
		specifications						
IEC61508-3 A.7 – Software aspects of system safety validation	1	Probabilistic testing	확률론적 테스트	---	R	R	HR	
	2	Process simulation	공정 시뮬레이션	R	R	HR	HR	부록 B.2.7
	3	Modelling	모델링	R	R	HR	HR	
	4	Functional and black-box testing	기능 및 블랙 박스 테스트	HR	HR	HR	HR	부록 B.2.8 부록 B.2.25
	5	Forward traceability between the software safety requirements specification and the software safety validation plan	소프트웨어 안전 요구 사항 사양과 소프트웨어 안전 유효성 검사 계획 간의 전향 추적성	R	R	HR	HR	
	6	Backward traceability between the software safety validation plan and the software safety requirements specification	소프트웨어 안전성 검증 계획과 소프트웨어 안전성 요구 사항 사양 간의 역 추적성	R	R	HR	HR	
IEC61508-3 A.8 - Modification	1	Impact analysis	영향 분석	HR	HR	HR	HR	
	2	Reverify changed software module	변경된 소프트웨어 모듈 재확인	HR	HR	HR	HR	
	3	Reverify affected software modules	영향을 받는 소프트웨어 모듈 재확인	R	HR	HR	HR	
	4a	Revalidate complete system	전체 시스템 재 검증	---	R	HR	HR	
	4b	Regression validation	회귀 검증	R	HR	HR	HR	
	5	Software configuration management	소프트웨어 구성 관리	HR	HR	HR	HR	
	6	Data recording and analysis	데이터 기록 및 분석	HR	HR	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	7	Forward traceability between the Software safety requirements specification and the software modification plan (including reverification and revalidation)	소프트웨어 안전 요구 사항 사양과 소프트웨어 수정 계획 (재 검증 및 재 검증 포함) 간의 전향적 추적성	R	R	HR	HR	
	8	Backward traceability between the software modification plan (including reverification and revalidation)and the software safety requirements specification	소프트웨어 수정 계획 (재 검증 및 재 검증 포함)과 소프트웨어 안전 요구 사항 명세 사이의 역 추적성	R	R	HR	HR	
IEC61508-3 A.9 - Software verification	1	Formal proof	정식 증명	---	R	R	HR	
	2	Animation of specification and design	명세 및 디자인의 생기	R	R	R	R	
	3	Static analysis	정적 분석	R	HR	HR	HR	부록 B.2.9
	4	Dynamic analysis and testing	동적 분석 및 테스트	R	HR	HR	HR	부록 B.2.28
	5	Forward traceability between the software design specification and the software verification (including data verification) plan	소프트웨어 설계 사양과 소프트웨어 검증 (데이터 검증 포함) 계획 간의 포워드 추적성	R	R	HR	HR	
	6	Backward traceability between the software verification (including data verification) plan and the software design specification	소프트웨어 검증 (데이터 검증 포함) 계획과 소프트웨어 설계 명세 간의 역 추적성	R	R	HR	HR	
	7	Offline numerical analysis	오프라인 수치 분석	R	R	HR	HR	
	Software module testing and integration		소프트웨어 모듈 테스트 및 통합	See IEC61508-3 A.5				
	Programmable electronics integration testing		프로그래밍 가능한 전자 통합 테스트	See IEC61508-3 A.6				
	Software system testing (validation)		소프트웨어 시스템 테스트 (검증)	See IEC61508-3 A.7				
IEC61508-3	1	Checklists	점검표	R	R	R	R	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
A.10 - Functional safety assessment	2	Decision/truth tables	의사 결정 / 진리표	R	R	R	R	
	3	Failure analysis	고장 분석	R	R	HR	HR	부록 B.2.29
	4	Common cause failure analysis of diverse software (if diverse software is actually used)	다양한 소프트웨어의 공통 원인 실패 분석 (다양한 소프트웨어가 실제로 사용되는 경우)	---	R	HR	HR	
	5	Reliability block diagram	신뢰성 블록 다이어그램	R	R	R	R	부록 B.2.10
	6	Forward traceability between the requirements of Clause 8 and the plan for software functional safety assessment	8 절의 요구 사항과 소프트웨어 기능 안전성 평가 계획 사이의 전방 추적성	R	R	HR	HR	
IEC61508-3 B.1 - Design and coding standards	1	Use of coding standard to reduce likelihood of errors	오류 가능성을 줄이기위한 코딩 표준의 사용	HR	HR	HR	HR	
	2	No dynamic objects	동적 객체 없음	R	HR	HR	HR	
	3a	No dynamic variables	동적 변수 없음	---	R	HR	HR	
	3b	Online checking of the installation of dynamic variables	동적 변수 설치의 온라인 검사	---	R	HR	HR	
	4	Limited use of interrupts	제한된 인터럽트 사용	R	R	HR	HR	
	5	Limited use of pointers	포인터의 사용 제한	---	R	HR	HR	
	6	Limited use of recursion	제한된 재귀 사용	---	R	HR	HR	
	7	No unstructured control flow in programs in higher level languages	고수준 언어의 프로그램에서 구조화되지 않은 제어 흐름이 없음	R	HR	HR	HR	
	8	No automatic type conversion	자동 유형 변환 없음	R	HR	HR	HR	
IEC61508-3 B.2 - Dynamic analysis and testing	1	Test case execution from boundary value analysis	경계 값 분석을 통한 테스트 케이스 실행	R	HR	HR	HR	
	2	Test case execution from error guessing	오류 추측에서 테스트 사례 실행	R	R	R	R	
	3	Test case execution from error seeding	오류 시드에서 테스트 사례 실행	---	R	R	R	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	4	Test case execution from model-based test case generation	모델 기반 테스트 케이스 생성으로부터 테스트 케이스 실행	R	R	HR	HR	
	5	Performance modelling	성능 모델링	R	R	R	HR	
	6	Equivalence classes and input partition testing	동등한 클래스와 입력 파티션 테스트	R	R	R	HR	부록 B.2.11
	7a	Structural test coverage (entry points) 100 % **	구조 테스트 커버리지 (진입 점) 100 % **	HR	HR	HR	HR	
	7b	Structural test coverage (statements) 100 %**	구조 테스트 커버리지 (명세서) 100 % **	R	HR	HR	HR	
	7c	Structural test coverage (branches) 100 %**	구조 테스트 커버리지 (지점) 100 % **	R	R	HR	HR	
	7d	Structural test coverage (conditions, MC/DC) 100 %**	구조 테스트 커버리지 (조건, MC / DC) 100 % **	R	R	R	HR	
IEC61508-3 B.3 - Functional and black-box testing	1	Test case execution from cause consequence diagrams	원인 결과 다이어그램에서 테스트 사례 실행	---	---	R	R	
	2	Test case execution from model-based test case generation	모델 기반 테스트 케이스 생성으로부터 테스트 케이스 실행	R	R	HR	HR	
	3	Prototyping/animation	프로토 타이핑 / 애니메이션	---	---	R	R	
	4	Equivalence classes and input partition testing, including boundary value analysis	경계 값 분석을 포함한 동등한 클래스와 입력 파티션 테스트	R	HR	HR	HR	부록 B.2.11 부록 B.2.12
	5	Process simulation	공정 시뮬레이션	R	R	R	R	부록 B.2.7
IEC61508-3 B.4 – Failure analysis	1a	Cause consequence diagrams	원인 다이어그램	R	R	R	R	부록 B.2.29.2
	1b	Event tree analysis	이벤트 트리 분석	R	R	R	R	
	2	Fault tree analysis	결함 트리 분석	R	R	R	R	부록 B.2.29.9
	3	Software functional failure analysis	소프트웨어 기능 장애 분석	R	R	R	R	
IEC61508-3	1	Data flow diagrams	데이터 흐름도	R	R	R	R	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
B.5 - Modelling	2a	Finite state machines	유한 상태 기계	---	R	HR	HR	
	2b	Formal methods	정형 기법	---	R	R	HR	
	2c	Time Petri nets	시간 페트리 그물	---	R	HR	HR	부록 B.2.13.3
	3	Performance modelling	성능 모델링	R	HR	HR	HR	
	4	Prototyping/animation	프로토 타이핑 / 애니메이션	R	R	R	R	
	5	Structure diagrams	구조 다이어그램	R	R	R	HR	
IEC61508-3 B.6 - Performance testing	1	Avalanche/stress testing	눈사태 / 스트레스 테스트	R	R	HR	HR	
	2	Response timings and memory constraints	응답 타이밍 및 메모리 제약	HR	HR	HR	HR	
	3	Performance requirements	성능 요구 사항	HR	HR	HR	HR	
IEC61508-3 B.7 - Semi-formal methods	1	Logic/function block diagrams	논리 / 기능 블록 다이어그램	R	R	HR	HR	
	2	Sequence diagrams	시퀀스 다이어그램	R	R	HR	HR	
	3	Data flow diagrams	데이터 흐름도	R	R	R	R	
	4a	Finite state machines/state transition diagrams	유한 상태 기계 / 상태 전이 다이어그램	R	R	HR	HR	
	4b	Time Petri nets	시간 페트리 그물	R	R	HR	HR	부록 B.2.13.3
	5	Entity-relationship-attribute data models	엔터티 관련 특성 데이터 모델	R	R	R	R	
	6	Message sequence charts	메시지 시퀀스 차트	R	R	R	R	
	7	Decision/truth tables	의사 결정 / 진리표	R	R	HR	HR	
	8	UML	UML	R	R	R	R	
IEC61508-3 B.8 – Static analysis	1	Boundary value analysis	경계 값 분석	R	R	HR	HR	
	2	Checklists	점검표	R	R	R	R	
	3	Control flow analysis	제어 흐름 분석	R	HR	HR	HR	
	4	Data flow analysis	데이터 흐름 분석	R	HR	HR	HR	

Category		Technique/Measure	한글명(Technique/Measure)	SIL 1	SIL 2	SIL 3	SIL 4	제조 안전 관리활동
	5	Error guessing	오류 추측	R	R	R	R	
	6a	Formal inspections, including specific criteria	특정 기준을 포함한 공식 검사	R	R	HR	HR	부록 B.2.14
	6b	Walk-through (software)	워크 쓰루 (소프트웨어)	R	R	R	R	부록 B.2.15
	7	Symbolic execution	상징적 실행	---	---	R	R	
	8	Design review	디자인 검토	HR	HR	HR	HR	부록 B.2.16
	9	Static analysis of run time error behaviour	런타임 오류 동작의 정적 분석	R	R	R	HR	
	10	Worst-case execution time analysis	최악의 실행 시간 분석	R	R	R	R	
IEC61508-3 B.9 - Modular approach	1	Software module size limit	소프트웨어 모듈 크기 제한	HR	HR	HR	HR	
	2	Software complexity control	소프트웨어 복잡성 제어	R	R	HR	HR	
	3	Information hiding/encapsulation	정보 숨기기 / 캡슐화	R	HR	HR	HR	
	4	Parameter number limit / fixed number of subprogram parameters	매개 변수 개수 제한 / 고정 된 서브 프로그램 매개 변수 수	R	R	R	R	
	5	One entry/one exit point in subroutines and functions	서브 루틴과 함수에서 한 개의 엔트리 포인트 / 한 개의 출구 포인트	HR	HR	HR	HR	
	6	Fully defined interface	완전히 정의 된 인터페이스	HR	HR	HR	HR	

B.2. 안전관리활동 상세

B.2.11 소프트웨어 다양성 (다양한 프로그래밍) (Software diversity (diverse programming))

항 목	설 명
안전관리활동 ID	• SMA-01
안전관리활동명	• 소프트웨어 다양성 (다양한 프로그래밍) (Software diversity (diverse programming))
목 표	• 시스템의 안전에 치명적인 고장을 방지하고 높은 신뢰성을 위한 연속적인 운영을 위해 프로그램 실행 중 잔여 소프트웨어 설계 및 구현 결함을 감지하고 막는다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

다양한 프로그래밍에서 주어진 프로그램 명세는 다른 방식으로 N번 설계되고 구현된다. 동일한 입력 값이 N버전에 주어지며 N버전에 의해 생성된 결과가 비교된다. 결과가 유효한 것으로 간주되면 결과는 컴퓨터 출력으로 전송된다.

필수적인 요구 사항은 N버전은 어떤 의미에서는 서로 독립적이어서 동일한 원인으로 인해 모두 동시에 실패하지 않는다. 실제로 N버전 접근 방식의 기본인 버전 독립성을 달성하고 입증하는 것은 매우 어려울 수 있다.

N버전을 별도의 컴퓨터에서 병렬로 실행하거나 모든 버전을 동일한 컴퓨터에서 실행하고 결과를 내부 투표로 처리 할 수 있다. 다음과 같이 애플리케이션 요구 사항에 따라 N 버전에서 다양한 투표 전략을 사용할 수 있다.

시스템이 안전한 상태인 경우, 완전한 합의를 요구할 수 있다 (모든 N이 동의). 그렇지 않으면 출력 값이 사용되어 시스템이 안전한 상태에 도달하게 된다. 간단한 여행 시스템의 경우 투표가 안전한 방향으로 기울어 질 수 있다. 이 경우 두 버전 중 하나가 여행을 요구하면 안전 조치가 실행된다. 이 방법은 일반적으로 두 가지 버전 (N = 2) 만 사용한다.

안전 상태가 없는 시스템의 경우, 다수결 투표 전략을 사용할 수 있다. 단체 협약이 없는 경우에는 올바른 값을 선택할 기회를 극대화하기 위해 예를 들어 중간 값을 취하

거나 합의된 값이 반환이 될 때까지 일시적으로 출력을 고정시키는 등의 확률론적 접근법을 사용할 수 있다.

이 기법은 잔여 소프트웨어 설계 오류를 제거하거나 사양 해석 시 오류를 방지하지 않지만 안전에 영향을 미치기 전에 감지 및 막는 방법을 제공한다.

B.2.21 모듈방식(Modular approach)

항 목	설 명
안전관리활동 ID	• SMA-02
안전관리활동명	• 모듈방식(Modular approach)
목 표	• 시스템의 복잡성을 제한하기 위해 소프트웨어 시스템을 이해 가능한 작은 부분으로 분해한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

모듈 방식 또는 모듈화는 소프트웨어 프로젝트의 설계, 코딩 및 유지 관리 단계에 대한 몇 가지 규칙을 포함한다. 규칙은 설계 중에 사용 된 설계 방법에 따라 다르지만 대부분의 모듈에는 다음과 같은 규칙이 있다.

소프트웨어 모듈 (또는 이와 동등한 서브 프로그램)은 정의된 단일 작업 또는 기능을 갖추어야 한다.

소프트웨어 모듈 간의 연결은 엄격하게 제한 및 정의되어야 하며, 하나의 소프트웨어 모듈에서 일관성을 가져야 한다.

여러 레벨의 소프트웨어 모듈을 제공하여 서브 프로그램 컬렉션을 만들어야 한다.

서브 프로그램 크기는 지정된 값, 일반적으로 2-4 개의 화면 크기로 제한되어야 한다.

서브 프로그램은 단일 항목과 단일 종료만을 가져야 한다.

소프트웨어 모듈은 인터페이스를 통해 다른 소프트웨어 모듈과 통신해야 한다.

전역 변수 또는 공통 변수가 잘 구조화되어야 하고, 액세스가 제어되어야 하며, 각 인스턴스에서 그 사용이 정당화되어야 한다.

모든 소프트웨어 모듈 인터페이스는 완전히 문서화되어야 한다.

모든 소프트웨어 모듈의 인터페이스는 기능에 필요한 매개 변수만 포함해야 한다.

프로그래밍 언어가 기본 매개 변수를 허용하거나 객체 지향 접근 방식이 사용되는 가능성에 따라 복잡해진다.

B.2.31 소프트웨어 복잡성 제어 (Software complexity control)

항 목	설 명
안전관리활동 ID	• SMA-03
안전관리활동명	• 소프트웨어 복잡성 제어 (Software complexity control)
목 표	• 소프트웨어 자체의 속성 및 개발 또는 테스트 기록에서 프로그램의 특성을 예측한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

소프트웨어의 일부 구조적 특성을 평가하고 이를 신뢰성 또는 복잡성과 같은 원하는 특성과 연결한다. 소프트웨어 도구는 대부분의 측정 값을 평가해야 하며 적용 할 수 있는 측정 항목 중 일부는 다음과 같다.

그래프 이론 복잡성: 수명주기의 초기에 적용되어 트레이드 오프를 평가할 수 있으며 프로그램 제어 그래프의 복잡성에 기반한다.

특정 소프트웨어 모듈을 활성화하는 방법의 수 (액세스 가능성): 소프트웨어 모듈에 액세스 할 수 있으면 디버그 할 가능성이 높다.

Halstead 유형 메트릭 과학: 연산자 및 피연산자 수를 계산하여 프로그램 길이를 계산하고 미래 개발 자원을 추정 할 때 비교를 위한 기준선을 형성하는 복잡성과 규모의 척도를 제공한다.

소프트웨어 모듈 당 출입구 수 - 출입구 수를 최소화하는 것은 구조화 된 설계 및 프로그래밍 기술의 특징이다.

B.2.41 신뢰할 수 있고 검증된 소프트웨어 요소의 사용 (Use of trusted/verified software elements(if available))

항 목	설 명
안전관리활동 ID	• SMA-04
안전관리활동명	• 신뢰할 수 있고 검증된 소프트웨어 요소의 사용 (Use of trusted/verified software elements(if available))
목 표	• 소프트웨어 설계 및 요소(element)가 새로운 응용 프로그램마다 광범위하게 재확인 및 재설계 되는 것을 방지한다. 정형적 또는 엄격한 검증은 되지 않았으나, 오랜 운영 이력으로 확인된 소프트웨어 요소를 설계에 활용한다. 다른 응용 프로그램에서 검증되고 검증의 근거가 있는 기존 소프트웨어 요소를 활용한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

소프트웨어 요소가 오류 또는 작동 불능 상태로부터 충분히 자유로운지를 확인한다. 일반적으로 기본적인 부분부터 복잡한 시스템을 개발하는 것은 비실용적이다. 몇몇 유용한 기능을 제공하기 위해 이전에 개발된 주요 하위 어셈블리를 사용하여 새로운 시스템의 일부를 구현하기 위해 재사용 할 수 있다. 잘 설계되고 구조화된 PES는 명확하게 구별되고 세분화된 방식으로 상호 작용하는 소프트웨어 요소로 구성된다. 여러 응용 프로그램에서 재사용할 수 있는 일반적으로 적용 가능한 소프트웨어 요소의 라이브러리를 작성하면 둘 이상의 응용 프로그램에서 공유하는 디자인을 확인하는데 필요한 많은 자원을 사용할 수 있다.

그러나 안전 관련 응용 프로그램의 경우 기존 요소가 포함된 새 시스템에 필요한 안전 무결성이 있으며 기존 요소의 잘못된 동작으로 인해 안전이 손상되지 않는다는 것을 확인해야 한다.

기존 요소의 동작을 정확히 확인하기 위해 확인해야 할 사항은 다음과 같다.
요소의 포괄적인 운영 내역을 분석하여 해당 요소가 입증된 것을 확인 요소가 요구사항을 충족하는지 확인하기 위해 요소의 동작에 대해 수집된 증거를 평가

4.1 증명된 사용 (Proven-in-use)

항 목	설 명
안전관리활동 ID	• SMA-04-01
안전관리활동명	• 증명된 사용 (Proven-in-use)
목 표	• 소프트웨어 설계 및 요소(element)가 새로운 응용 프로그램마다 광범위하게 재확인 및 재설계 되는 것을 방지한다. 정형적 또는 엄격한 검증은 되지 않았으나, 오랜 운영 이력으로 확인된 소프트웨어 요소를 설계에 활용한다. 다른 응용 프로그램에서 검증되고 검증의 근거가 있는 기존 소프트웨어 요소를 활용한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

드문 경우지만, 신뢰할 수 있는 소프트웨어 요소(element)가 필요한 안전 무결성을 달성한다는 것을 "증명된 사용"이라 한다. 운영체제와 같은 다양한 기능을 갖추 복잡한 요소의 경우, 기능이 실제로 충분히 사용됨을 확인하는 것이 필수다. 예를 들어, 고장을 검출하기 위해 자가진단 루틴이 제공되는 경우, 작동 기간 내에 고장이 발생하지 않으면 고장 검출을 위한 자가진단 루틴을 사용 중이라고 볼 수 없다.

소프트웨어 요소는 다음 기준을 충족하는 경우 사용중인 것으로 간주된다.

변경되지 않은 사양

다른 응용 분야의 시스템

적어도 1 년 이상의 서비스 이력

안전 무결성 등급 또는 적절한 수요에 따른 작동 시간

비 안전 관련 실패율의 시연

수요 당 연간 10^{-2} 건 95% 신뢰의 300 건의 운영 필요

수요 당 연간 10^{-5} 건 99.9%의 신뢰의 690,000 건의 운영 필요 위 수치 계산 방법은 IEC-61508-7의 부록 D 를 참조한다. 통계적 접근에 대해서는 B.5.2 현장 경험(Field experience)을 참조한다.

특정한 상황에서 안전과 관련되지 않은 고장이 다른 상황에서 안전과 관련되어 있을 수 있다. 소프트웨어 요소가 기준을 충족하는지 확인하려면 다음 사항을 문서화해야 한다.

버전 번호를 포함한 각 시스템 및 요소의 정확한 식별 (소프트웨어 및 하드웨어)
사용자의 신원 및 사용 시간
작동 시간
사용자 응용 시스템 및 응용 사례의 선택 절차
고장을 검출하고 등록하고 제거하는 절차

4.2 검증 증거의 바디 평가 (Assess a body of verification evidence)

항 목	설 명
안전관리활동 ID	• SMA-04-02
안전관리활동명	• 검증 증거의 바디 평가 (Assess a body of verification evidence)
목 표	• 소프트웨어 설계 및 요소(element)가 새로운 응용 프로그램마다 광범위하게 재확인 및 재설계 되는 것을 방지한다. 정형적 또는 엄격한 검증은 되지 않았으나, 오랜 운영 이력으로 확인된 소프트웨어 요소를 설계에 활용한다. 다른 응용 프로그램에서 검증되고 검증의 근거가 있는 기존 소프트웨어 요소를 활용한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발

상 세

새로운 시스템을 개발하기 위해서 기존의 소프트웨어를 사용할 수 있다. 기존 소프트웨어 요소(element)란 이미 개발되었지만 현재 프로젝트 또는 SRS 용으로 개발되지 않은 것을 뜻한다. 기존 소프트웨어는 시중에 판매되는 제품이거나 이전 제품이나 시스템을 위해 일부 조직에서 개발한 소프트웨어일 수 있다. 기존 소프트웨어는 표준의 요구 사항에 따라 개발되었거나 개발되지 않았을 수 있다.

그러므로 기존 소프트웨어 요소를 활용하여 새로운 시스템을 개발하기 위해서는 기존 소프트웨어를 통합한 시스템의 안전 무결성을 확인해야 한다.

기존 소프트웨어를 통합하는 새로운 시스템의 안전 무결성을 평가하려면 기존 요소의 동작을 확인하는 검증이 필요하다. 이것은 공급 업체의 자체 문서 및 요소 개발 프로세스의 기록 문서나 새로운 안전 관련 시스템의 개발자 또는 제 3자를 통해 만들거나 보완 할 수 있다. 이것은 잠재적으로 재사용 가능한 소프트웨어 요소의 기능과 한계를 정의하는 "준수 품목 안전 수칙(Safety Manual for compliant items)" 이다. 어떤 경우에도 준수 품목에 대한 안전 수칙을 지켜야 하며, 특정 안전 기능의 무결성에 대한 평가를 가능하게 하기에 충분하다.

준수 품목에 대한 안전 수칙은 다음과 같다.

요소의 설계가 알려지고 문서화되어 있음

요소는 모든 요소 설계와 코드의 문서화된 테스트와 리뷰를 포함하는 체계적인 방법을 사용하여 검사 및 검증됨

안전 요구사항을 충족하며 요소의 사용되지 않거나 불필요한 기능으로부터 새로운 시스템이 방해 받지 않음
새로운 시스템에서 요소의 신뢰할 수 있는 모든 고장 메커니즘이 구현되었는지 확인
새로운 시스템의 기능안전성 평가는 재사용 된 요소가 증거와 안전 수칙 준수에 따라 엄격히 적용되어야 함.

B.2.51 방어적 프로그래밍 (Defensive programming)

항 목	설 명
안전관리활동 ID	• SMA-05
안전관리활동명	• 방어적 프로그래밍 (Defensive programming)
목 표	• 비정상적인 제어 흐름, 데이터 흐름 또는 데이터 값을 실행 중에 탐지하고 이를 미리 결정된 허용 가능한 방식으로 처리하는 프로그램을 만든다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발 • 코딩 & 구현

상 세

많은 기법들이 제어 비정상 또는 데이터 비정상을 검사하기 위하여 프로그래밍 중 사용될 수 있다. 이들 기법은 잘못된 데이터 처리 가능성을 감소하기 위하여 시스템의 프로그래밍 처음부터 끝까지 체계적으로 적용될 수 있다.

방어적 기법들의 두 가지 공통 영역이 식별될 수 있다. 본질적으로 오류-안전 소프트웨어가 그 자신의 설계 결점을 수용하기 위하여 설계 된다. 이러한 결점들은 설계 또는 코딩의 간단한 오류, 또는 잘못된 요구사항 때문일 수 있다.

다음 리스트는 몇 가지 방어적 기법들이다.

변수들은 범위가 검사되어야 한다.

가능하다면, 값이 타당성 있는지 검사되어야 한다.

프로시저에 대한 인자들은 유형이 있어야 하며, 차원과 범위가 프로시저 시작에서 검사되어야 한다.

이 세 가지 권고는 프로그램에서 다루어 지는 숫자들이 프로그램 기능적 및 변수 물리적 중요성 양쪽 관점에서 합리적임을 보증하는 것을 돕는다. 읽기-전용 및 읽기-쓰기 인자들은 분리되어야 하며 그들의 입출력은 검사되어야 한다. 함수들은 모든 인자들을 읽기 전용으로 다루어야 한다. 문자 상수는 쓰기 가능해서는 안 된다. 이것은 우연한 겹쳐 쓰기 또는 변수의 잘못된 사용 탐지를 돕는다. 오류 허용 소프트웨어는 그것의 환경에서 또는 명목적인 범위를 넘는 사용 또는 기대되는 조건에서 고장을 예상하고 설계되었다.

기법은 다음을 포함한다.

입력 변수들과 물리적 중요성을 갖는 중간 변수들은 타당성에 대해서 검사되어야 한다.

출력 변수들의 영향은 되도록 관련된 시스템 상태 변경의 직접적인 관찰에 의해서 검사되어야 한다.

소프트웨어는 그것의 구성을 검사해야 한다. 이것은 기대되는 하드웨어의 존재 및 접근성 모두를 포함할 수 있으며 또한 소프트웨어 자체로 완전하다. 이것은 특별히 유지보수 절차 후에 무결성 유지를 위해 중요하다.

제어 흐름 순서 검사 같은 몇몇 방어적 프로그래밍 기법들은 또한 외부적인 고장을 극복한다.

B.2.61 디자인 및 코딩 표준 (Design and coding standards)

항 목	설 명
안전관리활동 ID	• SMA-06
안전관리활동명	• 디자인 및 코딩 표준 (Design and coding standards)
목 표	• 안전 관련 코드에서 오류의 가능성을 줄이고 그 확인을 용이하게 한다.
적용단계	• 응용 소프트웨어 설계 명세 • 응용 소프트웨어 개발 • 코딩 & 구현

상 세

규칙은 참여자 간 프로젝트 초기에 정하며 이는 설계 및 개발 방법 및 관련 코딩 표준으로 구성된다. 이러한 규칙은 개발, 검증, 평가 및 유지 관리가 용이하게 하며 사용 가능한 도구를 고려해야 한다.

규칙은 응용 프로그램이 사용되는 시스템 제조업체가 제공하는 개발 도구 및 제한 사항을 준수해야 한다.

다음의 원칙에 맞게 이루어져야 한다.

모듈방식

- 소프트웨어 모듈 크기 제한 및 소프트웨어의 복잡성 제어
  - ◆ 모듈의 크기 제한 및 소프트웨어의 복잡성 한계 지정
  - ◆ 전체적인 복잡도 및 한계 지정
  - ◆ 파라메터의 수 제한, 서브 프로그램의 파라메터의 수 고정
- 인터페이스는 완전히 정의 되어야 함
  - ◆ 모듈(함수)의 입출력의 명시적 지정
  - ◆ 모듈의 명시적인 사전조건과 사후조건을 근거로 오류 주장 프로그래밍과 데이터 검증이 가능해야 함

이해하기 용이

- 의미가 모호하지 않은 명명규칙
- 숫자 값을 정의하는 이름
- 소스코드 문서를 위한 절차와 가이드라인

검증 및 테스트 용이

- 주요 라이브러리 모듈을 위한 사전, 사후 조건 확인
- 특정 데이터 요소 또는 기능 (예 : const)의 사용에 대한 제한을 나타낼 수 있는 언어 기능 사용에 대한 인센티브
- 도구 지원 검증의 경우 : 선택한 도구의 제한 사항을 준수하기 위한 규칙
- 순환(recursion) 사용의 제한과 다른 형태의 순환 의존성

지정된 설계에 대한 적합성의 정적 검증

- 특정 디자인 개념 또는 제약 조건 구현을 위한 코딩 지침
- 디자인에 대한 추적성을 높이기 위한 지침

B.2.71 공정 시뮬레이션(Process simulation)

항 목	설 명
안전관리활동 ID	• SMA-07
안전관리활동명	• 공정 시뮬레이션(Process simulation)
목 표	• 소프트웨어 시스템의 기능을 실제 세계를 어떤 방식으로든 수정하지 않고, 외부 세계와의 인터페이스와 함께 테스트한다.
적용단계	• 응용 소프트웨어 요구사항 확인 • 안전요구사항 확인

상 세

테스트 목적으로만 통제중인 장비(equipment under control - EUC)의 동작을 모방한 시스템을 생성한다. 시뮬레이션은 소프트웨어 또는 소프트웨어와 하드웨어의 조합일 수 있다.

시뮬레이션은 다음을 따른다.

EUC 가 실제로 설치 될 때 존재할 수 있는 입력과 동등한 입력을 제공한다.

통제 대상 설비를 충실히 대표하는 방식으로 시험중인 소프트웨어의 출력에 응답한다.

시험중인 시스템이 대응해야 하는 모든 변화를 제공 할 수 있도록 운영자 입력을 제공한다.

소프트웨어가 테스트될 때, 시뮬레이션은 입력 및 출력과 함께 타겟 하드웨어의 시뮬레이션 일 수 있다.

B.2.81 기능 테스트 (Functional testing)

항 목	설 명
안전관리활동 ID	• SMA-08
안전관리활동명	• 기능 테스트 (Functional testing)
목 표	• 사양 및 설계 단계에서의 실패를 나타내고 구현 및 소프트웨어 및 하드웨어의 통합 중 실패를 방지한다.
적용단계	• 응용 소프트웨어 요구사항 확인 • 안전요구사항 확인

상 세

기능 테스트 중에 시스템의 지정된 특성이 달성되었는지를 확인하는 검토가 수행된다. 시스템은 정상적으로 예상되는 동작을 적절하게 특성화 하는 입력 데이터를 제공받는다. 출력은 관측되고 응답은 명세에 의해 주어진 것과 비교된다. 불완전한 명세의 표시 및 표시로부터의 편차가 문서화 된다.

다중 채널 아키텍처 용으로 설계된 전자 부품의 기능 테스트에는 사전 검증된 파트너 부품으로 테스트한 제조 부품이 포함된다. 이 외에도 제조 된 컴포넌트는 동일한 배치의 다른 파트너 컴포넌트와 함께 테스트하여 다른 방법으로는 가려진 공통 모드 오류를 표시하는 것이 좋다. 시스템의 작업 용량은 충분해야 하며, 성능모델링을 참조한다.

B.2.91 정적 분석 (Static analysis)

항 목	설 명
안전관리활동 ID	• SMA-09
안전관리활동명	• 정적 분석 (Static analysis)
목 표	• 조기 또는 수년간의 작동 후 시험중인 시스템에서 고장을 초래할 수 있는 시스템적 고장을 방지한다.
적용단계	• 코딩 & 구현 • 기능안전평가 • 검증

상 세

시스템적 및 가용적 컴퓨터 지원 접근법은 프로토타입 시스템의 특정 정적 특성을 검사하여 해당 요구 사항 (예: 설계 가이드라인, 시스템 명세 및 기기 데이터 시트)에 대한 완전성, 일관성, 낮은 모호성을 보장한다. 정적 분석은 재현 가능하며 정의된 단계에 도달한 프로토타입에 적용된다. 하드웨어 및 소프트웨어에 대한 정적 분석의 몇 가지 예는 다음과 같다.

데이터 흐름의 일관성 분석 (예: 데이터 객체가 어디에서나 같은 값으로 해석되는지 테스트)

제어 흐름 분석 (예: 경로 결정, 액세스 할 수 없는 코드 결정)

인터페이스 분석 (다양한 소프트웨어 모듈 간의 가변 전송 조사 등)

변수를 생성, 참조 및 삭제하는 시퀀스를 탐지하는 데이터 흐름 분석

특정 가이드라인 (예: 연면 거리 및 공간 거리, 조립 거리, 물리적 단위 배열, 기계적으로 민감한 물리적 단위, 도입된 물리적 단위의 배타적 사용)을 준수하는지 테스트한다.

B.2.101 신뢰성 블록 다이어그램 (Reliability block diagram)

항 목	설 명
안전관리활동 ID	• SMA-10
안전관리활동명	• 신뢰성 블록 다이어그램 (Reliability block diagram)
목 표	도식화된 형태로, 일어나는 일련의 사건과 시스템이나 작업의 성공적

	인 운영을 위해 충족되어야 하는 조건을 모델링한다.
적용단계	• 기능안전평가 • 안전요구사항 확인 • 운영 & 유지보수
상 세	
분석 대상은 블록, 라인 및 논리 접합으로 구성된 성공 경로로 표현된다. 성공 경로는 다이어그램의 한쪽에서 시작하여 블록 및 교차점을 통해 다이어그램의 반대쪽까지 계속된다. 블록은 조건 또는 이벤트를 나타내며 조건은 참이거나, 아니라면 이벤트가 발생한 경우 경로가 전달할 수 있다. 접합부에 경로가 오면 접합부의 논리가 충족되면 경로가 계속된다. 정점에 도달하면, 모든 출력 라인을 따라 계속 될 수 있다. 다이어그램을 통해 성공 경로가 하나 이상 존재하면 분석 대상이 올바르게 작동한 것이다.	

B.2.111 동등한 클래스와 입력 파티션 테스트 (Equivalence classes and input partition testing)

항 목	설 명
안전관리활동 ID	• SMA-11
안전관리활동명	• 동등한 클래스와 입력 파티션 테스트 (Equivalence classes and input partition testing)
목 표	• 최소한의 테스트 데이터를 사용하여 소프트웨어를 적절히 테스트한다. 테스트 데이터는 소프트웨어를 실행하는데 필요한 입력 도메인의 파티션을 선택하여 얻는다.
적용단계	• 통합시험
상 세	
이 테스트 전략은 입력 도메인의 파티션을 결정하는 입력의 등가 관계를 기반으로 한다. 테스트 케이스는 이전에 지정된 모든 파티션을 다루기 위해 선택된다. 적어도 하나의 테스트 케이스가 각 동등한 클래스에서 선택된다. 입력 파티셔닝에는 두 가지 기본 가능성이 있다.	

명세에서 파생 된 동등한 클래스
명세의 해석은 입력 지향적 일 수 있다.
예를 들어, 선택된 값이 같은 방식으로 처리되거나 출력 방향이 지정 될 수 있거나 값의 집합이 동일한 기능 결과를 가질 수 있다.
프로그램의 내부 구조에서 파생된 동등한 클래스
동등한 클래스 결과는 프로그램의 정적 분석에서 결정된다.
예를 들어, 동일한 경로로 이어지는 값의 집합이 실행된다.

B.2.121 경계값 분석 (Boundary value analysis)

항 목	설 명
안전관리활동 ID	• SMA-12
안전관리활동명	• 경계값 분석 (Boundary value analysis)
목 표	• 매개 변수 한계 또는 경계에서 발생하는 소프트웨어 오류를 감지한다.
적용단계	• 통합시험 • 검증

상 세

프로그램의 입력 영역은 동등한 클래스 (B.11 참조)에 따라 여러 입력 클래스로 나눈다. 테스트는 클래스의 경계와 극한을 다루어야 한다. 테스트는 명세 입력 영역의 경계가 프로그램의 경계와 일치하는지 확인한다.

직접 및 간접 해석에서 0 값을 사용하면 종종 오류가 발생하기 쉽다.

0으로 나누기
공백 ASCII 문자
빈 스택 또는 리스트 요소
전체 매트릭스
제로 테이블 엔트리

일반적으로 입력 경계는 출력 범위의 경계에 직접적으로 대응한다. 테스트 케이스는 출력을 제한된 값으로 강제 설정해야 하며, 또한 출력이 스펙 경계 값을 초과하게 하는 테스트 케이스를 지정할 수 있는지 고려해야 한다. 출력이 일련의 데이터 (예 : 인쇄 된 표) 인 경우 첫 번째 및 마지막 요소와 아무것도 포함 하지 않은 목록과 하나 및 두 개의 요소가 포함 된 목록에 주의해야 한다.

B.2.131 준 정형 기법 (Semi-formal methods)

13.1 일반 (General)

항 목	설 명
안전관리활동 ID	• SMA-13-01
안전관리활동명	• 준 정형 기법 (Semi-formal methods)
목 표	• 사양에 부합함을 증명하기 위함
적용단계	• 응용 소프트웨어 요구사항 명세 • 기능안전평가 • 검증
상 세	
준 정형 기법은 개발 과정의 일부 단계에서 시스템에 대한 설명을 개발하는 수단을 제공한다. 예를 들자면 명세, 설계 또는 코딩 같은 것이 있다. 기술은 경우에 따라 시스템 동작에 대한 다양한 측면을 표현하기 위해 기계 또는 애니메이션으로 분석 할 수 있다. 애니메이션은 시스템이 특정 요구 사항은 물론 실제 요구 사항을 충족한다는 추가적인 확신을 줄 수 있다.	

13.2 유한 상태 기계/상태 전이 다이어그램 (Finite state machines / state transition diagrams)

항 목	설 명
안전관리활동 ID	• SMA-13-02
안전관리활동명	• 유한 상태 기계/상태 전이 다이어그램 (Finite state machines / state transition diagrams)
목 표	• 시스템의 제어 구조를 모델링, 확인, 명세 또는 구현한다.
적용단계	• 응용 소프트웨어 요구사항 명세 • 기능안전평가 • 검증

상 세

많은 시스템이 상태, 입력 및 동작과 관련하여 설명된다. 따라서, 상태 S1 에서, 입력 I 를 수신하면 시스템은 동작 A 를 수행하고 상태 S2 로 이동할 수 있다. 모든 상태에서 모든 입력에 대해 시스템의 동작을 설명함으로써 시스템을 완전하게 설명 할 수 있다.

시스템의 결과 모델은 유한 상태 기계(finite state machine) 라고 불린다. 종종 시스템이 한 상태에서 다른 상태로 이동하는 방식을 나타내는 소위 상태 전이도 또는 차원이 상태 및 입력이고 행렬 셀에 동작 및 새 상태가 포함 된 행렬로 그려진다. 시스템이 복잡하거나 자연스러운 구조를 갖는 경우 계층화 된 유한 상태 기계에 이를 반영 할 수 있다. 상태차트는 중첩된 상태가 허용되는 상태 전이도 유형이다. 상태 전이 표기법의 표현력을 높여주지만 안전 관련 시스템에서 복잡성을 높일 수 있다. 상태 차트에는 정형 명세가 있다. 상태 전이도는 전체 시스템이나 그 안에 있는 어떤 객체나 요소에 적용될 수 있고 유한 상태 기계로 표현 된 명세 또는 설계를 확인할 수 있다.
완전성 (시스템 또는 객체는 모든 상태의 모든 입력에 대해 동작 및 새로운 상태를 표시함)
일관성 (각 상태/입력 쌍에 대해 하나의 상태 전이만 가능함)
도달 가능성 (입력의 순서에 따라 하나의 상태에서 다른 상태로 갈 수 있는지 여부)
무한 루프 또는 막다른 상태가 없음.

이는 시스템에 중요한 속성이며 점검을 지원하는 도구는 개발되어 유한 상태 오토

마타를 기반으로 하는 다양한 모델을 사용할 수 있다. 유한 상태 기계 구현을 검증하거나 유한 상태 기계 모델을 애니메이션화 하기 위한 테스트 케이스의 자동 생성을 허용하는 알고리즘도 존재한다.

상태 전이도와 상태 차트는 다이어그램을 그려서 검사 할 수 있는 도구와 시스템을 구현하는 코드를 생성하는 도구로 지원된다. 고장 확률 계산에 사용될 수 있다.

13.3 시간 페트리 그물 (Time Petri nets)

항 목	설 명
안전관리활동 ID	• SMA-13-03
안전관리활동명	• 시간 페트리 그물 (Time Petri nets)
목 표	• 시스템 동작 관련 측면을 모델링하고 분석 및 재설계를 통해 안전 및 작동 요구 사항을 평가하고 개선시킨다.
적용단계	• 응용 소프트웨어 요구사항 명세 • 기능안전평가 • 검증

상 세

페트리 네트는 유한 상태 오토마타의 특별 경우인데, 동시성을 보이고 비동기적인 동작을 하는 시스템에서 정보를 표현하고 흐름을 제어하는데 적합한 그래프 이론 모델의 클래스에 속한다. 페트리 네트는 장소와 전환점의 네트워크다. 장소는 "marked" 또는 "unmarked" 이며, 전환은 모든 입력 위치가 표시 될 때 "enabled"가 된다. 이 기능을 사용하면 "fire"할 수 있지만, 입력 전환 지점이 표시되지 않고 전환 지점의 각 출력 위치가 대신 표시된다. 잠재적 위험은 모델의 특정 상태로 표현된다. 페트리 네트 모델은 시스템의 타이밍 기능을 허용할 수 있다. "고전적인" 페트리 네트는 제어 흐름 측면에 집중하고 있지만 데이터 흐름을 모델에 통합하기 위한 몇 가지 확장이 제안되었다. 실패 확률 계산을 위해 몬테카를로 시뮬레이션을 수행을 효율적으로 지원한다.

B.2.141 정형 검사 (Formal inspections)

항 목	설 명
안전관리활동 ID	• SMA-14
안전관리활동명	• 정형 검사 (Formal inspections)
목 표	• 소프트웨어 요소의 결함을 밝힌다.
적용단계	• 코딩 & 구현 • 검증

상 세

정형 검사는 결함을 발견하고 생산자가 자료를 개선 할 수 있도록 자료를 생산하는 사람의 동료가 수행하는 소프트웨어 자료를 검사하는 구조화된 프로세스다. 생산자는 숙지 단계에서 검사원에게 간단한 설명을 하는 것 이외에는 검사 과정에 아무런 영향을 미치지 않는다. 정식 검사는 소프트웨어 개발 생명주기의 모든 단계에서 생산된 특정 소프트웨어 요소에서 수행 된다.

검사를 받기 전에 검사원은 검사할 재료에 익숙해야 하고 검사 과정에서 역할은 명확해야 한다. 검사 일정을 준비하고 시작 및 종료 기준은 소프트웨어 요소에 필요한 속성을 기반으로 정의한다. 시작 기준은 검사가 실시되기 전에 충족되어야 하는 기준 또는 요구 사항이며 종료 기준은 특정 프로세스를 완료하기 위해 충족되어야 하는 기준 또는 요구 사항이다.

검사하는 동안 검사의 결과는 중재자에 의해 공식적으로 기록되어야 한다. 모든 조사관은 결과에 대해 합의해야 한다. 결함은 인수 전에 수정을 요구하거나 주어진 시간/공정표에 의해 수정을 요구하는 것으로 분류되어야 한다. 확인된 결함은 검사가 완료된 후에 후속 수정을 위해 생산자에게 보고되어야 한다. 확인된 결함의 수와 범위에 따라 중재자는 소프트웨어 자료의 추가 검사를 위해 필요하다고 판단할 수 있다.

B.2.151 워크 쓰루 (소프트웨어) (Walk-through (software))

항 목	설 명
안전관리활동 ID	• SMA-15

안전관리활동명	• 워크 쓰루 (소프트웨어) (Walk-through (software))
목 표	• 명세와 구현 간의 불일치를 밝힌다.
적용단계	• 코딩 & 구현 • 검증
상 세	
워크 쓰루는 비 정형적인 기술로서, 소프트웨어 요소 제작자가 소프트웨어 요소의 결함을 찾는 목적으로 동료 들과 함께 수행한다. 소프트웨어 개발 생명주기의 모든 단계에서 생산된 특정 소프트웨어 요소에서 수행될 수 있다. 안전 관련 시스템이 명세에 주어진 요구 사항에 부합하는지 확인하기 위해 안전 관련 시스템의 특정 기능을 조사하고 평가한다. 제품의 구현 및 사용에 관한 의문점은 문서화되어 해결 할 수 있다. 정형 검사와 달리 작성자는 워크 쓰루 절차 중에 검사한다.	

B.2.161 설계 검토(Design review)

항 목	설 명
안전관리활동 ID	• SMA-16
안전관리활동명	• 설계 검토(Design review)
목 표	• 소프트웨어 설계의 결함을 찾는다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	
설계 검토는 설계 요구 사항을 평가 및 충족시키며 문제를 식별하고 해결책을 제시한다. 이는 설계 기능을 평가하기 위한 소프트웨어 설계에 대한 정형적이고 문서화된 포괄적이고 체계적인 검토를 의미한다. 설계 검토는 입력 요구 사항에 대한 설계 상태를 평가할 수 있는 방법과 향후 개선 기회를 식별할 수 있는 방법을 제공한다. 개발 생명주기 활동이 진행되고 주요 세부 설계 일정이 충족되면 모든 인터페이스 측면을 검토한다. 설계가 요구 사항을 충족하고 안전요구사항에 부합하는지 설계 검토를 실시한다. 이는 주로 설계자의 작업을 검	

증하기 위한 것이고 확인(confirmation)과 세부 활동(refining activity)으로서 다룬다.

잠재 장애 분석(sneak circuit analysis)과 같은 엄격 검사 기법은 예상불가능 경로 또는 논리 흐름, 의도하지 않은 출력, 잘못된 타이밍, 원하지 않는 동작 등과 같은 잘못된 소프트웨어 동작을 탐지하기 위해 사용한다.

B.2.171 프로그램 순서 모니터링 (Logical monitoring of program sequence)

결함이 있는 프로그램 순서를 탐지한다. 프로그램의 개별 요소(예: 소프트웨어 모듈, 서브 프로그램 또는 명령)가 잘못된 순서 또는 시간으로 처리되거나 프로세서 시계에 결함이 있는 경우 결함 있는 프로그램 순서가 존재한다고 한다.

17.1 타임 윈도우 없이 별도의 시간 기준이 있는 워치 독(Watch-dog with separate time base without time-window)

항 목	설 명
안전관리활동 ID	• SMA-17-01
안전관리활동명	• 타임 윈도우 없이 별도의 시간 기준이 있는 워치 독(Watch-dog with separate time base without time-window)
목 표	• 프로그램 순서의 행동과 타당성을 모니터링한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	
컴퓨터의 동작과 프로그램 시퀀스의 타당성을 모니터링하기 위해 별도의 시간 기준(예: 워치 독 타이머)이 있는 외부 타이밍 요소가 주기적으로 트리거 된다. 트리거 포인트가 프로그램에 올바르게 배치되어 있어야 한다. 워치 독은 고정된 기간에 트리거 되지는 않지만 최대 간격이 지정된다.	

17.2 별도의 시간 기준 및 타임 윈도우가 있는 워치 독 (Watch-dog with separate time base and time-window)

항 목	설 명
안전관리활동 ID	• SMA-17-02
안전관리활동명	• 별도의 시간 기준 및 타임 윈도우가 있는 워치 독 (Watch-dog with separate time base and time-window)
목 표	• 프로그램 순서의 행동과 타당성을 모니터링한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	

컴퓨터의 동작과 프로그램 시퀀스의 타당성을 모니터링하기 위해 별도의 시간 기준(예: 워치 독 타이머)가 있는 외부 타이밍 요소가 주기적으로 트리거 된다. 트리거 포인트가 프로그램에 올바르게 배치되어 있어야 한다. 워치 독 타이머에는 상한과 하한이 있다. 프로그램 순서가 예상보다 길거나 더 짧은 시간이 걸릴 경우, 응급 조치가 취해진다.

17.3 프로그램 순서의 논리적 모니터링 (Logical monitoring of program sequence)

항 목	설 명
안전관리활동 ID	• SMA-17-03
안전관리활동명	• 프로그램 순서의 논리적 모니터링 (Logical monitoring of program sequence)
목 표	• 개별 프로그램 섹션의 올바른 순서를 모니터링한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	
개별 프로그램 섹션의 올바른 순서는 소프트웨어(계산 프로시저, 주요 프로시저)를 사용하거나 외부 모니터링 장비를 사용하여 모니터링 된다. 검사 점이 프로그램에 올바르게 배치되는 것이 중요하다.	

17.4 프로그램 순서의 시간 및 논리적 모니터링 조합 (Combination of temporal and logical monitoring of program sequences)

항 목	설 명
안전관리활동 ID	• SMA-17-04
안전관리활동명	• 프로그램 순서의 시간 및 논리적 모니터링 조합 (Combination of temporal and logical monitoring of program sequences)
목 표	• 개별 프로그램 섹션의 올바른 순서를 모니터링한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	

프로그램 시퀀스를 모니터링하는 임시 기능 (예 : 감시 타이머)이 프로그램 섹션 시퀀스가 올바르게 실행 된 경우에만 다시 트리거 한다.

17.5 온라인 확인을 통한 시간 모니터링 (Temporal monitoring with on-line check)

항 목	설 명
안전관리활동 ID	• SMA-17-05
안전관리활동명	• 온라인 확인을 통한 시간 모니터링 (Temporal monitoring with on-line check)
목 표	• 시간 모니터링에서 오류를 감지한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	
시동 시 시동 모니터링이 점검되고, 시동 모니터링이 올바르게 작동하는 경우에만 시동이 가능하다. 예를 들어 열 센서는 시동 시 가열된 저항으로 점검할 수 있다.	

B.2.181 온라인 모니터링에 의한 고장 탐지 (Failure detection by on-line monitoring)

항 목	설 명
안전관리활동 ID	• SMA-18
안전관리활동명	• 온라인 모니터링에 의한 고장 탐지 (Failure detection by on-line monitoring)
목 표	• 통제중인 장비 (equipment under control: EUC)의 정상 (온라인) 작동에 대한 응답으로 E/E/PE 안전 관련 시스템의 동작을 모니터링하여 고장을 탐지한다.
적용단계	• 응용 소프트웨어 설계 명세 • 운영 & 유지보수
상 세	
특정 조건 하에서, 실패는 EUC의 시간 행동에 대한 정보를 사용하여 감지 할 수 있다. 예를 들어, E/E/PE 안전 관련 시스템의 일부인 스위치가 EUC에 의해 정상적으로 작동한 후 예상된 시간에 스위치가 상태를 변경하지 않으면 고장이 감지된다. 일반적으로 고장을 지역화 할 수는 없다.	

B.2.191 코드 보호 (Code protection)

항 목	설 명
안전관리활동 ID	• SMA-19
안전관리활동명	• 코드 보호 (Code protection)
목 표	• 입력/출력 데이터 흐름에서 임의 하드웨어 고장(random hardware failures) 및 계통적 고장(systematic failures)을 감지한다.
적용단계	• 응용 소프트웨어 설계 명세
상 세	
이 절차는 계통적 고장 및 임의 하드웨어 고장으로부터 입출력 정보를 보호한다. 코드 보호는 정보 중복 및 시간 중복을 기반으로 입출력 장치의 데이터 흐름에 따른 고	

장 감지를 제공한다. 일반적으로 중복 정보는 입출력 데이터에 중첩된다. 이것은 입출력 회로의 정확한 작동을 모니터하는 수단을 제공한다. 많은 기술이 가능하며, 예를 들어 반송파 주파수(carrier frequency) 신호가 센서의 출력 신호에 중첩 될 수 있다. 로직 유닛은 반송파 주파수의 존재를 체크하거나 중복 코드 비트(redundant code bits)가 출력 채널에 추가되어 로직 유닛과 최종 액추에이터 사이를 통과하는 신호의 유효성을 모니터링 할 수 있다.

B.2.201 오류 주장 프로그래밍 (Failure assertion programming)

항 목	설 명
안전관리활동 ID	• SMA-20
안전관리활동명	• 오류 주장 프로그래밍 (Failure assertion programming)
목 표	• 프로그램의 실행 중 소프트웨어 설계 오류를 감지하여 시스템의 안전에 치명적인 오류를 방지하고 높은 신뢰성을 위해 작동한다.
적용단계	• 응용 소프트웨어 설계 명세

상 세

이 프로그래밍 방법은 명령문이 실행되기 전 사전 조건과 사후조건을 검사하는 것이다. 사전 조건 또는 사후 조건 중 하나라도 충족되지 않으면 오류를 보고한다.

```
assert < pre-condition>;      action 1;
        :
        :
action x;        assert < post-condition>;
```

B.2.211 명세 검사 (Inspection of the specification)

항 목	설 명
안전관리활동 ID	• SMA-21
안전관리활동명	• 명세 검사 (Inspection of the specification)
목 표	• 명세에서 불완전성과 모순을 피한다.
적용단계	• 응용 소프트웨어 요구사항 명세

상 세

검사는 명세서의 다양한 품질을 독립적인 팀이 평가하는 일반적인 기술이다. 검사팀은 작성자에게 질문을 하고 작성자는 충분한 대답을 해야 한다. 시험은 (가능하다면) 명세 작성에 관여하지 않은 팀에 의해 수행되어야 한다. 요구되는 독립 정도는 시스템에 요구되는 안전 무결성 레벨에 의해 결정된다. 독립 검사관은 추가 명세를 언급하지 않고 확실한 방법으로 시스템의 작동 기능을 재구성 할 수 있어야 한다. 또한 운영 및

조직 조치의 모든 관련 안전 및 기술적 측면을 다루고 있는지 확인해야 한다. 이 절차는 실제로 매우 효과적이라는 것을 증명했다.

B.2.221 시뮬레이션 (Simulation)

항 목	설 명
안전관리활동 ID	• SMA-22
안전관리활동명	• 시뮬레이션 (Simulation)
목 표	• 전기 전자 회로의 기능적 성능과 컴포넌트의 올바른 치수 측정을 체계적이고 완벽하게 검사한다.
적용단계	• 응용 소프트웨어 설계 명세 • 기능안전평가 • 운영 & 유지보수
상 세	
안전 관련 시스템 회로의 기능은 소프트웨어 동작 모델을 통해 컴퓨터에서 시뮬레이션 된다. 회로의 개별 컴포넌트는 각각 고유한 시뮬레이션 된 동작을 가지며, 각 구성 요소의 주변 데이터를 조사하여 회로의 응답을 검사한다.	

B.2.231 검사 (리뷰 및 분석) (Inspection (reviews and analysis))

항 목	설 명
안전관리활동 ID	• SMA-23
안전관리활동명	• 검사 (리뷰 및 분석) (Inspection (reviews and analysis))
목 표	• 명세와 구현 간의 불일치를 드러낸다.
적용단계	• 응용 소프트웨어 설계 명세 • 기능안전평가
상 세	
안전 관련 시스템의 특정 기능을 검사 및 평가하여 안전 관련 시스템이 사양에 명시된 요구 사항을 준수하는지 확인한다. 제품의 구현 및 사용에 관한 의문점과 잠재적인 약점이 문서화되어 해결될 수 있다. 워크 쓰루(Walk-through)와 달리 검사하는 동안 작성자는 수동적이며 검사자는 능동적이다.	

B.2.241 워크 쓰루(Walk-through)

항 목	설 명
안전관리활동 ID	• SMA-24
안전관리활동명	• 워크 쓰루(Walk-through)
목 표	• 명세와 구현 간의 불일치를 드러낸다.
적용단계	• 응용 소프트웨어 설계 명세 • 기능안전평가

상 세

안전 관련 시스템 초안의 특정 기능을 검사하고 평가하여 안전 관련 시스템이 사양에 주어진 요구 사항을 준수하는지 확인한다. 제품의 구현 및 사용에 관한 의문점과 잠재적인 약점이 문서화되어 해결될 수 있다. 검사(inspection)와 달리 워크 쓰루를 하는 동안 작성자는 능동적이며 검사자는 수동적이다.

B.2.251 블랙 박스 테스트 (Black-box testing)

항 목	설 명
안전관리활동 ID	• SMA-25
안전관리활동명	• 블랙 박스 테스트 (Black-box testing)
목 표	• 실제 기능 조건에서 동적 동작을 확인한다. 기능 명세 충족하지 못하고 유틸리티 및 견고성을 평가하는데 실패했을 경우 결함을 밝힌다.
적용단계	• 통합시험 • 운영 & 유지보수

상 세

시스템 또는 프로그램의 기능은 지정된 환경에서 실행되며 지정된 테스트 데이터는 설정된 기준에 따라 명세에서 체계적으로 추출된다. 시스템의 동작을 공개하고 명세와의 비교를 허용한다. 시스템의 내부 구조에 대한 지식이 테스트에 사용되지 않는다. 목적은 기능 단위가 명세에서 요구하는 모든 기능을 올바르게 수행하는지 여부를 확인

하는 것이다. 입력 데이터 공간은 명세에 부합하게 특정 입력 값 범위 (등가 클래스)로 세분된다.

테스트 케이스는 다음 사항들로 구성된다.

허용 범위의 데이터
허용되지 않는 범위의 데이터
범위 한도의 데이터
극단 값
상위 클래스의 조합

다른 테스트 활동 (모듈 테스트, 통합 테스트 및 시스템 테스트)에서 테스트 케이스를 선택하기 위해서는 다른 기준이 효과적일 수 있다. 예를 들어, "극한 운영 조건" 기준은 유효성 확인 프레임워크 내에서 시스템 테스트에 의존한다.

B.2.261 결함 삽입 테스트 (Fault insertion testing)

항 목	설 명
안전관리활동 ID	• SMA-26
안전관리활동명	• 결함 삽입 테스트 (Fault insertion testing)
목 표	• 시스템 하드웨어에서 고장을 도입하거나 시뮬레이션하고 응답을 문서화한다.
적용단계	• 응용 소프트웨어 설계 명세 • 운영 & 유지보수

상 세

이것은 의존성을 평가하는 정성적 방법이다. 바람직하게는, 상세한 기능 블록, 회로 및 배선도가 위치 및 유형의 결함 및 그것이 어떻게 도입되는지를 설명하기 위해 사용된다.

예를 들면

다양한 모듈에서 전력을 차단할 수 있다.
전원, 버스 또는 주소 라인이 개방/단락 될 수 있다.
컴포넌트 또는 해당 포트를 열거나 단락 시킬 수 있다.
계전기가 닫히거나 열리지 않거나 잘못된 시간에 오류가 발생할 수 있다.

릴레이가 닫히거나 열리지 못하거나 잘못된 시간에 릴레이가 작동하지 않을 수 있다.

원칙적으로 단일 정상 상태 결함이 도입된다. 그러나 내장된 진단 검사에 의해 결함이 밝혀지지 않았거나 명백하게 나타나지 않는 경우에는 시스템에 그대로 두어 두 번째 결함의 영향을 고려할 수 있다. 고장의 수는 쉽게 수백 개까지 증가 할 수 있다.

이 작업은 여러 분야의 팀에 의해 수행되며 시스템 공급 업체가 참석하여 상의해야 한다. 걱정스러운 결과가 있는 결함에 대한 고장 간 평균 작동 시간을 계산하거나 추정해야 한다. 계산된 시간이 낮으면 수정해야 한다.

B.2.271 정적 분석 (Static analysis)

항 목	설 명
안전관리활동 ID	• SMA-27
안전관리활동명	• 정적 분석 (Static analysis)
목 표	• 조기 또는 수년간의 작동 후 시험중인 시스템에서 고장을 초래할 수 있는 시스템적 고장을 방지한다.
적용단계	• 기능안전평가 • 운영 & 유지보수

상 세

시스템적 및 가용적 컴퓨터 지원 접근법은 프로토타입 시스템의 특정 정적 특성을 검사하여 해당 요구 사항 (예: 설계 가이드라인, 시스템 명세 및 기기 데이터 시트)에 대한 완전성, 일관성, 낮은 모호성을 보장한다. 정적 분석은 재현 가능하며 정의된 단계에 도달한 프로토타입에 적용된다. 하드웨어 및 소프트웨어에 대한 정적 분석의 몇 가지 예는 다음과 같다.

데이터 흐름의 일관성 분석 (예: 데이터 객체가 어디에서나 같은 값으로 해석되는지 테스트)

제어 흐름 분석 (예: 경로 결정, 액세스 할 수 없는 코드 결정)

인터페이스 분석 (다양한 소프트웨어 모듈 간의 가변 전송 조사 등)

변수를 생성, 참조 및 삭제하는 시퀀스를 탐지하는 데이터 흐름 분석

특정 가이드라인 (예: 연면 거리 및 공간 거리, 조립 거리, 물리적 단위 배열, 기계적으로 민감한 물리적 단위, 도입된 물리적 단위의 배타적 사용)을 준수하는지 테스트한다.

B.2.281 동적 분석 및 테스트 (Dynamic analysis and testing)

항 목	설 명
안전관리활동 ID	• SMA-28
안전관리활동명	• 동적 분석 및 테스트 (Dynamic analysis and testing)
목 표	• 완료 상태에서 프로토타입의 동적 동작을 검사하여 명세 오류를 감지한다.

적용단계	• 응용 소프트웨어 설계 명세 • 운영 & 유지보수

상 세

안전 관련 시스템의 동적 분석은 안전 관련 시스템의 운영과 가까운 프로토타입을 의도된 운영 환경의 일반적인 입력 데이터에 적용함으로써 수행한다. 관찰된 안전 관련 시스템의 동작이 요구되는 동작에 부합한다면 분석은 만족된다. 안전 관련 시스템의 모든 오류는 시정되어야 하며 새로운 운영 버전은 재분석되어야 한다.

B.2.291 고장 분석 (Failure analysis)

29.1 고장 모드 및 영향 분석 (Failure modes and effects analysis (FMEA))

항 목	설 명
안전관리활동 ID	• SMA-29-01
안전관리활동명	• 고장 모드 및 영향 분석 (Failure modes and effects analysis (FMEA))
목 표	• 시스템 컴포넌트의 가능한 모든 고장 원인을 체계적으로 검사하고 이러한 오류가 시스템의 작동 및 안전에 미치는 영향을 결정하여 시스템 설계를 분석한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수
상 세	
분석은 일반적으로 엔지니어 회의를 통해 이루어진다. 시스템의 각 컴포넌트는 차례로 분석되어 컴포넌트에 대한 일련의 고장 모드, 원인 및 결과 (로컬 및 전체 시스템 수준에서), 탐지 절차 및 권장 사항을 제공한다. 권고 사항이 적용되면, 취해진 교정 조치를 문서화한다.	

29.2 원인 다이어그램 (Cause consequence diagrams)

항 목	설 명
안전관리활동 ID	• SMA-29-02
안전관리활동명	• 원인 다이어그램 (Cause consequence diagrams)
목 표	• 요약 이벤트를 조합한 결과로 시스템에서 발생할 수 있는 일련의 이벤트를 소형 다이어그램 형식으로 분석 및 모델링하여 어떻게 심각한 결과가 발생할 수 있는지를 나타낸다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수
상 세	
결함 트리와 이벤트 트리 분석의 조합이며, 시작과 같은 중요한 이벤트에서 시작하	

고 시퀀스 그래프는 일부 작업의 성공과 실패를 설명하는 YES/NO 게이트를 사용하여 표시된다. 이를 통해 사고 또는 마스터 된 상황을 유도하는 이벤트 시퀀스를 작성할 수 있다. 그리고 다음 각 고장에 대한 그래프 (즉, 결함 트리)가 작성된다. 다음, 우발적인 상황에서 시작하여 역방향으로 진행하며, 우발적인 상황을 가장 큰 사건으로 여기는 글로벌 결함 트리를 작성한다. 진행 방향에서 사건으로 인해 발생할 수 있는 결과가 결정된다. 그래프는 정점과 다른 가지를 따라 전파하기 위한 조건을 설명하는 정점 기호를 포함 할 수 있으며 시간 지연도 포함될 수 있다. 이러한 조건은 결함 트리로 설명 할 수 있다. 전파 라인을 논리 기호와 결합하여 다이어그램을 컴팩트하게 만들 수 있다. 원인 결과 다이어그램에 사용하기 위해 표준 기호 세트가 정의된다. 다이어그램은 결함 트리를 작성하고 특정 비판적인 결과가 발생할 확률을 계산하는 데 사용할 수 있다.

29.3 이벤트 트리 분석 (Event tree analysis (ETA))

항 목	설 명
안전관리활동 ID	• SMA-29-03
안전관리활동명	• 이벤트 트리 분석 (Event tree analysis (ETA))
목 표	• 개략적인 형태로 시작 이벤트 후 시스템에서 발생할 수 있는 일련의 이벤트를 모델링하여 심각한 결과가 발생할 수 있음을 보여준다. 이벤트 트리는 처음부터 작성하기가 어렵고 결과 다이어그램을 사용하는 것이 작성에 도움이 된다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

다이어그램의 맨 위는 시작 이벤트 다음에 진행되는 이벤트의 진행과 관련된 순서 조건이 기록된다. 분석 대상인 시작 이벤트에서 시작하여 첫 번째 조건으로 선이 그려진다. 거기서 다이어그램은 "예"와 "아니오" 가지로 나뉘어 미래 이벤트가 어떻게 상태에 의존 하는지 설명한다. 가지들 각각에 대해 비슷한 방식으로 다음 조건을 이어 나간다. 모든 지점이 모든 조건을 만족하는 것은 아니다. 하나는 시퀀스의 끝까지 계속되며, 이렇게 구성된 트리의 각 가지는 가능한 결과를 나타낸다. 시퀀스의 조건이 독립적인 경우 이벤트 트리를 사용하여 시퀀스의 조건 확률을 기반으로 다양한 결과의 확률을 계산할 수 있다. 조건이 거의 완전히 독립적이기 때문에 이러한 계산은 숙련 된 분석가가 수행해야한다.

29.4 고장 모드, 영향 및 중요도 분석(Failure modes, effects and criticality analysis (FMECA))

항 목	설 명
안전관리활동 ID	• SMA-29-04
안전관리활동명	• 고장 모드, 영향 및 중요도 분석(Failure modes, effects and criticality analysis (FMECA))
목 표	• 설계 또는 작동 중에 특별한 주의와 제어 조치가 필요한 컴포넌트

	를 결정하기 위해 단일 포인트 오류를 통해 부상, 손상 또는 시스템 저하를 초래할 수 있는 컴포넌트의 중요성을 순위 지정한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수
상 세	
FMEA 와 유사하지만 여러 가지 방법으로 순위를 매길 수 있는 중요도를 나타내는 하나 이상의 컬럼이 있다. 이 절차에서 모든 컴포넌트에 대한 중요도 번호는 중요 모드에서 발생하는 백만 건의 작업 중 예상되는 특정 유형의 오류 수로 표시된다. 임계수는 9개의 매개 변수의 함수이며 대부분이 측정되어야 한다. 중요도 결정을 위한 매우 간단한 방법은 컴포넌트 오류의 확률에 생성 될 수 있는 손상을 곱하는 것이다.	

29.5 결함 트리 분석 (Fault tree analysis)

항 목	설 명
안전관리활동 ID	• SMA-29-05
안전관리활동명	• 결함 트리 분석 (Fault tree analysis)
목 표	• 사건의 분석이나 사건의 조합을 위해 위험이나 심각한 결과를 초래하는 사건의 확률을 계산한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

위험 또는 심각한 결과의 직접적인 원인인 이벤트에서 시작하여 이벤트의 원인을 식별하기 위한 분석을 수행한다. 논리 연산자 등을 사용하여 여러 단계로 수행된다. 중간 원인은 같은 방식으로 분석되며, 분석을 중지하면 기본 이벤트로 돌아간다. 이 분석은 그래픽으로 되어있으며 표준화된 기호 세트가 결함 트리를 그리는 데 사용된다. 분석이 끝나면 결함 트리는 기본 이벤트 (일반적으로 컴포넌트 고장)를 상위 이벤트(전체 시스템 고장)에 연결하는 논리적 기능을 표시한다. 주로 하드웨어 시스템 분석을 위한 것이지만, 소프트웨어 오류 분석에 적용할 수 있다. 이 기법은 고장 분석 및 상위 이벤트의 확률적 계산에 사용할 수 있다.

29.6 마르코프 모델 (Markov models)

항 목	설 명
안전관리활동 ID	• SMA-29-06
안전관리활동명	• 마르코프 모델 (Markov models)
목 표	• 상태 전이 그래프를 사용하여 시스템의 동작을 모델링하고 시스템의 확률론적 시스템 매개 변수 (예 : 비 신뢰성, 비 가용성, MTTF, MUT, MDT 등)를 평가한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

마르코프 모델은 방향성이 있는 그래프로 표현된 유한 상태 오토마타 (IEC-61508-7 B.2.3.2 참조)이다. 노드 (원)는 상태를 나타내고 노드 사이의 가장자리(화살표)는 상태 사이에서 발생하는 전이(고장, 수리 등)를 나타낸다. 에지는 해당 고장율 또는 수리율로 가중치가 부여된다. 동종 마르코프 프로세스의 근본적인 특성은 미래가 현재에만 의존한다는 것이다. 상태의 변화 N은 후속 상태 N+1로 이전 상태 N-1과 독립적이다. 이것은 모델의 모든 확률론적 법칙들이 기하 급수적이라는 것을 의미한다.

증명 시험 간격 또한 한 단계의 끝 (예: 증명 테스트 직전)에 있는 상태의 확률이 다음 단계 (예: 증명 테스트가 수행된 후의 여러 상태의 확률)의 초기 조건을 계산하는데 사용될 수 있는, 소위 다중 단계 마르코프 (Multi-phase Markov) 프로세스를 사용하여 적절하게 모델링 할 수 있다.

마르코프 기술은 컴포넌트 고장 및 복구로 인해 중복성 수준이 시간에 따라 변하는 여러 시스템을 모델링하는데 적합한다. FMEA와 FTA와 같은 다른 고전적 방법은 해당 확률을 계산하기 위한 간단한 조합 공식이 없으므로 시스템의 생명주기 전반에 걸쳐 실패 영향을 모델링하는데 쉽게 적용 할 수 없다.

가장 간단한 경우에, 시스템의 확률을 기술하는 공식은 문헌에서 쉽게 이용 가능하거나 수동으로 계산될 수 있으며, 보다 복잡한 경우를 다루기 위한 몇몇의 단순화 방법 (즉, 상태의 수를 감소 시킴)도 존재한다.

그럼에도 불구하고, 수학적으로 말하면, 동종 마르코프 그래프는 상수 계수를 갖는 단순하고 일반적인 선형 미분 방정식 집합이다. 이것은 오랫동안 분석되었으며 강력한

알고리즘이 개발되어 이를 처리 할 수 있다. 따라서 모델의 크기가 커지면 다양한 컴퓨터 소프트웨어 패키지에 구현된 위의 알고리즘을 사용하는 것이 매우 효율적이다.

그래프의 크기는 컴포넌트의 수에 따라 기하 급수적으로 증가한다는 점에 유의해야 한다. 이는 소위 조합 폭발이라고 한다. 따라서 이 기술은 소형 시스템에서만 근사치 없이 사용할 수 있다.

비 지수 법칙을 준-마르코프 모델로 처리해야 한다면 몬테카를로 시뮬레이션 (B.13.8 참조)을 사용해야 한다.

29.7 신뢰도 블록 다이어그램 (RBD) (Reliability block diagrams (RBD))

항 목	설 명
안전관리활동 ID	• SMA-29-07
안전관리활동명	• 신뢰도 블록 다이어그램 (RBD) (Reliability block diagrams (RBD))
목 표	• 시스템 또는 작업의 성공적인 운영을 위해 수행되어야 하는 이벤트 및 일련의 상황을 도식적으로 모델링한다. 이것은 분석 방법보다 표현의 방법이다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

분석 대상은 블록, 선 및 논리 접합으로 구성된 성공 경로로 표시된다. 성공 경로는 다이어그램의 한쪽에서부터 시작하여 블록 및 교차점을 통해 다이어그램의 다른 쪽까지 계속된다. 블록은 조건 또는 이벤트를 나타내며 조건은 참이거나 이벤트가 발생한 경우 경로가 전달할 수 있다. 경로가 접합부에 도착하여 접합부의 논리가 충족되면 경로가 계속된다. 정점에 도달하면, 모든 출력 라인을 따라 계속 될 수 있다. 다이어그램을 통해 성공 경로가 하나 이상 존재하면 분석 대상이 올바르게 작동한다.

RBD는 모델링 된 시스템의 구조적 표현이다. 이것은 일종의 전기 회로이다. 전류가 입력에서 출력까지의 경로를 찾으면 모델링 된 시스템이 제대로 작동하고 있는 것이다. 즉, 회로가 끊어 졌을 때 모델링 된 시스템이 고장 났음을 의미 한다. 이는 모델링 된 시스템의 실패를 초래하는 고장(즉, RBD가 "절단"된 곳)의 조합을 나타내는 최소 절단 세트의 개념으로 이어진다.

수학적으로 RBD는 결함 트리와 유사하다. 개별 컴포넌트의 상태(고장 또는 작동)를 전체 시스템의 상태 (고장 또는 작동)와 연결하는 논리적 기능을 나타낸다. 따라서 계산은 결함 트리에 대해 설명한 것과 유사하다.

29.8 몬테카를로 시뮬레이션 (Monte-Carlo simulation)

항 목	설 명
안전관리활동 ID	• SMA-29-08
안전관리활동명	• 몬테카를로 시뮬레이션 (Monte-Carlo simulation)
목 표	• 분석 방법을 실행할 수 없을 때 난수를 생성하여 실제 현상을 시뮬레이션 한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

몬테카를로 시뮬레이션은 두 가지 문제를 해결하는데 사용한다.

확률론적 현상을 생성하기 위해 난수가 사용되는 확률론적 문제

수학적 등가 확률 문제(예: 적분 계산)로 변환되는 결정론적 문제

몬테카를로 시뮬레이션의 원리는 연구중인 시스템의 행동 기능 및 기능 장애 모델을 애니메이션화 하기 위해 난수를 사용하는 것이다. 이러한 행동 모델은 상태 전이 모델 (마르코프 그래프, 페트리 네트, 형식 언어 등)에 의해 제공된다. 몬테카를로 시뮬레이션을 실행하여 통계 결과를 얻을 수 있는 큰 통계 샘플을 생성한다.

몬테카를로 시뮬레이션을 사용할 때 바이어스(biases), 공차(tolerances) 또는 노이즈(noise)가 합리적인 값을 갖도록 주의를 기울여야한다. 이것은 시뮬레이션으로부터 쉽게 얻을 수 있는 신뢰 구간을 통해 관리되어야 한다. 분석 방법과 달리 몬테카를로 시뮬레이션은 자기 근사법이다. 무시할 수 있는 이벤트는 모델을 단순화하기 위해 식별할 필요없이 표시되지 않는다.

몬테카를로 시뮬레이션의 일반적인 원리는 처음에 언급한 문제를 해결하는 것보다 얻은 결과가 가능한 정확하도록 문제를 재명시하여 재구성하는 것이다.

이 표준의 컨텍스트에서, 몬테카를로 시뮬레이션은 SIL 계산을 위해 그리고 신뢰성 데이터 불확실성을 고려하기 위해 사용될 수 있다. 현재 컴퓨터를 사용하면 SIL4 계산을 쉽게 수행 할 수 있다.

29.9 결함 트리 모델 (Fault tree models)

항 목	설 명
안전관리활동 ID	• SMA-29-09
안전관리활동명	• 결함 트리 모델 (Fault tree models)
목 표	• 체계적인 탑 다운 그래픽 (결과-원인) 접근 방식으로 구축하기 위한 방법. 기본 이벤트 (고장 모드)를 상위 이벤트 (원하지 않는 이벤트)에 연결하는 논리적 기능이다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

이것은 분석가가 단계 별로 모델을 개발하는데 도움이 되는 분석 방법이자 확률적 계산을 위한 수학적 모델이다.

결함 트리 모델은 다음을 수행 할 수 있다 :

고장 시나리오를 식별하고 분류하여 정성적 분석 (최소 절단 세트 또는 주요 함축)
발생 확률에 따라 시나리오를 순위 매김하여 준-정량적 분석,
상위 이벤트의 확률을 계산하여 정량적 분석.

결함 트리는 RBD (Reliability Block Diagrams)와 마찬가지로 개별 컴포넌트의 상태 (고장 또는 작동)와 전체 시스템 (고장 또는 작동)의 상태를 연결하는 논리 (부울) 기능을 나타낸다. 따라서 컴포넌트가 독립적인 경우 논리 함수에 적용되는 확률의 기본 특성을 적용하는 것만으로 확률적 계산을 수행 할 수 있다. 이는 기본적으로 진 확률(즉, 상수)로만 작동하는 정적 모델이기 때문에 쉽지 않다. 시간 의존적 확률은 조심스럽게 다루어야 한다. 예를 들어 주기적으로 검증된 컴포넌트를 포함하는 안전 시스템의 PFD_{avg}는 직접 계산할 수 없으며 연속 모드로 작동하는 안전 시스템의 PFH에 대해서는 훨씬 더 어렵다. 따라서 기본 수학에 대한 올바른 이해가 있는 믿을 만한 엔지니어만이 이 방법으로 비 가용성/PFD 및 비 신뢰성/PFH 계산을 수행해야 한다.

매우 단순한 결함 트리에 대해서는 계산을 손으로 수행할 수 있지만 지난 50년 동안 복잡한 논리 방정식을 처리하기 위해 많은 알고리즘이 개발 및 구현되었다. 현재의 기술 수준은 BDD (Binary Decision Diagrams)를 사용하는데, 이는 논리 방정식을 컴퓨터 메모리로 압축하는 기술이다. 현재 산업 규모 시스템에 대한 근사치없이 확률적 계

산을 수행할 수 있는 유일한 방법이다. 몬테카를로 시뮬레이션으로 불확실성을 처리할 수 있을 정도로 충분히 빠르다.

29.10 일반화된 확률론적 페트리 네트 모델 (Generalised Stochastic Petri net models (GSPN))

항 목	설 명
안전관리활동 ID	• SMA-29-10
안전관리활동명	• 일반화된 확률론적 페트리 네트 모델 (Generalized Stochastic Petri net models (GSPN))
목 표	• 몬테카를로 시뮬레이션에 대한 효율적인 지원을 제공하기 위해 실제 모델링 된 시스템과 가능한 가깝게 행동하는 기능 모델과 기능 장애 모델을 그래픽으로 작성한다.
적용단계	• 안전요구사항 확인 • 운영 & 유지보수

상 세

GSPN은 비동기 유한 상태 오토마타이다. 단, 안전성 평가 시스템의 기능 불량 행동을 모델링 할 때 준 정형 검증을 수행 할 때 추적되는 양호한 특성은 더 이상 존재하지 않는다. 이른바 장소 (원으로 묘사 됨)는 잠재적 상태를 나타내며 이른바 장면 전환 (직사각형으로 묘사 됨)은 발생할 가능성이 있는 사건을 나타낸다. 장소 표시 (B.17.3 참조) 이외에도 메시지 또는 술어를 사용하여 전환을 검증 (활성화) 할 수 있으며 전환의 유효성 검사에서부터 경과 지연은 결정적 또는 확률적일 수 있다. 이것이 왜 그 페트리 네트가 "일반화된 확률론적 페트리 네트"라고 불리는 이유이다.

페트리 네트는 몬테카를로 시뮬레이션 지원 (B.13.8 참조)과 같이 매우 효율적인 것으로 입증된 유연한 행동 모델을 구성한다. 어쨌든 항상 알려진 몬테카를로 시뮬레이션의 정확성을 제외하면 다른 방법 (의존성, 조합 폭발, 비지수 규칙 등)의 모든 한계가 극복된다. 현재 컴퓨터에서는 SIL4 평가에서도 더 이상 문제가 없다.

B.2.301 최악의 케이스 분석 (Worst-case analysis)

항 목	설 명
안전관리활동 ID	• SMA-30
안전관리활동명	• 최악의 케이스 분석 (Worst-case analysis)

목 표	• 환경 조건과 컴포넌트 공차(tolerances)의 바람직하지 못한 조합으로 인해 발생하는 계통적 고장(systematic failures)을 방지한다.
적용단계	• 안전요구사항 확인

상 세

시스템의 운영 용량 및 컴포넌트 치수는 이론적 근거에 따라 조사되거나 계산된다. 환경 조건은 허용 가능한 최대 한계 값으로 변경된다. 시스템의 가장 필수적인 응답을 검사하고 명세와 비교한다.

부록 C. 기능안전 생명주기

C.1. 기능안전 생명주기 단계별 목록

아래의 목록은 [그림 15 기능 안전 생명주기 구조]의 단계별 목표, 이해 관계자, 입/출력물 등을 용이하게 확인할 수 있도록 한다. 목록의 크기로 인해 두 개의 목록으로 나뉘어서 표시되었다.

목록은 다음의 항목으로 이루어졌다.

(1) 분류

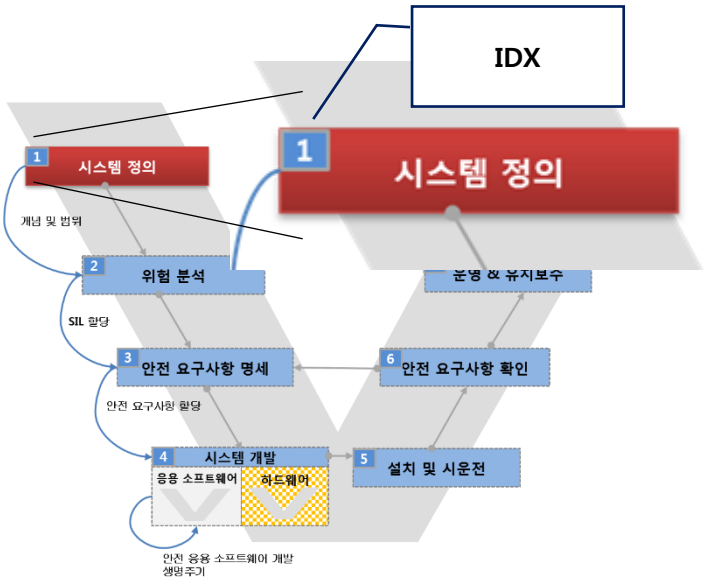
(2) SYS: 시스템

(3) SW: 응용 소프트웨어

(4) FSM: 기능안전 관리

(5) V&V: 검증

(6) IDX: 기능안전 생명주기의 구조에 표시된 인덱스 번호



(7) 기능안전 생명주기: 기능안전 생명주기의 구조에 표시된 단계명(한글)

(8) 목표: 단계를 달성하기 위한 목표

(9) 이해 관계자: 단계의 이해관계자

(10) 입력물: 단계를 시작하기 위한 입력물

(11) 출력물: 단계가 종료될 때 나오는 출력물

(12) 선행기준: 단계가 시작되기에 앞서 갖춰야할 기준

(13) 완료기준: 단계가 완료됨을 판단할 수 있는 기준

(14) 안전관리활동ID: 단계를 수행하기 위해 권장되는 안전관리활동(기술/기법)의 ID 목록

(15) 안전관리활동명: 단계를 수행하기 위해 권장되는 안전관리활동(기술/기법) 목록 (이름)

(16) 챕터: 본 가이드라인에서 각 단계를 설명하기 위한 참조 챕터

표 42 기능안전 생명주기 단계별 목록 Part 1

분류	IDX	기능안전 생명주기	목표	이해 관계자	입력물	출력물	챕터
SYS	1	시스템 정의	대상 시스템에 대한 정보를 식별하여 개념(기능/물리/제약) 및 개발 범위를 정의	시스템 개발자 응용소프트웨어 개발 담당자 하드웨어 개발 담당자	시스템 범위 이해당사자 요건 운용개념 및 운용모드 인터페이스 환경요소 제약조건 주요성능 수명주기 기반 프로세스	시스템 샤양서 시스템 기능 및 물리 정보 안전관련 기능 식별 시스템 아키텍처 시스템 개발 베이스라인 확립	0
SYS	2	위험 분석	대상 시스템이 잠재적으로 지닌 위험요소에 대한 분석 및 식별	시스템 안전 담당자 시스템 개발자	시스템 사양서	시스템 안전분석 산출물(FTA, HAZOP, LOPA)	3.2
SYS	3	안전 요구사항 명세	대상 시스템의 안전성 확보를 위한 의도된 기능이 작동 될 수 있거나, 안전한 상태로 유지할 수 있도록 설계적 방안을 명세	시스템 안전 담당자	시스템 기능 요구사항 사양서 시스템 안전 기능 요구사항 사양서 시스템 구조 정의서	시스템 안전 요구사항 명세서 시스템 안전 아키텍처 명세서 시스템 안전 검증 보고서 시스템 안전요구사항 추적표	0
SYS	4	시스템 개발	시스템의 의도된 목적을 부합하도록 대상이 지니고 있는 설계적/안전측면의 방안을 고려한 시스템 개발 산출물 명세	시스템 개발자 응용소프트웨어 개발 담당자 하드웨어 개발 담당자	시스템 정의서 시스템 안전 요구사항 사양서 시스템 제약조건	시스템 요구사항 사양서 시스템 기능 아키텍처 시스템 물리 아키텍처 시스템 요구사항 추적표	0
SW	4-1	응용 소프트웨어 요구사항 명세	응용 소프트웨어 안전 요구사항 및 요구사항 확인 방법 명세	• 응용 소프트웨어 요구사항 분석 담당자 • 응용 소프트웨어 테스트 담당자	• 안전 시스템 아키텍처 설계서 • 안전 시스템 안전 기능 정의서 • 안전 시스템 안전 요구사항 명세서 • 안전 시스템 안전 매뉴얼 및 안	• 응용 소프트웨어 안전 요구사항 명세서 • 응용 소프트웨어 안전 요구사항 검증 보고서 • 응용 소프트웨어 안전 요구사항	4.1

분류	IDX	기능안전 생명주기	목표	이해 관계자	입력물	출력물	챕터
					전 계획서	추적표	
SW	4-2	응용 소프트웨어 설계	응용 소프트웨어의 구조를 설계하고 모듈(기능 단위) 상세 설계서를 명세	• 응용 소프트웨어 요구사항 분석 담당자 • 응용 소프트웨어 아키텍처 및 상세 설계 담당자	• 안전 시스템 아키텍처 설계서 • 안전 시스템 하드웨어 아키텍처 설계 제약사항 • 안전 시스템 사용자 매뉴얼 • 응용 소프트웨어 안전 요구사항 명세서 • 응용 소프트웨어 안전 요구사항 추적표	• 응용 소프트웨어 구조 설계서 • 응용 소프트웨어 및 하위 시스템 통합 테스트 명세서 • 응용 소프트웨어 구조 검증 보고서	4.2
SW	4-3	응용 소프트웨어 개발	응용 소프트웨어 구현을 위해 필요한 언어 선택 및 기능별 구현 패턴 명세	• 응용 소프트웨어 개발자 • 응용 소프트웨어 테스트 담당자	• 안전 시스템 아키텍처 설계서 • 안전 시스템 하드웨어 아키텍처 설계 제약사항 • 응용 소프트웨어 구조 및 상세 설계서 • 응용 소프트웨어 및 하위 시스템 통합 테스트 명세서	• 응용 소프트웨어 구현 언어 • 응용 소프트웨어 구현 설명서 • 응용 소프트웨어 단위 테스트 계획서	4.3
SW		코딩 & 구현	응용 소프트웨어 모듈, 프로그램, 기능 블록을 개발	• 응용 소프트웨어 개발자 • 응용 소프트웨어 단위 테스트 담당자	• 안전 시스템 아키텍처 설계서 • 안전 시스템 하드웨어 아키텍처 설계 제약사항 • 응용 소프트웨어 구조 및 상세 설계서 • 응용 소프트웨어 단위 테스트 정의서	• 코드 • 테스트 코드	4.4

분류	IDX	기능안전 생명주기	목표	이해 관계자	입력물	출력물	챕터
SW	4-4	단위 시험	소프트웨어 단위 모듈들이 상세 설계와 안전 요구사항을 준수하도록 구현되었는지 검증	• 응용 소프트웨어 아키텍처 설계자 • 응용 소프트웨어 단위 설계자 • 응용 소프트웨어 개발자 • 응용 소프트웨어 단위 테스트 담당자	• 응용 소프트웨어 단위 설계서 • 응용 소프트웨어 단위 테스트 계획서 • 응용 소프트웨어 단위 테스트 명세서 • 응용 소프트웨어 단위 설계 리뷰 결과 • 응용 소프트웨어 단위 테스트 계획 / 명세 리뷰 결과 • 소스 코드	• 응용 소프트웨어 단위 테스트 계획서 (갱신) • 응용 소프트웨어 단위 테스트 명세서 (갱신) • 응용 소프트웨어 단위 테스트 결과서	4.5
SW	4-5	통합 시험	모든 응용 소프트웨어 모듈과 컴포넌트 / 서브 시스템이 소프트웨어 아키텍처 설계와 안전 무결성 등급을 준수하도록 의도된 기능을 수행하기 위해 서로 및 기본 내장 소프트웨어와 정확하게 상호 작용하는지 그리고 안전 기능을 위태롭게 할 수 있는 의도하지 않은 기능을 수행하지 않는지 검증	• 응용 소프트웨어 아키텍처 설계자 • 응용 소프트웨어 개발자 • 응용 소프트웨어 통합 담당자 • 응용 소프트웨어 통합 테스트 담당자	• 응용 소프트웨어 아키텍처 설계서 • 응용 소프트웨어 통합 테스트 계획서 • 응용 소프트웨어 통합 테스트 명세서 • 응용 소프트웨어 아키텍처 설계 리뷰 결과 • 응용 소프트웨어 통합 테스트 계획 / 명세 리뷰 결과 • 응용 소프트웨어 단위 테스트 결과서 • 단위 테스트 완료 소스 코드	• 응용 소프트웨어 통합 테스트 계획서 (갱신) • 응용 소프트웨어 통합 테스트 명세서 (갱신) • 응용 소프트웨어 통합 테스트 결과서 • 통합 바이너리 파일	4.6
HW	4-1	하드웨어 안전 요구사항					N/A
HW	4-1-1	프로그램 가능한 하드웨어					N/A
HW	4-1-2	프로그램 불가능한 하드웨어					N/A

분류	IDX	기능안전 생명주기	목표	이해 관계자	입력물	출력물	챕터
HW	4-2	프로그램 가능한 하드웨어 선정					N/A
SYS	5	설치 및 시운전					N/A
SYS	6	안전 요구사항 확인					N/A
SYS	7	운영 & 유지보수					N/A
SYS	8	변경					N/A
FSM		기능안전 관리					N/A
FSM		기능안전 평가					N/A
V&V		검증					N/A

표 43 기능안전 생명주기 단계별 목록 Part 2

분류	IDX	기능안전 생명주기	선행기준	완료기준	안전관리활동 ID	안전관리활동명	챕터
SYS	1	시스템 정의	1. 이해당사자 정의 2. 이해당사자 요구도 정의 3. 운용개념도 정의	이해당사자 소요 정의 시스템 내외부 인터페이스 정의 시스템 운용개념도 기반		기능컨셉 구성컨셉	0
SYS	2	위험 분석	1.시스템 사양서 정의 2.시스템 구조/기능 분석서 3.개발/운용 제약조건 정의	시스템 구조/기능 정의 시스템 인터페이스 정의 시스템 제약사항 정의		FTA FMEA HAZOP LOPA	3.2
SYS	3	안전 요구사항 명세	시스템사양서 정의 시스템 구조/기능 분석서`	시스템 오류/영향 분석 완료 시스템 안전 요구사항 명세 완료		시스템 구조분석 시스템 기능분석	0
SYS	4	시스템 개발	시스템 사양서 정의 시스템 안전분석 산출물 정의	시스템 사양서 완료 시스템 안전 요구사항 명세서 완료		시스템 안전 분석	0
SW	4-1	응용 소프트웨어 요구사항 명세	1. 안전 시스템의 안전 기능 식별 및 서브 시스템 할당 완료 2. 안전 시스템 안전 기능을 만족하는 시스템 요구사항 정의 완료 3. 안전 시스템 안전 무결성 등급 할당 완료	1. 응용 소프트웨어 요구사항 분석 완료 2. 응용 소프트웨어 요구사항 검증 완료 3. 응용 소프트웨어 요구사항 추적표 작성 완료	SMA-13 SMA-21	준 정형 기법 명세 검사	4.1

분류	IDX	기능안전 생명 주기	선행기준	완료기준	안전관리 활동 ID	안전관리활동명	챕터
SW	4-2	응용 소프트웨어 설계 명세	1. 안전 시스템 아키텍처 설계 완료 2. 안전 시스템 안전 기능 식별 완료 3. 응용 소프트웨어 안전 요구사항 식별 완료	1. 응용 소프트웨어 외부 시스템 상호 연결 적용 완료 2. 응용 소프트웨어 운영 모드 및 세부 수행 흐름 적용 완료 2. 응용 소프트웨어 설계서 작성 완료 3. 응용 소프트웨어 구조 추적표 작성 완료	SMA-1 SMA-2 SMA-3 SMA-4 SMA-5 SMA-6 SMA-16 SMA-17 SMA-18 SMA-19 SMA-20 SMA-22 SMA-23 SMA-24	소프트웨어 다양성 (다양한 프로그래밍) 모듈방식 소프트웨어 복잡성 제어 신뢰할 수 있고 검증된 소프트웨어 요소의 사용 방어적 프로그래밍 디자인 및 코딩 표준 설계 검토 프로그램 순서 모니터링 온라인 모니터링에 의한 고장 탐지 코드 보호 오류 주장 프로그래밍 시뮬레이션 검사 (리뷰 및 분석) 워크 쓰루	4.2
SW	4-3	응용 소프트웨어 개발	1. 응용 소프트웨어 외부 시스템 상호 연결 적용 완료 2. 응용 소프트웨어 운영 모드 및 세부 수행 흐름 적용 완료 2. 응용 소프트웨어 설계서 작성 완료 3. 응용 소프트웨어 구조 추적표 작성 완료	1. 응용 소프트웨어 구현 언어 선택 완료 2. 응용 소프트웨어 구현 설명서 작성 완료 3. 응용 소프트웨어 단위 테스트 계획서 (갱신)	SMA-1 SMA-2 SMA-3 SMA-4 SMA-5 SMA-6	소프트웨어 다양성 (다양한 프로그래밍) 모듈방식 소프트웨어 복잡성 제어 신뢰할 수 있고 검증된 소프트웨어 요소의 사용 방어적 프로그래밍 디자인 및 코딩 표준	4.3
SW	4-4	코딩 & 구현	1. 응용 소프트웨어 구현 언어 선택 완료 2. 응용 소프트웨어 구현 설명서 작성 완료 3. 응용 소프트웨어 단위 테스트 계	1. 응용 소프트웨어 기능별 코드 2. 응용 소프트웨어 단위 테스트 코드	SMA-5 SMA-6 SMA-9 SMA-14 SMA-15	방어적 프로그래밍 디자인 및 코딩 표준 정적 분석 정형 검사 워크 쓰루 (소프트웨어)	4.4

분류	IDX	기능안전 생명 주기	선행기준	완료기준	안전관리 활동 ID	안전관리활동명	챕터
			획서 갱신 완료				
SW	4-5	단위 시험	1. 응용 소프트웨어 단위 설계 완료 2. 응용 소프트웨어 단위 테스트 계획 수립 완료 3. 응용 소프트웨어 단위 테스트 명세 완료 4. 응용 소프트웨어 단위 설계 리뷰 완료 5. 응용 소프트웨어 단위 테스트 계획 / 명세 리뷰 완료 6. 응용 소프트웨어 구현 완료	1. 응용 소프트웨어 단위 테스트 계획서 갱신 완료 2. 응용 소프트웨어 단위 테스트 명세서 갱신 완료 3. 소스 코드 리뷰 및 후속 치 완료 4. 응용 소프트웨어 단위 테스트 및 결함 해결 완료 5. 응용 소프트웨어 단위 테스트 결과서 작성 완료 6. 응용 소프트웨어 단위 설계와 테스트 결과의 추적성 확보 7. 응용 소프트웨어 단위 설계와 테스트 결과의 일관성 확보	SMA-11 SMA-12	동등한 클래스와 입력 파티션 테스트 경계값 분석	4.5
SW	4-6	통합 시험	1. 응용 소프트웨어 아키텍처 설계 완료 2. 응용 소프트웨어 통합 테스트 계획 수립 완료 3. 응용 소프트웨어 통합 테스트 명세 완료 4. 응용 소프트웨어 아키텍처 설계 리뷰 완료 5. 응용 소프트웨어 통합 테스트 계획 / 명세 리뷰 완료 6. 응용 소프트웨어 단위 테스트 완	1. 응용 소프트웨어 통합 테스트 계획서 갱신 완료 2. 응용 소프트웨어 통합 테스트 명세서 갱신 완료 4. 응용 소프트웨어 통합 테스트 및 결함 해결 완료 5. 응용 소프트웨어 통합 테스트 결과서 작성 완료 6. 응용 소프트웨어 아키텍처 설계와 테스트 결과의 추적성 확보 7. 응용 소프트웨어 아키텍처 설계	SMA-11 SMA-12 SMA-25	동등한 클래스와 입력 파티션 테스트 경계값 분석 블랙 박스 테스트	4.6

분류	IDX	기능안전 생명 주기	선행기준	완료기준	안전관리 활동 ID	안전관리활동명	챕터
			료	와 테스트 결과의 일관성 확보 8. 응용 소프트웨어 통합 바이너리 생성 완료			
HW	4-1	하드웨어 안전 요구사항					N/A
HW	4-1-1	프로그램 가능한 하드웨어					N/A
HW	4-1-2	프로그램 불가능한 하드웨어					N/A
HW	4-2	프로그램 가능한 하드웨어 선정					N/A
SYS	5	설치 및 시운전					N/A
SYS	6	안전 요구사항 확인			SMA-7 SMA-8 SMA-30	공정 시뮬레이션 기능 테스트 최악의 케이스 분석	N/A

분류	IDX	기능안전 생명 주기	선행기준	완료기준	안전관리 활동 ID	안전관리활동명	챕터
SYS	7	운영 & 유지보수			SMA-18 SMA-22 SMA-25 SMA-26 SMA-27 SMA-28 SMA-29	온라인 모니터링에 의한 고장 탐지 시뮬레이션 블랙 박스 테스트 결함 삽입 테스트 정적 분석 동적 분석 및 테스트 고장 분석	N/A
SYS	8	변경					N/A
FSM		기능안전 관리					N/A
FSM		기능안전 평가			SMA-9 SMA-10 SMA-13	정적 분석 신뢰성 블록 다이어그램 준 정형 기법	N/A
V&V		검증			SMA-9 SMA-10 SMA-12 SMA-13 SMA-14 SMA-15 SMA-16 SMA-22 SMA-23 SMA-24	정적 분석 신뢰성 블록 다이어그램 경계값 분석 준 정형 기법 정형 검사 워크 쓰루 (소프트웨어) 설계 검토 시뮬레이션 검사 (리뷰 및 분석) 워크 쓰루	N/A

본 가이드는 현재 개발이 진행 중이며,
최종 완료된 문서가 아님을 알려드립니다.
개발 완료 시점은 2018년 12월입니다.
가이드 활용에 이 점 참고하시기 바라며,
문의사항이나 개선사항은
safety@nipa.kr로 보내주시길 바랍니다.
고맙습니다.