

신호설비 공통 플랫폼 개발 및 철도시스템 인증체계 수립 방안 기획 최종보고서

2015. 01.

Infrastructure
R&D Report

주관연구기관 / 한국철도기술연구원
공동연구기관 / 대아티아이(주)
(주)한터기술

국 토 교 통 부
국토교통과학기술진흥원

제 출 문

국토교통부장관귀하

이 보고서를 “신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획”
과제의 보고서로 제출합니다.

2015.01.15.

주관연구기관명 : 한국철도기술연구원

주관연구책임자 : 신덕호 책임연구원

연구원 : 이재호 책임연구원

연구원 : 이강미 선임연구원

연구원 : 조현정 선임연구원

연구원 : 채은경 선임연구원

공동연구기관명 : 대아티아이(주)

공동연구책임자 : 안 진 전무

공동연구기관명 : (주)한터기술

공동연구책임자 : 차기호 전무

보고서 요약서

과제고유번호		해 당 단 계 연 구 기 간	기획연구	단 계 구 분	기획연구
연 구 사 업 명	국토교통연구기획사업				
연 구 과 제 명	최 상 위 과 제 명	신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획			
	단위과제명	주관연구	신호설비 공통 플랫폼 개발 전략수립 및 인증체계 수립 기획		
		공동연구	신호설비 공통 플랫폼 개발을 위한 동향분석 및 로드맵 수립		
		공동연구	신호설비 공통 플랫폼 수요조사 및 실용화 방안 수립		
연 구 책 임 자	신덕호 책임연구원	총연구기간 참 여 연구원수	총 : 20 명 내부 : 5 명 외부 : 15 명	총연구비	정부 : 80,000천원 기업 : 천원 계 : 80,000천원
연구기관명 및 소 속 부 서 명	한국철도기술연구원 철도안전인증센터		참여기업명	대아티아이(주), (주)한터기술	
국제공동연구	상대국명 : 해당 없음		상대국연구기관명 : 해당 없음		
요약(연구결과를 중심으로 개조식 500자 이내)				보고서면수	
철도신호설비의 핵심제어기를 조사 분석하여 공통 플랫폼 개발 및 표준화의 필요성을 시장 규모 및 실용화 효과분석을 통해 검토하고, 플랫폼 표준화의 대상, 구조 및 인터페이스에 적용해야 할 철도안전관련 국내법령, 운영건설기관 규정, 국제표준에 부합하는 인증체계 수립방안을 기획					
색 인 어 (각 5개 이상)	한 글	철도신호, 제어기, 안전필수, 표준화, 안전인증			
	영 어	Railway Signaling, Controller, Safety Critical, Standardization, Safety Certification			

요 약 문

○ 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립을 위해 공통 플랫폼 개발을 위한 기술키워드를 바탕으로 제2장에서 특허, 논문, 시장분석을 실시하였다.

○ 특허분석결과 한국의 경우 특허건수, 시장확보력, 인용도 등 기술영향력 등 대부분의 지수에서 선진국대비 크게 낮은 수준을 보이고 있어, 관련 분야 기술의 고도화가 시급히 요구되는 상황이며, 논문분석결과 1994년부터 현재까지 총 61건의 SCI 논문이 발표되고 있으며, 저널별로는 PROFESSIONAL ENGINEERING PUBLISHING, SAGE PUBLICATIONS LTD, PERGAMON-ELSEVIER SCIENCE LTD 등 유럽, 미국의 저널에서 많은 논문이 발표되고 있는 것으로 조사되었다. 또한, 시장분석결과 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획의 특허 출원/공개 및 논문 발표 추이를 통해 시장 발전단계 위치를 추정해 보면 현재 성장하고 있는 기술 분야로 조사되었다.

○ 3장과 4장의 기술동향조사는 신호설비 공통플랫폼 개발의 대상을 조사하기 위해 일반과 고속철도 주요 신호설비 18종에 대한 구성품을 조사하였으며, 조사결과 공통플랫폼이 적용 가능한 신호설비는 15종으로 주요신호설비의 83%가 적용대상이 될 수 있을 것으로 분석되었으며, 기능안전에 대한 국제표준인 IEC 61508의 SIL만족을 위한 요구사항분석과 철도시스템 RAMS에 대한 국제표준인 IEC 62278의 수명주기별 요구사항을 정리하였다.

○ 5장에서는 현재까지의 기획연구를 통해 다음의 3가지의 후보과제를 발굴하였다. 후보과제 1은 신호설비 공통플랫폼의 요구사항 도출과 개발단계의 국제표준기반 인증을 위한 활동을 수행한다. 후보과제 2와 3은 후보과제 1에서 도출한 요구사항을 바탕으로 결합허용 및 안전설계를 반영한 공통플랫폼을 개발하고, 국제표준기반의 안전인증 취득을 위한 RAMS 문서화를 핵심활동으로 한다. 후보과제 2는 전자연동장치, 차상신호장치 등 고성능 플랫폼을 개발하고, 후보과제 3은 자동폐색장치, 궤도회로 등 저비용 플랫폼을 개발한다. 32bit와 16bit는 프로세서의 데이터 버스 사이즈를 기준으로 한다.

SUMMARY

○ To develop signaling equipment common platform and to establish a railway signaling system certification scheme, the analysis on patents, papers and markets was implemented in the chapter 2 on the basis of technical keyword to develop the common platform.

○ As a result of analysis on the patent, in case of the Republic of Korea, in most of the indices such as the number of patents, power to secure markets, degree of citation and technology impact, etc., it is in a situation where enhancement of technology in the related fields is urgently required since they are in the greatly lower level in comparison with those for developed countries. As a result of analysis on the paper, total of 61 SCI papers had been published from 1994 until now, and by journal, it was investigated that many papers were published in the European and American journals such as the PROFESSIONAL ENGINEERING PUBLISHING, SAGE PUBLICATIONS LTD, PERGAMON-ELSEVIER SCIENCE LTD, etc. In addition, as a result of analysis on the market, when estimating a position of market development stage through the trend of application for patent/disclosure and publication of papers concerning development of the platform common to the signal equipment and the planning on the plan to establish certification systems for railway signal system, it was investigated that they are in the technical fields being grown now.

○ Survey on technology trends in chapters 3 and 4 was for the survey on components for 18 kinds of main signal equipment for general and high-speed railways to investigate targets for development of platform common to the signal equipment. As a result of survey, signal equipment to which the common platform is applicable was 15 kinds, and it was analyzed that 83% of the main signal equipment can be the applicable targets, and the analysis on requirements to satisfy the SIL of IEC 61508 which is the international standard for functional safety and the requirements by life cycle stated in the IEC 62278 which is the international standard for RAMS of railway system

were organized.

○ In chapter 5, the following three candidate tasks were discovered through planning and study up to now. Candidate task 1 draws requirements for platform common to the signal equipment and performs activities for certification based on the international standard in the development stage. Candidate tasks 2 and 3 develop a common platform which reflects fault tolerance and safe design on the basis of requirements drawn from the candidate task 1, and make RAMS documentation to acquire safety certification as their core activities based on the international standard. Candidate task 2 develops high performance platforms such as the electronic interlocking devices and on-board signal equipment, etc. And candidate task 3 develops low cost platforms such as automatic blocking devices and track circuit, etc. 32bit and 16bit is based on the data bus size of processor.

신호설비 공통 플랫폼 개발 및 철도신호시스템 인증 체계 수립 방안 기획

□ 연구목적

- 철도신호설비의 핵심제어기를 조사 분석하여 공통 플랫폼 개발 및 표준화의 필요성을 시장규모 및 실용화 효과분석을 통해 검토하고, 플랫폼 표준화의 대상, 구조 및 인터페이스에 적용해야 할 철도안전관련 국내법령, 운영건설기관 규정, 국제표준에 부합하는 인증체계 수립방안을 기획

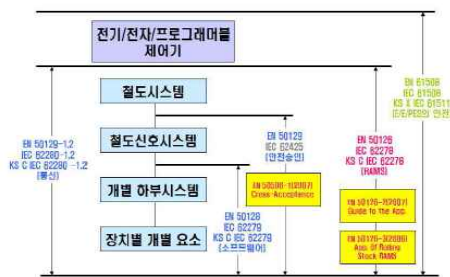
□ 연구개요

- 연구기간 : 8개월
- 총연구비 : 80백만원(정부 80백만원)
- 주요 연구내용

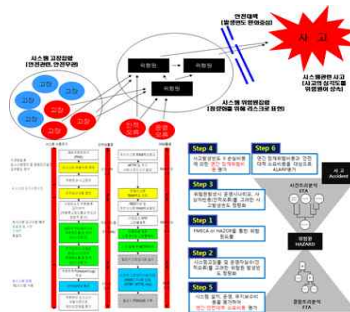
세부 과제	주요 연구내용
‘신호설비 공통플랫폼 개발 및 철도신호시스템 인증체계 수립방안’의 기획	• 신호설비 공통플랫폼 개발 및 검증을 위한 핵심기술 정의 - 국제규격에 부합하기 위한 요구조건 분석 및 인증수준(SIL인증 등) 제시 - 기술개발 추진방법 및 사양 도출 - 검증 방안 및 검증결과의 신뢰성 확보 방안 마련 - 검증에 필요한 구축장비 수요조사 - 경제적 효과 및 적용범위 분석 • 철도신호시스템 안전성 인증 체계 수립 - 관련 국제규격 및 해외 사례 조사 - 국제규격에 부합하기 위한 요구조건 분석 - 인증절차, 인증기관 지정 등 인증기반 및 대내외적 공신력 확보 방안 제시

※ 신호설비 공통플랫폼 개념

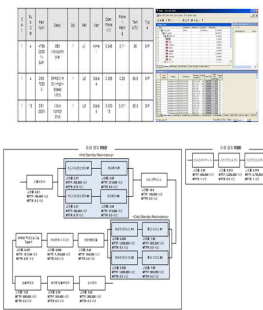
- 철도신호시스템의 국제시장 규모는 20조원/년('14년 기준)이며, 국내 시장 규모는 850억원/년 (한국철도시설공단 신호분야 자재비용 최근 5년 평균), '02년 철도시스템의 안전표준이 제정됨에 따라 국내외 신호설비의 코어제어기의 외산잠식이 빠르게 진행되고 있으며, 국외전문기관 중심의 안전인증 시장 형성(71억원/년)
- 철도신호설비에 공통 적용되는 내장형제어기 기반의 플랫폼을 공통적용이 가능하도록 개발하고 관련 국제표준에 따라 안전인증을 취득하여 제작사별 중복투자 최소화는 물론 우리 철도신호산업의 대내외 경쟁력 향상필요



[철도 RAMS관련 국제표준현황]



[IEC 62278 수명주기별 요구사항]

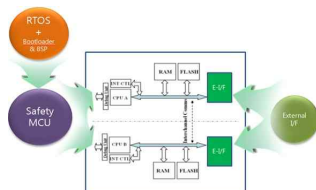


[플랫폼 고장률 정량화]

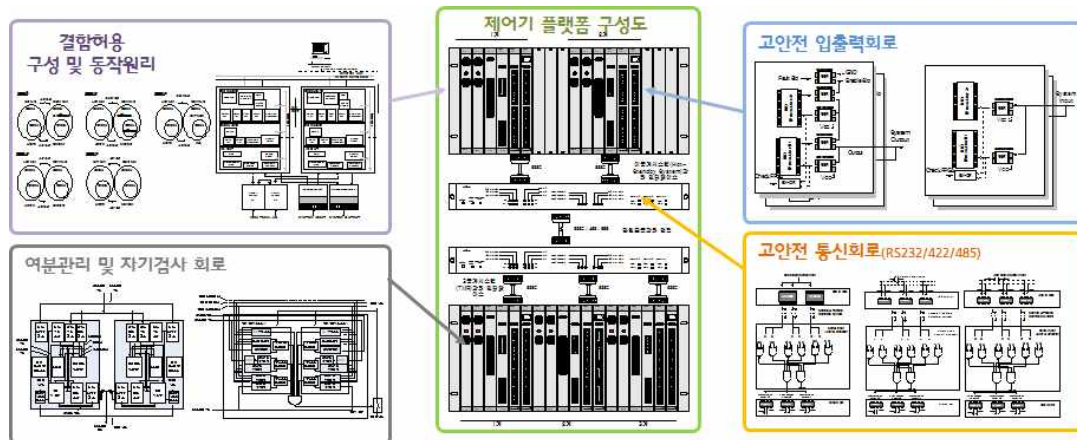
- 철도안전 국제표준 기반 안전인증이 확보된 최신 신호설비 플랫폼 동향을 독일과 미국의 사례를 분석하여 우리나라의 공통플랫폼 연구개발 방향을 정립



[기존 신호시스템의 플랫폼 예]



[안전인증을 취득한 외산 공통플랫폼]



[신호설비 공통 플랫폼과 적용 안전기술의 개념도]

- 안전인증 취득을 위해 필요한 관련 국제표준(IEC 62278)의 수명주기별 요구사항을 분석하여 공통플랫폼의 인증취득을 위한 기반조성
- 신호설비의 인증체계 수립과 관련하여 국내에서 활동하는 국외전문기관의 현황과 인증서발행의 근거를 조사하였으며, 이를 바탕으로 우리나라 철도신호설비의 자체 인증을 위해 필요한 인정 및 인증제도 제시



[제품인증관련 국제표준 현황]

	Lloyd's Register Lloyd's Register Asia	TUV Rheinland TUV Rheinland	TUV SUD TUV SUD	DNV-GL DNV GL
ISA인증 발행근거	ISO 17020 ISO 17065(영국) (IEC 62278, IEC 62279 IEC 62425, IEC 62280)	ISO 17020 ISO 17025 ISO 17065(독일) (IEC 62278, IEC 62279 IEC 62425, IEC 62280)	ISO 17020 ISO 17025 ISO 17065(독일) (IEC 62278, IEC 62279 IEC 62425, IEC 62280)	ISO 17020 ISO 17025 ISO 17065(중국)

[국내활동 중인 국외전문기관 현황]

□ 연구 필요성

- 바이탈 정보를 처리할 수 있는 SIL인증 공통플랫폼은 현재 외산만 존재하며 국내 Safety Critical System에 적용되어 막대한 비용으로 국내자본의 해외유출, 기술지원의 어려움으로 인한 운영효율성 저감 및 호환성 미흡 등 다양한 문제가 발생되고 있음
- 국내의 기술과 인력으로 SIL인증된 처리장치가 개발된다면 위와 같은 문제점은 해결될 수 있으며, 더불어 해외수출의 기반을 마련할 수 있을 것으로 전망됨

- Safety Critical System에 국내에서 개발된 SIL인증 공통플랫폼이 적용된 사례는 전무한 실정이며, 철도분야의 해외 메이저급 철도신호제어시스템 공급사는 SIL인증을 받은 제품과 그 제품의 바이탈 정보 처리를 위한 핵심장치 또한 SIL인증된 모듈을 탑재하여 국내에 공급하고 있음
- 본 연구과제에서는 철도분야의 Safety Critical System에 적용할 수 있는 공통플랫폼을 개발하여, 국내 공급사에 대한 안정적 공급은 물론 해외 프로젝트에 적용할 수 있는 기반 마련이 기대됨
- 경제적인 면에서의 단편적인 예를 들면, 현재 국내 일반철도의 전자연동장치의 수는 545개로 철도안전법에 따라 SIL인증 전자연동장치로 전면 교체하게 되므로 이를 비용으로 비교하게 되면 외산보드를 적용하는 경우에 비해 403억 원을 절감할 수 있음
- 또한 도시철도 열차제어시스템(ATP/ATO시스템)의 1개 구간을 사례로 들었을 경우, 외산 시스템에 비해 53억 원을 절감할 수 있고, 국내 도시철도 5개소에 적용될 경우, 약 265억 원의 경제적 효과를 볼 수 있음
- 따라서, 국내 철도신호산업의 보호와 해외진출을 위한 공통플랫폼의 개발과 안전인증 취득을 위한 핵심 요구사항의 정리를 통해 중소기업 위주의 국내 철도신호산업의 국제화를 위한 기반구축을 위해 연구개발의 조속한 실행 필요

□ 정부 지원 타당성

- 국내 교통안전공단 보고서인 ‘2011년 철도사고분석’에 따르면 일반 및 도시철도 열차 사고와 장애원인분석 결과, 아래와 같이 차량과 시설에서 일반철도 84%, 도시철도 74%의 높은 장애발생률이 보고됨

일반철도 사고 및 장애 구분	건수	비율(%)
차량요인(부품 및 정비불량 등 차량결함)	122	68.2
인적요인(규정위반, 취급오류등 인적결함)	11	6.1
시설요인(신호, 전철분야 등의 시설결함)	29	16.2
외적요인(자살, 선로무단통행 등 외적요인)	16	8.9
기타	1	0.5
합계	179	100

도시철도 사고 및 장애 구분	건수	비율(%)
차량요인(부품 및 정비불량 등 차량결함)	25	43.9
인적요인(규정위반, 취급오류등 인적결함)	4	7.0
시설요인(신호, 전철분야 등의 시설결함)	18	31.6
외적요인(자살, 선로무단통행 등 외적요인)	8	14.0
기타	1	3.5
합계	57	100

- 위 분석결과와 같이 철도사고 및 장애는 단 한 번의 발생으로 대규모 인명피해와 복구 및 지연 등으로 인한 경제적 피해를 동반하는 위험원임
- 특히 철도의 고속화와 고밀도화를 위해서는 이러한 결함을 제거하거나 상쇄시키는 제품 안전성 확보가 전제되어야 하며, 유럽 등 선진철도에서는 철도신호시스템 및 장치의 안전성을 확보하기 위해 다각적인 노력을 기울여 왔으며, 이에 따라 국제표준을 제정하여 적용하고 있음
- 국내에서도 열차사고 제로화를 위해 정부에서도 지속적으로 철도의 기술개발과 발전을 위한 지원으로 상당 부분 국산화가 이루어져 그 비율을 높이고 있지만 국산화 된 국내 철도기술의 해외진출을 위해서는 바이탈 공통 플랫폼 및 Safety Critical System의 안전성 확보가 필요하며, 이를 위해 정부 주도의 안전기술의 독립과 해외 수출의 기반마련 차원에서 적극적인 지원이 반드시 필요함

□ 기술개발 실용화(또는 적용) 방안

- 철도안전법 시행으로 철도신호의 주요장치는 반드시 안전성을 확보하여야 하며 이를 위해 형식승인 및 제작자승인을 수행해야 함. 신호통신분야의 경우 총 55개 품목 중 50%이상이 공통플랫폼 적용대상이며, 구체적 적용대상은 다음과 같음

대분류	소분류(지상설비 기준)	공통플랫폼 적용대상
일반철도(9종)	전자연동장치(EIS형, Relayless형)	○
	신호기장치(LED형)	-
	선로전환기(NS, NS-AM, MJ81)	-
	궤도회로장치(임펄스, TI21형, AF-ATC형)	○
	자동폐색장치(ABS)	○
	전원공급장치(일체)	○
	건널목보안장치(지장물, 출구측포함)	○
	열차자동정지장치(ATS)	-
	열차자동방호장치(ATP)	○
고속철도(8종)	전자연동장치(SS형)	○
	정보처리장치(FEPOL)	○
	선로변환기능모듈(TFM)	○
	열차자동제어장치(ATC)	○
	궤도회로장치(UM71C형)	○
	선로전환기장치(MJ81, 하이드로스타형)	○
	전원공급장치	○
	안전설비(HBD, 끌림검지장치, 지진감시장치, 선로침입검지장치 등)	○
공통사항	열차집중제어장치(CTC)	○

- 향후 공통플랫폼 개발성과는 위 철도신호 장치를 대상으로 적용이 예상되며, 효과적인 성과확산을 위해 국내 철도신호공급사에 대한 기술 및 인증에 대한 체계적 지원이 요구됨

분류	세부 내용
공통플랫폼 공급	• 공통플랫폼 공급 • I/O보드 공급 • 관련 장치 및 자재 공급
SIL인증 및 기술 지원	• 공통플랫폼 세팅 기술지원 • 어플리케이션 기술지원 • 유지보수 및 확장 지원 • SIL인증 프로세스 및 문서화지원

□ 기대 효과 (본사업 추진 시)

- 철도산업 세계시장은 2010년 1,310억 유로에서 2015년에는 1,600억 유로 수준으로 증가할 것으로 예측되며, 2015년까지 약 4.1%의 연평균 증가율로 증가할 것으로 예측되고 있음. 도심지의 경우 다양한 종류의 경전철 시스템(모노레일, 노면전차, 자기부상열차 등)의 도입이 검토되고 있으며, 경전철 시스템의 특성에 따른 전력, 통신, 제어, 관제기술 개발이 절실히 요구되고 있음

- 오른쪽 그림과 같이 세계철도시장의 성장률 가운데 열차제어(Rail Control)는 6.8%의 높은 성장세 임



<출처 : 국토교통R&D 동향조사_2013>

- SIL인증을 취득한 공통 플랫폼의 경제적 효과는 외산 처리장치 도입 비용 대비 절감 효과로 표현할 수 있으며, 개발되는 범용 처리장치 1set의 예상 공급비용은 약 2천만원으로 외산 처리장치 1set당 5천7백만 원 대비 35%에 해당하여 1set당 약 2천7백만원 가량을 절감예상

- 현재 국내 SIL인증된 연동장치는 전무한 상태이며 추후 공통플랫폼을 전자연동장치에 적용할 경우 적용대상은 아래의 표와 같이 총 545개 예상

기계 연동장치	집중 연동장치	전기 연동장치	전자 연동장치	총 합계
2	30	110	398	545

- 또한, 국내 공급되는 도시철도 열차제어시스템 외산시스템의 실제 공급수량을 고려할 경우 공급되는 핵심 처리장치의 수는 약 290개이며, 이에 따른 비용을 계산한 결과 아래와 같이 추정됨

[단위: 천원]

분류(국내)	설명	외산모듈 적용 Case	공통플랫폼 적용 Case	차액
연동장치(545개)	전체 개량/교체	62,130,000	21,800,000	40,330,000
도시철도 핵심장치 (외산Thales사례)	차상제어장치(37편성, 전후방)	4,218,000	1,480,000	2,738,000
	지상현장제어장치(14개소, 이중계)	1,596,000	560,000	1,036,000
	지상중앙제어장치(1개소, 이중계)	114,000	40,000	74,000
	스크린도어제어장치(20개소, 이중계)	2,280,000	800,000	1,480,000
	소 계	8,208,000	2,880,000	5,328,000
총 계		70,338,000	24,680,000	45,658,000

※핵심모듈 적용단가, 외산 1식(57,000천원), 개발품 1식(20,000천원)

- 위와 같이 철도신호제어시스템 중 전자연동장치의 범용 처리장치를 국산화 할 경우 절감할 수 있는 비용은 403억 원으로 경제적 효과는 매우 높으며, 이를 국내 다수의 도시철도 구간과 신설/개량되는 일반철도를 고려할 경우 그 절감효과는 약 1000억원(1개 도시 철도 절감효과 : 53억 원)으로 기대됨
- 따라서, 위 철도분야의 일부분에 적용된 분석결과를 철도 및 산업전반으로 확대하여 해석하는 경우 수천억원의 경제적 효과를 가져 올 것으로 판단되며, 이를 기반으로 해외 메이저 공급업체와의 가격경쟁력 확보는 물론 해외 진출 기회의 확대가 기대됨

목 차

제 1 장 기획연구의 필요성	1
제 1 절 기획연구의 범위	1
제 2 절 과제추진 배경 및 필요성	8
제 2 장 특허, 논문, 시장분석 보고서	14
제 1 절 분석개요	14
제 2 절 특허분석	17
제 3 절 논문분석	32
제 4 절 시장분석	35
제 5 절 특허, 논문, 시장분석 결론	48
제 3 장 신호설비 현황분석	51
제 1 절 주요 신호설비 현황분석	51
제 2 절 주요 신호설비 현황분석 결과	72
제 4 장 신호설비 안전인증 체계	75
제 1 절 안전인증 체계 조사분석	75
제 2 절 IEC 61508의 SIL별 요구사항 분석	79
제 3 절 IEC 62278의 수명주기 단계별 요구사항 분석	114
제 5 장 연구개발과제 구성 및 추진전략	137
제 1 절 비전 및 목표	137
제 2 절 핵심기술요소 선정 및 TRL목표	139
제 3 절 연구개발과제 구성	142
제 4 절 세부과제 주요내용 및 추진전략	146
제 5 절 과제별, 연차별 기술로드맵 및 성과로드맵	148
제 6 절 성과활용 방안	151
제 7 절 연구수행 체계	156

제 6 장 과제 제안요구서 157

제 1 절 과제 제안요구서 157

제 2 절 평가기준 설정 161

제 1 장 기획연구의 필요성

제 1 절 기획연구의 범위

본 기획연구는 공고된 「신호설비 공통 플랫폼 개발 및 철도신호시스템 인증 체계 수립 방안 기획」의 연구기획 범위를 준수하여 다음과 같이 시행한다.

1. 신호설비 플랫폼 표준화 및 검증을 위한 핵심기술 정의

가. 국제규격에 부합하기 위한 요구조건 분석 및 인증수준(SIL 인증 등) 제시

- 신호설비 플랫폼은 내장형제어기로 구성된 하드웨어와 운영체제 및 응용프로그램으로 구성된 소프트웨어가 결합하여 장치에 요구된 사양을 수행하는 신호설비의 핵심 구성품으로써 일반적인 구성은 다음 그림과 같다.

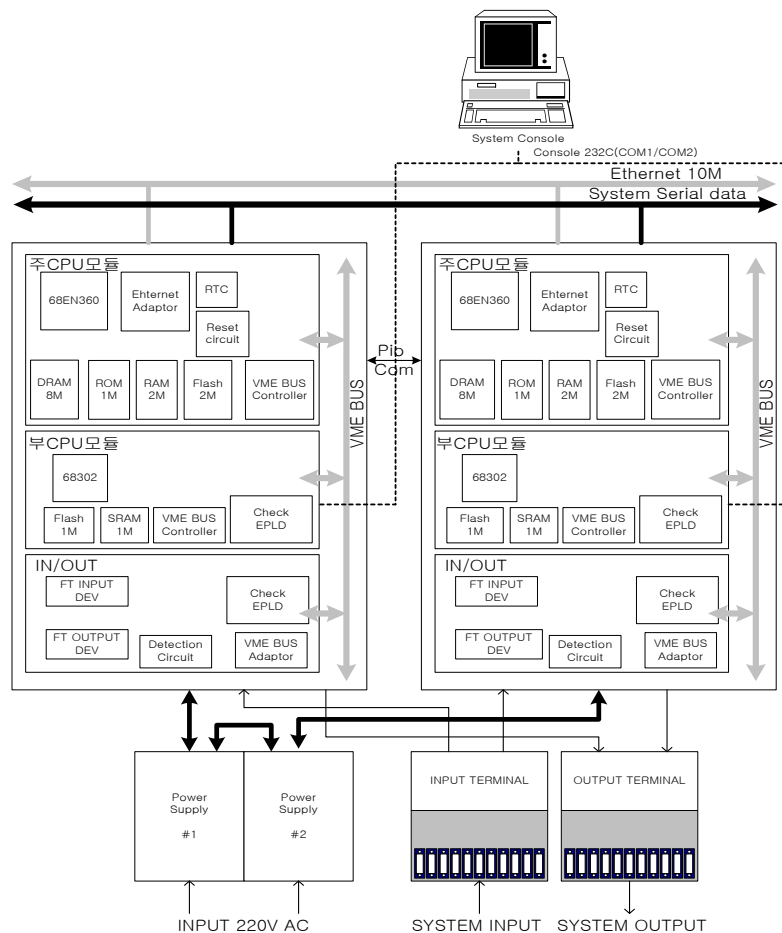


그림 1-1. 신호설비 플랫폼의 기본구성 및 외형

- 안전필수(Safety Critical)분야에 속하는 철도신호설비는 다음과 같은 국제규격을 적용하여 설계, 제작, 시험, 운영, 유지보수를 실행해야 하므로 일반적인 상용 내장형제어기 플랫폼의 적용이 어려우며, 개발제품뿐 아니라 개발과정에서 단계별 검증을 통해 안전이 검증되어야 한다.

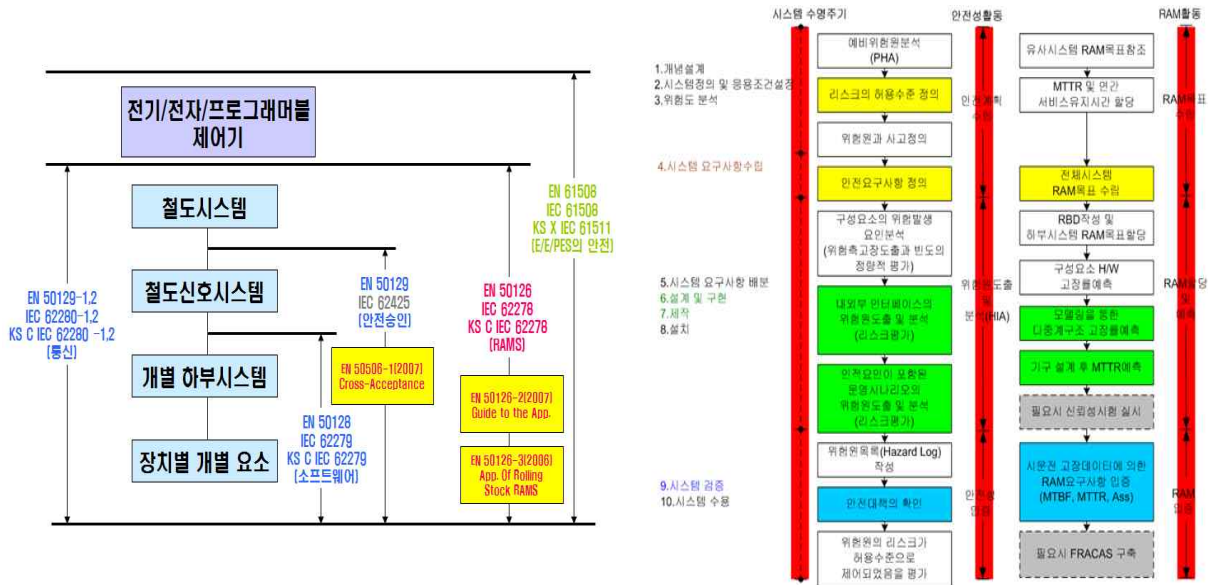


그림1-2. 신호설비 관련 국제표준과 수명주기별 검증활동 요약

- 따라서, 신호설비 공통플랫폼 개발 및 검증을 위한 핵심기술의 정의를 위해서는 공통화가 가능한 플랫폼의 범위와 기능을 정의하고, 국제표준에서 요구하는 수명주기별 검증활동을 반영하여 표준플랫폼의 설계 및 제작요건을 제시한다.
- 향후 다양한 응용환경에서 사용할 수 있는 개발환경의 제공과 함께 응용프로그램을 제외한 운영체제와 디바이스 드라이버에 대한 검증방안도 제시되어야 한다.

나. 기술개발 추진방법 및 사양 도출

- 신호설비 표준플랫폼은 신호설비 제어기 현황의 분석을 통해 궤도회로, 지상신호장치 구성유니트(예, ATP의 선로변제어기)와 같이 상대적으로 단순한 기능을 수행하는 중저성능 표준플랫폼(16bit급)과, 연동장치 및 차상신호제어기와 같이 상대적으로 복잡한 기능을 수행하는 고성능 표준플랫폼(32bit급, 상용 운영체제 포팅)이 요구될 수 있으며, 운영환경 및 수요에 따라 목표성능을 설정하고 입출력 기능분성을 통해 위험도에 따른 SIL할당과 세부사양을 기획한다.

- 또한, 표준플랫폼의 산업계 활성화를 위해 설비의 소형화, 에너지 효율, 디자인 등도 고려되어야 하며, 가장 중요한 구현에 소요되는 비용(가격)목표를 정량적으로 수립하여 설계 단계부터 부품선택과 양산의 용이성 등도 검토한다.

다. 검증 방안 및 검증결과의 신뢰성 확보 방안 마련

- 신호설비 플랫폼의 표준화를 위해서는 기능적 측면 뿐 아니라 국제규격의 수명주기별 요건을 만족해야 한다. 따라서 신호설비 플랫폼의 적용대상이 될 수 있는 신호설비의 예비위험원분석(PHA)을 기획단계에서 수행하여 표준 플랫폼의 성능별 안전입출력의 적정 포트 수, 인터페이스 방법에 대하여 검토한다.
- 또한, 검증 방안 및 검증결과의 신뢰성 확보를 위해 해당 표준의 요구사항을 만족하기 위한 신호설비 검증 문서목록을 다음과 같이 제시하고 적용 국제표준의 항목을 정리하여 체크리스트를 생성한다.

표1-1. 검증을 위한 문서목록의 예, 경부양방향 ATP구축사업 산출물

순번	문서명	주요평가항목
1	RAMS 관리계획서	IEC62278기준 수명주기 RAMS 관리계획 시스템 및 SW V&V계획, FRCAS포함 RAM 입증계획
2	PHA 보고서	철도사고관련 프로젝트 위험원 도출
3	SW 품질보증계획서	IEC62279기준 소프트웨어 안전보증계획
4	SW 요구사항서	SW 요구사항(RFP의 소프트웨어 관련 기능명세) SW 응용 요구사항
5	SW 요구사항 시험사항서	SW 요구사항별 시험계획
6	SW 요구사항 확인보고서	초기설계 단계의 SW 요구사항 확인 결과
7	SW 데이터준비 및 시험계획서	텔레그램 생성까지의 데이터준비 및 시험계획 발리스별 텔레그램 검증 계획
8	SW 데이터 시험보고서	설치, 시험, 시운전의 소프트웨어 요구사항 확인결과 텔레그램 무결성 시험 및 입증자료
9	RAM 분석보고서	시스템 정량적 RAM분석
10	SSHA 보고서	하부장치 위험원도출 및 위험도제어
11	IHA 보고서	인터페이스 위험원도출 및 위험도제어
12	O&SHA 보고서	운영 및 유지보수 위험원도출 및 위험도제어
13	V&V 보고서	RAM 및 안전대책의 확인 및 검증
14	SW 보증보고서	IEC62279기준 소프트웨어 안전보증 SW 관련 SRAC의 종결상태
15	SW 유지보수계획서	안전유지를 위한 사용자요구사항 및 교육자료
16	Safety Case	IEC62425기준 상세적용 안전활동보고서 Hazard Log 포함

표1-2. 검증결과와 신뢰성확보를 위한 체크리스트의 예, 경부고속선 SSI국산화 사업

 한국철도기술연구원 정보통신연구실 http://www.krii.co.kr Doc ID KH060505DK11076601v01	 한국철도기술연구원 정보통신연구실 http://www.krii.co.kr Doc ID KH060505DK11076601v01																						
나. 부속록자 3.6의 세부별가검 본 절에서는 데이터 작성 및 시험 계획을 제시한다. 본 절과 관련하여 IEC 62279의 요구사항 표10을 만족해야 한다.	<table border="1"> <tr> <td>17.4.2.5</td><td>요건 데이터와 관련된 문서는 반드시 본 표준규격의 15항의 설명과 요구사항을 만족해야 한다. 설명과 요구사항은 반드시 데이터 설정을 위해 사용된 상용소프트웨어의 버전리스트와 데이터 기록 절차에서 사용된 도구를 변인을 기록해야 한다.</td></tr> <tr> <td>17.4.3</td><td>응용데이터에 의한 시스템설정에 사용된 상용소프트웨어의 개발은 반드시 본 규격의 14항 16 조항까지의 요구사항을 모두 만족해야 한다. 또한 다음의 추가적인 요구사항에 대해서도 고려되어야 한다.</td></tr> <tr> <td>17.4.3.1</td><td>소프트웨어 요구사항 단계에서 각각의 시스템과 서브시스템에 대한 응용데이터를 사용한 기능은 반드시 명확히 되어야 한다. 시스템 안전유형설 계별은 각각의 서브시스템에 할당되어 시스템의 모든 설계에 대한 연속된 개발에 대한 적용기준을 결정한다.</td></tr> <tr> <td>17.4.3.2</td><td>상용 소프트웨어와 응용데이터와의 인터페이스를 설계하는 소프트웨어 설계 단계에서 인터페이스에 대한 내용은 요구사항의 결과와 응용분야에 정의된 언어에 사용되는 경우와 같이 수행자의 이관단계에서 사전에 정의된 경우를 제외하면 반드시 명확하게 기술되어야 한다.</td></tr> <tr> <td>17.4.3.3</td><td>소프트웨어 모듈 설계 단계에서 프로그램 코드와 데이터의 명확한 분리는 반드시 이루어져야 한다. 즉, 데이터와 인터페이스가 일반소프트웨어 또는 데이터가 다른 코드의 인터페이스가 필요 없이 소프트웨어와 데이터의 인터페이스 정의에 변화할 수 주지 않아야 한다. 마찬가지로 응용분야 데이터는 다른 데이터로부터 분리되어야 한다.</td></tr> <tr> <td>17.4.3.4</td><td>소프트웨어 유지보수 단계에서 변경관리절차는 어떠한 상용소프트웨어의 수정도 소프트웨어 수정에 대한 문서화가 충분히 존재, 설명되거나 필요한 경우에만 데이터가 변경하는 것을 분명히 하여 한다.</td></tr> <tr> <td>17.4.3.5</td><td>요건 관련 데이터의 조정에 대한 조사를 위한 소프트웨어 확인과정과 소프트웨어 검증단계에서 검증을 수행해야 한다.</td></tr> <tr> <td>17.4.3.6</td><td>상용소프트웨어는 사용자 설정데이터의 충돌을 방지할 수 있도록 설계되어야 한다.</td></tr> </table>	17.4.2.5	요건 데이터와 관련된 문서는 반드시 본 표준규격의 15항의 설명과 요구사항을 만족해야 한다. 설명과 요구사항은 반드시 데이터 설정을 위해 사용된 상용소프트웨어의 버전리스트와 데이터 기록 절차에서 사용된 도구를 변인을 기록해야 한다.	17.4.3	응용데이터에 의한 시스템설정에 사용된 상용소프트웨어의 개발은 반드시 본 규격의 14항 16 조항까지의 요구사항을 모두 만족해야 한다. 또한 다음의 추가적인 요구사항에 대해서도 고려되어야 한다.	17.4.3.1	소프트웨어 요구사항 단계에서 각각의 시스템과 서브시스템에 대한 응용데이터를 사용한 기능은 반드시 명확히 되어야 한다. 시스템 안전유형설 계별은 각각의 서브시스템에 할당되어 시스템의 모든 설계에 대한 연속된 개발에 대한 적용기준을 결정한다.	17.4.3.2	상용 소프트웨어와 응용데이터와의 인터페이스를 설계하는 소프트웨어 설계 단계에서 인터페이스에 대한 내용은 요구사항의 결과와 응용분야에 정의된 언어에 사용되는 경우와 같이 수행자의 이관단계에서 사전에 정의된 경우를 제외하면 반드시 명확하게 기술되어야 한다.	17.4.3.3	소프트웨어 모듈 설계 단계에서 프로그램 코드와 데이터의 명확한 분리는 반드시 이루어져야 한다. 즉, 데이터와 인터페이스가 일반소프트웨어 또는 데이터가 다른 코드의 인터페이스가 필요 없이 소프트웨어와 데이터의 인터페이스 정의에 변화할 수 주지 않아야 한다. 마찬가지로 응용분야 데이터는 다른 데이터로부터 분리되어야 한다.	17.4.3.4	소프트웨어 유지보수 단계에서 변경관리절차는 어떠한 상용소프트웨어의 수정도 소프트웨어 수정에 대한 문서화가 충분히 존재, 설명되거나 필요한 경우에만 데이터가 변경하는 것을 분명히 하여 한다.	17.4.3.5	요건 관련 데이터의 조정에 대한 조사를 위한 소프트웨어 확인과정과 소프트웨어 검증단계에서 검증을 수행해야 한다.	17.4.3.6	상용소프트웨어는 사용자 설정데이터의 충돌을 방지할 수 있도록 설계되어야 한다.						
17.4.2.5	요건 데이터와 관련된 문서는 반드시 본 표준규격의 15항의 설명과 요구사항을 만족해야 한다. 설명과 요구사항은 반드시 데이터 설정을 위해 사용된 상용소프트웨어의 버전리스트와 데이터 기록 절차에서 사용된 도구를 변인을 기록해야 한다.																						
17.4.3	응용데이터에 의한 시스템설정에 사용된 상용소프트웨어의 개발은 반드시 본 규격의 14항 16 조항까지의 요구사항을 모두 만족해야 한다. 또한 다음의 추가적인 요구사항에 대해서도 고려되어야 한다.																						
17.4.3.1	소프트웨어 요구사항 단계에서 각각의 시스템과 서브시스템에 대한 응용데이터를 사용한 기능은 반드시 명확히 되어야 한다. 시스템 안전유형설 계별은 각각의 서브시스템에 할당되어 시스템의 모든 설계에 대한 연속된 개발에 대한 적용기준을 결정한다.																						
17.4.3.2	상용 소프트웨어와 응용데이터와의 인터페이스를 설계하는 소프트웨어 설계 단계에서 인터페이스에 대한 내용은 요구사항의 결과와 응용분야에 정의된 언어에 사용되는 경우와 같이 수행자의 이관단계에서 사전에 정의된 경우를 제외하면 반드시 명확하게 기술되어야 한다.																						
17.4.3.3	소프트웨어 모듈 설계 단계에서 프로그램 코드와 데이터의 명확한 분리는 반드시 이루어져야 한다. 즉, 데이터와 인터페이스가 일반소프트웨어 또는 데이터가 다른 코드의 인터페이스가 필요 없이 소프트웨어와 데이터의 인터페이스 정의에 변화할 수 주지 않아야 한다. 마찬가지로 응용분야 데이터는 다른 데이터로부터 분리되어야 한다.																						
17.4.3.4	소프트웨어 유지보수 단계에서 변경관리절차는 어떠한 상용소프트웨어의 수정도 소프트웨어 수정에 대한 문서화가 충분히 존재, 설명되거나 필요한 경우에만 데이터가 변경하는 것을 분명히 하여 한다.																						
17.4.3.5	요건 관련 데이터의 조정에 대한 조사를 위한 소프트웨어 확인과정과 소프트웨어 검증단계에서 검증을 수행해야 한다.																						
17.4.3.6	상용소프트웨어는 사용자 설정데이터의 충돌을 방지할 수 있도록 설계되어야 한다.																						
표10. 데이터 작성 및 시험 계획 관련 IEC 62279의 요구사항 <table border="1"> <thead> <tr> <th>Code</th><th>Requirement</th></tr> </thead> <tbody> <tr> <td>17.4.1.3</td><td>데이터 작성 데이터의 작성절차는 상세한 정보영역(예를 들어 테이블), 데이터 코드코드의 생성, 이 코드들의 링크 및, 검사 그리고 다른 확인절차와 응용데이터의 시험을 반드시 포함해야 한다.</td></tr> <tr> <td>17.4.1.4</td><td>통일과 적용 모든 시스템의 응용데이터는 일반적인 하드웨어, 소프트웨어와 함께 통합설계 이전에 공칭시험 단계에서 통합된다. 이러한 경우에는 다른 요건들에 의해 충분한 수준의 신뢰가 요구된다. 설계는 통합설계 이전에 새로운 설계가 추가되면 반드시 통합시험을 실시해야 한다. 마지막으로 시스템은 최종 설계시에 시스템 전체기능에 대한 시험과 최종 적용절차를 반드시 수행해야 한다.</td></tr> <tr> <td>17.4.1.5</td><td>검증과 평가 검증과 평가절차는 반드시 시스템 설계단계에서 각각의 단계의 성능에 대하여 수행되어야 한다.</td></tr> <tr> <td>17.4.2</td><td>데이터 작성절차와 도구들 각각의 새로운 설계 시스템의 응용데이터, 상세데이터 작성절차 및 도구에 의한 설명은 반드시 17.4.1에서 설명한 데이터작성 수행자에게 부여되어 새로운 시스템 설계에 적합하도록 개발되어야 한다. 이러한 절차와 도구의 개발은 반드시 본 규격의 시스템의 일반적인 소프트웨어 하드웨어의 개발성과 일치해야 한다. 확인, 검증 그리고 평가절차는 반드시 데이터 작성절차와 일반적인 소프트웨어에 대하여 호환성을 가져야 한다.</td></tr> <tr> <td>17.4.2.1</td><td>시스템 소프트웨어 설계단계는 응용데이터에 의해 설계되고, 데이터 작성계획서는 데이터 작성과정의 문서구조에 대한 정의에 의해 생성되어야 한다. 이러한 문서는 반드시 17.4.1에 포함된 데이터 작성 수행주기 요건을 준수해야 한다. 데이터 작성계획서는 반드시 데이터 작성절차와 도구에 대한 상세한 설명을 시스템 안전유형설 계별에서 요구된 수준을 만족하도록 수행해야 하며, 확인, 검증 그리고 설계 직전에 상세한 관리절차를 포함하여 모든 소프트웨어를 포함한 기록해야 한다.</td></tr> <tr> <td>17.4.2.2</td><td>데이터 작성계획서는 반드시 데이터 작성 수행주기에서 사용되는 모든 하드웨어 또는 소프트웨어 도구에 대한 안전유형설 계별을 포함해야 한다. 데이터 안전유형설 계별은 반드시 시스템 안전유형설 계별로부터 유도되어야 하며, 각각의 도구에 의한 결과는 다른 매뉴얼 또는 자동화된 절차에 의해 확인되어야 한다.</td></tr> <tr> <td>17.4.2.3</td><td>가능한 데이터 작성 계획은 반드시 작성에 사용되는 표기에 대한 요구사항을 명확히 하고, 표준화된 신 호체계와 데이터타입과 같이 응용분야 전지니언어에 친숙하게 설계해야 한다. 새로운 표기법을 사용하는 경우 그 표기법 사용의 적합성에 대한 문서화해야 한다.</td></tr> <tr> <td>17.4.2.4</td><td>확인, 시험, 검증 그리고 평가 보고서는 각각의 설계에 대한 문서화에서 최소한의 체크리스트 형태로 표준화된 작성계획과 동일함을 입증해야 한다. 이러한 정보는 반드시 각각의 데이터 시험 계획을 포함해야 하고, 그 결과는 반드시 데이터 시험 보고서에 기록되어야 한다.</td></tr> </tbody> </table>	Code	Requirement	17.4.1.3	데이터 작성 데이터의 작성절차는 상세한 정보영역(예를 들어 테이블), 데이터 코드코드의 생성, 이 코드들의 링크 및, 검사 그리고 다른 확인절차와 응용데이터의 시험을 반드시 포함해야 한다.	17.4.1.4	통일과 적용 모든 시스템의 응용데이터는 일반적인 하드웨어, 소프트웨어와 함께 통합설계 이전에 공칭시험 단계에서 통합된다. 이러한 경우에는 다른 요건들에 의해 충분한 수준의 신뢰가 요구된다. 설계는 통합설계 이전에 새로운 설계가 추가되면 반드시 통합시험을 실시해야 한다. 마지막으로 시스템은 최종 설계시에 시스템 전체기능에 대한 시험과 최종 적용절차를 반드시 수행해야 한다.	17.4.1.5	검증과 평가 검증과 평가절차는 반드시 시스템 설계단계에서 각각의 단계의 성능에 대하여 수행되어야 한다.	17.4.2	데이터 작성절차와 도구들 각각의 새로운 설계 시스템의 응용데이터, 상세데이터 작성절차 및 도구에 의한 설명은 반드시 17.4.1에서 설명한 데이터작성 수행자에게 부여되어 새로운 시스템 설계에 적합하도록 개발되어야 한다. 이러한 절차와 도구의 개발은 반드시 본 규격의 시스템의 일반적인 소프트웨어 하드웨어의 개발성과 일치해야 한다. 확인, 검증 그리고 평가절차는 반드시 데이터 작성절차와 일반적인 소프트웨어에 대하여 호환성을 가져야 한다.	17.4.2.1	시스템 소프트웨어 설계단계는 응용데이터에 의해 설계되고, 데이터 작성계획서는 데이터 작성과정의 문서구조에 대한 정의에 의해 생성되어야 한다. 이러한 문서는 반드시 17.4.1에 포함된 데이터 작성 수행주기 요건을 준수해야 한다. 데이터 작성계획서는 반드시 데이터 작성절차와 도구에 대한 상세한 설명을 시스템 안전유형설 계별에서 요구된 수준을 만족하도록 수행해야 하며, 확인, 검증 그리고 설계 직전에 상세한 관리절차를 포함하여 모든 소프트웨어를 포함한 기록해야 한다.	17.4.2.2	데이터 작성계획서는 반드시 데이터 작성 수행주기에서 사용되는 모든 하드웨어 또는 소프트웨어 도구에 대한 안전유형설 계별을 포함해야 한다. 데이터 안전유형설 계별은 반드시 시스템 안전유형설 계별로부터 유도되어야 하며, 각각의 도구에 의한 결과는 다른 매뉴얼 또는 자동화된 절차에 의해 확인되어야 한다.	17.4.2.3	가능한 데이터 작성 계획은 반드시 작성에 사용되는 표기에 대한 요구사항을 명확히 하고, 표준화된 신 호체계와 데이터타입과 같이 응용분야 전지니언어에 친숙하게 설계해야 한다. 새로운 표기법을 사용하는 경우 그 표기법 사용의 적합성에 대한 문서화해야 한다.	17.4.2.4	확인, 시험, 검증 그리고 평가 보고서는 각각의 설계에 대한 문서화에서 최소한의 체크리스트 형태로 표준화된 작성계획과 동일함을 입증해야 한다. 이러한 정보는 반드시 각각의 데이터 시험 계획을 포함해야 하고, 그 결과는 반드시 데이터 시험 보고서에 기록되어야 한다.	오. 부속록자 4.1의 세부별가검 본 절에서는 SSI 소프트웨어 요구사항 분석의 일반사항을 제시한다. 본 절과 관련하여 IEC 62279의 요구사항 표11을 만족해야 한다. 표11. SSI 소프트웨어 요구사항분석 일반 관련 IEC 62279의 요구사항 <table border="1"> <thead> <tr> <th>Code</th><th>Requirement</th></tr> </thead> <tbody> <tr> <td>5.2.1</td><td>IEC 62278과 ENV 50129에 부합하여 다음과 같은 사항이 생성되어야 한다. - 시스템 요구사항 명세서 - 시스템 안전요구사항 명세서 - 시스템 구조 설명서 - 시스템의 안전계획서 위 결과물들은 다음의 사항을 포함한다: - 안전기능 - 시스템의 구성 또는 구조 - 하드웨어 실행용 요구사항</td></tr> </tbody> </table> 2011-07-06 Project Name: 고속선 전자연동장치(5S) 시험개발 Page 18 / 43 Title: 소프트웨어 안전보고서 작성지침 Compiled By: dukso SHN Approved By: Jaeho LEE	Code	Requirement	5.2.1	IEC 62278과 ENV 50129에 부합하여 다음과 같은 사항이 생성되어야 한다. - 시스템 요구사항 명세서 - 시스템 안전요구사항 명세서 - 시스템 구조 설명서 - 시스템의 안전계획서 위 결과물들은 다음의 사항을 포함한다: - 안전기능 - 시스템의 구성 또는 구조 - 하드웨어 실행용 요구사항
Code	Requirement																						
17.4.1.3	데이터 작성 데이터의 작성절차는 상세한 정보영역(예를 들어 테이블), 데이터 코드코드의 생성, 이 코드들의 링크 및, 검사 그리고 다른 확인절차와 응용데이터의 시험을 반드시 포함해야 한다.																						
17.4.1.4	통일과 적용 모든 시스템의 응용데이터는 일반적인 하드웨어, 소프트웨어와 함께 통합설계 이전에 공칭시험 단계에서 통합된다. 이러한 경우에는 다른 요건들에 의해 충분한 수준의 신뢰가 요구된다. 설계는 통합설계 이전에 새로운 설계가 추가되면 반드시 통합시험을 실시해야 한다. 마지막으로 시스템은 최종 설계시에 시스템 전체기능에 대한 시험과 최종 적용절차를 반드시 수행해야 한다.																						
17.4.1.5	검증과 평가 검증과 평가절차는 반드시 시스템 설계단계에서 각각의 단계의 성능에 대하여 수행되어야 한다.																						
17.4.2	데이터 작성절차와 도구들 각각의 새로운 설계 시스템의 응용데이터, 상세데이터 작성절차 및 도구에 의한 설명은 반드시 17.4.1에서 설명한 데이터작성 수행자에게 부여되어 새로운 시스템 설계에 적합하도록 개발되어야 한다. 이러한 절차와 도구의 개발은 반드시 본 규격의 시스템의 일반적인 소프트웨어 하드웨어의 개발성과 일치해야 한다. 확인, 검증 그리고 평가절차는 반드시 데이터 작성절차와 일반적인 소프트웨어에 대하여 호환성을 가져야 한다.																						
17.4.2.1	시스템 소프트웨어 설계단계는 응용데이터에 의해 설계되고, 데이터 작성계획서는 데이터 작성과정의 문서구조에 대한 정의에 의해 생성되어야 한다. 이러한 문서는 반드시 17.4.1에 포함된 데이터 작성 수행주기 요건을 준수해야 한다. 데이터 작성계획서는 반드시 데이터 작성절차와 도구에 대한 상세한 설명을 시스템 안전유형설 계별에서 요구된 수준을 만족하도록 수행해야 하며, 확인, 검증 그리고 설계 직전에 상세한 관리절차를 포함하여 모든 소프트웨어를 포함한 기록해야 한다.																						
17.4.2.2	데이터 작성계획서는 반드시 데이터 작성 수행주기에서 사용되는 모든 하드웨어 또는 소프트웨어 도구에 대한 안전유형설 계별을 포함해야 한다. 데이터 안전유형설 계별은 반드시 시스템 안전유형설 계별로부터 유도되어야 하며, 각각의 도구에 의한 결과는 다른 매뉴얼 또는 자동화된 절차에 의해 확인되어야 한다.																						
17.4.2.3	가능한 데이터 작성 계획은 반드시 작성에 사용되는 표기에 대한 요구사항을 명확히 하고, 표준화된 신 호체계와 데이터타입과 같이 응용분야 전지니언어에 친숙하게 설계해야 한다. 새로운 표기법을 사용하는 경우 그 표기법 사용의 적합성에 대한 문서화해야 한다.																						
17.4.2.4	확인, 시험, 검증 그리고 평가 보고서는 각각의 설계에 대한 문서화에서 최소한의 체크리스트 형태로 표준화된 작성계획과 동일함을 입증해야 한다. 이러한 정보는 반드시 각각의 데이터 시험 계획을 포함해야 하고, 그 결과는 반드시 데이터 시험 보고서에 기록되어야 한다.																						
Code	Requirement																						
5.2.1	IEC 62278과 ENV 50129에 부합하여 다음과 같은 사항이 생성되어야 한다. - 시스템 요구사항 명세서 - 시스템 안전요구사항 명세서 - 시스템 구조 설명서 - 시스템의 안전계획서 위 결과물들은 다음의 사항을 포함한다: - 안전기능 - 시스템의 구성 또는 구조 - 하드웨어 실행용 요구사항																						

라. 검증에 필요한 구축장비 수요조사

- 신호설비 표준플랫폼의 검증은 기능과 품질안전으로 구분할 수 있다. 품질안전의 검증을 위해서는 성능별 안전 및 비안전 입출력에 대한 사양의 검증을 위한 상용계측기의 활용이 예상되며, 전자파, 온도습도, 충격 등의 시험을 위해서는 전문기관의 비용추정을 실시하여 표준플랫폼 활용시의 경제적 효과를 분석한다.
- 또한, 표준플랫폼에 특정사양이 적용되는 경우 다음 그림과 같이 해당 사양의 검증을 위해 필요한 구축장비 목록을 제시한다.



그림1-3. 플랫폼 검증을 위한 구축장비 예, 경부고속선 SSI국산화 사업

마. 경제적 효과 및 적용범위 분석

- 품질안전이 검증된 표준플랫폼의 실용화를 통해 현재 제작사별 개발과 독립안전평가에 소요되는 비용은 물론, 구성품 단위 안전인증을 취득한 핵심하드웨어와 운영체제의 중복 사용 비용의 절감이 예상된다.
- 다음 그림은 전자연동장치 국산화 과정에서 국제표준의 안전검증을 만족하기 위해 기업 별도 지출되는 비용과 표준플랫폼의 일반제품(Generic Product) 인증을 취득한 후의 경제적 효과를 2011년의 산업환경을 반영하여 추정한 모델이다. 본 기획을 통해 시장 현황과 인증관련 비용을 조사분석하여 보다 방대한 데이터를 기반으로 하는 경제적 효과예측을 실시한다.

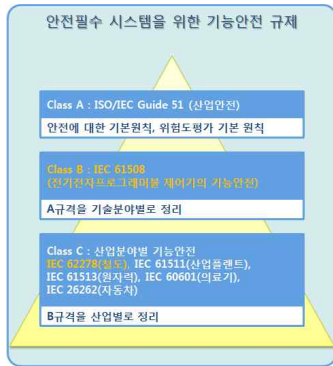


그림1-4. 인증을 취득한 표준플랫폼 활용에 따른 기업의 비용부담 예측

2. 철도신호시스템 안전성 인증 체계 수립

가. 관련 국제규격 및 해외 사례 조사

- 철도신호시스템이 포함된 안전필수분야의 기능안전을 위해 다음 그림과 같이 국제표준이 적용되고 있으며, 특히 안전기능에 대해서는 위험측고장의 실패확률을 정략적으로 제시하고 있다.



SIL	On-Demand [/cycle]	Dangerous Failure [/hour]
4	$10E-6 \leq x < 10E-5$	$10E-9 \leq x < 10E-8$
3	$10E-5 \leq x < 10E-4$	$10E-8 \leq x < 10E-7$
2	$10E-4 \leq x < 10E-3$	$10E-7 \leq x < 10E-6$
1	$10E-3 \leq x < 10E-2$	$10E-6 \leq x < 10E-5$

Req. 1) Management of Functional Safety

1. Random Hardware Failure
2. S/W : IEC 62278(IEC 61508 Part3)
3. H/W : Architectural Constraints(Hardware Fault)

Req. 2) Technical Requirements

1. Functional Test
2. Environment Test
3. Operating Test

Req. 3) Competence of Persons

1. Personal Information
2. Evidence of Competence

Req. 4) Functional Safety Assessment(FSA)

1. Functional Safety Review
2. Evidence of Independence

그림 1-5. 국제표준의 계층 및 SIL의 정량적 기준

표1-3. 철도신호 안전관련 대표적 국제표준

순번	규격명
Std.01	IEC 62278 , “Railway applications-Specification and demonstration of reliability, availability, maintainability and safety(RAMS)”, 2002.09.
Std.02	IEC 62279 , “Railway applications-Communications, signaling and processing systems-Software for railway control and protections systems”, 2002.09.
Std.03	IEC 62280-1 , “Railway applications-Communications, signaling and processing systems-Part 1:Safety-related communication in closed transmission systems”, 2002.10.
Std.04	IEC 62280-2 , “Railway applications-Communications, signaling and processing systems-Part 2: Safety-related communication in open transmission systems”, 2002.10.
Std.05	IEC 62425 , “Railway applications-Communications, signaling and processing systems-Safety related electronic systems for signaling”, 2007.09.

- 철도신호시스템의 안전성 인증은 위 표와 같이 관련 적용규격에 대한 부합성을 독립된 전문기관이 평가하여 만족여부를 평가보고서로 작성하고, 작성된 평가보고서의 요약으로 인증서(Certificate)를 발행한다.
- 따라서, 본 기획연구에서는 관련 국제표준의 요구사항을 분석 및 체크리스트화 하며, 요구사항 만족을 위한 단계(수명주기)별 문서의 템플릿을 제시하여 표준플랫폼의 인증범위와 세부방법에 대하여 제시한다.

나. 국제규격에 부합하기 위한 요구조건 분석

- 국제표준에 품질안전을 만족하는 플랫폼 표준화를 위해 국제표준의 요구사항을 적용하기 위한 세부기술 개발 방향을 연구한다.

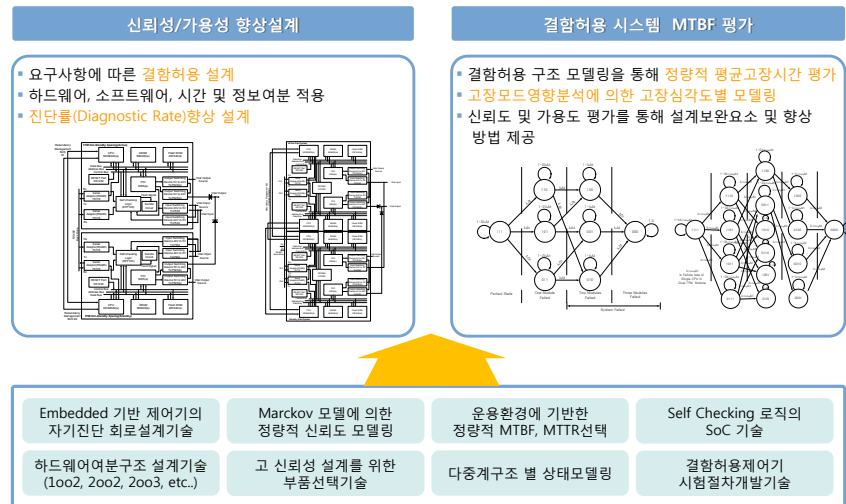


그림 1-6. 국제표준의 안전설계 요소기술 예시

다. 인증절차, 인증기관 지정 등 인증기반 및 대내외적 공신력 확보방안 제시

- 신호설비 표준플랫폼의 인증은 다음 그림과 같이 국제표준에서 요구하는 수명주기별 검증단계에 따라 수행해야 하며, 본 기획연구에서는 검증단계별 문서화 요건 및 평가기준에 대하여 제시한다. 제시된 문서화 요건 및 평가 기준을 바탕으로 플랫폼을 표준화하는 본 과제에서의 개발품 인증의 가능성을 가시적 수준으로 입증한다.

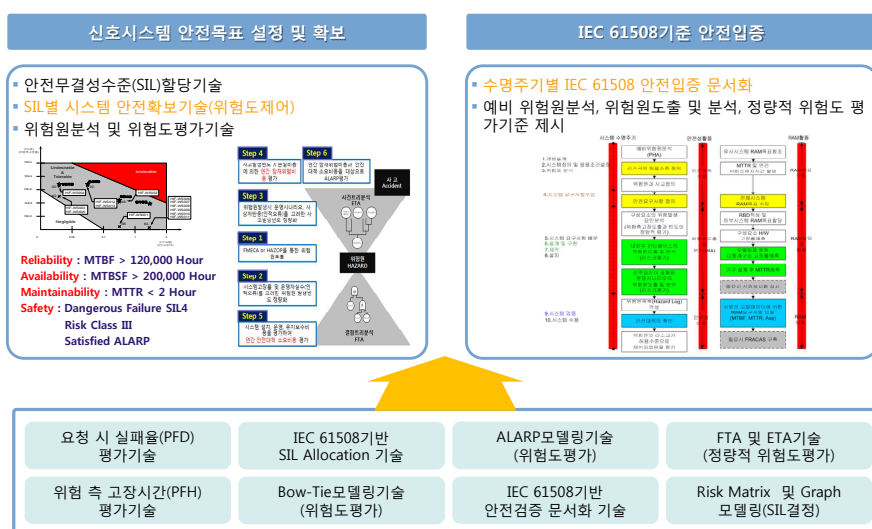


그림 1-7. 국제표준의 인증관련 핵심검증방법 예시

제 2 절 과제추진 배경 및 필요성

1. 국외 기술 및 연구 동향

- IEC 61508 규격이 1998년 12월 IEC TC 65에 의해 산업안전의 정의 및 수명주기별 기준마련을 위해 제정되었으며, IEC Guide 51 및 IEC 61508을 통해 철도신호설비를 포함한 모든 전기/전자/프로그램어블 제어기에 대한 기능안전을 확보하도록 강제하고 있다.
- 이러한 국제표준은 현재 세계적으로 프로젝트 안전관리 및 구매의 필수 사항으로 적용 중이며, 고부가 안전필수시장에 대한 무역장벽 구축을 통해 철도분야에 있어서도 대부분의 사업이 안전관련 규격을 필수요건으로 제시하고 있다.

표1-4. 해외 사업의 안전인증 강제여부 현황

순번	사업 및 안전요건	적용규격
사례1	미국 플로리다 고속철도 RFP(제어 및 진단시스템 SIL4)	EN 50126(IEC 62278)
사례2	사우디 고속철도제어시스템 RFP(SIL4)	EN 50126(IEC 62278)
사례3	브라질고속철도사업 예비RFP : 모든 전자제어 구성요소에 대한 규제(열차제어 SIL4)	EN 50126(IEC 62278)

- 따라서, 안전성이 검증된 신호설비에 대한 요구는 1996년 고속철도기술개발 사업 중 미국 모터롤라사의 2003 결함허용 시스템(Fault Tolerant System, FX Series)을 전자연동장치 코어로직으로 활용을 검토한 것이 대표적 사례이며, 대당 높은 가격(당시 기준, 약 10억원/set)으로 인해 도입은 보류되었다.
- 이후 국내 기업은 모터롤라사의 상용 CPU보드인 Mo Serise를 다중계로 구현하여 전자연동장치 중심으로 결함허용 시스템을 구현하였으나, 철도안전법 이후 건설운영기관에서 국제표준의 적용 및 인증을 요구하게 됨에 따라 제조사 별로 별도의 비용으로 전문기관의 독립안전평가를 받아 제품을 공급하고 있다.
- 해외 철도신호 제조사의 경우 국제표준에 따른 독립안전평가(인증)비용을 줄이기 위해 노력하고 있으며, 국내 경부호남선 차상신호시스템 구축사업에 도입된 Bombardier사의 차상신호장치(EBCAB 2000)의 경우에는 바이탈 연산모듈, 바이탈 입출력, 일반입출력, 통신모듈을 각각 분리하여 모듈단위로 안전성을 검증하고, 적용환경에 따라 구성된 모

들의 안전성 평가시에는 각각의 모듈의 안전성은 이미 취득한 일반제품(Generic Product) 인증을 활용하여 안전검증 비용의 최소화 하고 있다.

- 비안전 분야에서는 표준플랫폼이 보편화 되어 있으며, 활용도가 높은 제품으로는 미국 National Instrument 사의 제품군이 있으나, 철도신호설비의 적용은 국제표준에서 요구하는 품질안전에 미흡하여 활용이 어려운 실정이다.
- 따라서, 최근에는 독일 MEN사의 산업용 제어기와 미국 GE사의 Tempo ETCS Solution과 같이 SIL인증 취득한 하드웨어 플랫폼을 전문기업이 생산하고 철도신호설비 제조사는 하드웨어 플랫폼을 구매하여 응용프로그램만 포팅하여 상세응용(Specific Application) 인증을 취득하는 사업모델이 새롭게 형성되고 있다. 하지만 이러한 사업모델은 국내 철도신호설비 제조기업의 경영수지를 악화시키고 향후에는 국내 철도건설비용의 증가원인으로 작용하여 교통분야에서의 철도산업의 입지에 악영향이 우려되고 있다.



[Motorola FX Serie]



[Bombardier 사의 EB CAB2000]



[NI Pomact Rio]



[독일 MEN사의 안전필수 플랫폼 코어]

그림1-8. 해외 철도신호설비와 일반산업의 대표적 플랫폼

표1-5. 국내 적용중인 외산시스템 현황

장치명	제조사	인증	CPU	시스템 구조
Compact PCI System	MEN	EN50128 & 50129 SIL 4	3 x PPC 750CL	2 out of 3 Voting
SICAS S7	SIMENS	IEC 62061 SIL 3	SIMATIC S7-300 CPU Module	Fail-safe, Modular logic control
HIMax	HIMA	EN50128 & 50129 SIL4	-	2oo4, I/O 이중화

- 해외 철도분야 전문기업인 Alstom사의 사례를 보면, 본 기획과제와 유사한 개념을 다음 그림과 같이 도입하여 운영하고 있다. Alstom사는 철도신호시스템 핵심장치에 대한 개발을 3단계로 구성하였으며, 핵심장치의 기반이 되는 플랫폼의 개발이 선행되어 4종 (CBTC시스템, Fixed Block, RBC 그리고 전자연동장치)의 공급 가능한 시스템을 개발하였음을 볼 수 있다. SIL인증 또한 플랫폼에 대한 인증(Generic Platform) 1건, Generic Application 4건을 확보하였다. 고객의 요구에 의해 Specific Application에 대한 인증을 받아 안전을 확보하고 있다.
- 이러한 국외 환경을 고려할 때 본 기획을 통한 국내 표준플랫폼의 개발방향과 안전인증에 대한 해법의 강구는 매우 절실하다.

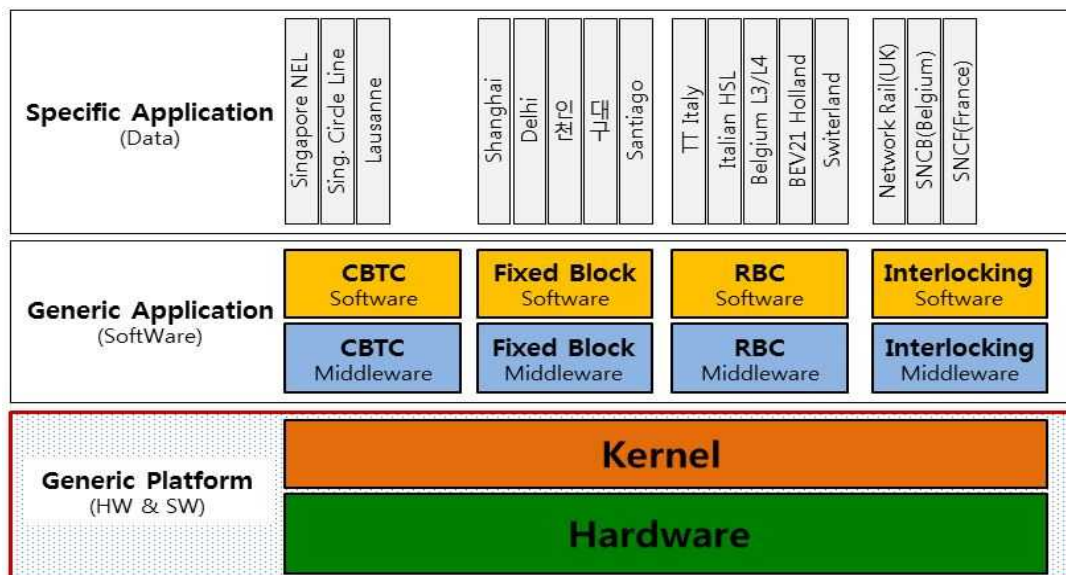


그림1-9. Alstom사의 철도신호시스템 플랫폼과 인증계층

2. 국내 기술 및 연구 동향

- 해외 메이저 철도신호제어시스템 공급업체들은 국제공인인증기관으로부터 SIL인증을 획득한 제어시스템을 기반으로 전세계적인 Market을 형성하여 공급하고 있지만, 현재 국내 철도신호 공급업체의 실적은 전무한 상태이다.
- 일반적으로 SIL인증을 필요로 하는 핵심장치는 다음과 같다.

표1-6. 철도신호시스템 중 안전필수 설비

	지상설비	차상설비
대표설비	궤도회로, 전자연동장치, 관제설비, 지상신호(ATP, ATC, ATO)제어기, 영상감시장치, 건널목제어유니트 등	차상신호(ATP, ATC, ATO)제어기 운전자표시장치(MMI) 운행기록장치(RU) 운전지원제어시스템(TMC) 등

- 최근 발주되는 해외프로젝트는 상기 장치에 대한 SIL인증을 반드시 요구하고 있어 국산품을 공급하는 국내 공급업체의 수주는 매우 어려운 상황이며, 국내 발주 프로젝트 또한 유사한 형태로 운영되어 핵심장치 대부분은 해외 시스템이 적용되고 있으며, 이로 인해 해외 기업의 국내진출은 활성화된 반면, 국내 기업의 해외진출과 국내시장의 점유율이 계속 떨어지고 있다.
- 이러한 불평형은 첫 번째 국내기업의 사업투자금액의 증가로 인한 수직악화를 가져오며, 두 번째로 기능구현이 핵심시스템(해외)에 종속되어 시스템 개량시에 국내 공급자가 공급하는 주변 타 시스템의 변경(인터페이스, 프로토콜 등)이 빈번하게 발생하는 등 시스템의 안정성에 악영향을 미치고 있다. 마지막으로 운영상에서 발생하는 문제점(오류, 결함 등)에 대한 유지보수의 어려움과 보수지연 등으로 인해 서비스중단이 발생되어 유지보수에 대한 비용증가와 국민의 눈높이에 맞는 서비스 공급에 막대한 지장이 발생하고 있다.
- 국내 최근 도시철도에 적용된 철도신호제어시스템에 대한 다음의 현황을 보면 대부분의 핵심장치가 외산시스템임을 확인할 수 있다.

표1-7. 최근의 철도신호사업 및 핵심시스템 공급현황

프로젝트	공급사	장치
김해-부산 CBTC	Thales	지상/차상 ATP/ATO
부산4호선(반송선)	교산	지상/차상 ATP/ATO
인천국제공항철도	알스톰	지상/차상 ATP/ATO
신분당선	Thales	지상/차상 ATP/ATO
		Axle Counter
인천2호선	Thales	지상/차상 ATP/ATO
김포경전철	일본신호	지상/차상 ATP/ATO

- 최근 핵심설비의 국외장비 의존도가 높고, 주변설비만 국산화하는 산업구조로 인한 안전성 미흡을 방지하고자, 2013년 ‘철도안전법’을 개정하여 시스템단위 검증을 강화하는 등의 개선이 시작되었으며, 핵심장치에 해당되는 우선순위 장치를 선정하여 이에 대한 형식승인과 제작자승인을 수행하고자 기술기준을 마련 중에 있다.
- 또한 막연한 요구사항의 SIL표기 보다는 인증의 범위와 재사용을 가능하게 함으로써 산업에서의 중복투자를 방지하기 위해 다음과 같이 국제표준의 인증단계를 구분하여 일반제품과 응용을 취득한 장치의 활용은 상세응용 인증단계에서 안전확보조건(SRAC, Safety Related Application Condition)만 확인하는 등의 개선을 지속적으로 수행하고 있다.

표1-8. 안전인증의 단계, IEC 62278

Generic Product	모든 산업분야에 적용할 수 있는 제품
Generic Application (Railway)	철도분야에 적용할 수 있는 제품
Specific Application (Railway)	Generic Application 인증 제품을 특정 현장에 적용할 경우

- 철도안전 배경에서 나열된 핵심장치는 Generic Application에 해당되며, 철도신호 시스템 표준규격을 준수하여 개발되어야 한다.
- 하지만, 이러한 Generic Application 핵심장치는 각종 Vital제어명령을 처리할 수 있는 CPU와 이에 따른 국제표준규격에 따라 안전성이 확보된 플랫폼이 구현되어야 하는데 이러한 기반이 되는 제품인증이 Generic Product이다.

- Generic Product인증은 IEC61508에 따라 안전설계와 구현 프로세스를 준수하여 SIL인증을 획득하게 되며, Generic Product SIL 인증 제품은 철도신호제어시스템의 Generic Application 인증에 적극적으로 활용될 수 있다.
- 이러한 안전성이 확보된 플랫폼은 하드웨어 부문인 CPU메인보드와 Boot Loader, RTOS부문인(Real Time Operation System) Kernel과 BSP(Board Support Package)로 구성되는데, 각 해외의 철도신호시스템 제작사마다 적용하는 플랫폼이 상이하며, 국내 또한 핵심시스템에 적용되는 플랫폼이 각기 상이하게 개발되는 실정이다.
- SIL인증 핵심시스템에 적용되는 플랫폼 구현 비용은 매우 높은 수준으로 시스템별 중복적으로 부담되고 있으며, 이는 추후 시스템의 개·보수 및 상호호환성에 따라 부가되는 추가적인 비용이 매우 높을 것으로 전망된다. 따라서 개발과 인증비용의 최적화를 위해서는 다음 그림과 같이 인증된 공통 플랫폼의 활용이 필요하다.

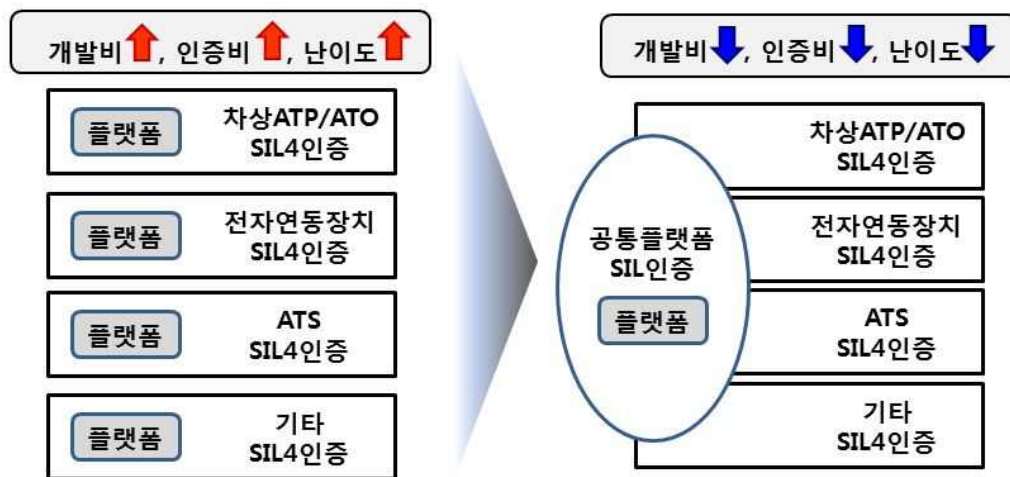


그림1-10. 인증된 플랫폼 표준화의 효과 예측

제 2 장 특허, 논문, 시장분석 보고서

제 1 절 분석개요

1. 기술의 정의(안전필수 신호설비 공통 플랫폼)

신호설비 플랫폼은 내장형제어기로 구성된 하드웨어와 운영체제 및 응용프로그램으로 구성된 소프트웨어가 결합하여 장치에 요구된 사양을 수행하는 신호설비의 핵심 구성품으로써 일반적인 구성은 다음과 같다.



<16bit급 신호설비 플랫폼의 예>



<32bit급 신호설비 플랫폼의 예>

따라서, 신호설비 플랫폼 표준화 및 검증을 위한 핵심기술의 정의를 위해서는 표준화가 가능한 플랫폼의 범위와 기능을 정의하고, 국제표준에서 요구하는 수명주기별 검증활동을 반영하여 표준플랫폼의 설계 및 제작요건을 제시한다. 향후 다양한 응용환경에서 사용할 수 있는 개발환경의 제공과 함께 응용프로그램을 제외한 운영체제와 디바이스 드라이버에 대한 검증방안도 제시되어야 한다.

신호설비 표준플랫폼은 신호설비 제어기 현황의 분석을 통해 궤도회로, 지상신호장치 구성 유닛(예, ATP의 선로변제어기)와 같이 상대적으로 단순한 기능을 수행하는 중저성능 표준플랫폼(16bit급)과, 연동장치 및 차상신호제어기와 같이 상대적으로 복잡한 기능을 수행하는 고성능 표준플랫폼(32bit급, 상용 운영체제 포팅)이 요구될 수 있으며, 운영환경 및 수요에 따라 목표성능을 설정하고 입출력 기능분석을 통해 위험도에 따른 SIL할당과 세부사양을 기

확한다. 또한, 표준플랫폼의 산업계 활성화를 위해 설비의 소형화, 에너지 효율, 디자인 등도 고려되어야 하며, 가장 중요한 구현에 소요되는 비용(가격)목표를 정량적으로 수립하여 설계단계부터 부품선택과 양산의 용이성 등도 검토한다.

신호설비 플랫폼의 표준화를 위해서는 기능적 측면 뿐 아니라 국제규격의 수명주기별 요건을 만족해야 한다. 따라서 신호설비 플랫폼의 적용대상이 될 수 있는 신호설비의 예비위험원분석(PHA)을 기획단계에서 수행하여 표준 플랫폼의 성능별 안전입출력의 적정 포트 수, 인터페이스 방법에 대하여 검토한다.

검증 방안 및 검증결과와 신뢰성 확보를 위해 해당 표준의 요구사항을 만족하기 위한 신호설비 검증 문서목록을 다음과 같이 제시하고 적용 국제표준의 항목을 정리하여 체크리스트를 생성한다.

2. 기술의 구성

신호설비 공통 플랫폼 개발은 내장형제어기(Embedded Controller) 제어기를 국제표준이 요구하는 안전무결성수준(SIL)을 만족하기 위해 결함검출(Fault Detection), 결함회피(Fault Avoidance), 결함격리(Fault Isolation) 등의 결함허용(Fault Tolerance)토록 설계하고, 허용할 수 없는 결함이 안전필수(Safety Critical) 기능에서 발생하는 경우 안전측동작(Fail Safe)하도록 구현하는 것이 핵심기술 임. 이와 관련된 기술로써는 하드웨어 여분(Hardware Redundancy)의 이용과 데이터의 오류정정(Error Correcting), 자기검사(Self Checking) 등의 이론이 적용되기도 하며, 본 연구에서는 이러한 고안전, 고신뢰성 기능을 갖는 철도신호분야 내장형제어기를 공통 플랫폼(Common Platform)으로 적용하기 설계와 평가를 통해 국제표준의 안전기준을 만족하기 위한 연구를 수행한다.

3. 기술의 분류

대분류 (영문)	중분류 (영문)	소분류 (영문)	키워드 (영문)
기능안전기술 (Technologies for Functional Safety)	A. 결함허용 내장형제어기 (Fault tolerant embedded system)	AA. 철도신호 결함허용 (Fault tolerant for railway signaling)	고신뢰성 철도신호장치 High reliable railway signaling equipment
		AB. 결함허용 시스템 (Fault tolerant system)	결함검출, 회피, 억제, 격리, 자기검사, 고장검출률 Fault detection, Fault avoidance, Fault isolation, Self checking, Fault coverage
		AC. 다중계 시스템 (Hardware redundancy)	능동형 다중계, 수동형 다중계, 하이브리드형 다중계 Active hardware redundancy, Passive hardware redundancy, Hybrid hardware redundancy, 2 out of 3, Standby sparing
	B. 안전측 동작설계 (Fail-Safety Design)	BA. 인터페이스 안전측설계 (Fail-safe interface)	안전직렬인터페이스, 안전병렬인터페이스, 안전통신인터페이스 Safety serial interface Safety parallel interface Safety communication interface
		BB. 위험측고장 검지 (Dangerous failure detection)	위험측고장, 위험측 고장검출률 Dangerous failure, Dangerous failure coverage
		BC. 기능안전 설계 (Functional safety hardware design)	안전필수 시스템, 안전필수 설계, 안전무결성수준 Safety critical system, Safety critical hardware design, SIL, Safety integrity level
	C. 공통플랫폼 (Common platform)	CA. 하드웨어 호환성 (Hardware flexibility)	고신뢰성 버스, 고안전 버스, High reliable data bus, Safety data bus
		CB. 하드웨어 표준화 (Hardware standardization)	산업용제어기표준 Industrial controller standardization

제 2 절 특허분석

1. 특허분석 범위

구 분	분석 기준				
특허검색 DB	Thomson Innovation				
검색국가	미국	유럽	일본	한국	중국
	출원, 등록	출원, 등록	출원, 등록	출원, 등록	출원
분석구간	1990.01.01.~2014.07.10				
검색범위	Title, Abstract, Claim				

2. 특허기술 동향

가. 출원년도 및 국가별 특허출원 동향

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 분야의 전체적인 특허 동향을 살펴보면, 1990년부터 현재까지 총 83건의 관련 유효특허가 출원되었음

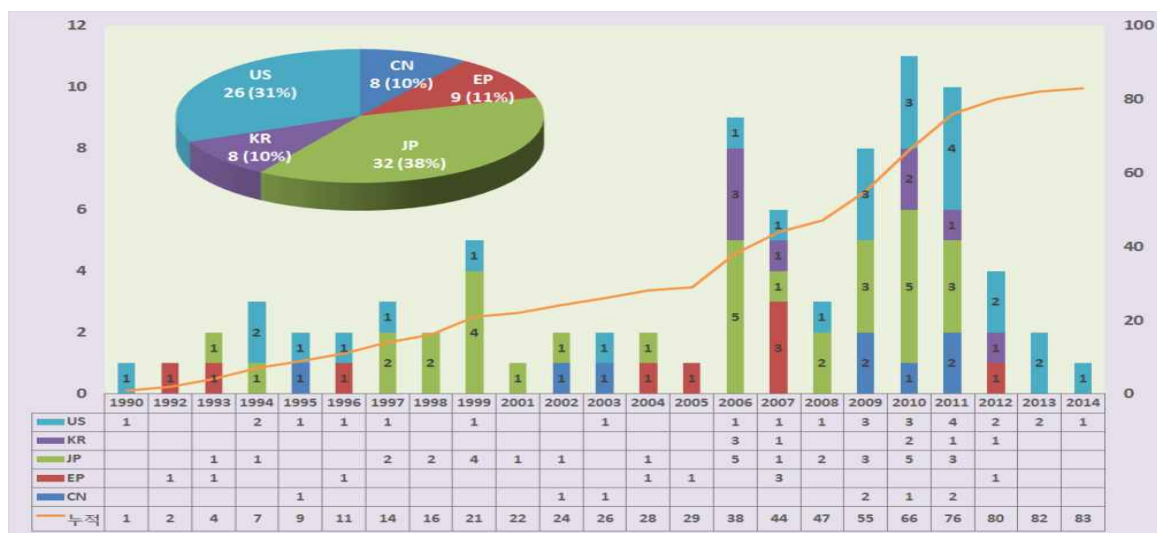


그림2-1. 출원년도 및 국가별 출원추이

- 국가별로는 일본이 32건(38%)으로 최다이며, 미국, 유럽, 한국, 중국의 순으로 출원되고 있음
- 일본은 90년대부터 지속적으로 출원이 있었으며 2012년 이후로는 출원이 없음
- 미국은 90년대부터 현재까지 지속적으로 관련 분야 기술을 출원하고 있음

- 전체적으로 2001년부터 2005년 사이에 출원이 적었고, 2006년 이후부터 출원이 급격히 증가하는 추세임

나. 주요 출원인 분석

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 분야 전반에 걸쳐 3개 이상의 특허를 출원한 상위 7개의 출원인을 분석해 보면, 일본 Hitachi LTD, TOSHIBA Corp., Mitsubishi Electric Corp., Nippon Signal Col. ltd, 미국 Cent Signal llc., 캐나다 Thales Canada Inc., 한국 KRRI가 출원을 많이 하고 있음을 알 수 있음

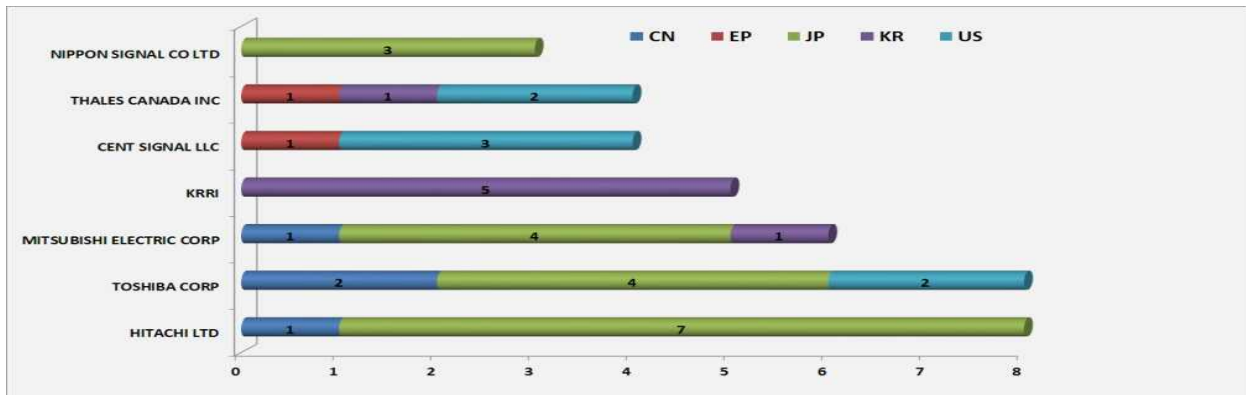


그림2-2. 주요 출원인 동향

- 주요 출원인의 연도별 특허출원을 보면 최다 출원인인 Hitachi와 Toshiba는 2006년부터 2011년 사이에 출원을 많이 하였고, 최근에는 캐나다의 Thales Canada가 관련특허를 계속 출원하고 있음

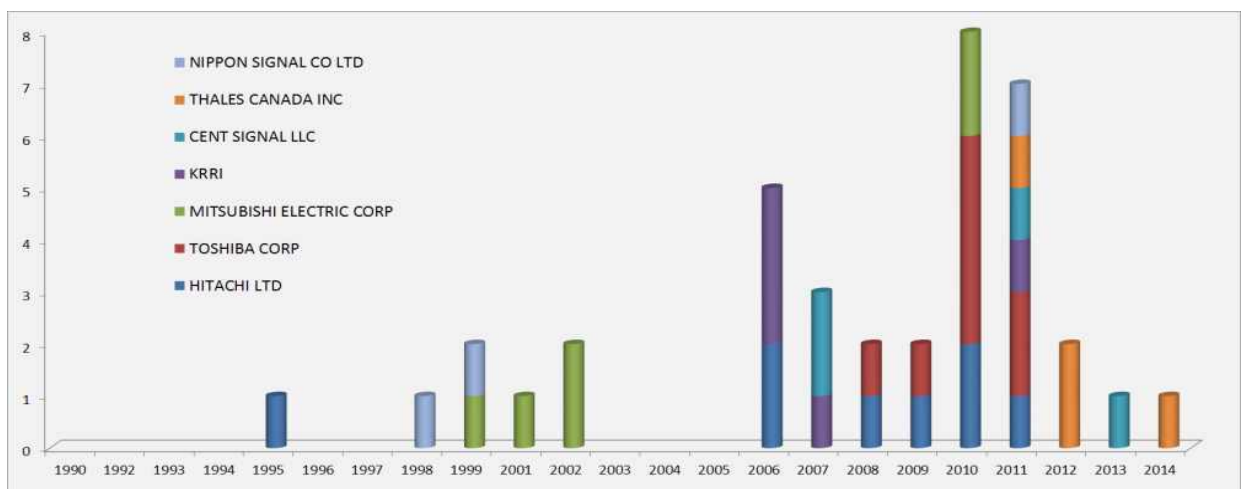


그림2-3. 연도별 주요 출원인 동향

다. 국가별 특허분포 지수분석

(1) 시장확보지수 (PFS : Patent Family Size)

- (지표 설명) 특정 국가에서 상업적인 이익 또는 기술경쟁 관계에 있을 때 해외에 특허를 출원하므로, Family Patent 數가 많을 때 특허를 통한 시장성이 크다고 판단되어 이를 시장확보력의 지표로 사용함
- (계산식) 국가별 시장확보지수(PFS) = ($\sum$ 특허별 패밀리) / 해당국가 특허건수
- 해당국가는 국가별 기술력을 판별하기 위하여 기술 개발 국가의 가능성이 높은 우선지정국(priority country)을 기준으로 하였음
- (분석결과)

- 유럽과 미국의 시장확보지수 (PFS)가 6.62와 5.71로 가장 높게 나타남
- 미국은 출원과 PFS가 모두 높았던 반면, 유럽은 출원건수는 상대적으로 적음에도 불구하고 PFS가 높아 영향력 있는 특허를 보유하고 있는 것으로 판단됨
- 우리나라는 출원 및 PFS가 모두 낮은 것으로 분석됨

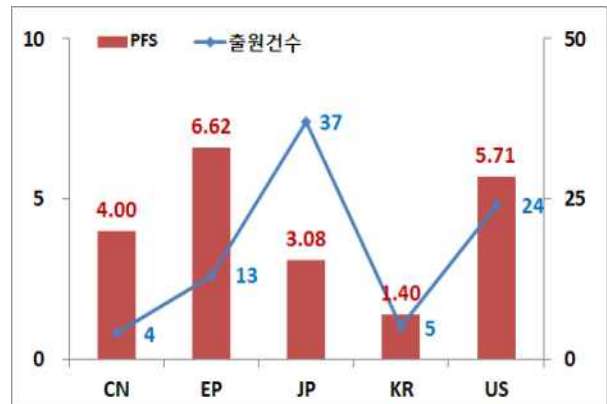


그림2-4. 국가별 출원건수 및 시장확보지수

(2) 인용도지수 (CPP : Cites Per Patent)

- (지표 설명) 특정 국가의 특허들이 이후 등록되는 특허들에 의해 인용되는 횟수가 많을수록 기술경쟁력이 높으므로, 인용도지수(CPP)가 클수록 원천특허/핵심특허를 많이 보유한 정도를 나타내는 지표로 사용함
- (계산식) 국가별 인용도 지수(CPP) = ($\sum$ 해당국가 특허별 피인용수) / 해당국가 특허건수
- 해당국가는 국가별 기술력을 판별하기 위하여 기술 개발 국가의 가능성이 높은 우선지정국(priority country)을 기준으로 하였음

● (분석결과)

- 미국과 유럽의 인용도지수(CPP)가 3.75와 2.23으로 가장 높게 나타나므로, 원천특허를 보유하고 있을 가능성이 높은 것으로 판단됨
- 반면, 한국과 중국은 인용도지수(CPP)가 많이 낮아, 원천특허/핵심특허를 거의 보유하지 못한 것으로 판단됨

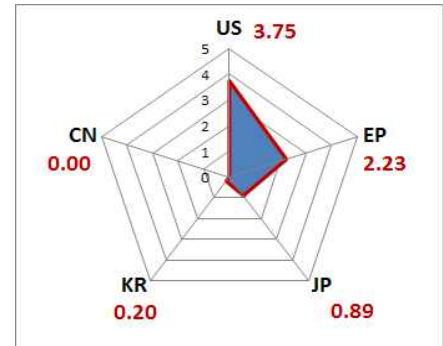


그림2-5. 국가별 인용도지수

(3) 영향력지수(PII : Patent Impact Index) 및 기술력지수(TS : Technology Strength)

- (지표 설명) 영향력지수는 특정 국가가 소유한 기술의 질적수준을 측정하는 지수이며, 기술력 지수는 특정 국가의 기술보유 양적수준(특허건수)과 영향력지수(질적수준)을 함께 나타냄

● (계산식)

- 국가별 영향력 지수(PII) = 해당국가 특허 인용도지수 / 전체(모든국가) 특허 인용도지수
- 국가별 기술력 지수(TS) = 해당국가 특허건수 × 해당국가 영향력 지수

- 해당국가는 국가별 기술력을 판별하기 위하여 기술 개발 국가의 가능성이 높은 우선지정국(priority country)을 기준으로 하였음

● (분석결과)

- 미국의 영향력지수(PII)가 2.03로 가장 높게 나타나 질적 수준에서 가장 우수한 것으로 판단되며, 양적 수준(특허건수)을 고려한 기술력지수(TS)에서도 미국이 48.82로 가장 높게 나타나고 있음
- 우리나라는 영향력지수, 기술력 지수 모두 하위 수준으로, 향후 지속적인 기술역량 강화가 필요함

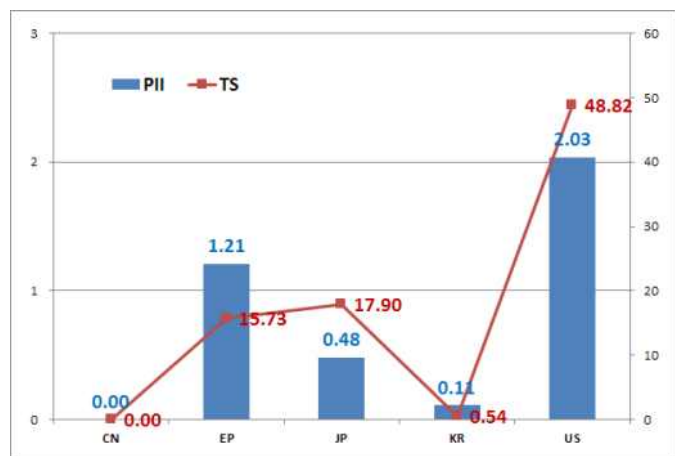
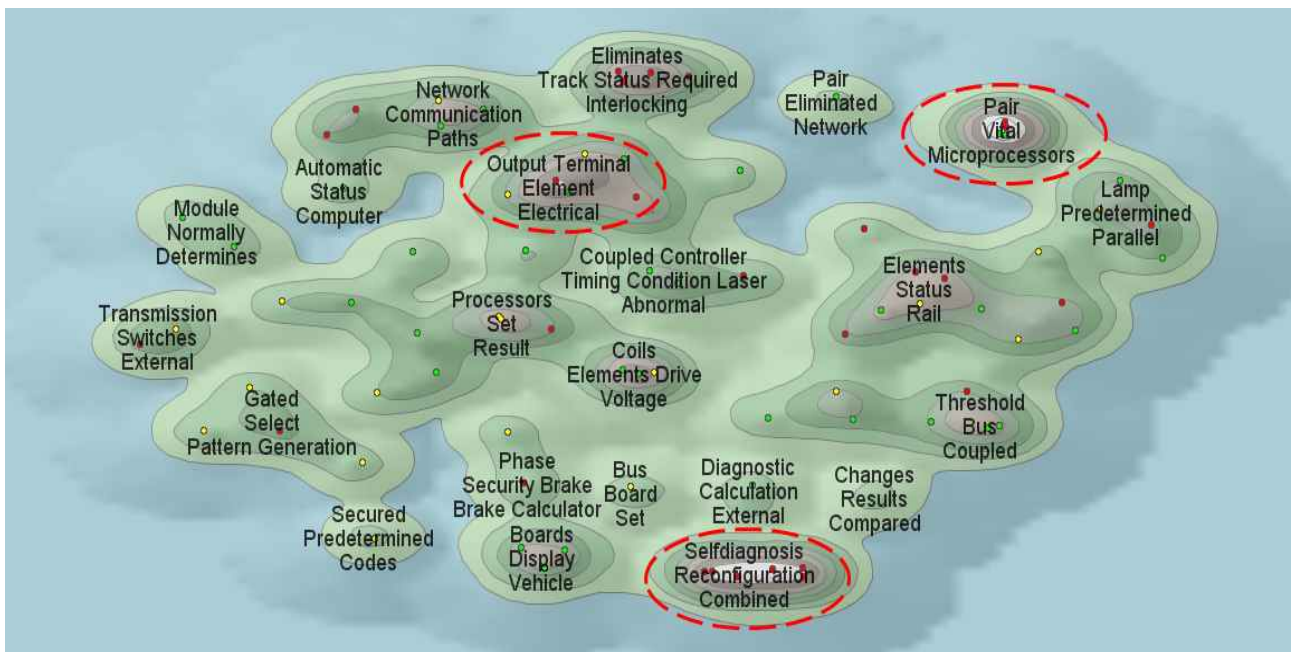


그림2-6 국가별 영향력지수 및 기술력지수

라. 기술분야 특허 분포도

(1) Text mining을 통한 특허 분포

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 관련 검색결과 결과, 400건 중 검색 특허 중 최종 83건의 유효 특허기술이 분포함
- 등고선 꼭짓점이 높은 Self-diagnosis/Re-configuration/Combined, Pair/Vital/Micro-processors, Output Terminal/Element/Electrical 등 3개 기술에 특허가 많이 분포하고 있어, 관련 분야가 기술 집중도가 높은 기술로 볼 수 있음
- 특히, 최근 특허기술을 보면 Safety switch device, redundant controller, Fault-detection 등과 관련된 기술이 나타나고 있어 관련 기술이 최근 주목받고 있는 기술로 판단할 수 있음



● 2010년 이후 ● 2000-2009 ● 1990-1999

그림2-7. 특허 등고선 맵

마. 주요 핵심특허 현황

- 전체 관련 특허 중 피인용수가 가장 높은 10건의 특허는 아래와 같으며, 이 중에서 특허 Union Switch & Signal 社の 미국 등록특허 US5561762A건의 피인용 건수가 43건으로 가장 높음

표2-1. 주요 핵심특허 현황

공개번호	발명의 명칭	출원인 정리	피인용수
US5561762A	Malicious Fault List Generation Method	Union Switch & Signal Inc	43
US5504860A	System Comprising A Processor	Westinghouse Brake & Signal	13
US20110026411A1	Methods And Systems For Fail-Safe Communication	General Electric Co	10
US6381506B1	Fail-Safe Microprocessor-Based Control And Monitoring Of Electrical Devices	Grappone V	10
US5483639A	Device For Detecting Transmission Errors In Balanced Two-Wire Bus Lines And Two-Bus Interfaces	Mercedes-Benz Ag	8
US20040132409A1	Test Method For Message Paths In Communications Networks And Redundant Network Arrangements	Siemens Ag	8
JP2004194471A	Protector Which Detects Ground Fault Inside Dc Machine	Mitsubishi Electric Corp	7
JP2000172986A	Fault Detector Of Signal Lamp	Nippon Signal Co Ltd	7
US5990685A	Apparatus For And Method Of Monitoring An Earth-Leakage State Of A Power Distribution System	Cegelec Controls Ltd	6
US8028961B2	Vital solid state controller	CENT SIGNAL LLC	6

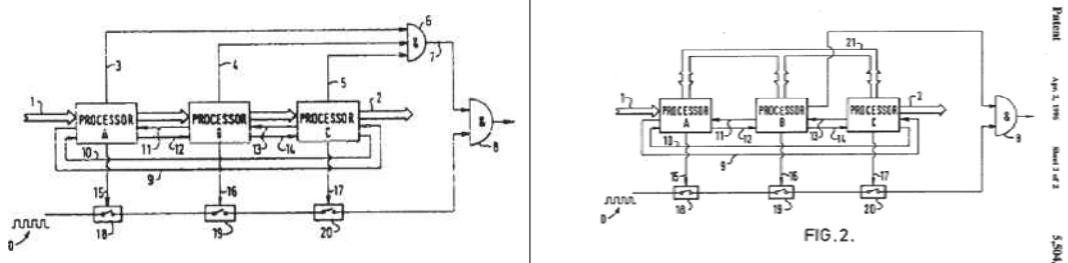
바. 주요 핵심특허 심층 분석

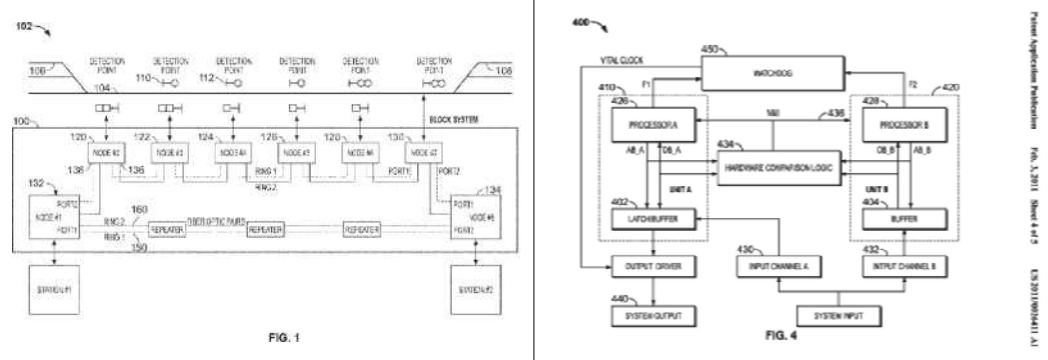
(1) 주요 핵심특허 심층분석 (권리성 분석)

- 피인용수가 가장 많은 UNION SWITCH & SIGNAL INC社의 미국 등록특허 US5561762A 건은 Malicious fault list generation method와 관련된 특허로 1995년 출원하여 1997년에 특허등록 되었으나, 2000년부터 연차료를 납부하지 않아 권리를 포기하여 현재는 공개된 자유기술에 해당함

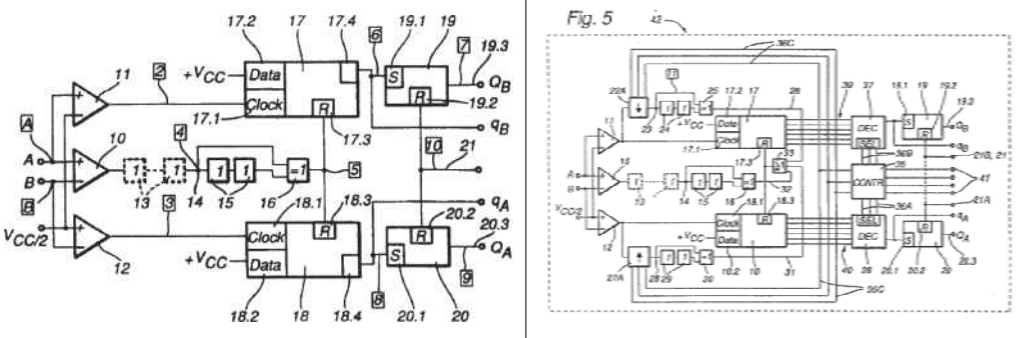
표2-2. 주요 핵심특허 현황

1	기술 분류	A. 결합허용 시스템	특허번호 (출원번호)	US1995471417A	특허번호 (공개번호)	US5561762A
출원인		UNION SWITCH & SIGNAL INC	출원일	1995-06-06	공개일	1996-10-01
발명의 명칭		Malicious fault list generation method				
대표도면						

2	기술 분류	AB. 결함허용 시스템	특허번호 (출원번호)	US1996610684A	특허번호 (공개번호)	US5504860A
	출원인	WESTINGHOUSE BRAKE & SIGNAL	출원일	1994-11-17	공개일	1996-04-02
	발명의 명칭	System comprising a processor				
	대표도면					
	주요 내용	철도 신호등의 인터로킹 시스템으로서, 제어 정보를 제공하기 위한 입력 정보 프로세서를 가지며 각각의 프로세서는 자신과 다른 프로세서를 테스트할 수 있는 능력을 가지고 있음				
	주요 청구항	1. A single channel interlocking system comprising: a plurality of processors for collectively receiving external input information, deriving internal interlocking information from the external input information, and providing external control information based on the external input information and the internal interlocking information, such that each of said plurality of processors is responsive to different information and performs a different function of the interlocking system; a common internal bus connecting said plurality of processors into a single hardware channel, said common internal bus including at least one external input for inputting said external input information and at least one external output for outputting said external control information; first fault-detection means for causing each of the processors to test itself to check whether it is operating correctly and to provide a respective first operation signal dependent on the result of that test; second fault-detection means for causing each of the processors to be tested for correct operation by a respective other of the processors and for causing said respective other processor to provide a respective second operation signal dependent on the result of that test; first logic means for subjecting the first operation signals to a first logical function to provide a first status signal, the first status signal being of a first kind if the first operation signals are such that each of the processors determines it is operating correctly and of a second kind if the first operation signals are such that at least one of the processors determines it is not operating correctly; and				
	법적상태 (회피전략)	- 본 특허는 1996.4.2. 등록된 특허로서 2014.4.2.에 특허권 존속기간이 만료 되었으므로, 현재는 자유기술에 속함. - 특허권 만료 직전까지 연차료를 계속 납부하여 권리가 유지되었음 - 피인용 횟수가 13건으로 비교적 많은 편인 것으로 판단컨대, 해당 기술 분야의 원천 기술 중 하나 일 것으로 보임				

3	기술 분류	BA. 인터페이스 안전측설계	특허번호 (출원번호)	US2009511144A	특허번호 (공개번호)	US20110026411 A1
	출원인	GENERAL ELECTRIC CO	출원일	2009-07-29	공개일	2011-2-3
	발명의 명칭	METHODS AND SYSTEMS FOR FAIL-SAFE COMMUNICATION				
	대표도면	 FIG. 1 is a block diagram of a communication network 100. It shows a central 'BLOCK SYSTEM' connected to multiple 'DETECTION PORT' units (102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200, 202, 204, 206, 208, 210, 212, 214, 216, 218, 220, 222, 224, 226, 228, 230, 232, 234, 236, 238, 240, 242, 244, 246, 248, 250, 252, 254, 256, 258, 260, 262, 264, 266, 268, 270, 272, 274, 276, 278, 280, 282, 284, 286, 288, 290, 292, 294, 296, 298, 300, 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322, 324, 326, 328, 330, 332, 334, 336, 338, 340, 342, 344, 346, 348, 350, 352, 354, 356, 358, 360, 362, 364, 366, 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 396, 398, 400, 402, 404, 406, 408, 410, 412, 414, 416, 418, 420, 422, 424, 426, 428, 430, 432, 434, 436, 438, 440, 442, 444, 446, 448, 450, 452, 454, 456, 458, 460, 462, 464, 466, 468, 470, 472, 474, 476, 478, 480, 482, 484, 486, 488, 490, 492, 494, 496, 498, 500, 502, 504, 506, 508, 510, 512, 514, 516, 518, 520, 522, 524, 526, 528, 530, 532, 534, 536, 538, 540, 542, 544, 546, 548, 550, 552, 554, 556, 558, 560, 562, 564, 566, 568, 570, 572, 574, 576, 578, 580, 582, 584, 586, 588, 590, 592, 594, 596, 598, 600, 602, 604, 606, 608, 610, 612, 614, 616, 618, 620, 622, 624, 626, 628, 630, 632, 634, 636, 638, 640, 642, 644, 646, 648, 650, 652, 654, 656, 658, 660, 662, 664, 666, 668, 670, 672, 674, 676, 678, 680, 682, 684, 686, 688, 690, 692, 694, 696, 698, 700, 702, 704, 706, 708, 710, 712, 714, 716, 718, 720, 722, 724, 726, 728, 730, 732, 734, 736, 738, 740, 742, 744, 746, 748, 750, 752, 754, 756, 758, 760, 762, 764, 766, 768, 770, 772, 774, 776, 778, 780, 782, 784, 786, 788, 790, 792, 794, 796, 798, 800, 802, 804, 806, 808, 810, 812, 814, 816, 818, 820, 822, 824, 826, 828, 830, 832, 834, 836, 838, 840, 842, 844, 846, 848, 850, 852, 854, 856, 858, 860, 862, 864, 866, 868, 870, 872, 874, 876, 878, 880, 882, 884, 886, 888, 890, 892, 894, 896, 898, 900, 902, 904, 906, 908, 910, 912, 914, 916, 918, 920, 922, 924, 926, 928, 930, 932, 934, 936, 938, 940, 942, 944, 946, 948, 950, 952, 954, 956, 958, 960, 962, 964, 966, 968, 970, 972, 974, 976, 978, 980, 982, 984, 986, 988, 990, 992, 994, 996, 998, 1000). The network is connected to a 'SYSTEM INPUT' and a 'SYSTEM OUTPUT'. FIG. 4 is a block diagram of a hardware architecture 400. It shows a 'SYSTEM INPUT' connected to 'INPUT CHANNEL A' and 'INPUT CHANNEL B'. These channels feed into 'UNIT A' and 'UNIT B' respectively. Each unit contains a 'PROCESSOR' (410A, 410B) and a 'BUFFER' (420A, 420B). The processors are connected to a 'HARDWARE COMPARISON LOGIC' (430). The logic outputs to 'OUTPUT DRIVER' (440) and 'SYSTEM OUTPUT' (450). The system also includes a 'VITAL CLOCK' (460) and a 'PROCESSOR' (470).				
	주요 내용	통신 네트워크로서, 통신 매체 및 통신 매체에 의해 결합된 네트워크의 복수의 노드를 포함하며, 복수의 네트워크 노드들 각각은 제1통신 채널 및 제2통신 채널을 포함한다. 제1통신 채널은 제1물리 계층트랜시버(PHY 장치)를 포함하고, 제2통신채널은 제2 PHY 장치를 포함한다. 복수의 네트워크 노드는 듀얼 링타입 토폴로지(topology)로 연결된다.				
	주요 청구항	1. A communication network comprising: communication media; and a plurality of network nodes coupled by said communication media, each of said plurality of network nodes comprising a first communication channel and a second communication channel, said first communication channel comprising a first physical layer transceiver (PHY device), said second communication channel comprising a second PHY device, said plurality of network nodes coupled in a dual ring-type topology. 2. A communication network in accordance with claim 1, wherein said plurality of network nodes are configured to distribute a network token between said network nodes, said network token grants permission to transmit data packets.				
	법적상태 (회피전략)	- 본 특허는 2009년 출원하였으나, 그 이후 특허 미등록으로 자유기술로 공개되었음 - 등록은 되지 않았지만 피인용건수가 10건으로 비교적 높아, 관련 분야 연구를 진행함에 있어 해당 특허기술을 참고하여 기술을 개발하는 것이 바람직할 것으로 보임				

4	기술 분류	C. 공통플랫폼	특허번호 (출원번호)	US1999274523A	특허번호 (공개번호)	US6381506B1
출원인	GRAPPONE VICTOR	출원일	1999-03-23	공개일	2002-04-30	
발명의 명칭	Fail-safe microprocessor-based control and monitoring of electrical devices					
대표도면	U.S. Patent Apr. 30, 2002 Sheet 15 of 15 US 6,381,506 B1 <pre> graph TD 74[MONITOR A DEVICE] --> 76[GENERATE A CODE INCLUDING PULSES IN PREDEFINED WINDOWS] 76 --> 78[APPLY THE CODE AS A SIGNAL TO A FIRST CONTACT OF A DEVICE] 78 --> 80[DETECT FOR A RESPONSE SIGNAL AT A SECOND CONTACT OF THE DEVICE] 80 --> 82[COMPARE THE RESPONSE SIGNAL TO THE CODE] 82 --> 84[DETERMINE THE CONDITION OF THE DEVICE] </pre> FIG. 13 <pre> graph TD 86[CONTROL A DEVICE] --> 88[GENERATE A CONTROL SIGNAL WHICH INCLUDES CHECKS TO VERIFY THE OPERATION OF THE DEVICE] 88 --> 90[CONTROL THE DEVICE USING THE CONTROL SIGNAL] 90 --> 92[PERFORM VERIFICATION OF OPERATION OF THE DEVICE] 92 --> 94[IF DEVICE OPERATION CANNOT BE VERIFIED: A) FOR SAFE STATE OFF DEVICES, REMOVE POWER TO ALL SUCH DEVICES BY CONTROLLING THE CONDITIONED BUSES B) FOR SAFE STATE ON DEVICES, APPLY POWER TO ALL SUCH DEVICES BY CONTROLLING THE INVERSE CONDITIONING BUSES] </pre> FIG. 14					
주요 내용	활성상태와 생성된(generated) 1차(primary) 및 2차(secondary) 코드를 이용하여 결함을 모니터링하는 마이크로프로세서를 갖는 전자장비의 결함-안전 마이크로프로세서 기반 제어와 모니터링 시스템					
주요 청구항	1. A fail-safe system for monitoring of at least one device, each of said at least one device having at most two pairs of positive and negative output points and at most two pairs of positive and negative inputs, said fail-safe system comprising: a processor, operating using a program, for generating a primary code comprising at least one predefined interval of time during which a first input signal is positive in polarity and at least another predefined interval of time during which the first input signal is negative in polarity, for applying the primary code to the output points, for detecting a first response signal at the input points, and for comparing the first response signal with the primary code to detect an active state of said at least one device, wherein the processor generates at least one secondary code, each of said at least one secondary code comprising a predefined interval of time selected from the group consisting of:					
법적상태 (회피전략)	- 본 특허는 2010년 이후로 연차료를 납부하지 않아 자유기술로 공개되었음 - 현재는 특허권이 유지되고 있지 않지만 피인용건수가 10건으로 비교적 높아, 관련 분야 연구를 진행함에 있어 해당 특허기술을 참고하여 기술을 개발하는 것이 바람직할 것으로 보임					

5	기술 분류	C. 공통플랫폼	특허번호 (출원번호)	US1994212885A	특허번호 (공개번호)	US5483639A
출원인	DAIMLER BENZ AG	출원일	1994-03-14	공개일	1996-01-09	
발명의 명칭	Device for detecting transmission errors in balanced two-wire bus lines and two-bus interfaces					
대표도면						
주요 내용	평형 2-와이어 버스 라인과 2-와이어 버스 인터페이스 모니터가 각각의 와이어 전위와 기준값을 비교하여 비교 결과의 각 차이로부터 리셋 펄스를 생성하는 장치					
주요 청구항	1. Device for monitoring balanced two-wire bus lines and two-wire bus interfaces for serial data transmission, the bus lines and the bus interfaces having first and second line conductors that change their polarity in antiphase in the normal state, the device comprising: first, second and third comparison means, the first comparison means having a positive input operationally connected to the first bus conductor and a negative input connected to a reference potential ($V_{CC}/2$); the second comparison means having a negative input connected to the second bus conductor and a positive input connected to said reference potential ($V_{CC}/2$); and the third comparison means having an input side connected to the first and second bus conductors; a first shift register or counter having a clock input operationally connected to an output of the first comparison means; a second shift register or counter having a clock input operationally connected to an output of the second comparison means; means for processing signal edges to form pulses, the means for processing being connected downstream of the third comparison means and having an output connected to reset inputs of the shift registers or counters;					
법적상태 (회피전략)	- 본 특허는 1996년 등록되었으나 2004년 이후로 연차료를 납부하지 않아 자유기술로 공개되었음 - 현재는 특허권이 유지되고 있지 않지만 피인용건수가 8건으로 비교적 높아, 관련 분야 연구를 진행함에 있어 해당 특허기술을 참고하여 기술을 개발하는 것이 바람직할 것으로 보임					

(2) 주요 핵심특허 심층 분석 (우수성 분석)

- 특허청 발명진흥회의 특허분석 평가시스템(SMART3)를 활용하여, 분석 가능한 특허 중에서 피인용수가 가장 높은 특허인 공개번호 US5504860A에 대해 상세 분석한 결과, 종합 평가점수가 68.4점으로 B로 평가됨

평가결과 세부내용

- 권리성 21.6점, 기술성 16.6점, 활용성 30.1점으로 물리/재료분야의 평균인 권리성 25.3점, 기술성 15.6점, 활용성 29.4점에 비하여, 기술성·활용성에서 높게 평가되었으며 권리성은 낮게 평가되었음
- 독립 청구항이 세밀하게 작성되어 있지만, 권리의 제한 어구는 적은 편이며, 관련된 해외 특허 출원이 15개가 있어 해외 특허망을 형성하고 있고, 총 피인용수가 13회로 다른 후출원 특허로부터 다수의 인용을 받고 있음

평가지표	점수	등급	대분류(물리/재료)			중분류(기구2)			소분류(측정)		
			백분위(%)	평균	표준편차	백분위(%)	평균	표준편차	백분위(%)	평균	표준편차
권리성 (40점)	21.6	C	96.9	25.3	2.2	97.0	25.5	2.2	97.4	25.5	2.2
기술성 (20점)	16.6	AA	4.8	15.6	0.6	4.4	15.6	0.6	5.3	15.6	0.6
활용성 (40점)	30.1	AA	9.8	29.4	0.9	9.7	29.4	0.8	10.7	29.4	0.8
총점 (100점)	68.4	B	74.3	70.3	2.8	76.2	70.4	2.8	81.2	70.8	2.8

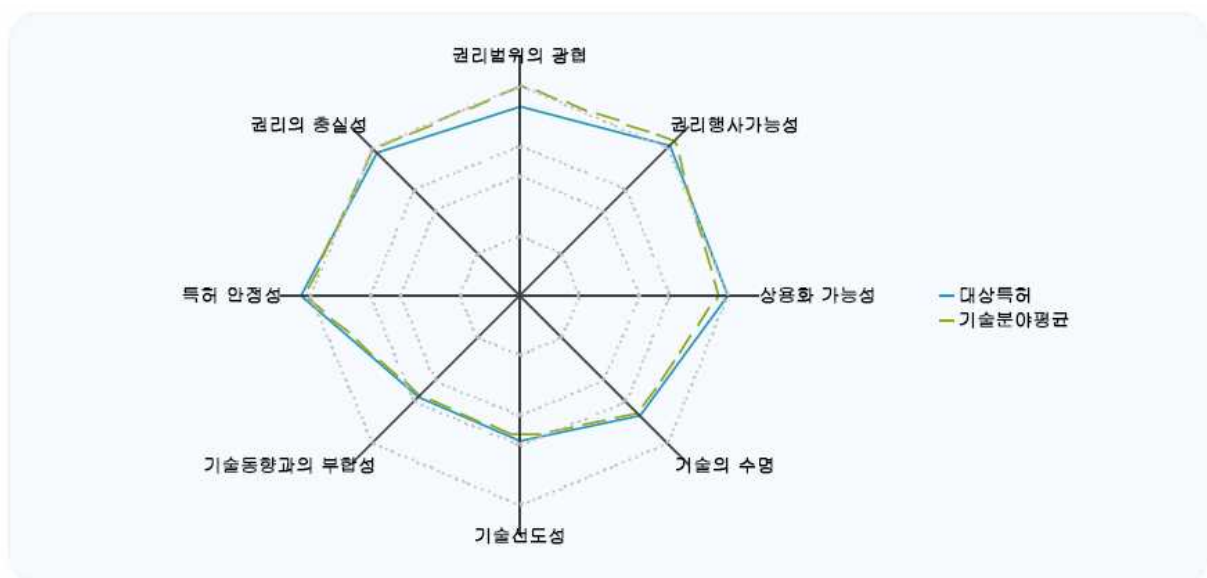
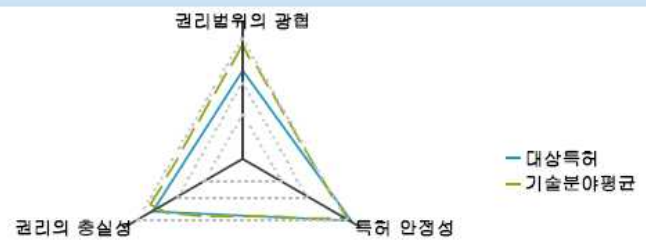


그림2-8. 핵심특허(US5504860A) 평가결과

■ 권리성 (40점)

중분류	점수	평균
권리범위의 광협	11.6	15.0
권리의 충실성	13.7	14.6
특허 안정성	-3.6	-4.3
총점	21.6	25.3



권리성에 대한 평가점수는 "21.6"점으로 "C"등급으로 평가되었습니다. "특허 안정성"의 평가점수가 -3.6점으로 상대적으로 권리성에 기여하고는 있으나, 다른 부분은 상당히 부족합니다. 본 특허는 청구항 수가 7개로 많아 다양한 기술적 관점을 권리화하였으며, 미국 내에 유사한 패밀리 특허가 1건이 있습니다.

* 평가 지표로서의 특허의 권리성이란 권리로서의 우수한 특허권이 가져야 할 다양한 속성(권리의 광협, 권리의 완성도 및 권리가 처한 법률적 무결성 등)의 충족 정도를 의미합니다. 특허권의 보호범위가 넓고 다면적이며, 권리 행사에 제약이 없는 특허는 권리성이 우수한 특허라고 할 수 있습니다.

■ 기술성 (20점)

중분류	점수	평균
기술동향과의 부합성	3.8	3.7
기술선도성	4.4	4.0
기술의 수명	8.4	7.9
총점	16.6	15.6

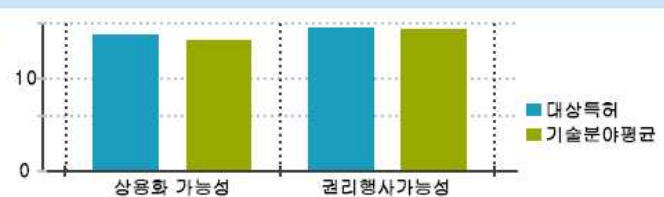


기술성에 대한 평가점수는 "16.6"점으로 "AA"등급으로 평가되었습니다. "기술선도성"의 평가점수가 4.4점, "기술의 수명"의 평가점수가 8.4점으로 높게 평가되었습니다. 본 특허는 총 피인용수가 13회로 다른 후출원 특허로부터 인용을 받고 있으며, 본 특허의 출원일로부터 최대6984일 뒤진 후출원으로부터 인용되고 있으며, IPC수가 6개로 다양한 기술적 관점을 포함하고 있습니다.

* 평가 지표로서의 특허의 기술성이란 특허에 개시된 기술이 해당 기술 분야 특허군에서 상대적 우위를 차지하기 위해 가져야 할 다양한 속성의 충족 정도를 의미합니다. 특허에 개시된 기술이 특허 동향과 부합되면서, 자기 또는 타인의 특허와의 관계에서 선도적이고, 지속적으로 사용될 수 있는 특허는 기술성이 우수한 특허라고 할 수 있습니다.

■ 활용성 (40점)

중분류	점수	평균
상용화 가능성	14.7	14.1
권리행사가능성	15.4	15.2
총점	30.1	29.4



활용성에 대한 평가점수는 "30.1"점으로 "AA"등급으로 평가되었습니다. "권리행사가능성"의 평가점수가 15.4점으로 긍정적으로 작용하였으나, 전체적으로 활용성이 낮은 것으로 평가되었습니다. 본 특허는 권리자 변동이 3회 있어, 상용화 가능성이 높다고 할 수 있으며, 또한 최종 양수인이 권리를 행사할 가능성도 배제할 수 없으며, 관련된 해외 특허 출원이 15개가 있어 해외 특허망을 형성하고 있습니다. 참고적으로, 권리의 제한 어구는 적은 편이나, 독립 청구항이 세밀하게 작성되어 있어, 타인이 본 특허를 회피하여 상용화할 가능성을 배제할 수 없으며, 본 특허가 유사한 후행 특허에 대해 선행기술로 사용되기도 하였으나, 후행특허가 13건 등록된 점에 비추어 보면, 후행 특허가 본 특허를 회피하였는지 면밀히 검토할 필요가 있습니다.

* 평가 지표로서의 특허의 활용성이란 특허에 포함된 기술이 널리 활용되기 위해 가져야 할 다양한 속성의 충족 정도를 의미합니다. 특허에 포함된 기술을 타인이 회피하기가 쉽지 않고, 그에 따라 자기 또는 타인에 의해서 널리 활용되어, 특허권자가 권리를 행사하는데 지장이 없을 때, 활용성이 높은 특허라고 할 수 있습니다.

(3) 주요 핵심특허 인용도 분석 (사례)

- 한국과학기술정보연구원(KISTI) 경쟁분석서비스(COMPAS)의 특허인용 분석시스템을 활용하여 피인용수가 높은 특허(공개번호 US6381506B1)의 인용도 분석을 통해, 최근 이 분야 특허의 출원추이와 기술경쟁 현황을 살펴보고자 함

※ (분석대상 선정방식)

: KISTI COMPAS는 미국등록 특허를 대상으로 유사특허·인용도분석 등 경쟁정보를 제공하고 있음. KISTI COMPAS에서 제공하는 미국특허 중 피인용도가 가장 높은 특허(US6381506B1 ; Fail-safe microprocessor-based control and monitoring of electrical devices)를 분석대상으로 하였음 (US5561762A, US5504860A 등은 분석 결과가 제공되지 않음)

- US6381506B1 특허는 1999년에 출원하여, 2002년 공개된 특허로서, 청구항 27개, 1단계 인용 34건, 1단계 피인용 10건을 나타내는 특허임. 인용·피인용 관계를 3단계까지 확대하면, 총 1,813건의 특허와 직·간접적으로 유사성을 나타내고 있음

표2-3. US6381506B1 특허 인용현황

구 분	Backward (인용)				Forward(피인용)			
	1단계	2단계	3단계	합 계	1단계	2단계	3단계	합계
특허건수	34	317	1363	1714	10	46	43	99

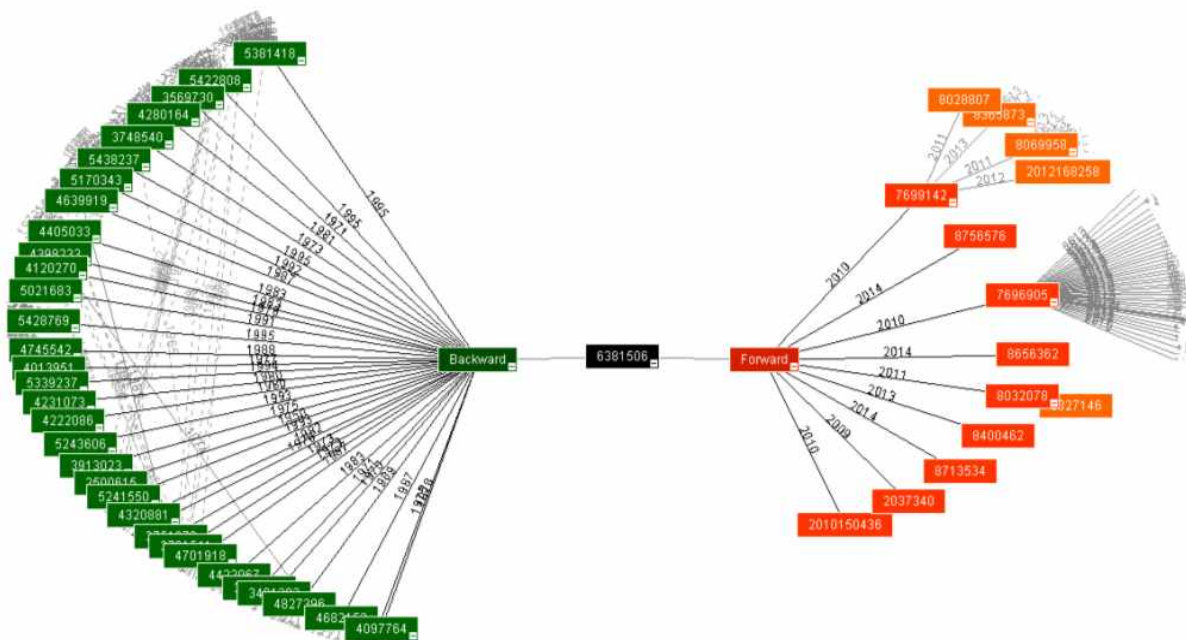


그림2-9. US6381506B1 특허인용맵

- US6381506B1 특허는 2009년 이후 피인용도가 급격히 증가하고 있는 특허로서, 최근 관심이 확대되고 있는 주요 특허로 판단할 수 있음

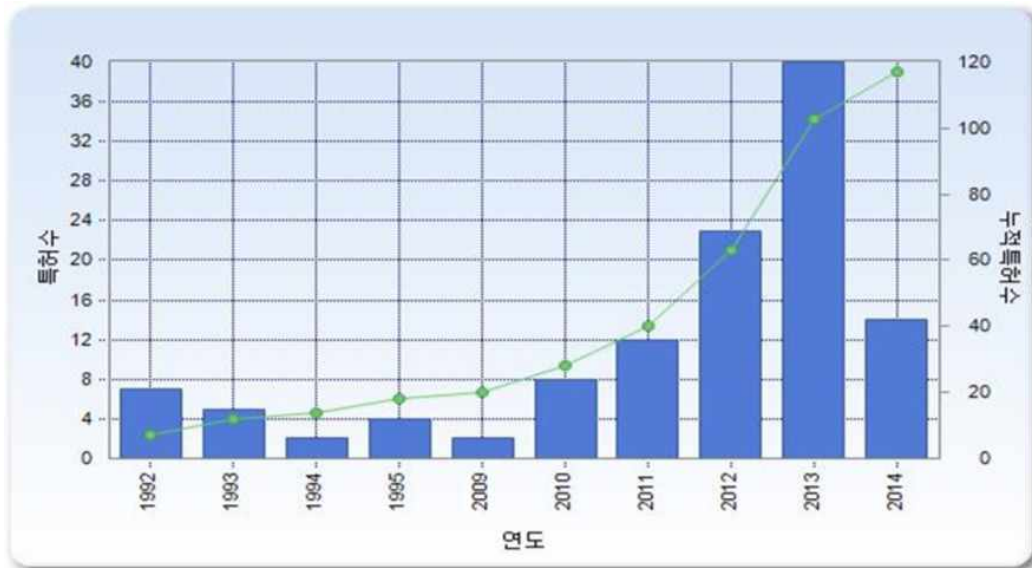


그림2-10. 연도별 인용특허 분포

- US6381506B1 특허를 인용·피인용한 출원인들을 살펴보면, IBM(International Business Machines Corporation), Hitachi, BELL TELEPHONE, Honeywell 등 철도분야·신호통신 분야 기관들이 많이 있으며, 특허법인으로 보여지는 Nant Holdings IP 등도 있음. 이들 출원인을 통해, 이 기술분야 글로벌 경쟁기관들을 살펴볼 수 있을 것임

표2-4. US6381506B1 인용·피인용 특허 출원인 현황

번호	출원인	특허 수
1	International Business Machines Corporation	44
2	Hitachi, Ltd.	39
3	Nant Holdings IP, LLC	33
4	Westinghouse Electric Corp.	20
5	BELL TELEPHONE LABORATORIES, INCORPORATED	19
6	Honeywell Inc.	18
7	WESTINGHOUSE ELECTRIC CORPORATION	18
8	INTERNATIONAL BUSINESS MACHINES CORPORATION	17
9	General Electric Company	16
10	WESTINGHOUSE AIR BRAKE COMPANY	16

제 3 절 논문분석

1. 논문분석 범위

구 분	분석 기준
논문검색 DB	Web of Science, Thomson Innovation
분석구간	1990.01.01.~2014.07.10.
검색범위	Title, Abstract

2. 논문기술 동향

가. 연도별 논문 발표 추이 및 주요 등재저널 동향

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 분야 논문 추이를 살펴 보면, 1994년부터 현재까지 총 61건의 관련 논문이 발표되고 있으며, 일부 증감이 있지만 대체적으로 2009년대 이후 증가하는 추세를 나타내고 있음
- 관련 분야 논문은 모두 47개의 저널에 다양하게 게재되어 있으며, 특히 Reliability Engineering & System Safety에 B. 안전측 동작설계(Fail-Safety Design) 기술 분야와 관련된 논문이 8편으로 가장 많이 게재되어있음



그림2-11. 연도별 논문 발표 추이 및 주요 등재 저널

나. 주요 핵심논문 분석

● Stack JR 등이 2004년 IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS 게재한 Bearing fault detection에 관한 논문이 36건으로 가장 많이 인용되었음

표2-5. 주요 피인용 논문 현황

번호	논문제목	저널명	발표연도	피인용수
1	Bearing fault detection via autoregressive stator current modeling	IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS	2004	36
2	Multiple-failure signal validation in nuclear power plants using artificial neural networks	NUCLEAR TECHNOLOGY	1996	24
3	Failure rates of leads, pulse generators, and programmers have not diminished over the last 20 years: Formal monitoring of performance is still needed	PACE-PACING AND CLINICAL ELECTROPHYSIOLOGY	1996	22
4	Modeling the effects of combining diverse software fault detection techniques	IEEE TRANSACTIONS ON SOFTWARE ENGINEERING	2000	20
5	A formal verification environment for railway signaling system design	FORMAL METHODS IN SYSTEM DESIGN	1998	17
6	A prediction tool for real-time application in the disruption protection system at JET	NUCLEAR FUSION	2007	17
7	A design condition for incorporating human judgement into monitoring systems	RELIABILITY ENGINEERING & SYSTEM SAFETY	1999	14
8	Recognition of Fault Transients Using a Probabilistic Neural-Network Classifier	IEEE TRANSACTIONS ON POWER DELIVERY	2011	14
9	Adaptive Kalman filter and neural network based high impedance fault detection in power distribution networks	INTERNATIONAL JOURNAL OF ELECTRICAL POWER & ENERGY SYSTEMS	2009	11
10	High impedance fault detection in power distribution networks using time-frequency transform and probabilistic neural network	IET GENERATION TRANSMISSION & DISTRIBUTION	2008	11
11	Failure mode and effect analysis for safety-critical systems with software components	COMPUTER SAFETY, RELIABILITY AND SECURITY, PROCEEDINGS	2000	10

● 핵심논문 세부내용

- 논문제목 : Bearing Fault Detection via Autoregressive Stator Current Modeling
- 저널명 : IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, VOL. 40, NO. 3, MAY/JUNE 2004
- 저자 : Jason R. Stack, Thomas G. Habetler, and Ronald G. Harley
- 주요 내용 : Stator current를 통한 developing bearing fault를 감지 방법 제시

740

IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, VOL. 40, NO. 3, MAY/JUNE 2004

746

IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, VOL. 40, NO. 3, MAY/JUNE 2004

Bearing Fault Detection via Autoregressive Stator Current Modeling

Jason R. Stack, Member, IEEE, Thomas G. Habetler, Fellow, IEEE, and Ronald G. Harley, Fellow, IEEE

Abstract—This paper proposes a method for detecting developing bearing faults via stator current. Current-based condition monitoring offers significant economic savings and implementation advantages over vibration-based techniques. This method begins by filtering the stator current to remove most of the significant frequency content unrelated to bearing faults. Afterward, the filtered stator current is used to train an autoregressive signal model. This model is first trained while the bearings are healthy, and a baseline spectrum is computed. As bearing health degrades, the modeled spectrum deviates from its baseline value; the mean spectral deviation is then used as the fault index. This fault index is able to track changes in machine vibration due to developing bearing faults. Due to the initial filtering process, this method is robust to many influences including variations in supply voltage, cyclical load torque variations, and other nonbearing fault sources. Experimental results from ten different bearings are used to verify the proficiency of this method.

Index Terms—Bearings (mechanical), condition monitoring, fault diagnosis, motor current signature analysis (MCSA), vibration.

I. INTRODUCTION

ELECTRIC machines are used in a continuously expanding variety of applications. In many applications, electric machine failures are costly and result in significant process down time. When an electric machine fails, a bearing fault is the most likely cause. While the vast majority of bearing faults are detected via vibration-based techniques, the cost of obtaining these vibration measurements is relatively high. In many applications, stator current is routinely monitored for protection purposes (overcurrent, overload, ground current, etc.). In these instances, a stator-current-based condition monitoring scheme is inexpensive to implement and requires no additional sensors, wiring, etc. In other instances, it is often preferable and cost effective to add current sensors at the electrical supply rather than attaching a vibration sensor directly to the machine. This motor current-based bearing condition monitoring attractive and desirable in many applications.

Paper BCDSD-04-008, presented at the 2003 Industry Applications Society Annual Meeting, Salt Lake City, UT, October 12–16, and approved for publication in the IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS by the Electric Machines Committee of the IEEE Industry Applications Society. Manuscript received for review July 15, 2003 and revised for publication March 13, 2004. J. R. Stack was with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA. He is now with the Signal and Image Processing Branch, Naval Surface Warfare Center, Panama City, FL 32407 USA (e-mail: jason.stack@nswc.navy.mil). T. G. Habetler and R. G. Harley are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA. (e-mail: habetler@ece.gatech.edu; rharley@ece.gatech.edu). Digital Object Identifier 10.1109/TIA.2004.827797

0093-9994/04/\$20.00 © 2004 IEEE

The main disadvantage of stator-current-based bearing fault detection is that the effects of a bearing fault are often subtle and difficult to predict. Therefore, this paper proposes a modeling technique where the changes in the stator current spectrum are compared to a baseline spectrum, rather than searching for specific fault components. These changes in spectral content are then used to identify developing faults. Before this modeling technique is applied, the stator current is filtered to remove the significant nonbearing fault components such that only changes in bearing health are tracked. For the following discussion, only line-connected electric machines are considered.

II. STATOR CURRENT SPECTRAL CONTENT

The origin of virtually all significant frequency components in the stator current is well understood; thus, the removal of those components unrelated to bearing faults is straightforward. Furthermore, the presence of most of the significant frequency components in the stator current can be predicted *a priori* with little more knowledge than the speed of the machine. In general, this intimate understanding of the stator current spectral content facilitates the identification of most electric machine faults once their signatures become significant. However, bearing fault signatures in particular are often subtle, difficult to predict, and difficult to detect. This section reviews the origin of most of the significant, predictable frequency components in the stator current.

From three-phase circuit theory, the current flowing in an electric machine will contain only odd harmonics provided the phase impedances and voltages are balanced. Furthermore, the triplen harmonics (i.e., the third harmonic and its integer multiples) are not present in this balanced circuit. However, upon examination of the stator current spectrum from an actual machine, it is apparent that the fundamental frequency component and all of its harmonics are present in the frequency spectrum.

This apparent discrepancy between circuit theory and observed machine data is due to two main reasons. First, virtually all voltage sources (three-phase or single-phase) contain some degree of asymmetry from one half-cycle to the next. The amount of asymmetry in a sinusoidal voltage source fluctuates in time as a direct result of changes in the various, nonlinear loads drawing power from that source. Therefore, since the voltage at the machine terminals is not a pure sinusoid, the even multiples of the fundamental are present, albeit at lesser amplitudes compared to the odd harmonics. Second, all electric machines contain some amount of inherent asymmetries. These asymmetries are both electrical (e.g., differences in stator winding impedances from phase to phase) and mechanical

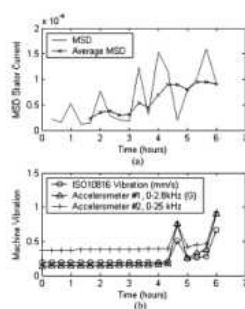


Fig. 8. The MSD for bearing B2 operated at a 100% load level. (a) The average MSD index indicates an upward trend as the bearing begins to fail. (b) The high load level attenuates the increase in machine vibration until the fault enters an advanced stage. This bearing catastrophically fails after the sixth hour.

stage, which is illustrated in Fig. 8. In Fig. 8(a), the MSD exhibits a high variance throughout the trial, but the average MSD exhibits an upward trend as the bearing begins to fail. While this increase in average MSD is not as pronounced as with the data sampled at the lower load levels, the average MSD still reflects the increase in machine vibration.

One of the main reasons for this decrease in sensitivity is that the magnitude of the harmonics of the fundamental increase substantially at the higher load levels. Since the dynamic range of the sampling hardware must accommodate these components, there are fewer bits left to resolve the subtle fault information. Consequently, the MSD and the average MSD experience a decrease in sensitivity as the load level increases toward 100%. It is possible that increasing the sampling hardware from 12-bit resolution to 16-bit resolution could uncover fault information that has been lost due to finite precision sampling effects. It is also possible that other electric machines with different design, power ratings, or configurations might allow more fault information to be passed into the stator current at the higher load levels. Even with these effects, the average MSD is able to indicate developing bearing faults at load levels up to 100%.

The results discussed for these six bearings are indicative of all results obtained during this research from the application of the MSD fault index. In all, the MSD was applied to ten bearings. For all of these bearing failures, an increase in machine vibration is accompanied by an increase in the MSD fault index or in the average MSD. Therefore, the MSD successfully identifies the development of the faults in all of these bearings.

VI. CONCLUSIONS

This research presents a method for performing stator-current-based bearing condition monitoring. To introduce this method, a review of the sources of significant frequency components observed in a typical stator current spectrum was presented. This knowledge allowed the significant nonbearing fault components to be removed from the stator current. The sources removed included supply voltage fluctuations, cyclical load torque variations, and other nonbearing fault sources. The need for an efficient and compact spectral representation was then motivated, and the AR spectrum estimation technique was reviewed to fill this need.

A bearing fault index developed by this research and based on the mean spectral deviation was then introduced. In this method, the frequency content of the filtered stator current was modeled. A baseline or reference model was compared while the bearings were healthy. As the bearing health degraded, the deviation in spectral content from its baseline measurement increased. This increase in spectral deviation was then used as the fault index.

From the ten sets of experimental results, the following conclusions are drawn. The MSD fault index developed by this research is a reliable indicator of the increase in machine vibration resulting from a developing bearing fault. While the MSD fault index is most sensitive at low load levels, it also tracks changes in vibration as the load level increases. However, computing the average value of several MSD measurements provides more salient fault information at these increased loads. In some instances, the MSD exhibits a high variance while the machine vibration is relatively constant. This is most likely due to changes in the stator current that are neither removed by the filtering process nor modeled by the AR spectrum.

The experimental results presented in this discussion were chosen to represent the full range of machine load levels and illustrate how the MSD fault index performs under the various load conditions. Specifically, for bearings operated at a 50% load level and below, a 50% increase in machine vibration caused an increase in the MSD fault index ranging from 100% to 400%. For bearings operated at loads above 50%, an increase in machine vibration of 50% typically corresponded to a 50% increase in the average MSD reading. Presently, there are no current-based bearing condition monitoring schemes employed in industry. Therefore, the successful development and deployment of this method is a significant contribution to the practice of current-based electric machine condition monitoring.

REFERENCES

- [1] R. R. Schoen and T. G. Habetler, "Effects of time-varying loads on motor fault detection in induction machines," *IEEE Trans. Ind. Appl.*, vol. 31, pp. 905–906, July/Aug. 1995.
- [2] G. B. Klewin and J. J. Stok, "Reducing motor fault detection via passive current monitoring," in *Proc. Int. Conf. Electric Machines*, 1999, pp. 15–17.
- [3] J. R. Cameron, W. T. Thomson, and A. B. Dow, "Vibration and current monitoring for detecting large eccentricity in large induction motors," *Proc. Inst. Elect. Eng.*, pt. B, vol. 135, pp. 155–163, 1988.
- [4] W. Delort, "Broken bar in squirrel cage motor of an induction motor, Part I: Description by asynchronous fault currents," *Arch. Elektrotech.*, vol. 67, pp. 91–99, 1984.

그림2-12. 핵심논문 발표현황

제 4 절 시장분석

1. 시장현황

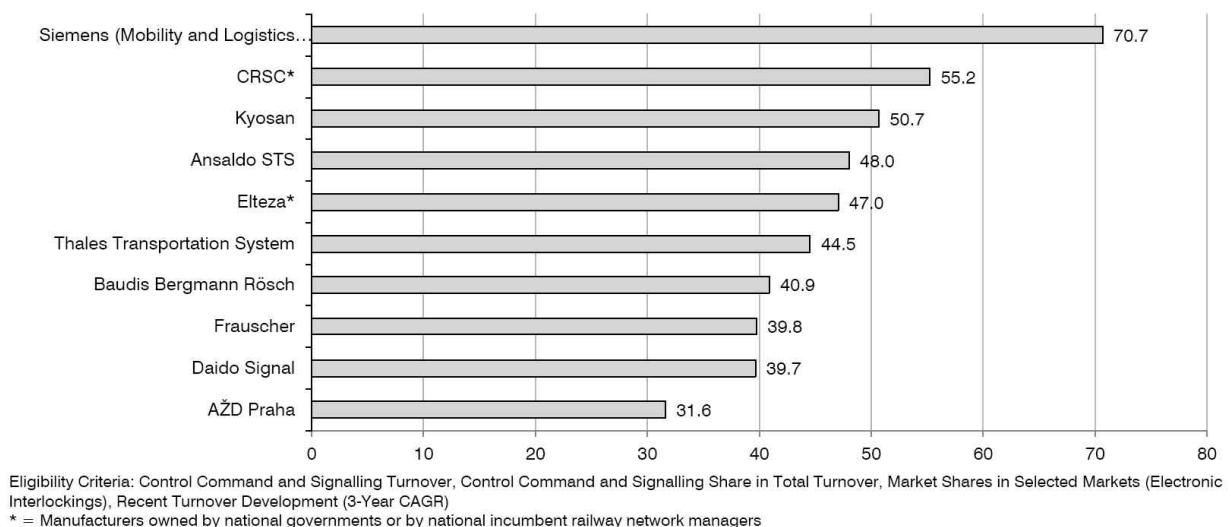
Overview of Top Manufactures

철도 신호제어에 대한 5대 글로벌 기업 중에서, Siemens, Ansaldo, Thales 등 3개 기업이 Top 10에 들어가 있음. Alstom과 Bombardier는 각각 10위와 15위 수준을 나타냄. 이외에도 중국 CRSC, 러시아 Elteza, 체코 AZD Paraha 등의 국영기업, 일본 Kyosan, Daido Signal이 높은 경쟁력을 나타냄. Siemens가 17억 유로/年 이상의 신호제어 매출규모를 보이는 등 가장 높은 경쟁력을 갖는 것으로 판단됨. 한국 LS산전은 1.2억 유로/年の 매출을 보임

(※ 출처 : SCI Verkehr GmbH (2014), Worldwide Manufactures of Rail Infrastructure 2014)

● ①신호제어 매출액 규모(40%), ②전체 매출액 대비 신호제어매출 비중(30%), ③핵심품목(Electronic interlockings) 시장점유율(20%), ④최근 3년간 매출액 평균증가율(10%)을 가중 평균하여 경쟁력 지수를 도출하고, 상위 10개 글로벌 기업의 순위를 제시하면 아래 그림과 같음. Siemens의 경쟁력이 월등히 높게 나타남

(※ 출처 : SCI Verkehr GmbH (2014), Worldwide Manufactures of Rail Infrastructure 2014)



※ ①~④항목별 1위 기업을 만점으로 하여 각 기업별 상대점수를 부여하고, 항목별 가중치에 따라 합산하여 경쟁력지수 도출
 그림2-13. Control Command and Signalling - Top 10 Manufactures

표2-6. Control Command and Signalling : Results for the Top 20 Manufacturers

Rank	Criteria:	Control Command and Signalling Turnover		Control Command and Signalling Turnover Share in Total Turnover		Market Shares in Core Product Markets [2]	Recent Turnover Development		Total Score	
		[EUR million]	Score	[%]	Score	Score	3-Year CAGR [%]	Score	Before Extrapolation [4]	After
	Weighting [3]:	none	40%	none	30%	20%	none	10%	none	none
1.	Siemens (Mobility and Logistics)	1 710e	40.0	26e	7.8	20.0	+1.5	2.9	70.7	70.7
2.	CRSC [1]	500e	11.7	100	30.0	8.0	–	–	49.7	55.2
3.	Kyosan	500e	11.7	91e	27.3	0.0	–3.7	1.6	40.5	50.7
4.	Ansaldo STS	760	17.8	61	18.3	9.6	–0.9	2.3	48.0	48.0
5.	Elteza [1]	330	7.8	100	30.0	2.4	+17.5	6.9	47.0	47.0
6.	Thales Transportation Systems	890e	20.9	15e	4.5	16.0	+2.4	3.1	44.5	44.5
7.	Baudis Bergmann Rösch	25	0.6	100	30.0	0.8	+28.0	9.5	40.9	40.9
8.	Frauscher	35	0.8	100	30.0	0.8	+22.6	8.1	39.8	39.8
9.	Daido Signal	210	4.9	100	30.0	0.8	n/a	0.0	35.7	39.7
10.	Alstom Transport	820e	19.2	15e	4.5	5.6	–0.9	2.3	31.6	31.6
11.	AŽD Praha	140e	3.2	85e	25.5	0.8	–1.6	2.1	31.6	31.6
12.	Kapsch CarrierCom	130e	3.1	70e	21.0	0.0	–6.9	0.8	24.9	31.1
13.	Nippon Signal Co. Ltd.	300e	7.0	65e	19.5	1.6	+1.3	2.8	30.9	30.9
14.	Mont-Ele	10e	0.2	80e	24.0	0.0	–8.4	0.4	24.6	30.7
15.	Bombardier Transportation	700e	16.3	11e	3.3	6.4	–	–	26.0	28.9
16.	MERMEC	60e	1.3	70e	21.0	0.0	–7.2	0.7	23.0	28.8
17.	GE Transportation	650e	15.3	15e	4.5	0.8	+18.5	7.1	27.8	27.8
18.	Prysmian	220e	5.2	15e	4.5	0.0	+47.8	10.0	19.7	24.6
19.	LS Industrial Systems	120e	2.9	30e	9.0	1.6	+8.4	4.6	18.1	18.1
20.	Hitachi	500e	11.6	4e	1.2	1.6	+4.3	3.6	18.0	18.0
[1] = Manufacturers owned by national governments or by national incumbent rail infrastructure managers										
[2] = Core Product Market: Electronic interlockings.										
[3] = Weighting: In order to reflect the different significance of the different criteria used, a comparative weighting between them was established. It occurs when the relative assessment of the respective values, which ranges between 100.0 for the best and 0.0 for the worst of them, is transferred into score points. On this occasion, the respective weighting is multiplied. Thus, e.g. valuation of 100.0 for the best track system turnover (see Siemens) results in 40.0 score because infrastructure turnover is weighted 40% of all criteria.										
[4] = Extrapolation: In cases where data was not available, or core product market shares not existent, the respective criteria or market shares have been omitted and the remaining criteria's' or market shares' weighted values taken as the total score.										
e = estimated; – = unknown										

Market Shares in the Core Product Market

- 신호제어 부문 핵심품목으로서, 전자연동장치(Electronic Interlocking)가 있음. 전자연동장치의 Top 5 제작기업을 살펴보면, Siemens, Thales, Ansaldo의 순으로 나타남. Siemens를 포함한 5대 기업의 매출액 비중이 전체 세계시장의 75%를 점유하는 과점 시장구조임

(※ 출처 : SCI Verkehr GmbH (2014), Worldwide Manufactures of Rail Infrastructure 2014)

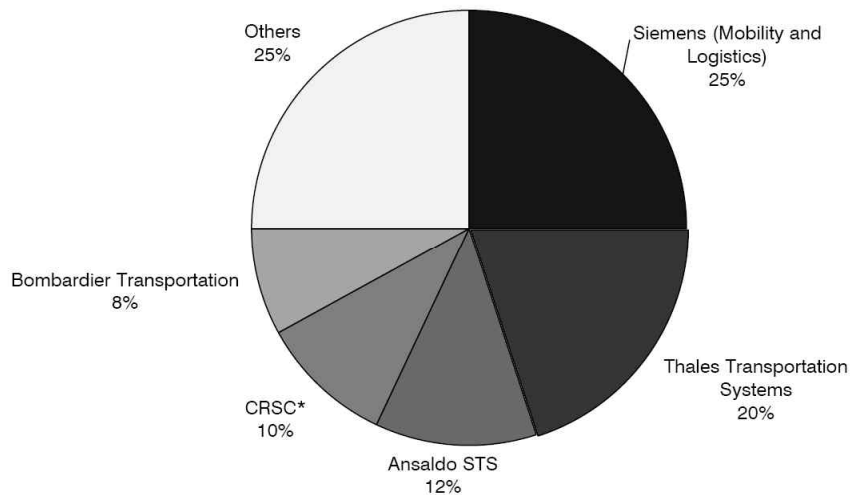
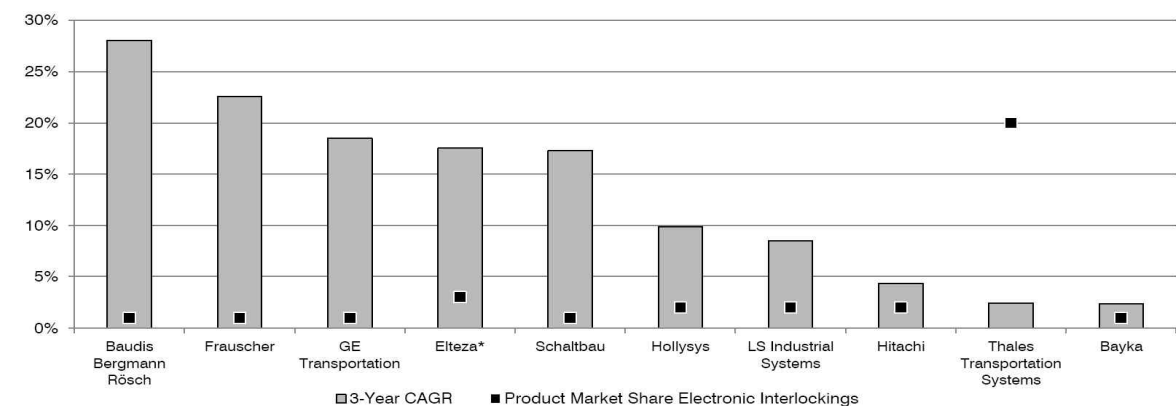


그림2-14. Control Command and Signalling : Electronic Interlocking - Market Shares

- 전자연동장치에 대한 최근 3년간 평균 매출성장율이 높은 글로벌 기업을 살펴보면, 독일 Baudis Bergmann Rosch, 독일 Frauscher가 20%가 넘는 높은 성장을 보이고 있음. 한국 LS산전은 최근 3년간 8.4%의 높은 성장을 보이고 있음

(※출처 : SCI Verkehr GmbH (2014), Worldwide Manufactures of Rail Infrastructure 2014)



The selection has been restricted to manufacturers for which there is sufficient data available.
 * = Manufacturers owned by national governments or by national incumbent railway network managers

그림2-15. Control Command and Signalling : Electronic Interlocking
 - Top Market Players by 3-Year CAGR and Product Market

서유럽 도시철도 CBTC 시장

- 2011년 현재 유럽 도시철도 CBTC 시장은 성장기(Growth)에 있으며 총 350km 구간에서 운영되고 있음. 시장 규모는 2011년 9.9억 유로에서 2021 까지 年 평균 14.4%씩 높은 성장을 통해 35.9억 유로 수준까지 증가할 것으로 예측됨. CBTC 구축에 km당 120만 유로 ~470만 유로가 소요되며, 평균 240만 유로가 소요되는 것으로 추정됨

(※ 출처 : Strategic Analysis of CBTC in the Western European Urban Rail Market, Frost & Sullivan, 2013)

MEASUREMENT NAME	MEASUREMENT	TREND
Market Stage (Nascent, Growth, Mature)	Growth	—
Market Value	€993.0 Million	▲
Market Volume (Total Length Operational, 2011)	350 km	▲
Average Price per km*	€2.4 Million	▲
Market Value at End of Forecast Period (2021)	€3.59 Billion	▲
Base Year Market Growth Rate	N/A	—
Compound Annual Growth Rate (CAGR) Total Operational Network Length, 2011–2021	14.4%	—
Market Concentration (% of base year market controlled by top three competitors)	78.3%	▲
Number of Competitors (active market competitors from 2001–2011)	6	▼
Average R&D Spend by Product	N/A	—

TREND Decreasing Stable Increasing
 ▼ ● ▲

*Signalling has a very custom approach. Each contract has to be tailored accounting for various factors. CBTC prices vary from €1.2 to €4.7 Million per km. Hence we assume average cost of €2.37 Million per km.
 Note: All figures are rounded. The base year is 2011. Source: Frost & Sullivan

그림2-16. Market Overview : Urban Rail CBTC Market, Western Europe, 2011

- 서유럽에서 무선 기반 CBTC 프로젝트가 급속히 확대될 것으로 예측됨. 2011~2021년 기간 중 총 811.9km의 프로젝트가 완료될 예정인데, 2001~2010년 기간의 100.6km와 비교하면 매우 높은 증가임을 알 수 있음. 이 중, Siemens는 2021년까지 총 10개의 프로젝트로 280km 건설을 통해 시장을 지배할 것으로 예측됨 (※ 출처 : Strategic Analysis of CBTC in the Western European Urban Rail Market, Frost & Sullivan, 2013)

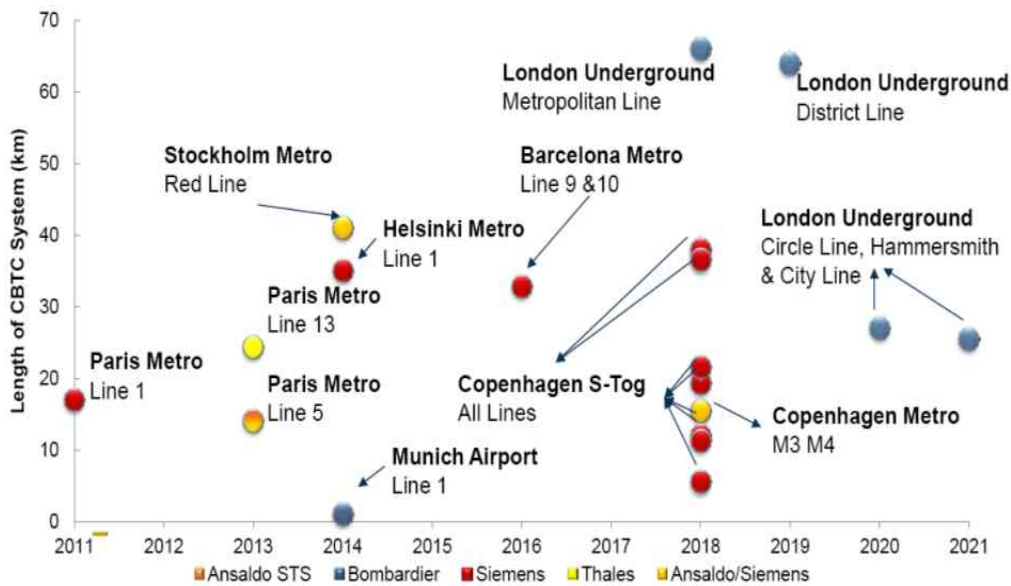


그림2-17. Urban Rail Market : Expected Completion of Radio-based CBTC Projects, Western Europe, 2011~2021

- 서유럽에서 무선 기반 CBTC 네트워크는 2018년까지 500km가 넘게 구축될 것으로 보임. Thales는 파리 지하철 13호선 사업을 통해 무선 기반 CBTC 시장에 진입할 것으로 예측되며, 최근 유럽 경제위기로 인하여 스페인 CBTC 사업은 다소 지연될 것으로 전망됨

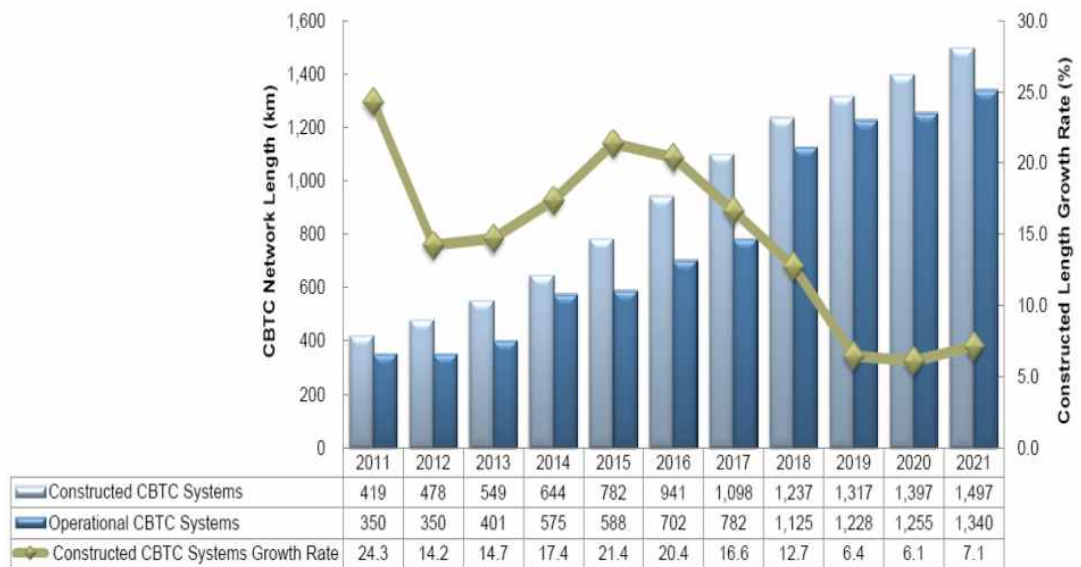


그림2-18. Urban Rail Market : CBTC Network Length Forecast by Stage, Western Europe, 2011~2021

- 서유럽에서 무선 기반 CBTC 네트워크는 2011년에 127km구간에서 운영 중이며, 2021년 까지 年평균 20.2%씩 증가하여 988km에 달할 것으로 전망됨. 2017년에 완성되는 London지하철의 CBTC 프로젝트가 서유럽에서의 Induction-based CBTC의 마지막 시스템이 될 전망이다 (※ 출처 : Strategic Analysis of CBTC in the Western European Urban Rail Market, Frost & Sullivan, 2013)

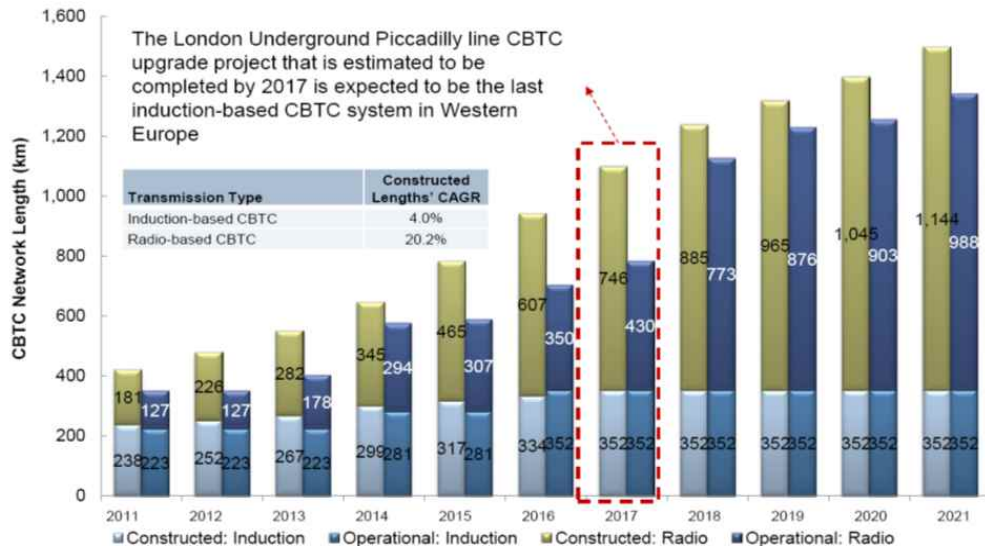


그림2-19. Urban Rail Market : CBTC Network Length Forecast by Transmission Type, Western Europe, 2011~2021

- 서유럽에서 CBTC 수입(Revenue)규모는 유럽 경제상황 등을 고려하여 전망하면, 2021년까지 年평균 8.8~14.8%의 성장을 보일 것이며, 2021년 수입액이 23억~39억 유로 수준까지 확대 될 것으로 예측됨

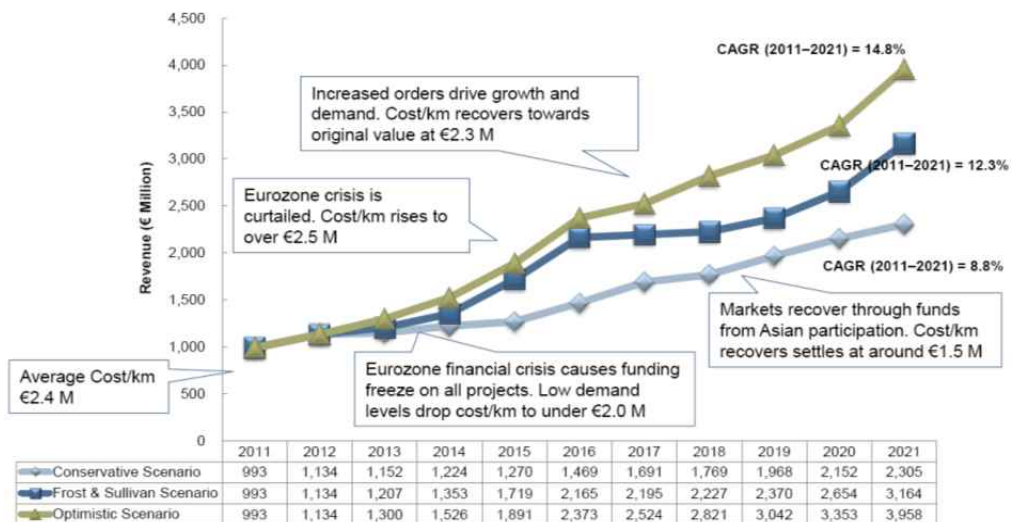


그림2-20. Urban Rail Market : CBTC Revenue Forecast, Western Europe, 2011~2021

Embedded System 시장

- 글로벌 임베디드 시스템(Embedded System) 시장은 2008년 92billion달러에서 2013년 112.5billion달러로 증가하여 년평균성장률(CAGR) 4.1% 증가가 예상됨. 특히 임베디드 하드웨어(H/W) 시장은 2008년 89.8billion달러에서 2013년 109.6billion달러로 증가하여 년평균성장률(CAGR) 4.1% 증가가 예상되고, 임베디드 소프트웨어(S/W) 시장은 2008년 2.2billion달러에서 2013년 2.9billion달러로 증가하여 년평균성장률(CAGR) 5.6% 증가가 예상됨.

(※ 출처 : Embedded Systems: Technologies and Markets, BCC Research, April 2009)

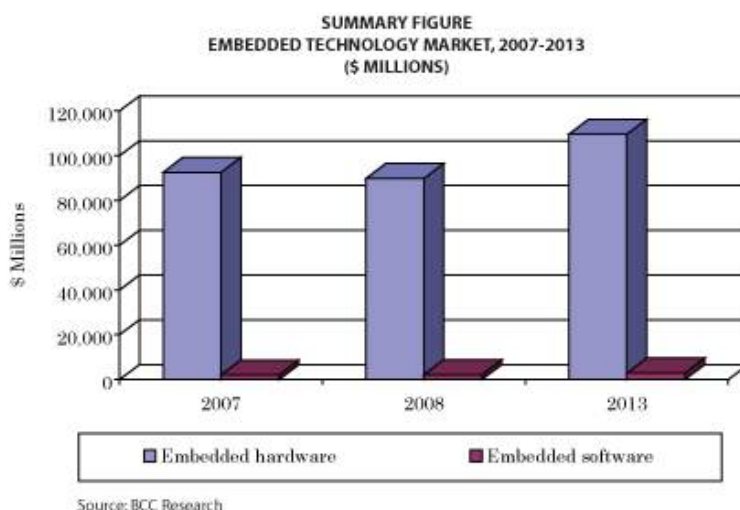


그림2-21. Embedded Technology Market, 2007-2013

- 센서, 액추에이터 및 컨트롤러간의 다중계(redundant), 결함허용(fault-tolerant) 무선연결을 제공하는 통신제품은 센서시장 산업에 포함되어 글로벌 센서 시장을 살펴보면, 2013년 79.5billion달러에서 2014년 86.3billion달러, 2015년 95.3billion달러에 달하고 2020년까지 154.4billion에 달할 것으로 전망함. 2015년부터 2020년까지 년평균성장률(CAGR)은 10.1%성장할 것으로 예상됨.

(※ 출처 : Global Markets and Technologies for Sensors, BCC Research, July 2014)

- 공통플랫폼(Common Platform)은 집중화된 센서와 비디오 데이터를 전송을 위해 데이터베이스 형태로 센서 네트워크를 통해 제공되고 있고, 이러한 공통플랫폼을 프로세싱하는 감시 및 보안 장비의 총 시장 수요는 2011년 80billion달러, 2012년 81.3billion달러에 달하였고 2017년까지 127.6billion달러로 성장하여 2012년부터 2017년까지 년평균성장률 (CAGR) 9.4% 성장할 것으로

예상됨. (※ 출처 : Surveillance and Security Equipment: Technologies and Global Markets, BCC Research, January 2013)

- Embedded S/W는 Application Layer(H/W 작동), Middleware(Networking, Communication), Operating System(BSD 4.4, freeRTOS 등 OS)의 3항목으로 구성됨. 통상 Embedded S/W는 RTOS(Real Time Operating System)로 인식됨. Embedded S/W에 대한 글로벌 시장규모는 상기 3항목을 모두 포함한 전체로서 조사되고 있음. Embedded S/W 시장은 통신, 산업자동화, 자동차 등 교통수단을 중심으로 시장이 형성되어 있음

(※ 출처 : Global Market for Embedded Software, 2012, Frost & Sullivan)

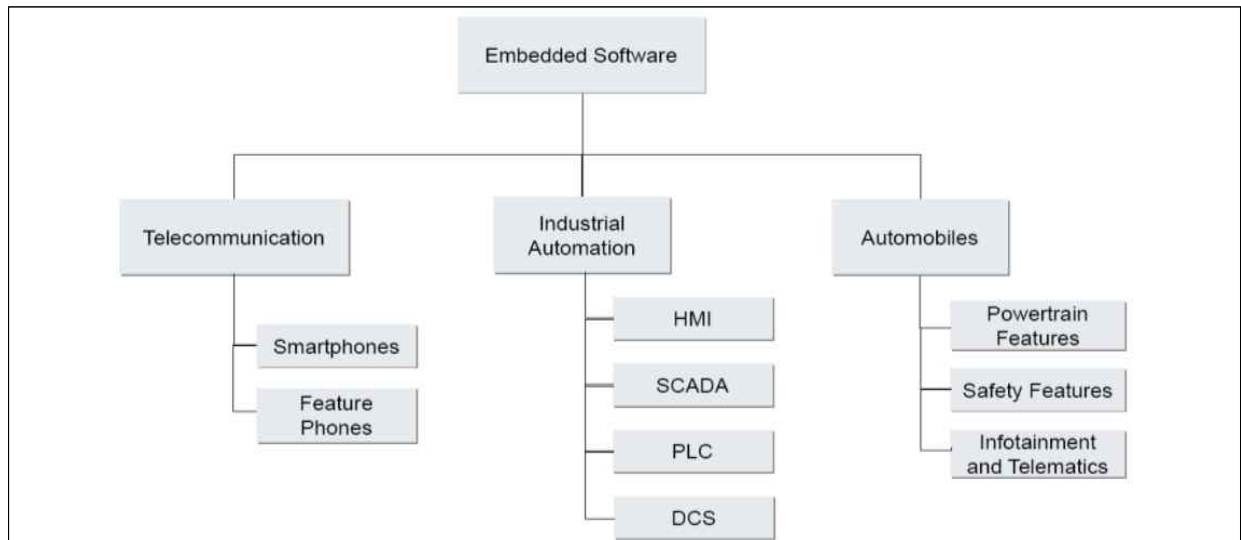


그림2-22. Total Embedded Software Market : Segmentation, Global, 2010

- 스마트폰에 대한 수요증가, 기술변화 촉진 등의 요인으로 Embedded S/W 글로벌 시장은 2010년 408억 달러 수준에서 2017년 1,598억 달러 수준까지 年평균 21.5%씩 크게 성장할 것으로 예측됨

(※ 출처 : Global Market for Embedded Software, 2012, Frost & Sullivan)

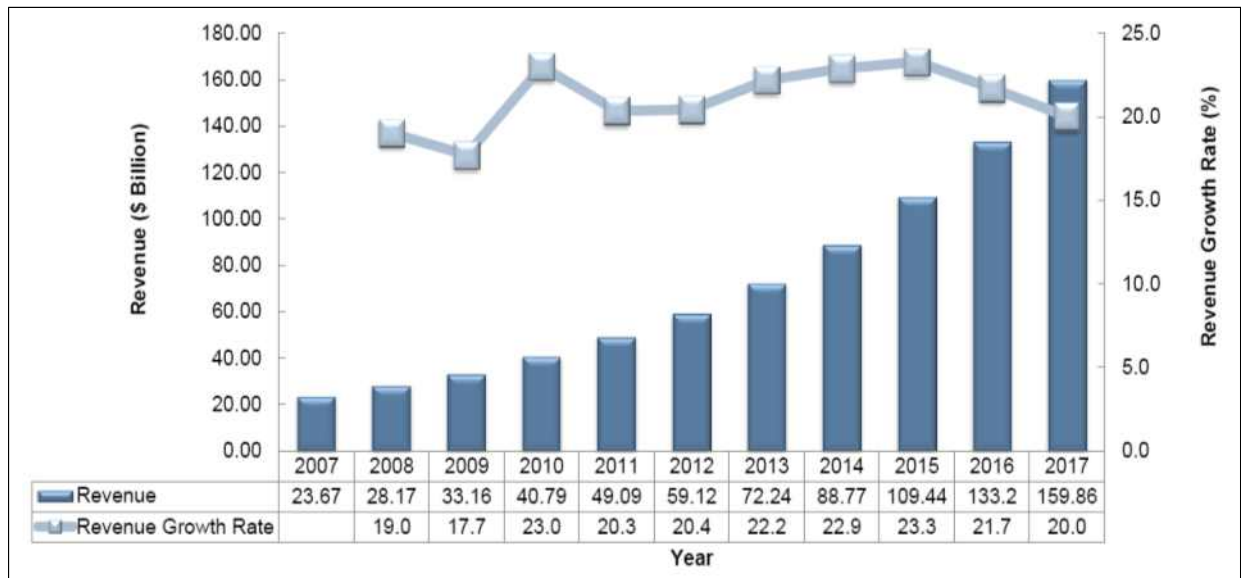
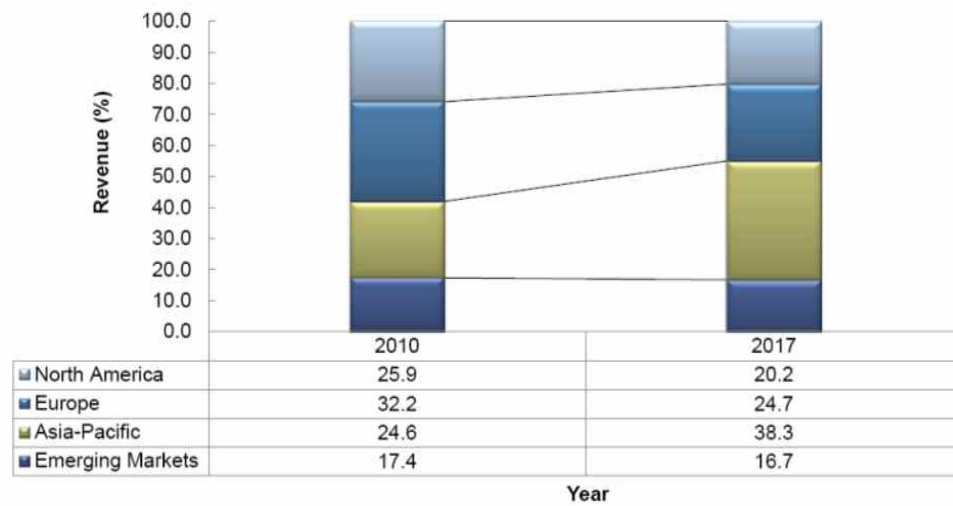


그림2-23. Total Embedded Software Market : Revenue Forecast, Global, 2007~2017

- Embedded S/W 글로벌 시장을 지역별로 살펴보면, 북미, 유럽, 아시아-태평양 지역이 80% 이상을 차지하고 있으며, 아프리카/남미 등의 지역이 Emerging Market으로 부상하고 있음. 특히 아시아-태평양 지역의 시장성장율이 매우 높게 성장하고 있어 주목할 필요가 있음APEC지역 2010년 24.6%(100억달러)에서, 2017년 38.3%(612억달러)까지 성장이 예상됨

(※ 출처 : Global Market for Embedded Software, 2012, Frost & Sullivan)



Year	North America (\$ Billion)	Europe (\$ Billion)	Asia-Pacific (\$ Billion)	Emerging Markets (\$ Billion)
2007	5.42	7.77	5.74	4.73
2008	6.70	9.08	7.07	5.32
2009	8.20	10.40	8.50	6.06
2010	10.55	13.12	10.04	7.08
2011	12.57	15.56	12.49	8.47
2012	14.87	17.94	16.47	9.84
2013	17.74	20.49	22.34	11.66
2014	21.03	23.81	29.71	14.21
2015	24.48	28.26	39.04	17.66
2016	28.21	33.66	49.71	21.62
2017	32.36	39.54	61.22	26.73
CAGR	17.4%	17.1%	29.5%	20.9%

그림2-24. Total Embedded Software Market : Percent Revenue Forecast by Region, 2007~2017

- Embedded S/W 글로벌 시장을 산업별로 살펴보면, 통신시장이 대부분을 차지하고 있고 성장률도 매우 높게 나타나고 있음. 자동차 등 교통부문(Automotive) 산업에서도 2010년 46억 달러에서, 2017년 61억 달러까지 성장이 예상되고 있음.

(※ 출처 : Global Market for Embedded Software, 2012, Frost & Sullivan)

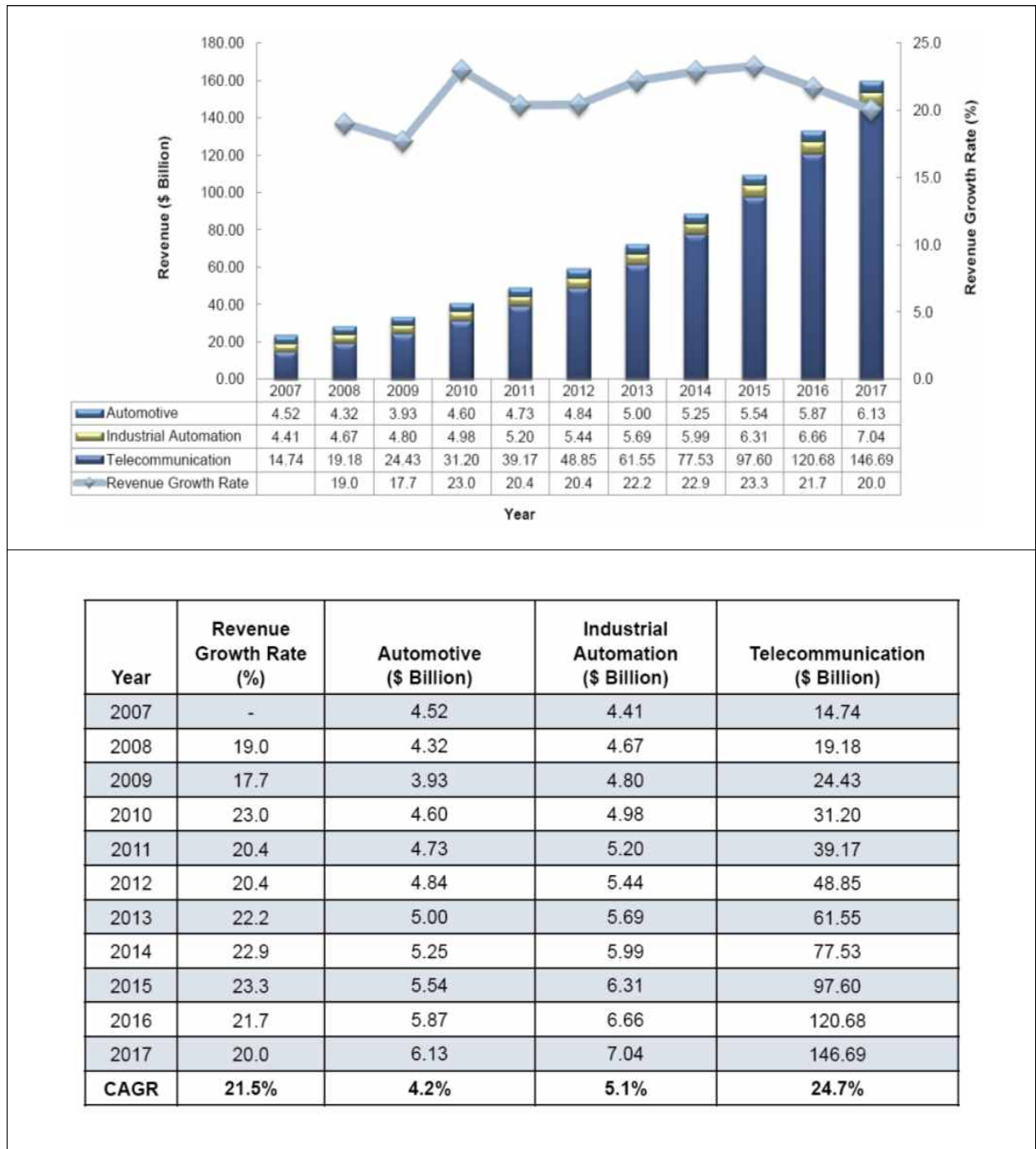


그림2-25. Total Embedded Software Market : Percent Revenue Forecast by Vertical Market, 2007~2017

■ 시장 발전단계

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획의 특허 출원/공개 추이를 통해 시장 발전단계 위치를 추정해 보면 현재 성장하고 있는 기술 분야로 판단할 수 있음
- 특허 출원/공개 추이를 보면, 전반적으로 우상향하고 있으며 2011년부터 출원 특허(청색선)보다 해외 공개 특허(적색선)가 더 많이 나타나 최근 해외시장에서 중요한 기술로 부각되고 있는 분야임을 알 수 있음

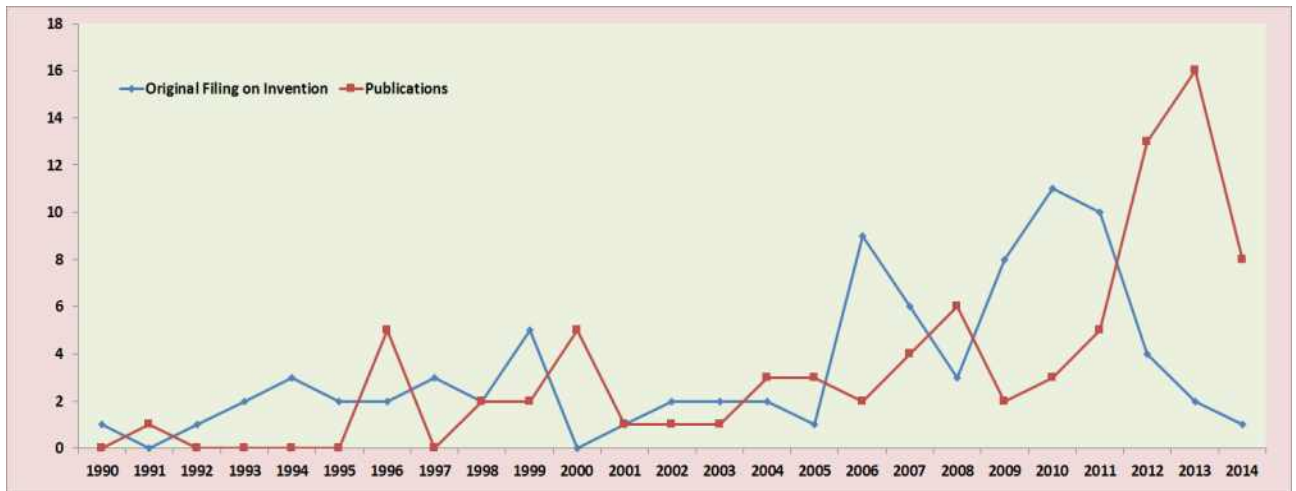


그림2-26. 특허기술 연계 기술발전 추이

- 논문 발표추이를 통해 시장 발전단계 위치를 추정하면, 전반적으로 우상향하는 추세를 보이고 있어 성장기에 있는 기술 분야임을 알 수 있음

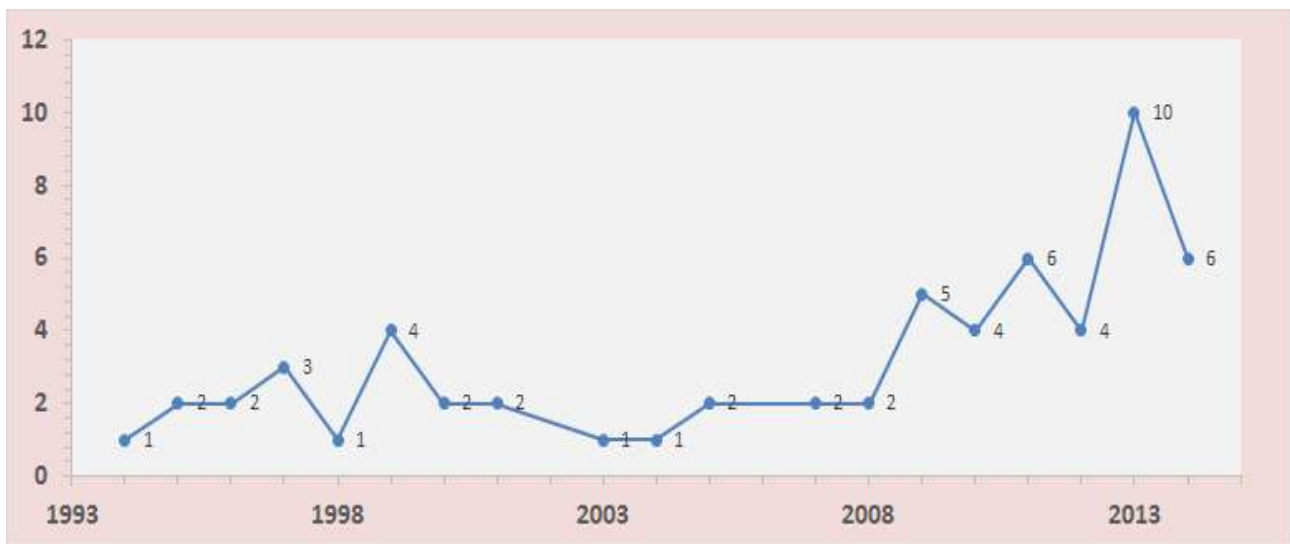


그림2-27. 논문 발표 연계 기술발전 추이

제 5 절 특허, 논문, 시장분석 결론

1. 특허분석 결론

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 분야의 전체적인 특허 동향을 살펴보면, 1990년부터 현재까지 총 83건의 관련 유효특허가 출원되었으며, 일본이 32건 (38%)으로 최다이며, 미국, 유럽, 한국, 중국의 순으로 출원되고 있음
- 특허를 출원한 상위 7개의 출원인을 분석한 결과, 일본 Hitachi LTD, TOSHIBA Corp., Mitsubishi Electric Corp., Nippon Signal Col. ltd, 미국 Cent Signal llc., 캐나다 Thales Canada Inc., 한국 KRRI가 출원을 많이 하고 있음을 알 수 있으며, 최다 출원인인 Hitachi와 Toshiba는 2006년부터 2011년 사이에 출원을 많이 하였고 , 최근에는 캐나다의 Thales Canada가 관련특허를 계속 출원하고 있음
- 국가별로 보면 해외 특허 시장확보력을 의미하는 시장확보지수(PFI)는 유럽이 가장 높았으며, 원천/핵심 특허 보유와 관련이 높은 인용도지수(CPP), 질적 수준을 나타내는 영향력지수(PII), 양적 수준(특허건수)을 고려한 기술력지수(TS) 지표는 미국이 가장 높은 경쟁력을 나타나고 있음. 이에 따라, 향후 量的・質的으로 가장 우수한 유럽과 미국 특허를 중심으로 세부 선행기술을 분석하되, 특허 출원 건수가 가장 많은 일본 특허도 병행하여 검토하는 것이 필요할 것으로 판단됨
- 한국의 경우 특허건수, 시장확보력, 인용도 등 기술영향력 등 대부분의 지수에서 선진국대비 크게 낮은 수준을 보이고 있어, 관련 분야 기술의 고도화가 시급히 요구되는 상황임

2. 논문분석 결론

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획 분야의 전체적인 논문 동향을 살펴보면, 1994년부터 현재까지 총 61건의 SCI 논문이 발표되고 있으며, 저널별로는 PROFESSIONAL ENGINEERING PUBLISHING, SAGE PUBLICATIONS LTD, PERGAMON-ELSEVIER SCIENCE LTD 등 유럽, 미국의 저널에서 많은 논문이 발표되고 있음

- 관련 분야 논문은 모두 47개의 저널에 다양하게 게재되어 있으며, 특히 Reliability Engineering & System Safety에 B. 안전측 동작설계(Fail-Safety Design) 기술 분야와 관련된 논문이 8편으로 가장 많이 게재되어있음

- Stack JR 등이 2004년 IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS 게재한 Bearing fault detection에 관한 논문이 36건으로 가장 많이 인용되었음

3. 시장분석 결론

- 철도 신호통신(Control command and signalling) 분야 전세계 신규/개량시장(New development and upgrade market)은 2011년 약 64.1억 유로(약 9.2조원)이며, 2016년까지 年 평균 3.5% 증가할 것으로 예측됨 (※ 출처 : Worldwide Market for railway technology, 2012, 독일 SCI)
- 철도 신호통신(Control command and signalling) 분야 전세계 유지보수 및 교체(Renewal and Maintenance) 시장의 경우 2011년 약 68.2억 유로(약 9.8조원)이며, 2016년까지 年 평균 3.1% 증가할 것으로 예측됨 (※ 출처 : Worldwide Market for railway technology, 2012, 독일 SCI)
- 2011년 현재 유럽 도시철도 CBTC 시장은 성장기(Growth)에 있으며 총 350km 구간에서 운영되고 있음. 시장 규모는 2011년 9.9억 유로에서 2021 까지 年 평균 14.4%씩 높은 성장을 통해 35.9억 유로 수준까지 증가할 것으로 예측됨. CBTC 구축에 km당 120만 유로 ~470만 유로가 소요되며, 평균 240만 유로가 소요되는 것으로 추정됨 (※ 출처 : Strategic Analysis of CBTC in the Western European Urban Rail Market, Frost & Sullivan, 2013)
- 글로벌 임베디드 시스템(Embedded System) 시장은 2008년 92billion달러에서 2013년 112.5billion달러로 증가하여 년평균성장률(CAGR) 4.1% 증가가 예상됨. 특히 임베디드 하드웨어(H/W) 시장은 2008년 89.8billion달러에서 2013년 109.6billion달러로 증가하여 년평균성장률(CAGR) 4.1% 증가가 예상되고, 임베디드 소프트웨어(S/W) 시장은 2008년 2.2billion달러에서

2013년 2.9billion달러로 증가하여 년평균 성장률(CAGR) 5.6% 증가가 예상됨. (※ 출처 : Embedded Systems: Technologies and Markets, BCC Research, April 2009)

- 공통플랫폼(Common Platform)은 집중화된 센서와 비디오 데이터를 전송을 위해 데이터베이스 형태로 센서 네트워크를 통해 제공되고 있고, 이러한 공통플랫폼을 프로세싱하는 감시 및 보안 장비의 총 시장 수요는 2011년 80billion달러, 2012년 81.3billion달러에 달하였고 2017년까지 127.6billion달러로 성장하여 2012년부터 2017년까지 년평균성장률 (CAGR) 9.4% 성장할 것으로 예상됨. (※ 출처 : Surveillance and Security Equipment: Technologies and Global Markets, BCC Research, January 2013)

- 신호설비 공통 플랫폼 개발 및 철도신호시스템 인증체계 수립 방안 기획의 특허 출원/공개 및 논문 발표 추이를 통해 시장 발전단계 위치를 추정해 보면 현재 성장하고 있는 기술 분야로 판단할 수 있음

제 3 장 신호설비 현황분석

제 1 절 주요 신호설비 현황분석

신호설비 공통플랫폼의 개발을 위해 주요장치 18종의 구성품을 조사 및 정리하였다. 각 장치의 구성품은 해당 규격에 해당하는 KRS를 기준으로 정리하였으며, KRS가 없는 고속철도 주요장치의 경우 한국철도시설공단의 기술문서를 기반으로 정리하였다.

표3-1. 주요장치 정의

	주요장치의 정의
일반철도 (9종)	- 전자연동장치(EIS형, Relayless형), 신호기장치(LED형), 선로전환기(NS, NS-AM- MJ81), - 궤도회로장치(임펄스형, TI21형, AF-ATC형), 자동폐색장치(ABS), 전원공급장치(일체), - 건널목보안장치(지장물, 출구측포함), 열차자동정지장치(ATS), 열차자동방호장치(ATP)
고속철도 (8종)	- 전자연동장치(SSi형), 정보처리장치(FEPOL), 선로변환기능모듈(TFM), 열차자동제어장치(ATC), - 궤도회로장치(UM71C형), 선로전환기장치(MJ81형, 하이드로스타형), 전원공급장치(일체), - 안전설비(HBD, 끌림검지장치, 지진감시장치, 선로침입검지장치)
공통사항(1종)	열차집중제어장치(CTC)

검토 대상인 일반철도 KRS는 다음과 같다.

- 한국철도표준규격 KRS SG 0040-09(R)] : 건널목경보장치
- 한국철도표준규격[KRS SG 0041-10(R)] : 건널목전동차단기
- 한국철도표준규격[KRS SG 0042-09(R)] : 건널목제어유닛
- 한국철도표준규격[KRS SG 0043-09(R)] : 건널목지장물검지장치
- 한국철도표준규격[KRS SG 0044-09(R)] : 건널목경보기용 경보등
- 한국철도표준규격[KRS SG 0045-09(R)] : 건널목경보기(현수형)
- 한국철도표준규격[KRS SG 0046-10(R)] : 건널목전동차단기(장대형)

- 한국철도표준규격〔KRS SG 0047-09(R)〕 : 건널목정보분석장치
- 한국철도표준규격〔KRS SG 0048-09(R)〕 : 건널목정시간제어기
- 한국철도표준규격〔KRS SG 0049-09(R)〕 : 건널목출구측차단검지기
- 한국철도표준규격〔KRS SG 0050-09(R)〕 : 건널목원격감시장치
- 한국철도표준규격〔KRS SG 0051-09(R)〕 : 건널목제어유니트(삼입형식)
- 한국철도표준규격〔KRS SG 0052-09(R)〕 : 건널목경보장치(가교형)
- 한국철도표준규격〔KRS SG 0053-09(R)〕 : 건널목지장물검지 조작스위치
- 철도신호설비 보수매뉴얼 V-1 건널목보안장치

표3-2. 전자연동장치(EIS, Relayless) 기능 및 구성품 분석

범 위			
기능 요약	1.연동장치 상호간의 연동 및 채정 등의 조건을 프로그램화하여 마이크로 컴퓨터에 의하여 제어하는 것으로 시스템의 안전성을 확보하기 위해 연동 장치의 연산논리를 수행 2.연동 Data Base를 구동하여 신호제어에 필요한 계전기를 제어하고 제어 및 표시정보의 송·수신, 유지보수 컴퓨터에서 통신라인을 통한 연동 Data Base의 업데이트와 현장상태 표시, 표시제어 컴퓨터와 필요한 데이터를 송·수신		
위험원	1.열차점유를 위험측으로 수신 2.신호기의 위험측 현시 3.선로전환기의 위험측 동작 4.위험측 진로취급 방호실패		
관련사고	열차충돌 및 탈선		
구성품목록	■ EIS형		
	구분	구성요소	
	기구	연동논리부 기기랙, 광통신부 광케이블 분배함, 광변환모듈, 광통신부 기기랙, 표시제어부 광케이블 분배함, 표시제어부 기기랙, 표시제어부 운전취급 탁자, 의자, 유지보수부 기기랙, 주파수 송수신부랙, 계전기랙 R1형, 계전기랙, R2형, 궤도랙 I형, 궤도랙 B형, 분선반 랙 T1, 분선반 랙 T2, 연동논리부 서버랙, 광통신부 서버랙, 폐색랙	
	카드류	모듈	연동논리부 인터페이스모듈, 연동논리부 입력모듈, 연동논리부 출력모듈, 선로전환기제어모듈, 연동논리부 확장모듈, 광통신부 전원모듈, 광통신부 광변환모듈, 표시제어부 절체스위치모듈 표시제어부 전원모듈, 표시제어부 광변환모듈, 연동논리부 CPU모듈, 연동논리부 전원모듈, 전원모듈, 송신모듈, 수신모듈, 표시제어부 절연변압기, 전원장치 절연변압기, 전원장치 정류기, 무정전전원장치
		계전기	무극선조계전기, 유극선조계전기, 직류자기유지계전기, 소등검지전류계전기,
	케이블	광통신부 광케이블, 통신케이블, 가간케이블, 테프론 배선	
소모품	표시제어부 산업용 컴퓨터, 표시제어부 모니터, 유지보수부 산업용컴퓨터, 유지보수부 모니터, 유지보수부 프린터, 표시제어부 키보드 및 마우스, 유지보수부 키보드 및 마우스, 냉각팬		

■ Relayless형		
구분	구성요소	
기구	표시제어부 광케이블 분배함, 표시제어부 기기랙, 표시제어부 운전취급 탁자, 의자, 유지보수부 기기랙, 연동논리부 기기랙, 연동논리부 서브랙, 광통신부 서브랙, 광통신부 기기랙, 광통신부 광케이블 분배함, 주파수 송수신부랙, 궤도랙 I형, 궤도랙 B형, 분선반 랙, 폐색랙	
카드류	모듈	연동논리부 전원모듈, 연동논리부 CPU모듈, 연동논리부 입환신호기모듈, 연동논리부 출력모듈, 연동논리부 선로전환기 모듈, 연동논리부 신호기모듈, 연동논리부 입력모듈, 연동논리부 인터페이스 모듈, 연동논리부 VME백프레임모듈, 연동논리부 광변환모듈,, 표시제어부 절체스위치모듈, 표시제어부 광변환모듈,, 연동논리부 확장모듈, 광통신부 광변환모듈, 송신모듈, 수신모듈, 광통신부 전원모듈, 전원모듈, 표시제어부 전원모듈, 표시제어부 절연변압기, 전원장치 무정전전원장치, 전원장치 절연변압기, 전원장치 정류기
	계전기	무극선조계전기
케이블	광통신부 광케이블, 통신케이블, 가간케이블, 테프론 배선	
소모품	표시제어부 산업용컴퓨터, 표시제어부 모니터, 유지보수부 산업용컴퓨터, 유지보수부 모니터, 유지보수부 기기랙, 표시제어부 키보드 및 마우스, 유지보수부 키보드 및 마우스, 냉각팬	

표3-3. 신호기(LED) 기능 및 구성품 분석

범 위		
기능 요약	1.기관사에게 열차의 정지, 진행 등을 신호로 현시하여 열차의 운행, 속도나 진로 등의 운전조건을 제시하는 장치	
위험원	1.신호를 위험측으로 현시	
관련사고	열차충돌 및 탈선	
구성품목록	구분	구성요소
	기구	렌즈, 합체, 취부금구
	카드류	모듈 LED모듈, 제어모듈
		계전기 소등검지계전기
	케이블	컨넥터
	소모품	설치 및 점검 도구

표3-4. 선로전환기(NS, NS-AM, MJ81) 기능 및 구성품 분석

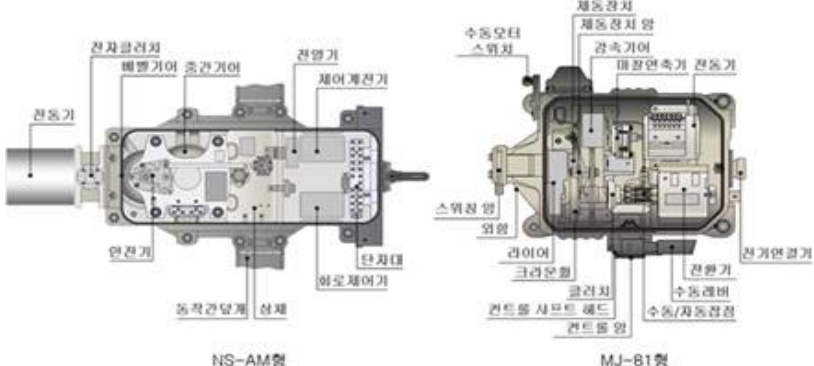
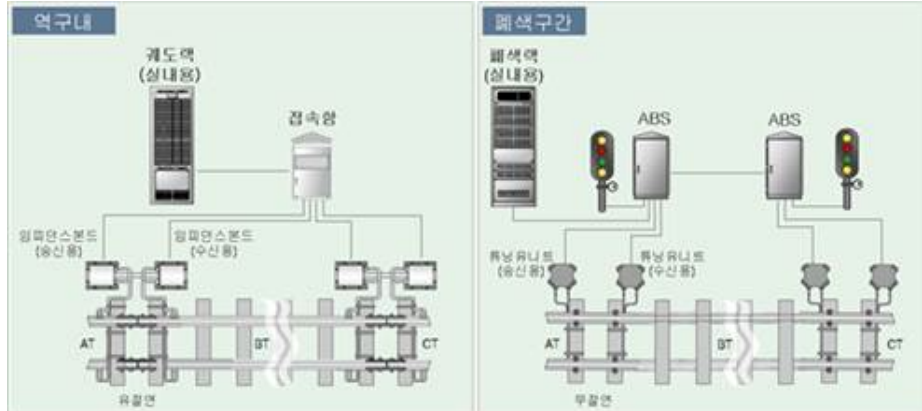
범 위	 NS-AM형 MJ-81형		
기능 요약	1.열차의 운행진로를 현재 선로에서 다른 선로로 변경하는 분기기에서 열차 진로방향을 전환시키는 장치로써 일반분기기에 적합한 선로전환기와 고속 분기기에 적합한 선로전환기를 갖는다		
위험원	1.선로전환기 밀착검지실패 2.선로전환기 불일치 3.선로전환기 도중전환(쇄정실패)		
관련사고	열차충돌 및 탈선		
구성품 목록	■ NS형		
	구분	구성요소	
	기구	상체, 하체, 커버	
	카드류	동작 기계	전동기, 동작간, 쇄정간, 삽입쇄정간(쇄정부), 삽입쇄정간(캠부), 중간기어, 전환기어, 베벨기어(소), 전환로라, 로라축, 급유장치, 베벨기어(대), 마찰클러치, 수동장치, 철관장치, 접속간, 침단간, 연결간, 유동방지간, 밀착조절간
		계전기	전열기, 동작계수기, 밀착검지기(함포함) 회로제어기, 전철제어계전기 [카드류]-밀착센서, 융설장치
	케이블	내부배선용 배선	
	소모품	설치 및 점검 도구, 할핀, 조핀, 풀림방지너트	
	■ NS-AM형		
	구분	구성요소	
	기구	상체, 하체, 커버	
카드류	동작 기계	전동기, 동작간, 쇄정간, 삽입쇄정간(쇄정부), 삽입쇄정간(캠부), 중간기어, 전환기어, 베벨기어(소), 전환로라, 로라축, 베벨기어(대), 급유장치, 전자클러치, 수동장치, 철관장치, 밀착조절간, 접속간, 침단간, 연결간, 유동방지간	
	계전기	전열기, 동작계수기, 밀착검지기(함포함), 회로계전기, 전철제어계전기 [카드류]-밀착센서, 융설장치	
케이블	내부배선용 배선		
소모품	설치 및 점검 도구할핀, 조핀, 풀림방지너트		

표3-5. 궤도회로장치(임펄스, TI21, AF-ATC1) 기능 및 구성품 분석

범 위		
기능 요약	1.열차가 운행하는 선로에 전기회로를 구성하여 열차점유 검지와 레일절손 유무를 검지하여 신호제어조건에 사용되는 장치	
위험원	1.열차점유 시 궤도계전기 여자유지 2.궤도파손 시 궤도계전기 여자유지 3.이웃 궤도의 사용주파수 출력(AF방식만 적용)	
관련사고	열차충돌 및 탈선	
구성품목록	■ 임펄스형	
	구분	구성요소
	기구	임펄스랙(실내용), 임펄스랙(실외용)
	카드류	전압안정기, 송신기, 수신기, 임피던스본드(송신기), 임피던스본드(수신기). 궤도계전기
	케이블	내부배선용 배선, 송신용케이블, 수신용케이블
	소모품	백열전구, 레일본드, 송착잠바, 귀선잠바, 공선잠바, 침단잠바, 크로싱잠바
	■ TI21형	
	구분	구성요소
	기구	정거장 구내용 AF궤도랙, 자동폐색구간용 서브랙, 중계궤도용 궤도기구함, 중계궤도용 궤도랙
	카드류	정거장 구내용 송신모듈, 정거장 구내용 수신모듈, 정거장 구내용 멀티포트, 정거장 구내용 선로증폭기, 정거장 구내용 전송모듈, 정거장 구내용 스위칭 허브, 정거장 구내용 라우터, 정거장 구내용 데이터종단장치, 자동폐색구간용 전원모듈, 자동폐색구간용 송신모듈, 자동폐색구간용 수신모듈, 자동폐색구간용 전송모듈, 자동폐색구간용 선로증폭기, 중계궤도용 전원모듈, 중계궤도용 송신모듈, 궤도용 수신모듈, 중계궤도용 선로증폭기, 중계궤도용 전송모듈, 중계궤도용 궤도계전기, 중계궤도용 전원절체기, 정거장 구내용 궤도계전기, 정거장 구내용 정류기, 정거장 구내용튜닝유닛(일반용), 정거장 구내용 튜닝유닛(종단용), 정거장 구내용 임피던스본드, 자동폐색구간용 튜닝유닛, 자동폐색구간용 임피던스본드(B2), 중계궤도용 변압기, 중계궤도용 튜팅유닛(일반용), 중계궤도용 튜팅유닛(종단용), 중계궤도용 임피던스본드(B2),
케이블	내부배선용 배선, 송신용케이블, 수신용케이블	
소모품	백열전구, 레일본드, 송착잠바, 귀선잠바, 공선잠바, 침단잠바, 크로싱잠바	

	■ AF-ATC형	
	구분	구성요소
	기구	AF케도랙, 전원공급랙
	카드류	모듈 송신카드, 수신카드, 감시카드, 중계카드,
		계전기 캐도계전기
		수동 소자 미니임피던스본드, 임피던스본드, 보안기, 정합트랜스
	케이블	내부배선용 배선, 송신용케이블, 수신용케이블, 루프코일
	소모품	설치 및 점검 도구, 레일본드, 송착잠마, 귀선잠마, 공선잠마, 침단잠마, 크로싱잠마

표3-6. 자동폐색장치(ABS) 기능 및 구성품 분석

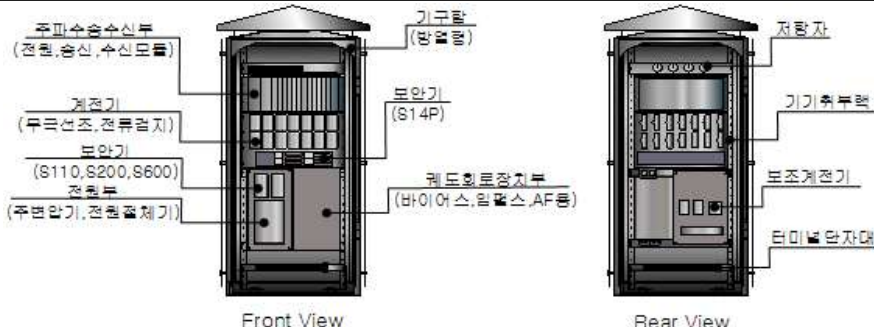
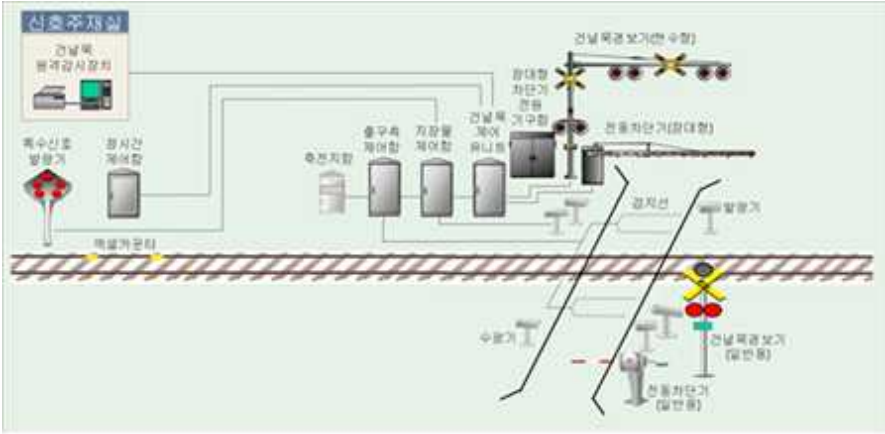
범 위	 Front View Rear View	
기능 요약	1. 열차운행을 일정한 간격을 유지하면서 운행될 수 있도록 폐색구간을 두고 한 폐색구간에 한 개의 열차만 운행할 수 있도록 역과 역 사이에 설치하는 장치	
위험원	1. 신호의 위험측 현시 2. 캐도회로의 위험측 검지	
관련사고	열차충돌 및 탈선	
구성품 목록	구분	구성요소
	기구	기구함 철제특수(방열형), 기기취부랙, 제어계전기부 소형 무극선조계전기 켜, 제어계전기부 전류검지계전기 켜, 주파수송수신부 랙, ABS용 보안기 S14P용 설치대
	카드류	모듈 주파수송수신부 전원모듈, 주파수송수신부 송신모듈, 주파수송수신부 수신모듈, 수신기, 송신기, AF송신기, AF수신기, AF감시유니트, AF선로중폭기, 전원절체기
		계전기 소형무극선조계전기, 제어계전기부전류검지계전기, 캐도계전기, 임펄스캐도계전기, 무극선조계전기 소형
		수동 소자 바이어스, 변압기류, 정류부, 쇼크, 전압안정기, ABS용 보안기(카운터 내장용), ABS용 보안기 S14P, ABS용 보안기 ST0405, 전원부 주변압기,
	케이블	내부배선용 배선
	소모품	백열전구

표3-7. 전원공급장치(신호기계실) 기능 및 구성품 분석

범 위			
기능 요약	1.도로가 평면 교차하는 개소에서 열차의 진입을 통행자에게 알려 사고를 방지하는 운전보안설비		
위험원	1.통행열차에 대한 건널목 차단실패		
관련사고	열차충돌, 탈선, 인명사상		
구성품목록	구분	구성요소	
	기구	사다리, 경표, 기주, 베이스, 취부금구, 건널목전동차단기 합체 및 지지대, 건널목전동차단기 평형축, 건널목전동차단기 차단간 취부금구, 건널목전동차단기 뚜껑, 건널목전동차단기 중간치차축, 건널목전동차단기 주축, 건널목 전동차단기 성형품, 건널목전동차단기 회로제어기 카바, 건널목전동차단기 차단간, 건널목전동차단기 차단간 보조품, 건널목제어유닛 기기취부가, 건널목제어유닛 2420 취부가, 건널목제어유닛 신호기구함, 건널목지장물검지장치 신호기구함, 건널목지장물검지장치 제어랙, 건널목전동차단기 동력부 합체 및 뚜껑, 차단간 및 취부금구, 건널목전동차단기(장대형) 차단간, 건널목경보기용 경보등 등함, 배관 및 쉘, 건널목경보기용 경보등 렌즈, 건널목정시간제어기 기구함, 건널목정시간제어기 기기랙, 건널목정시간제어기 합체, 건널목출구측차단간검지기 기구함, 기기랙, 제어부 합체, 건널목원격감시장치 분소장치 랙, 건널목원격감시장치 주재장치 랙, 건널목제어유닛 기기 취부랙, 건널목제어유닛 소형무극선조계전기 켜, 궤도시소계전기 켜, 궤도계전기 켜, 건널목제어유닛 기구함 철제 특수, 건널목제어유닛(삽입형식)제어검지부 외함, 건널목경보장치(가교형) 강관주 및 브라켓, 경표, 계사판, 건널목지장물검지 조작스위치 합, 뚜껑, 판넬, 비상압구, 포호판, 반사재, 경광등, 수광기, 발광기	
	카드류	모듈	열차진행방향표시등, 고장/정지표시등, 건널목제어유닛 경보제어부, 건널목제어유닛 2440제어부, 건널목제어유닛 2420 제어부, 건널목제어유닛 음성안내장치, 건널목지장물검지장치 발광기, 건널목지장물검지장치 수광기, 건널목지장물검지장치 지장물검지제어기, 건널목지장물검지장치 지장경고등, 건널목지장물검지장치 고장표시등, 회로제어기, 건널목경보기용경보등 반도체, 건널목전동차단기(장대형) 제어부 제어함 및 제어카드, 건널목경보기용 경보등 전자회로판, 건널목경보기용경보등 발광다이오드, 건널목정보분석장치 검지장치 주제어기, 건널목정보분석장치 검지장치 정보입력기, 건널목 검지장치 정보출력기, 건널목정보분석장치 검지장치 LCD, 건널목정보분석장치 검지장치 전원기, 건널목정보분석장치 검지장치 분석장치, 건널목정시간제어기 제어부, 건널목정시간제어기 주제어보드, 건널목정시간제어기 제원설정보드, 건널목정시간제어기 입출력보드, 건널목정시간제어기 센서감도조정 보드, 건널목정시간제어기 차류검지기, 건널목출구측차단간검지기 제어부 주제어 보드, 건널목출구측차단간검지기 제어부 디지털 입력보드, 출력보드, 제어부 온도제어 보드, 건널목출구측차단간검지기 센서 지장물검지용, 다중전송장치, 건널목원격감시장치 정보분석장치 자동전송장치, 건널목원격감시장치 정보분석장치 궤도전압측정기, 건널목제어유닛(삽입형식) 2440모듈, 등중 제어모듈, 방향표시계전기 모듈, 고장검지송신모듈, 지장물검지장치, 음성경보 모듈, 혼스피커 모듈, 건널목경보장치(가교형) 경보등, 혼스피커, 음성안내경보장치, 수동조작기
	카드류	계전기	계전기, 스위치, 건널목제어유닛 계전기부, 건널목제어유닛 궤도계전기 및 쇼크, 건널목제어유닛 방향 표시계전기, 건널목제어유닛 수동조작기용 시소계전기, 건널목정시간제어기 계전기, 소형무극선조계전기, 궤도시소계전기, 궤도계전기 및 쇼크, 방향표시계전기(궤포함), 전동차단기 회로제어기 반응계전기(궤포함), 건널목제어유닛(삽입형) 수동조작기용 시소계전기(궤포함), 전동차단기 제어시소계전기(궤포함), 무경보방지용 시소계전기(궤포함)

	수동 소자	경보등, 경보종, 호스피커, 건널목전동차단기 치차, 클러치, 건널목전동차단기 스프링, 건널목전동차단기 베어링 축반이, 건널목전동차단기 전동축, 건널목전동차단기 유지전자석철심, 건널목전동차단기 브러쉬, 건널목전동차단기 전동기코일, 건널목전동차단기 유지전자석코일, 건널목전동차단기 코일인출선, 건널목전동차단기 점접스프링, 건널목전동차단기 점접스프링, 건널목전동차단기 회로제어기 축, 건널목전동차단기 점접, 저항기, 건널목제어유니트 신호용보안기(S220, T200), 건널목제어유니트 전원부, 건널목전동차단기 동력부 전동기, 감속기, 완충장치, 주축, 건널목경보기용경보등 저항, 건널목정시간제어기 전원보드, 건널목출구측차단감지기 제어부 전원보드, 건널목원격감시장치 분소장치 전원장치, 건널목원격감시장치 주재장치 전원장치, 전원부 50A, 안내표지등, 고장정지 표시등, 열차진행방향 표시등, 건널목지장물검지 조작스위치 비상압구, 건널목출구측차단감지기 전원장치 정류기
	케이블	건널목전동차단기 배선용전선(내부배선), 건널목경보기용경보등 배선,
	소모품	건널목출구측차단감지기 전원장치 축전지, 건널목원격감시장치 분소장치 주컴퓨터, 모니터, 멀티포트, 프린터, 건널목원격감시장치 주재장치 주컴퓨터, 모니터, 멀티포트, 프린터, 데이터전송장치, 백열전구, 축전지

표3-8. 건널목보안장치(지장물, 출구측포함) 기능 및 구성품 분석

범 위		
기능 요약	1. 신호보안설비에 안정된 전원을 공급하는 전원설비	
위험원	1. 해당 없음(전원공급 받는 장치에 안전확보 기능 포함 전제)	
관련사고	유지보수자 사상사고	
구성품목록	구분	구성요소
	기구	외함,
	카드류	모듈 전자소자류, 지시계기,
		수동소자 변압기, 전자개폐기, 역기전력 방호장치, 배선용 차단기
	케이블	배선용케이블
소모품	설치 및 점검도구	
	UPS용 축전지, 정류기용 축전지	

표3-9. 열차자동정지장치(ATS) 기능 및 구성품 분석

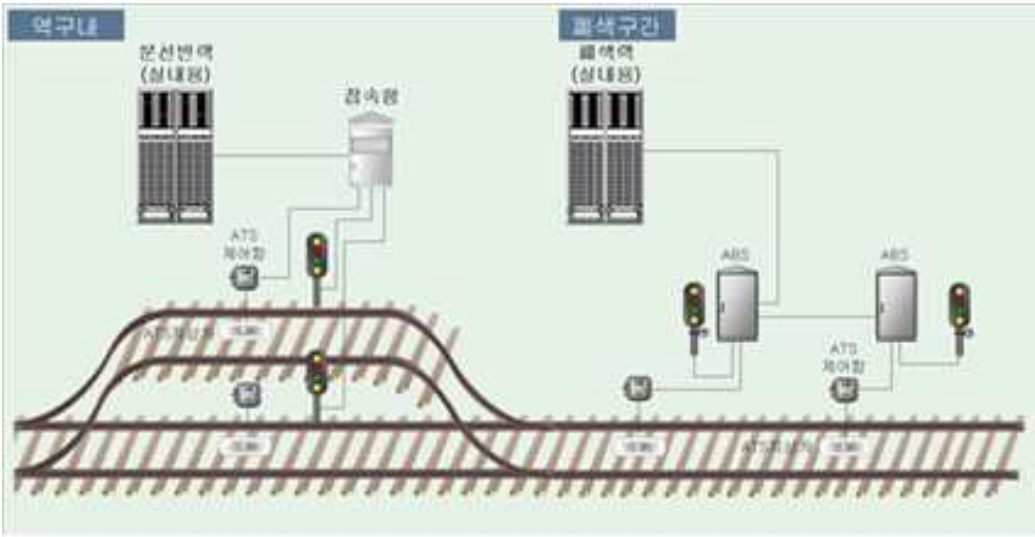
범 위																		
기능 요약	1.지상신호방식의 인위적인 조작에 의한 악천후 등의 한계를 극복하고 개인차에 의한 오인과 조작 착오로 인한 사고를 미연에 방지하기 위한 장치로써, 신호현시를 무시하고 운행할 시 자동으로 기관사에게 제동장치를 조작하도록 램프와 부저로 주의를 환기시키는 차내 경보로써 설정시간 이내에 제동 조작을 하지 않으면 자동으로 열차를 안전하게 정지(비상제동)시키는 장치																	
위험원	1.열차의 과속방호 실패 2.제한속도를 위험측으로 송신(지상장치)																	
관련사고	열차충돌, 탈선																	
구성품목록	<table><tr><td>구분</td><td colspan="2">구성요소</td></tr><tr><td>기구</td><td colspan="2">취부 금구류</td></tr><tr><td rowspan="2">카드류</td><td>모듈</td><td>ATS지상자</td></tr><tr><td>계전기</td><td>ATS지상자제어계전기</td></tr><tr><td>케이블</td><td colspan="2">ATS지상자~CR BOX간 제어케이블</td></tr><tr><td>소모품</td><td colspan="2">설치 및 점검 도구</td></tr></table>	구분	구성요소		기구	취부 금구류		카드류	모듈	ATS지상자	계전기	ATS지상자제어계전기	케이블	ATS지상자~CR BOX간 제어케이블		소모품	설치 및 점검 도구	
구분	구성요소																	
기구	취부 금구류																	
카드류	모듈	ATS지상자																
	계전기	ATS지상자제어계전기																
케이블	ATS지상자~CR BOX간 제어케이블																	
소모품	설치 및 점검 도구																	

표3-10. 열차자동방호장치(ATP) 기능 및 구성품 분석

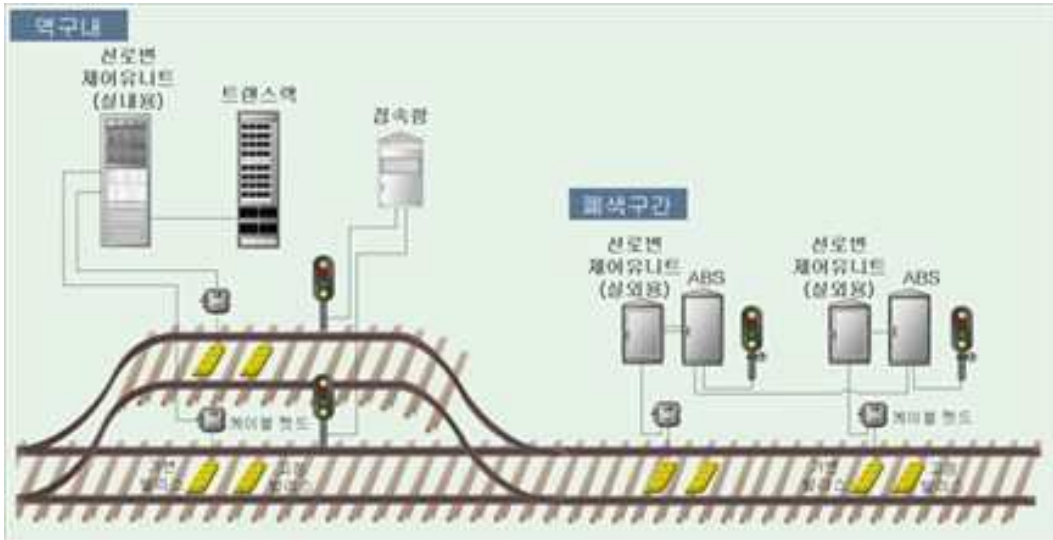
범 위			
기능 요약	1. 열차가 고속으로 주행하거나 우천, 안개 등과 같은 기상조건에서 기관사의 시계가 불량하더라도 신호현시 내용을 정확히 확인 할 수 있고 열차특성을 고려하는 안전운행간격이 확보되도록 지속적인 열차상태 감시 및 제어가 실행되고, 열차가 정지신호를 무시하고 운행되거나 지시된 속도를 넘어서는 과속을 하더라도 사전에 열차운행 제어범위가 계산되어 안전을 확보(상용제동 또는 비상제동 제어)하는 시스템		
위험원	1. 열차의 과속방호 실패 2. 제한속도를 위험측으로 송신(지상)		
관련사고	열차충돌, 탈선		
구성품목록	구분	구성요소	
	기구	신호변제어유닛함체	
	카드류	계전기	램프검지보드, 발리스 드라이브보드, 마더보드,
		수동소자	정류기, 전원모듈, 고정정보 발리스, 가변정보 발리스
	케이블	신호변제어유닛-발리스케이블, 신호변제어유닛함체-설비배선	
	소모품	설치 및 점검 도구	

표3-11. 고속철도 전자연동장치(SSi) 기능 및 구성품 분석

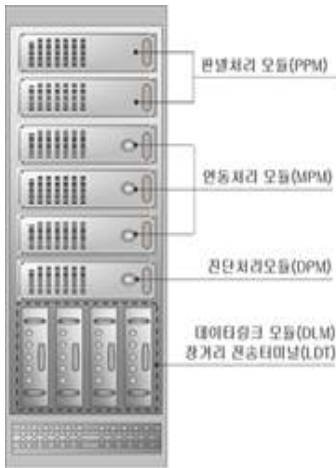
범 위											
기능 요약	1.역구내 및 중간 건널선에서 안전한 열차운행을 위하여 신호기, 선로전환기 및 궤도회로 등을 상호간 연쇄적으로 동작하도록 하여 사고를 방지하며, 취급자의 착오에 의한 오취급으로 부터 열차의 안전운행을 확보										
위험원	1. 열차점유를 위험측으로 수신 2. 신호기의 위험측 현시 3. 선로전환기의 위험측 동작 4. 위험측 진로취급 방호실패										
관련사고	열차충돌 및 탈선										
구성품목록	<table><tr><td>구분</td><td>구성요소</td></tr><tr><td>기구</td><td>랙</td></tr><tr><td>카드류 (모듈)</td><td>제어표시반 처리모듈,(PPM) 다중처리모듈(MPM) 진단모듈,(DIA) 통신데이터링크모듈(EDLM)</td></tr><tr><td>케이블</td><td>내부배선용 배선</td></tr><tr><td>소모품</td><td>보수자단말기(TT)</td></tr></table>	구분	구성요소	기구	랙	카드류 (모듈)	제어표시반 처리모듈,(PPM) 다중처리모듈(MPM) 진단모듈,(DIA) 통신데이터링크모듈(EDLM)	케이블	내부배선용 배선	소모품	보수자단말기(TT)
구분	구성요소										
기구	랙										
카드류 (모듈)	제어표시반 처리모듈,(PPM) 다중처리모듈(MPM) 진단모듈,(DIA) 통신데이터링크모듈(EDLM)										
케이블	내부배선용 배선										
소모품	보수자단말기(TT)										

표3-12. 고속철도 정보처리장치(FEPOL) 기능 및 구성품 분석

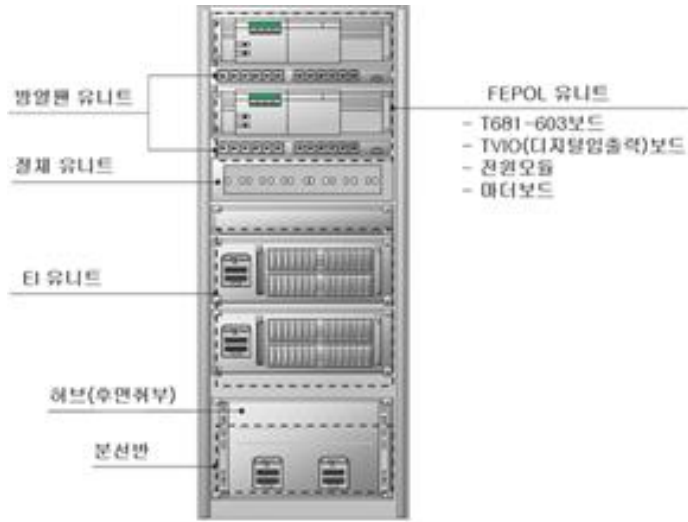
범 위																			
기능 요약	1.원격제어 및 로컬제어를 할 수 있는 다중처리 시스템이며, CTC 및 LCP에서 취급된 제어명령을 SSI를 통해 현장으로 전송하고 제어 확인된 표시정보를 수신하여 CTC 및 LCP로 전송하는 장치																		
위험원	1. 해당 없음																		
관련사고	운행지연																		
구성품목록	<table border="1"> <thead> <tr> <th>구분</th><th colspan="2">구성요소</th></tr> </thead> <tbody> <tr> <td>기구</td><td colspan="2">기기랙, FEPOL 서브랙, 절연통신(EI) 유니트서브랙</td></tr> <tr> <td rowspan="2">카드류</td><td>모듈</td><td>T681-603보드, TVIO보드, 상태표시 유니트, 마더보드, 절체유니트, 절연통신(EIB) 보드, 분선반유니트, 허브</td></tr> <tr> <td>수동소자</td><td>FEPOL 전원모듈, EI전원모듈,</td></tr> <tr> <td>케이블</td><td colspan="2">내부배선용 배선</td></tr> <tr> <td>소모품</td><td colspan="2">설치 및 점검 도구</td></tr> </tbody> </table>		구분	구성요소		기구	기기랙, FEPOL 서브랙, 절연통신(EI) 유니트서브랙		카드류	모듈	T681-603보드, TVIO보드, 상태표시 유니트, 마더보드, 절체유니트, 절연통신(EIB) 보드, 분선반유니트, 허브	수동소자	FEPOL 전원모듈, EI전원모듈,	케이블	내부배선용 배선		소모품	설치 및 점검 도구	
구분	구성요소																		
기구	기기랙, FEPOL 서브랙, 절연통신(EI) 유니트서브랙																		
카드류	모듈	T681-603보드, TVIO보드, 상태표시 유니트, 마더보드, 절체유니트, 절연통신(EIB) 보드, 분선반유니트, 허브																	
	수동소자	FEPOL 전원모듈, EI전원모듈,																	
케이블	내부배선용 배선																		
소모품	설치 및 점검 도구																		

표3-13. 고속철도 선로변기능모듈(TFM) 기능 및 구성품 분석

범 위			
기능 요약	1.선로변환기능모듈은 전자연동장치(SSI)로부터 제어명령을 받아 현장의 설비를 직접제어하고, 현장설비의 동작상태 표시를 전자연동장치(SSI)로 전송하는 역할을 하며, 연동장치에서 사용하는 선로변제어모듈(TFM)은 PM과 UM이 있으며, TFM-PM은 선로전환기를 제어하며, TFM-UM은 선로전환기를 제외한 일반적인 신호기장치 등의 입·출력 정보를 제어		
위험원	1.선로전환기 불일치 2.선로전환기 도중전환 3.신호기의 위험측 현시		
관련사고	열차충돌 및 탈선		
구성품목록	구분	구성요소	
	기구	TFM랙, 광데이터 링크모듈(SODLM) 랙, 전기데이터링크모듈(EDLM) 랙, LDT 인터페이스모듈(LIM) 랙, ECR계전기랙	
	카드류	모듈	UM모듈, PM모듈, 광데이터 링크모듈(SODLM), 전기데이터링크모듈(EDLM), LDT 인터페이스모듈(LIM), TFM구성보드, DLM구성보드, UM인터페이스 보드, PM인터페이스 보드, 램프검지기,
		계전기	ECR계전기
	케이블	내부배선용 배선	
	소모품	설치 및 점검도구	

표3-14. 고속철도 열차자동제어장치(ATC-지상) 기능 및 구성품 분석

범 위											
기능 요약	1.선행고속열차와의 간격과 선로조건 등을 고려하여 열차운전에 필요한 속도 정보를 레일을 통하여 차량으로 전송하고, 차량운전실에 허용속도를 현시하며, 열차의 실제 운행속도가 허용속도를 초과하면 자동으로 열차의 속도를 감속시키는 장치										
위험원	1.열차의 과속방호 실패 2.제한속도를 위험측으로 송신(지상)										
관련사고	열차충돌, 탈선										
구성품목록	<table border="1"> <thead> <tr> <th>구분</th><th>구성요소</th></tr> </thead> <tbody> <tr> <td>기구</td><td>정보처리랙(PTR), 절체랙(PCO), 폐색랙(PCA), 소규모 폐색랙(DPPCAs), 범용전송랙(PEUs), 전원공급랙(PAT), 입출력장치랙(BES), 폐색랙(PCA), 폐색랙(DPPCA), 범용전송랙(PEU), 분선반랙, NS계전기랙</td></tr> <tr> <td>카드류 (모듈)</td><td>정보처리랙(PTR/CUC1,2보드, CUC0보드, CKD보드, CSS보드, CCE보드, 폐색랙(PCA) CCM, CES, CSST, CSS, CRN, 환풍랙(PVE), 폐색랙(PCA) CAL 1보드 CCM, CES, CRN, CSS, CSST, CEN, CSN, 폐색랙(DPPCA) CAL 2보드, CCM, CES, CRN, CSST, CEN, CSN, 범용전송랙(PEU) CEU, CEP, CEP1, CEP2, CEP 증폭모듈, CEP 루프제어모듈</td></tr> <tr> <td>케이블</td><td>내부배선용 배선</td></tr> <tr> <td>소모품</td><td>설치 및 점검도구</td></tr> </tbody> </table>	구분	구성요소	기구	정보처리랙(PTR), 절체랙(PCO), 폐색랙(PCA), 소규모 폐색랙(DPPCAs), 범용전송랙(PEUs), 전원공급랙(PAT), 입출력장치랙(BES), 폐색랙(PCA), 폐색랙(DPPCA), 범용전송랙(PEU), 분선반랙, NS계전기랙	카드류 (모듈)	정보처리랙(PTR/CUC1,2보드, CUC0보드, CKD보드, CSS보드, CCE보드, 폐색랙(PCA) CCM, CES, CSST, CSS, CRN, 환풍랙(PVE), 폐색랙(PCA) CAL 1보드 CCM, CES, CRN, CSS, CSST, CEN, CSN, 폐색랙(DPPCA) CAL 2보드, CCM, CES, CRN, CSST, CEN, CSN, 범용전송랙(PEU) CEU, CEP, CEP1, CEP2, CEP 증폭모듈, CEP 루프제어모듈	케이블	내부배선용 배선	소모품	설치 및 점검도구
구분	구성요소										
기구	정보처리랙(PTR), 절체랙(PCO), 폐색랙(PCA), 소규모 폐색랙(DPPCAs), 범용전송랙(PEUs), 전원공급랙(PAT), 입출력장치랙(BES), 폐색랙(PCA), 폐색랙(DPPCA), 범용전송랙(PEU), 분선반랙, NS계전기랙										
카드류 (모듈)	정보처리랙(PTR/CUC1,2보드, CUC0보드, CKD보드, CSS보드, CCE보드, 폐색랙(PCA) CCM, CES, CSST, CSS, CRN, 환풍랙(PVE), 폐색랙(PCA) CAL 1보드 CCM, CES, CRN, CSS, CSST, CEN, CSN, 폐색랙(DPPCA) CAL 2보드, CCM, CES, CRN, CSST, CEN, CSN, 범용전송랙(PEU) CEU, CEP, CEP1, CEP2, CEP 증폭모듈, CEP 루프제어모듈										
케이블	내부배선용 배선										
소모품	설치 및 점검도구										

표3-15. 고속철도 궤도회로장치(UM71) 기능 및 구성품 분석

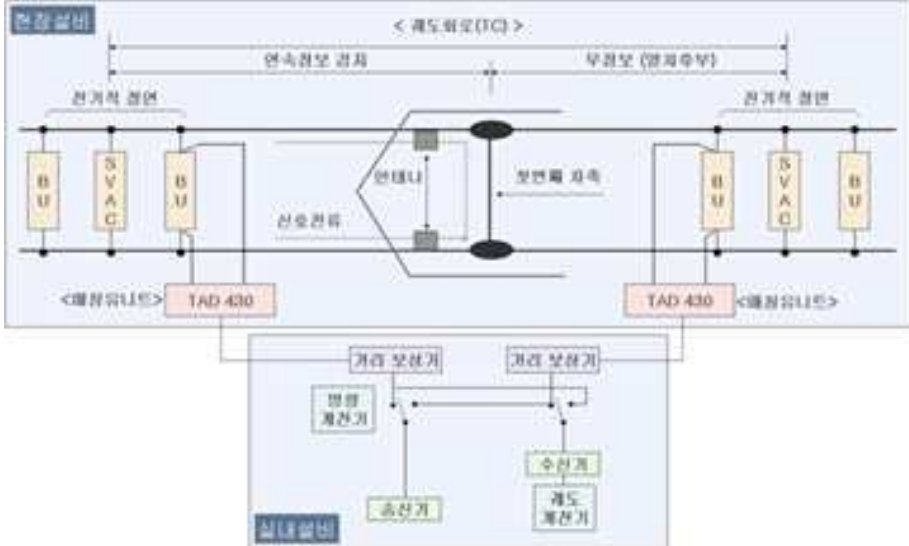
범 위																					
기능 요약	1.궤도회로 경계부에 절연이음매 대신 두 개의 동조유닛과 그 사이 중앙에 공심유도자가 한 Set로 결합하여 전기적인 회로를 구성하는 것으로 국내 고속철도 궤도회로방식에 사용하는 AF궤도회로 방식																				
위험원	1.열차점유 시 궤도계전기 여자유지 2.궤도파손 시 궤도계전기 여자유지 3.이웃 궤도의 사용주파수 출력																				
관련사고	열차충돌 및 탈선																				
구성품목록	<table><tr><td>구분</td><td colspan="2">구성요소</td></tr><tr><td>기구</td><td colspan="2">랙 함체</td></tr><tr><td rowspan="3">카드류</td><td>모듈</td><td>궤도회로 송신기(CEU), 궤도수신기,</td></tr><tr><td>계전기</td><td>방향계전기, 궤도계전기</td></tr><tr><td>수동 소자</td><td>양극자 블록장치(DB), 보상용 콘덴서, 유절연용 공심유도자(SVA), 무절연용 공심유도자(SVAc), 유절연 동조유닛(BA), 유니버설 동조유닛(BUI), 매칭유닛(TAD 430), 임피던스본드, 정합트랜스, 거리조정기</td></tr><tr><td>케이블</td><td colspan="2">내부배선용 배선</td></tr><tr><td>소모품</td><td colspan="2">설치 및 점검 도구</td></tr></table>		구분	구성요소		기구	랙 함체		카드류	모듈	궤도회로 송신기(CEU), 궤도수신기,	계전기	방향계전기, 궤도계전기	수동 소자	양극자 블록장치(DB), 보상용 콘덴서, 유절연용 공심유도자(SVA), 무절연용 공심유도자(SVAc), 유절연 동조유닛(BA), 유니버설 동조유닛(BUI), 매칭유닛(TAD 430), 임피던스본드, 정합트랜스, 거리조정기	케이블	내부배선용 배선		소모품	설치 및 점검 도구	
	구분	구성요소																			
	기구	랙 함체																			
	카드류	모듈	궤도회로 송신기(CEU), 궤도수신기,																		
		계전기	방향계전기, 궤도계전기																		
		수동 소자	양극자 블록장치(DB), 보상용 콘덴서, 유절연용 공심유도자(SVA), 무절연용 공심유도자(SVAc), 유절연 동조유닛(BA), 유니버설 동조유닛(BUI), 매칭유닛(TAD 430), 임피던스본드, 정합트랜스, 거리조정기																		
	케이블	내부배선용 배선																			
소모품	설치 및 점검 도구																				

표3-16. 고속철도 선로전환기(MJ81, 하이드로스타) 기능 및 구성품 분석

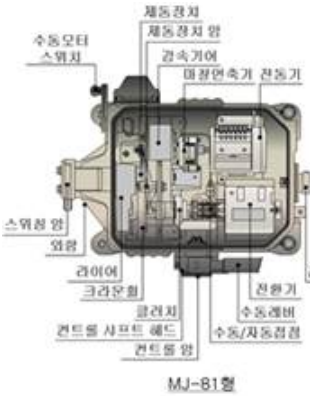
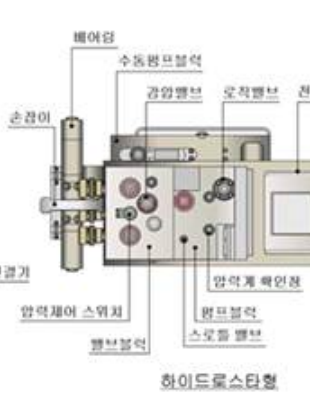
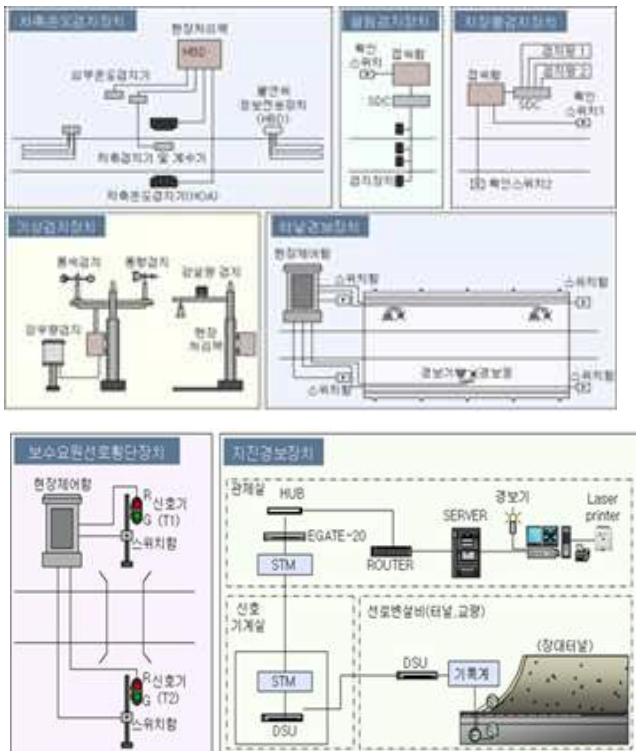
범 위	 																																		
기능 요약	1.열차의 운행진로를 현재 선로에서 다른 선로로 변경하는 분기기에서 열차진로방향을 전환시키는 장치																																		
위험원	1.선로전환기 밀착검지실패 2.선로전환기 불일치 3.선로전환기 도중전환(쇄정실패)																																		
관련사고	열차충돌 및 탈선																																		
구성품목록	■ MJ81형 <table border="1"> <tr> <th>구분</th><th colspan="2">구성요소</th></tr> <tr> <td>기구</td><td colspan="2">MJ81형 외부기기 커버, MJ81형 외부기기 명판, MJ81형 외부기기 수동 작동레버, MJ81형 외부기기 잠금 보호 카바, MJ81형 내부기기 철제주물 케이스, 철관장치</td></tr> <tr> <td rowspan="2">카드류</td><td>동작기계</td><td>MJ81형 외부기기 수동/자동 플랩, 컨트롤 샤프트 헤드, 컨트롤 암, 후렌지, 내부기기 커버에 부착된 스프링클램프, 전기모타, 마찰연축기, 감속기어, 감속기어 점검구, 제동레버, 구동과 잠금 라이어, 크라운-휠, 클러치 베벨 피니언, 클러치, 샤프트 베벨 피니언, 선로전환장치(첨단부 및 크로싱부), VCC, VPM, 간류</td></tr> <tr> <td>계전기</td><td>전기 연결기(콘넥트), 수동/자동 전환스위치, 점검전환기, 동작계수기, 밀착검지기(첨단부 및 크로싱부)</td></tr> <tr> <td>케이블</td><td colspan="2">내부배선용 배선</td></tr> <tr> <td>소모품</td><td colspan="2">설치 및 점검도구, 활핀, 조핀, 풀림방지너트</td></tr> </table> ■ 하이드로스타형 <table border="1"> <tr> <th>구분</th><th colspan="2">구성요소</th></tr> <tr> <td>기구</td><td colspan="2">손잡이, 합체, 보호덮개</td></tr> <tr> <td rowspan="2">카드류</td><td>동작기계</td><td>압력계, 축압기, 첨단부 유압파이프, 첨단부/크로싱부 선로전환장치, 첨단부 중앙쇄정장치, 첨단부/크로싱부 유압연결호스</td></tr> <tr> <td>계전기</td><td>첨단부/크로싱부 선단쇄정장치, 크로싱부 중앙쇄정장치, 첨단부/크로싱부 밀착검지기, 첨단부 연결로드</td></tr> <tr> <td>케이블</td><td colspan="2">내부배선용 배선, 전기 분배기</td></tr> <tr> <td>소모품</td><td colspan="2">설치 및 점검도구</td></tr> </table>	구분	구성요소		기구	MJ81형 외부기기 커버, MJ81형 외부기기 명판, MJ81형 외부기기 수동 작동레버, MJ81형 외부기기 잠금 보호 카바, MJ81형 내부기기 철제주물 케이스, 철관장치		카드류	동작기계	MJ81형 외부기기 수동/자동 플랩, 컨트롤 샤프트 헤드, 컨트롤 암, 후렌지, 내부기기 커버에 부착된 스프링클램프, 전기모타, 마찰연축기, 감속기어, 감속기어 점검구, 제동레버, 구동과 잠금 라이어, 크라운-휠, 클러치 베벨 피니언, 클러치, 샤프트 베벨 피니언, 선로전환장치(첨단부 및 크로싱부), VCC, VPM, 간류	계전기	전기 연결기(콘넥트), 수동/자동 전환스위치, 점검전환기, 동작계수기, 밀착검지기(첨단부 및 크로싱부)	케이블	내부배선용 배선		소모품	설치 및 점검도구, 활핀, 조핀, 풀림방지너트		구분	구성요소		기구	손잡이, 합체, 보호덮개		카드류	동작기계	압력계, 축압기, 첨단부 유압파이프, 첨단부/크로싱부 선로전환장치, 첨단부 중앙쇄정장치, 첨단부/크로싱부 유압연결호스	계전기	첨단부/크로싱부 선단쇄정장치, 크로싱부 중앙쇄정장치, 첨단부/크로싱부 밀착검지기, 첨단부 연결로드	케이블	내부배선용 배선, 전기 분배기		소모품	설치 및 점검도구	
	구분	구성요소																																	
	기구	MJ81형 외부기기 커버, MJ81형 외부기기 명판, MJ81형 외부기기 수동 작동레버, MJ81형 외부기기 잠금 보호 카바, MJ81형 내부기기 철제주물 케이스, 철관장치																																	
	카드류	동작기계	MJ81형 외부기기 수동/자동 플랩, 컨트롤 샤프트 헤드, 컨트롤 암, 후렌지, 내부기기 커버에 부착된 스프링클램프, 전기모타, 마찰연축기, 감속기어, 감속기어 점검구, 제동레버, 구동과 잠금 라이어, 크라운-휠, 클러치 베벨 피니언, 클러치, 샤프트 베벨 피니언, 선로전환장치(첨단부 및 크로싱부), VCC, VPM, 간류																																
		계전기	전기 연결기(콘넥트), 수동/자동 전환스위치, 점검전환기, 동작계수기, 밀착검지기(첨단부 및 크로싱부)																																
	케이블	내부배선용 배선																																	
	소모품	설치 및 점검도구, 활핀, 조핀, 풀림방지너트																																	
	구분	구성요소																																	
	기구	손잡이, 합체, 보호덮개																																	
	카드류	동작기계	압력계, 축압기, 첨단부 유압파이프, 첨단부/크로싱부 선로전환장치, 첨단부 중앙쇄정장치, 첨단부/크로싱부 유압연결호스																																
계전기		첨단부/크로싱부 선단쇄정장치, 크로싱부 중앙쇄정장치, 첨단부/크로싱부 밀착검지기, 첨단부 연결로드																																	
케이블	내부배선용 배선, 전기 분배기																																		
소모품	설치 및 점검도구																																		

표3-17. 고속철도 전원공급장치(신호기계실) 기능 및 구성품 분석

범 위																		
기능 요약	1.신호보안설비에 안정된 전원을 공급하는 전원설비																	
위험원	1.해당 없음(전원공급 받는 장치에 안전확보 기능 포함 전제)																	
관련사고	유지보수자 사상사고																	
구성품목록	<table><tr><td>구분</td><td colspan="2">구성요소</td></tr><tr><td>기구</td><td colspan="2">AVR 정류기 랙, DCP 랙, UPS용 축전지 랙, 정류기용 축전지 랙</td></tr><tr><td rowspan="2">카드류</td><td>모듈</td><td>MDP 표시기능부, 보호기능부, UPS 입력변환기, 정류 및 충전부, 인버터부, 정지형 동기 절체스위치부, SC스위치, 제어부, 마이크로프로세서 제어스크린 운영반, 절연저하 감지장치, 자동전압조정기(AVR) MCCB, 전압 및 전류미터, SCR모듈, 정류기모듈, 직류분선반(DCP) 래그DCP계측표시기, 과전압보호기, 충전기 저전압 보호차단스위치, 축전지 회로차단기, 분배 회로차단기, 절연저하 감지기, DC/DC컨버터</td></tr><tr><td>수동 소자</td><td>주전원 차단기, 분기회로 차단기, UPS 입력 EMC 필터, 출력변압기, 절연변압기, 주변압기,</td></tr><tr><td>케이블</td><td colspan="2">내부배선용 배선</td></tr><tr><td>소모품</td><td colspan="2">UPS용 축전지, 정류기용 축전지</td></tr></table>	구분	구성요소		기구	AVR 정류기 랙, DCP 랙, UPS용 축전지 랙, 정류기용 축전지 랙		카드류	모듈	MDP 표시기능부, 보호기능부, UPS 입력변환기, 정류 및 충전부, 인버터부, 정지형 동기 절체스위치부, SC스위치, 제어부, 마이크로프로세서 제어스크린 운영반, 절연저하 감지장치, 자동전압조정기(AVR) MCCB, 전압 및 전류미터, SCR모듈, 정류기모듈, 직류분선반(DCP) 래그DCP계측표시기, 과전압보호기, 충전기 저전압 보호차단스위치, 축전지 회로차단기, 분배 회로차단기, 절연저하 감지기, DC/DC컨버터	수동 소자	주전원 차단기, 분기회로 차단기, UPS 입력 EMC 필터, 출력변압기, 절연변압기, 주변압기,	케이블	내부배선용 배선		소모품	UPS용 축전지, 정류기용 축전지	
구분	구성요소																	
기구	AVR 정류기 랙, DCP 랙, UPS용 축전지 랙, 정류기용 축전지 랙																	
카드류	모듈	MDP 표시기능부, 보호기능부, UPS 입력변환기, 정류 및 충전부, 인버터부, 정지형 동기 절체스위치부, SC스위치, 제어부, 마이크로프로세서 제어스크린 운영반, 절연저하 감지장치, 자동전압조정기(AVR) MCCB, 전압 및 전류미터, SCR모듈, 정류기모듈, 직류분선반(DCP) 래그DCP계측표시기, 과전압보호기, 충전기 저전압 보호차단스위치, 축전지 회로차단기, 분배 회로차단기, 절연저하 감지기, DC/DC컨버터																
	수동 소자	주전원 차단기, 분기회로 차단기, UPS 입력 EMC 필터, 출력변압기, 절연변압기, 주변압기,																
케이블	내부배선용 배선																	
소모품	UPS용 축전지, 정류기용 축전지																	

표3-18. 고속철도 안전설비 기능 및 구성품 분석

범 위	
기능 요약	1.차측 및 차륜 온도검지와 차측카운터는 과열된 차측베어링 및 휠의 온도, 차측위치, 경보수준을 표시하여 CTC장치에 전송하여야 하고, 위험경보표시는 자동으로 속도제한을 위해 ATC장치로 직접 전송 2.궤간감지장치는 선로상에 열차의 하부전체를 검지할 수 있도록 일정한 간격으로 연속적으로 검지기를 직렬로 설치하여 검지기의 절단 또는 이와 비슷한 경우에 자동으로 속도제한을 위해 ATC장치 및 CTC장치 양쪽으로 신호가 전송 3.지장물감지장치는 낙석에 의하여 보호망의 파손 또는 기타 지장물의 궤도 침입으로 인하여 선로 안전구간에 사고가 발생하여 보호선 절단 된 경우 자동으로 열차의 운행속도를 제한 4.기상감지장치는 CTC장치에서 감시 및 제어가 가능하여야 하며, 강우검지는 6단계로 표시하고, 풍속검지는 5%편차의 바람세기[m/sec]와 방향을 표시 하여야 한다. 또한 강설검지기는 20mm 단위로 강설량을 표시 5.터널정보장치의 경보기는 열차가 해당 터널을 진입하기 이전까지 동작하고 경보등은 열차가 터널을 통과할 때까지 연속적으로 분당 60~80회 점멸 6.지진경보장치는 선로변의 지진동을 측정한 관련정보를 CTC장치로 전송하여 CTC장치에서 감시하고 경보를 발령

위험원	1.각각의 위험검지 실패																																								
관련사고	유지보수자 사상사고																																								
구성품목록	■ HBD <table> <tr> <td>구분</td><td>구성요소</td></tr> <tr> <td>기구</td><td>현장처리랙</td></tr> <tr> <td>카드류 (모듈)</td><td>차측온도 감시장치(HBD)시스템, 차측검지기, 외부온도검지기, 차측온도검지기, 차측계수기</td></tr> <tr> <td>케이블</td><td>내부배선용 배선</td></tr> <tr> <td>소모품</td><td>설치 및 점검도구</td></tr> </table> ■ 끌림검지장치 <table> <tr> <td>구분</td><td>구성요소</td></tr> <tr> <td>기구</td><td>검지기 취부금구</td></tr> <tr> <td>카드류 (모듈)</td><td>검지기, 확인스위치, 검지계전기</td></tr> <tr> <td>케이블</td><td>내부배선용 배선</td></tr> <tr> <td>소모품</td><td>설치 및 점검 도구</td></tr> </table> ■ 지진감시장치 <table> <tr> <td>구분</td><td>구성요소</td></tr> <tr> <td>기구</td><td>기록계 보호함</td></tr> <tr> <td>카드류 (모듈)</td><td>지진기록계, 전송계, 지진센서, 전원장치</td></tr> <tr> <td>케이블</td><td>내부배선용 배선</td></tr> <tr> <td>소모품</td><td>설치 및 점검 도구</td></tr> </table> ■ 선로침입검지장치(보수요원 선로횡단장치) <table> <tr> <td>구분</td><td>구성요소</td></tr> <tr> <td>기구</td><td>현장스위치함</td></tr> <tr> <td>카드류 (모듈)</td><td>현장제어반(PSCB) 프로세스모듈, 디지털 입력모듈, 디지털 출력모듈, 전원공급모듈, 광변환기, 이상전압보호기, 자동전압조정기, 신호등</td></tr> <tr> <td>케이블</td><td>내부배선용 배선</td></tr> <tr> <td>소모품</td><td>설치 및 점검도구</td></tr> </table>	구분	구성요소	기구	현장처리랙	카드류 (모듈)	차측온도 감시장치(HBD)시스템, 차측검지기, 외부온도검지기, 차측온도검지기, 차측계수기	케이블	내부배선용 배선	소모품	설치 및 점검도구	구분	구성요소	기구	검지기 취부금구	카드류 (모듈)	검지기, 확인스위치, 검지계전기	케이블	내부배선용 배선	소모품	설치 및 점검 도구	구분	구성요소	기구	기록계 보호함	카드류 (모듈)	지진기록계, 전송계, 지진센서, 전원장치	케이블	내부배선용 배선	소모품	설치 및 점검 도구	구분	구성요소	기구	현장스위치함	카드류 (모듈)	현장제어반(PSCB) 프로세스모듈, 디지털 입력모듈, 디지털 출력모듈, 전원공급모듈, 광변환기, 이상전압보호기, 자동전압조정기, 신호등	케이블	내부배선용 배선	소모품	설치 및 점검도구
구분	구성요소																																								
기구	현장처리랙																																								
카드류 (모듈)	차측온도 감시장치(HBD)시스템, 차측검지기, 외부온도검지기, 차측온도검지기, 차측계수기																																								
케이블	내부배선용 배선																																								
소모품	설치 및 점검도구																																								
구분	구성요소																																								
기구	검지기 취부금구																																								
카드류 (모듈)	검지기, 확인스위치, 검지계전기																																								
케이블	내부배선용 배선																																								
소모품	설치 및 점검 도구																																								
구분	구성요소																																								
기구	기록계 보호함																																								
카드류 (모듈)	지진기록계, 전송계, 지진센서, 전원장치																																								
케이블	내부배선용 배선																																								
소모품	설치 및 점검 도구																																								
구분	구성요소																																								
기구	현장스위치함																																								
카드류 (모듈)	현장제어반(PSCB) 프로세스모듈, 디지털 입력모듈, 디지털 출력모듈, 전원공급모듈, 광변환기, 이상전압보호기, 자동전압조정기, 신호등																																								
케이블	내부배선용 배선																																								
소모품	설치 및 점검도구																																								

표3-19. 관제설비(CTC) 기능 및 구성품 분석

범 위											
기능 요약	1. 열차집중제어장치는 광범위한 구간의 열차운행상황과 선로상태 및 신호설비의 동작상태 등을 한 곳에서 집중감시하며, 주컴퓨터의 입력된 스케줄에 따라 운행진로를 자동과 수동으로 총괄 제어하며, 여객안내정보 등으로 열차운행 정보를 여객에게 제공하는 장치										
위험원	1. 해당 없음										
관련사고	유지보수자 사상사고										
구성품목록	<table border="1"> <thead> <tr> <th data-bbox="375 1265 478 1332">구분</th><th data-bbox="478 1265 1422 1332">구성요소</th></tr> </thead> <tbody> <tr> <td data-bbox="375 1332 478 1467">기구</td><td data-bbox="478 1332 1422 1467">사령탑자 및 각 지지기구</td></tr> <tr> <td data-bbox="375 1467 478 1691">카드류 (모듈)</td><td data-bbox="478 1467 1422 1691">월 컨트롤러, 운영관제실 통합 컨트롤 시스템, 영상시스템, GIS서버, 상황실 통합컨트롤 시스템, 상황실 음향시스템, CTC서버, 통합서버, 프로그램 컴퓨터, 스케줄 관리서버, 레굴레이션 서버, 네트워크 관리시스템, 터미널서버, L4스위치, 외부접속 라우터, UPS, LDTS, 백본스위치, 대형표시반(엔진)</td></tr> <tr> <td data-bbox="375 1691 478 1825">케이블</td><td data-bbox="478 1691 1422 1825">사령실 내부 배선</td></tr> <tr> <td data-bbox="375 1825 478 1977">소모품</td><td data-bbox="478 1825 1422 1977">대형표시반(램프), 관제사콘솔, 유지보수콘솔, 프로그래머콘솔, 칼라프린터, 흑백프린터, 플로터,</td></tr> </tbody> </table>	구분	구성요소	기구	사령탑자 및 각 지지기구	카드류 (모듈)	월 컨트롤러, 운영관제실 통합 컨트롤 시스템, 영상시스템, GIS서버, 상황실 통합컨트롤 시스템, 상황실 음향시스템, CTC서버, 통합서버, 프로그램 컴퓨터, 스케줄 관리서버, 레굴레이션 서버, 네트워크 관리시스템, 터미널서버, L4스위치, 외부접속 라우터, UPS, LDTS, 백본스위치, 대형표시반(엔진)	케이블	사령실 내부 배선	소모품	대형표시반(램프), 관제사콘솔, 유지보수콘솔, 프로그래머콘솔, 칼라프린터, 흑백프린터, 플로터,
구분	구성요소										
기구	사령탑자 및 각 지지기구										
카드류 (모듈)	월 컨트롤러, 운영관제실 통합 컨트롤 시스템, 영상시스템, GIS서버, 상황실 통합컨트롤 시스템, 상황실 음향시스템, CTC서버, 통합서버, 프로그램 컴퓨터, 스케줄 관리서버, 레굴레이션 서버, 네트워크 관리시스템, 터미널서버, L4스위치, 외부접속 라우터, UPS, LDTS, 백본스위치, 대형표시반(엔진)										
케이블	사령실 내부 배선										
소모품	대형표시반(램프), 관제사콘솔, 유지보수콘솔, 프로그래머콘솔, 칼라프린터, 흑백프린터, 플로터,										

제 2 절 주요 신호설비 현황분석 결과

1절의 신호설비 구성품 분석을 통해 공통플랫폼의 적용이 가능한 설비(장치)는 다음과 같이 차상설비를 제외한 지상설비 18종 중 15종으로 구분되었다.

구분된 17종의 신호설비에 본 기획을 통해 제안된 공통플랫폼을 적용하는 경우 중복개발 방지는 물론 개발된 제어기의 안전인증에 필요한 개발환경 및 인증비용의 절감이 예상된다.

표3-20. 주요장치(신호설비) 중 공통플랫폼 적용유무

대분류	소분류(지상설비 기준)	공통플랫폼 적용가능성
일반철도 (9종)	· 전자연동장치(EIS형, Relayless형)	○
	· 신호기장치(LED형)	-
	· 선로전환기(NS, NS-AM, MJ81)	-
	· 궤도회로장치(임펄스형, TI21형, AF-ATC형)	○
	· 자동폐색장치(ABS)	○
	· 전원공급장치(일체)	○
	· 건널목보안장치(지장물, 출구측포함)	○
	· 열차자동정지장치(ATS)	-
	· 열차자동방호장치(ATP)	○
고속철도 (8종)	· 전자연동장치(SSI형)	○
	· 정보처리장치(FEPOL)	○
	· 선로변기능모듈(TFM)	○
	· 열차자동제어장치(ATC)	○
	· 궤도회로장치(UM71C형)	○
	· 선로전환기장치(MJ81형, 하이드로스타형)	○
	· 전원공급장치(일체)	○
	· 안전설비(HBD, 끌림검지장치, 지진감시장치, 선로침입검지장치)	○
공통사항(1종)	· 열차집중제어장치(CTC)	○

주요장치를 대상으로한 공통플랫폼 적용유무와 관련하여 다음의 미적용 대상별 사유는 다음과 같다.

- 신호기장치 : 내부에 별도의 논리회로 없음
- 선로전환기(NS, NS-AM, MJ81) : 내부에 별도의 논리회로 없음
- 열차자동정지장치(ATS) : 지상장치를 기준으로 내부에 별도의 논리회로 없이 수동소자(RLC)로 구성됨

또한, 적용대상에 대해서도 내부의 논리회로의 복잡도와 기능요구사항을 기준으로 동시작업 수행(멀티타스킹)이 요구되는 기능에 대해서는 상용운영체제가 포함된 32bit급의 적용이 적절하며, 기능요구사항이 단순하고 동시처리 요건이 없는 장치에 대해서는 운영체제와 응용프로그램이 통합되어 순차프로그램화된 16bit급 이하의 플랫폼 적용이 적합하다.

표3-20의 공통플랫폼 적용가능 장치별 성능에 대한 분석결과는 다음과 같다.

- 32bit급 공통플랫폼
 - : 전자연동장치, 건널목보안장치, 열차자동방호장치, 정보처리장치, 열차자동제어장치, 안전설비, 열차집중제어장치
- 16bit급 공통플랫폼
 - : 궤도회로장치, 자동폐색장치, 전원공급장치, 선로변기능모듈, 선로전환기(고속), 전원공급장치

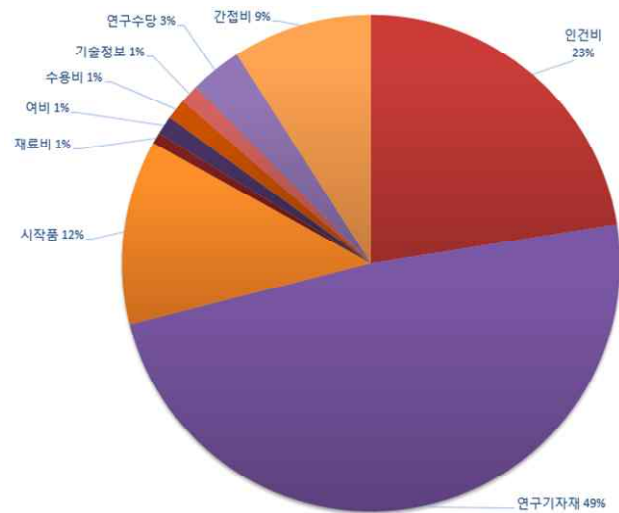
32bit와 16bit급 이하의 성능기준을 통합하여 공통플랫폼을 개발하는 경우 연구개발기간 및 재원에 대한 절약과 대량생산으로 인한 실용화가능성은 높아지나, 현장설치 후 부품의 개수가 상대적으로 많을수록 고장발생빈도와 유지보수 비용이 발생하여, 장치의 기능요구사항에 적합하도록 성능기준을 고성능과 보급형으로 구분하여 개발하는 것이 효과적으로 평가된다.

또한 고성능과 보급형 공통플랫폼 각각의 개발비용은 개발에 소요되는 개발환경구축, 시제품제작, 검증시험비용, 독립안전평가비용 등을 고려하여 다음과 같이 고성능(32bit급) 플랫폼의 경우 연구개발비 약 40억원, 보급형(16bit급 이하)의 경우 약 21억원으로 추정되었다.

■ 고성능 공통플랫폼 주요연구내용 및 예산구분

- 주요연구내용

- : 실시간 운영체제와 BSP간 응용기술 개발
- : Redundancy CPU보드 개발
- : 설비별 I/O보드 개발
- : 신호설비용 플랫폼 개발 및 인증
- : 검증용 플랫폼 적용 신호설비 개발 및 인증



[개발비용 약 40억원의 구성]

■ 보급형 공통플랫폼 주요연구내용 및 예산구분

- 주요연구내용

- : 운영체제와 응용프로그램 일체형 개발 환경 구축
- : CPU보드 개발
- : 설비별 I/O보드 개발
- : 공통 플랫폼 개발 및 인증
- : 검증용 플랫폼 적용 장치개발 및 인증



[개발비용 약 21억원의 구성]

제 4 장 신호설비 안전인증 체계

제 1 절 안전인증 체계 조사분석

안전필수(Safety Critical) 또는 안전관련(Safety Related) 철도시스템의 RAMS활동은 다음과 같은 수명주기로 수행된다.

1. 시스템분석 및 위험도 분석(첨부 1의 수명주기 1, 2)

- 시스템기능요구사항, 운영시나리오를 토대로 위험도분석
- 과거 유사시스템을 통한 위험원목록 및 사고목록 작성
- 예비위험원분석(PHA, Preliminary Hazard Analysis)기법을 통한 위험원에 대한 리스크 (사고의 발생빈도와 크기의 조합)예측
- 대상의 안전요구사항(Safety Requirement)제시

2. 리스크평가(첨부 1의 수명주기 3)

- 위 1에서 정의된 사고와 관련된 데이터를 토대로 정량적인 사고빈도 및 크기의 평가
- 평가된 리스크를 통해 적용대상의 안전무결성레벨(SIL, Safety Integrity Level)할당
- 안전무결성레벨에 따른 신뢰성측면과 안전성측면의 시스템고장률

SIL	신뢰성측면의 고장률(/Hour)	안전성측면의 위험측고장률(/Hour)	비 고
4	$\geq 10^{-5} \text{ to } < 10^{-4}$	$\geq 10^{-9} \text{ to } < 10^{-8}$	
3	$\geq 10^{-4} \text{ to } < 10^{-3}$	$\geq 10^{-8} \text{ to } < 10^{-7}$	
2	$\geq 10^{-3} \text{ to } < 10^{-2}$	$\geq 10^{-7} \text{ to } < 10^{-6}$	
1	$\geq 10^{-2} \text{ to } < 10^{-1}$	$\geq 10^{-6} \text{ to } < 10^{-5}$	

- 신뢰성측면의 고장률은 대상시스템 하드웨어소자 고장률과 여분을 고려하여 산출하며, 안전성측면의 위험측고장률은 아래 3에서 정의되는 위험측고장률을 모델링하여 관리한다. 또한 소프트웨어는 관련규격(철도시스템의 경우 IEC62279)에서 권고하는 SIL별 적용기술

과 평가방법으로 관리한다.

3. 시스템 위험원도출 및 분석(첨부 1의 수명주기 4, 5)

- 세부설계 자료를 토대로 대상시스템으로 인한 사고를 예측한다.
- 위험원도출에는 여러 가지 방법이 있으며 대표적인 방법으로 HAZOP(Hazard and Operability Study)기법이 있다.
- 위험원분석은 실제 대상시스템의 설계를 토대로 위험측고장률을 산출하기 위한 단계로 다양한 기법들이 존재하며 대표적인 방법으로 결함트리분석(FTA, Fault Tree Analysis)기법이 있다.

4. 안전대책수립 및 활동(첨부 1의 수명주기 6, 7, 8)

- 신뢰성측면의 고장률은 대상시스템 하드웨어소자 고장률과 여분을 고려하여 예측하며, 가속 스트레스시험 및 가속수명시험을 통해 분석한다.
- 안전성측면의 위험측고장률은 위 2에서 정의되는 SIL별 위험측고장률에 대하여 위 3에서 정의된 위험측고장관련 기능 및 소자를 모델링하여 관리한다. 또한 소프트웨어는 관련표준 (철도시스템의 경우 IEC62279)에서 권고하는 SIL별 적용기술과 평가방법으로 관리한다.)

5. RAMS확인 및 검증(첨부 1의 수명주기 9)

- 대상시스템의 기능 및 성능요구사항의 준수여부를 확인(Validation)한다.
- 대상시스템의 시스템요구사항 및 안전요구사항의 준수여부를 검증(Verification)한다.

6. RAMS인증(첨부 1의 수명주기 10)

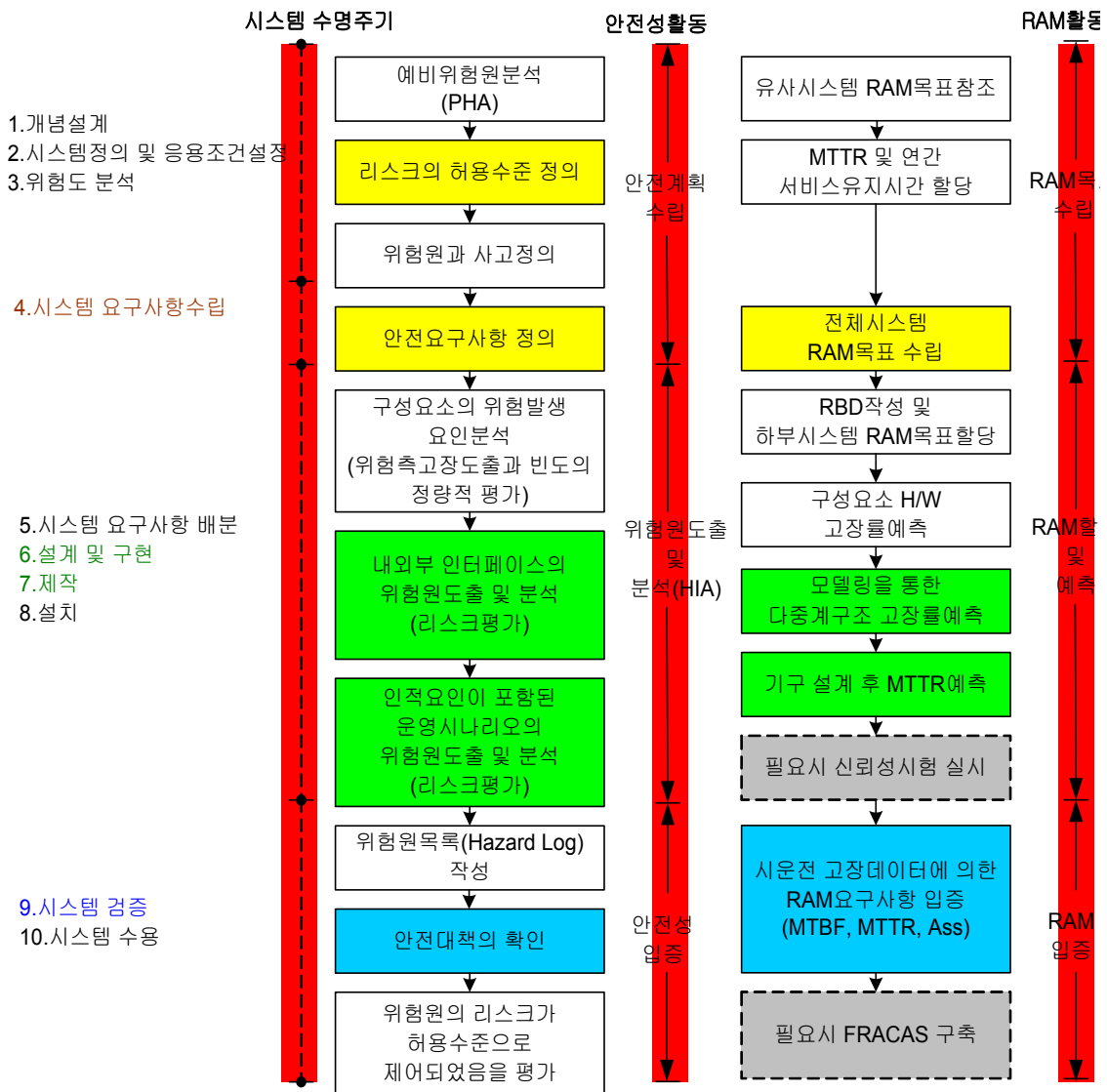
- 현재 국내에서는 최종사용자가 인정하는 절차의 수행, 또는 최종사용자가 RAMS활동 완성도의 판단을 위임하는 기관에서 작성하는 평가보고서에 따라 RAMS의 인증이 진행되고 있으며, RAMS활동의 완성도는 철도청지시 제2001-49호 “열차제어시스템 안전성확보 기술권고안(2001.07.13)”을 기준으로 평가한다.

7. RAMS관리(첨부 1의 수명주기 11, 12, 13, 14)

- 대상시스템이 영업운전을 시작한 이후부터 신뢰성 및 안전성측면의 유지보수 및 철거 프로

그럼으로써, 유지보수는 신뢰성과 안전성을 모두 고려하여 주기적 보수 및 고장에 의한 보수를 실시한다.

- 시스템의 노화는 시간에 따라 신뢰도가 변화하는 시스템의 하드웨어 성분을 충분히 고려해야 한다.



PHA : Preliminary Hazard Analysis

MTTR : Mean Time To Repair

RBD : Reliability Block Diagram

MTBF : Mean Time Between Failure

Ass : Steady State Availability

FRACAS : Failure Report, Analysis and Correct Action System

첨부1. IEC 62278기반 안전필수시스템의 수명주기별 RAMS활동

수명주기 단계	일반적인 과업	RAM 과업	안전성 과업
1. 개념 설정	·철도프로젝트의 범위와 목적 구축 ·철도프로젝트의 개념 정의 ·경영분석 및 실용성 연구의 착수 ·관리의 수립	·이전에 달성된 RAM 성과의 사전 검토 ·프로젝트의 RAM 관련성 고려	·이전에 달성된 안전성 성능의 사전검토 ·프로젝트의 안전성 관련사항 검토 ·안전성 정책과 안전성 목표 검토
2. 시스템 정의와 적용조건	·시스템 임무 프로파일의 수립 ·시스템 설명서 준비 ·운영과 유지보수 전략의 확인 ·운영조건의 확인 ·유지보수 조건의 확인 ·기존 설비의 제약조건의 영향 확인	·RAM에 위한 과거 경험 데이터 평가 ·예비 RAM 분석 수행 ·RAM 정책의 설정 ·장기 운영 및 유지보수 조건의 확인 ·기존 설비제약조건의 RAM에 대한 영향 확인	·안전성에 관한 과거 경험데이터 평가 ·사전 위험상태 조건 수행 ·全 Safety Plan 구축 ·위험도 기준의 허용도 정의(PHA) ·기존 설비의 제약조건의 안전성에 관한 영향 확인
3. 위험도 분석	·프로젝트 관련 위험도 분석의 착수	-	·시스템 위험상태와 안전성위험도 분석수행 ·위험상태 기록의 설정 ·위험도 평가(Risk Assessment) 수행
4. 시스템 요구사항	·요구사항 분석의 착수 ·시스템(全 요구사항)의 구체화 ·환경의 구체화 ·시스템 입증과 수용기준(全요구사항)의 정의 ·검증계획 수립 ·관리, 품질, 조직 요구사항의 수립 ·변경 제어 절차의 구현	·시스템 RAM 全 요구사항의 구체화 ·RAM 수용기준(전제)의 정의 ·시스템의 기능적 구조의 정의 ·RAM 프로그램의 수립 ·RAM 관리의 수립	·시스템 안전성 全 요구사항의 구체화 ·안전성 수용기준(전제)의 정의 ·안전성에 관련된 기능적인 요구사항 정의 ·안전성관리의 수립
5. 시스템 요구사항의 배분	·시스템 요구사항 배분 - 하부시스템과 부품의 요구사항 구체화 - 하부시스템과 부품의 수용기준정의	·시스템 RAM 요구사항의 배분 - 하부시스템과 부품의 RAM 요구사항 구체화 - 하부시스템과 부품의 RAM 수용기준 정의	·시스템 안전성 목표와 요구사항의 배분 - 하부시스템과 부품의 안전성 요구사항의 구체화 - 하부시스템과 부품의 안전성 수용기준의 정의 ·시스템 안전성계획의 갱신
6. 설계와 구현	·계획의 수행 ·설계와 개발 수행 ·설계분석과 시험의 수행 ·설계 증명의 수행 ·구현과 검증 수행 ·지원 자원 설계의 수행	·다음을 포괄하는 검토, 분석, 시험, 데이터 평가에 의한 RAM 프로그램의 구현 - 신뢰성과 가용성 - 유지보수와 유지보수성 - 최적 유지보수 정책 - 지원 ·다음을 포괄하는 프로그램 제어의 착수 - RAM 프로그램 관리 - 하부계약자 또는 공급자들의 관리	·다음을 언급하는 검토, 분석, 시험, 데이터 평가에 의한 Safety Plan 구현(HIA) - 위험상태 기록 - 위험분석 분석과 위험도 평가 - 안전성 관련된 설계 의사결정 정당화 ·다음을 포함하는 프로그램 제어 착수 - 안전성 관리 - 하부계약자 또는 공급자의 관리 ·일반적인 안전성 증빙문서(Generic Safety Case) 마련 ·일반적인 응용안전성 증명의 준비 마련(필요시)
7. 제조	·생산계획 수행 ·제조 ·구성요소 하부어셈블리 제조와 시험 ·문서화 마련 ·훈련 구축	·환경 용력 적격심사 수행 ·RAM 개선 시험 수행 ·고장보고분석 및 수정활동 시스템(FRACAS)	·검토, 분석, 시험, 데이터 평가에 의한 안전성계획을 구현 ·위험상태를 사용
8. 설치	·시스템 조립 ·시스템 설치	·유지보수자 훈련 시작 ·예비 부품과 공구 공급 구축	·설치 프로그램 구축 ·설치 프로그램 구현
9. 시스템 검증 (안전성 인수, 취약 포함)	·시운전 ·시범운영 수행 ·훈련 착수	·RAM 입증 수행	·시운전 프로그램 구축 ·시운전 프로그램 구현 ·특정적용 Safety Case 마련
10. 시스템인수	·인수 기준에 기초한 인수 절차 착수 ·인수를 위한 증빙자료 수집 ·운영 시작 및 시범 운영기간 지속	·RAM 입증 평가	·특정적용 Safety Case 평가
11. 운영과 유지보수	·장기간 시스템 운영 ·상시 유지보수 수행 ·상시 훈련 착수	·예비품과 공구의 상시 조달 ·상시 신뢰성중심의 유지보수 세부계획 지원실행	·상시 안전성 중심의 유지보수 착수 ·상시 안전 성능 감시 및 Hazard Log 유지보수 수행
12. 성능 감시	·운전중의 성능 통계자료 수집 ·자료의 획득, 분석과 평가	·성능과 RAM 통계량 수집, 분석, 평가,사용	·성능과 안전성 통계량 수집, 분석, 평가와 사용
13. 수정과개조	·변경요구 절차 구현 ·변경과 개선 절차 실행	·변경과 개선을 위한 RAM 관련사항 고려	·변경과 개선을 위한 안전성 관련사항 고려
14. 해체와 폐기	·사용중지 폐기 계획 ·사용중지 착수 ·폐기 착수	·RAM에 해당하는 활동 없음	·안전성 계획 수립 ·위험요소 분석과 위험도 평가 수행 ·안전성 계획 구현

참조 1: 변경관리나 형상경영활동은 모든 프로젝트 단계에 적용한다.

참조 2: verification과 validation 활동은 대부분의 수명주기활동에서 적용하고 본문에 포함되어 있다.

참조 3: RAM에 대해서 RAM 프로그램이란 용어가 공통적으로 사용되고 있으며 본 규격에서 채택되고 있다. 안전성에 대해서 Safety Plan이란 용어는 공통적으로 사용되고 있으며 본규격에서 채택되고 있다.

참조 4: 본 규격의 범위는 RAMS로 제한되어 있으며 모든 시스템 보증 활동들을 언급하고 있지 않는 점을 참조하시오. 그러나 RAMS 단계들과 프로젝트 관련 단계들 사이의 동기화를 보증하는 것이 필요하며 RAMS의 관점에서 한 단계에서 다음 단계로 통과하기 위한 조건들에 동의하는 것도 필요하다.

참조 5: 단계 9와 단계 10의 활동들은 고려중인 응용항목에 대해 따라서 통합되어도 좋다.

제 2 절 IEC 61508의 SIL별 요구사항 분석

IEC 61508은 안전관련분야 전기/전자/프로그래머블 제어기에 대한 기능안전에 대한 국제 규격이다(IEC 62278의 요구사항을 포함한 표준). 표4-1과 같이 총 7개의 장으로 구성된 IEC 61508은 산업플랜트, 원자력, 항공우주, 철도, 의료, 자동차 등의 전기/전자/프로그래머블 제어기를 이용하는 분야에서 전기/전자/프로그래머블 제어기의 오동작으로 인한 결과가 인명의 사상이나 대규모 재산손실의 원인이 되는 안전관련(Safety Related) 또는 안전필수(Safety Critical)분야 기능안전에 대한 국제표준이다.

표 4-1. IEC 61508의 구조

Code	Sub Title
IEC 61508-1	General Requirements
IEC 61508-2	Requirements for E/E/PE Safety-related System
IEC 61508-3	Software Requirements
IEC 61508-4	Definitions and Abbreviations
IEC 61508-5	Examples of Methods for the Determination of SIL
IEC 61508-6	Guidelines on the Application of IEC 61508-2 & IEC 61508-3
IEC 61508-7	Overview of Techniques and Measures

IEC 61508에서는 안전을 "모든 위험원(Hazard)의 위험도가 허용할 수 있는 수준으로 제어된 상태"로 정의하며, 허용할 수 있는 위험도의 수준을 전기/전자/프로그래머블 제어기의 각 기능에 대하여 안전무결성레벨(SIL)로 표현하고, SIL의 만족을 통해 안전확보를 확인하는 것을 목적으로 한다. 또한, 응용분야에 관련된 모든 요소를 고려하여, 해당 적용분야의 구체적인 요구를 충족할 수 있도록 하기 위한 안전관리절차를 그림4-1과 같이 16단계로 제시한다.

IEC 61508에서는 시스템 안전기능의 SIL을 정의하여 안전확보가 요구되는 산업전반에 대하여 기능안전의 무결성 수준을 레벨0부터 4까지 분류하였다.

레벨0은 안전과 무관한 위험원의 발생빈도이며, SIL4가 위험원의 발생빈도를 가장 많이 낮춘 수준의 시스템을 지칭하는 기준이다.

따라서, IEC 61508에서는 위험원의 결과인 사고(Accident)를 정의하여 시스템의 기능별 안전확보를 확인 및 검증하도록 권고하고 있으며, 본 보고서에서는 안전확보의 확인 및 검증기

준으로 제시된 각각의 요건을 분석하고, 요건만족을 위한 개발 가이드를 제공한다.

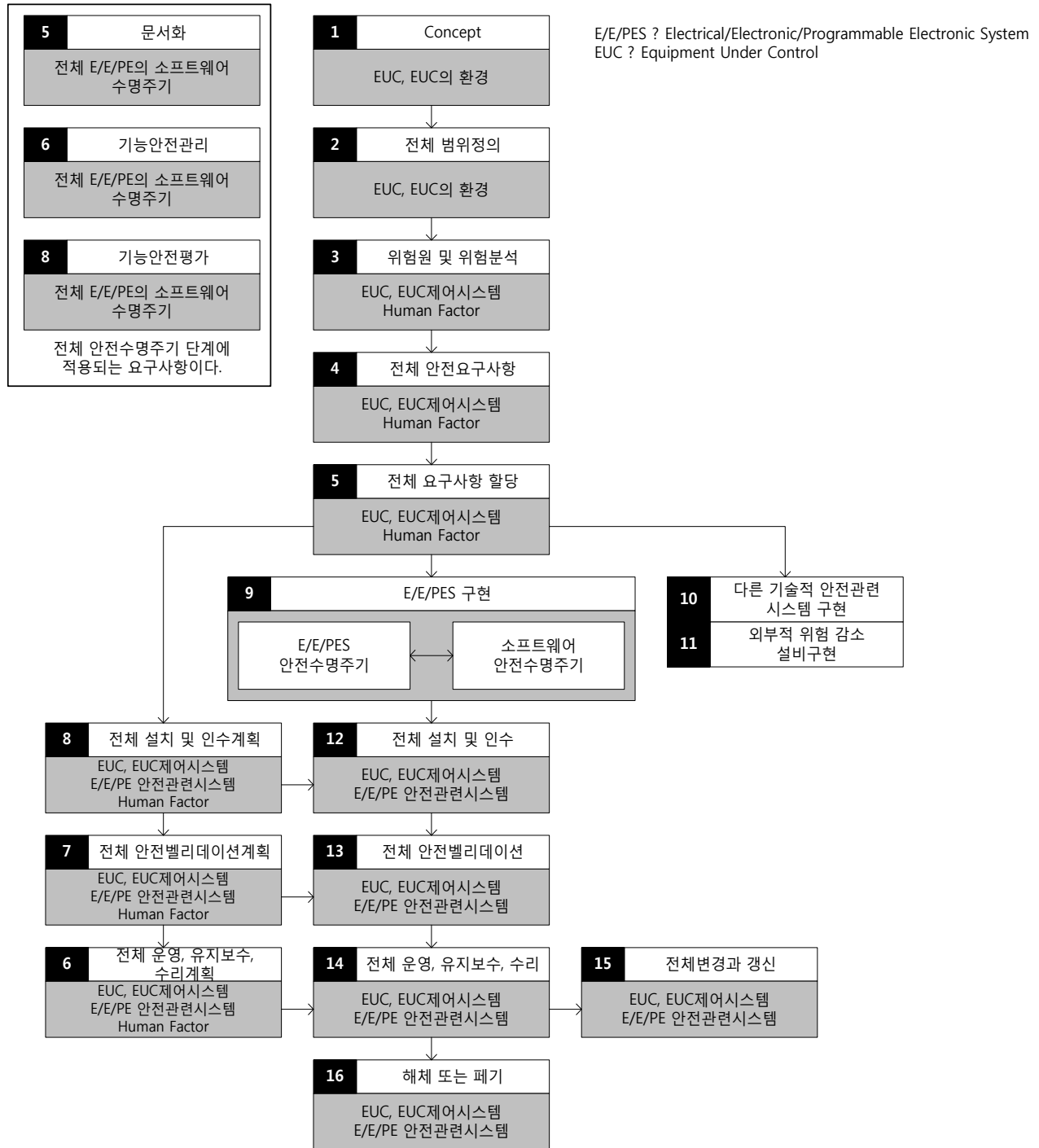


그림 4-1. IEC 61508의 시스템수명주기 16단계

1. IEC 61508의 SIL별 요구사항 분석

본 절에서는 IEC 61508의 SIL별 요구사항과 SIL할당과 위험도, 신뢰도 및 유지보수도 요구사항에 대하여 정리한다.

가. IEC 61508의 SIL별 요구사항

IEC 61508의 SIL을 만족하기 위해서는 표4-2와 같이 총 4가지의 요구사항을 모두 만족해야 한다. 표4-2의 내용 중 기술적 요구사항은 기존에 시스템 엔지니어링과정에서 수행되던 방법이며, 수행 인력의 능력과 기능안전평가와 관련된 요건은 SIL등급별 조직의 독립성을 위한 요구사항 만족의 확인을 목적으로 한다.

표4-2. IEC 61508의 요구사항 요약

검증항목	세부검증요소
1. 기능안전의 관리	가. 우발(Random) 하드웨어 고장 나. 소프트웨어 무결성(IEC 61508의 Part 3요건) 다. 하드웨어 구조 무결성(하드웨어 결함허용 능력)
2. 기술적 요구사항	가. 기능시험 나. 환경시험 다. 운영시험
3. 수행인력의 능력	가. 수행인력의 능력 나. 능력을 입증하는 증거
4. 기능안전평가	가. 기능안전의 검토 나. 독립성 입증의 증거

표4-2의 4가지 검증항목에서 기능안전의 관리는 할당된 SIL로 정량적 기준을 제시한다.

우발 하드웨어 고장에 대해서 IEC 61508은 안전관련 기능의 사용빈도에 따라 표4-3과 같이 Low Demand Mode와 High Demand Mode로 구분하고 있으며, 각 Mode의 구분은 IEC 61508-4의 3.5.12항에서 안전기능의 사용빈도가 1년 이하인 기능은 Low Demand Mode의 SIL기준을 적용하고, 사용빈도가 1년에 1회를 초과하는 경우 High Demand Mode(Continuous Mode)의 SIL기준을 적용하도록 하고 있다.

표4-3. Random Hardware Failure에 대한 모드별 정량적 SIL기준

SIL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

기능안전의 관리에서 소프트웨어 무결성은 SIL과 동일한 소프트웨어의 기능별 SIL인 SWSIL에 대한 다음 예(표4-4)와 같이 각각의 수명단계별 적용기준을 제시하고 있다.

표4-4. 소프트웨어 수명주기 논점과 문서화 관련 요건

문서명	SWSIL 0	SWSIL 1	SWSIL 2	SWSIL 3	SWSIL 4
1. Software Planning Documents 소프트웨어 계획서	R	HR	HR	HR	HR
2. S/W Requirements Documents 소프트웨어 요구사항 문서	R	HR	HR	HR	HR
3. S/W Design Documents 소프트웨어 설계문서	-	HR	HR	HR	HR
4. S/W Module Documents 소프트웨어 모듈 문서	-	HR	HR	HR	HR
5. Source Code and Documentation 소스코드 및 문서	R	HR	HR	HR	HR
6. S/W Test Reports 소프트웨어 시험보고서	-	HR	HR	HR	HR
7. S/W and H/W Integration Test Report 소프트웨어와 하드웨어 통합시험 보고서	-	HR	HR	HR	HR
8. S/W Validation Report 소프트웨어 검증보고서	R	HR	HR	HR	HR
9. S/W Assessment Report 소프트웨어 평가보고서	-	HR	HR	HR	HR
10. S/W Maintenance Records 소프트웨어 유지보수 기록	R	HR	HR	HR	HR
요구사항 ISO 9000-3의 승인은 모든 소프트웨어 안전무결성레벨에 대한 적합한 문서의 생산을 포함한다. 소프트웨어 안전무결성레벨 0에 대해서는 설계자는 반드시 적합한 형태의 문서를 선택한다.					

표4-4에서 SWSIL별 규제사항의 표기형식은 다음과 같다.

‘M’ 본 기호는 해당기술의 사용이 의무임을 의미한다.

‘HR’ 본 기호는 적용 기술 또는 측정방법이 해당하는 SWSIL에 대한 강한 권고사항임을 의미한다. 만약 적용기술 또는 측정방법이 사용되지 않으면 소프트웨어 품질 보증계획서 또는 보증계획서와 연관된 문서에 반드시 명시되어야 한다.

‘R’ 본 기호는 적용 기술 또는 측정방법이 해당하는 SWSIL에 대한 권장 사항임을 의미한다. 따라서 ‘HR’보다 낮은 수준의 권고사항이며, 이러한 기술들은 포장의 형태와 연관된다.

‘-’ 본 기호는 적용 기술 또는 측정방법이 권장하지 않거나 사용이 금지됨을 의미한다.

‘NR’ 본 기호는 적용 기술 또는 측정방법이 해당 SWSIL에 대하여 긍정적으로 권장되지 않음을 의미한다. 만약 적용 기술 또는 측정방법이 사용되면 소프트웨어 품질보증계획서 또는 품질보증계획서와 연관된 문서에 반드시 기록되어야 한다.

본 보고서에서는 1998년 발행된 IEC 61508-3의 SWSIL별 Table을 적용하지 않고, 2002년에 제정된 철도응용 소프트웨어 안전에 대한 기준인 IEC 62279를 기준으로 예를 제시하였다. SWSIL과 SIL의 등가처리는 SIL이 할당된 기능을 소프트웨어에 의해 수행하는 경우 해당 소프트웨어 기능은 SIL과 동일한 등급을 SWSIL에 적용한다.

나. SIL 할당

SIL 할당(Allocation)은 정의된 사고의 원인인 위험원을 발생시킬 수 있는 장치 또는 시스템의 기능별로 할당한다. SIL 할당은 다양한 방법에 의해 가능하지만 IEC 61508에서는 SIL 할당방법을 정성 및 반정량적인 방법과 정량적인 방법의 2가지로 아래와 같이 구분한다.

- 정성/반정량 방법
 - 위험도 그래프(Risk graph) 방법
 - 위험도평가매트릭스(S/F)
- 정량적 방법
 - FTA, ETA, Bow tie model
 - QRA(Quantitative risk assessment) : FTA와 유사

SIL 할당을 위해서는 먼저 기능을 정의해야 하며, 정의된 기능별로 위 방법을 사용하여 할당한다. 또한 표4-3의 Low Demand Mode와 High Demand Mode에 대한 구분 없이 위 방

법들을 적용하여 SIL을 할당할 수 있다.

위험도 그래프는 그림4-2와 같이 C: consequence 결과 (위험원으로 인한 심각도), F : Frequency 빈도(위험원 발생빈도), P : Probability of avoiding (위험원 발생시 회피확률), W : SIF의 요구빈도(SIF가 없을 대 발생될 위험원의 확률)를 임의로 정하여 경우에 따라 해당 기능에 대한 SIL을 할당하는 방법으로써, C, F, P, W에 대한 정량적 값을 주관적으로 결정하기 때문에 정성/반정량 방법에 속한다.

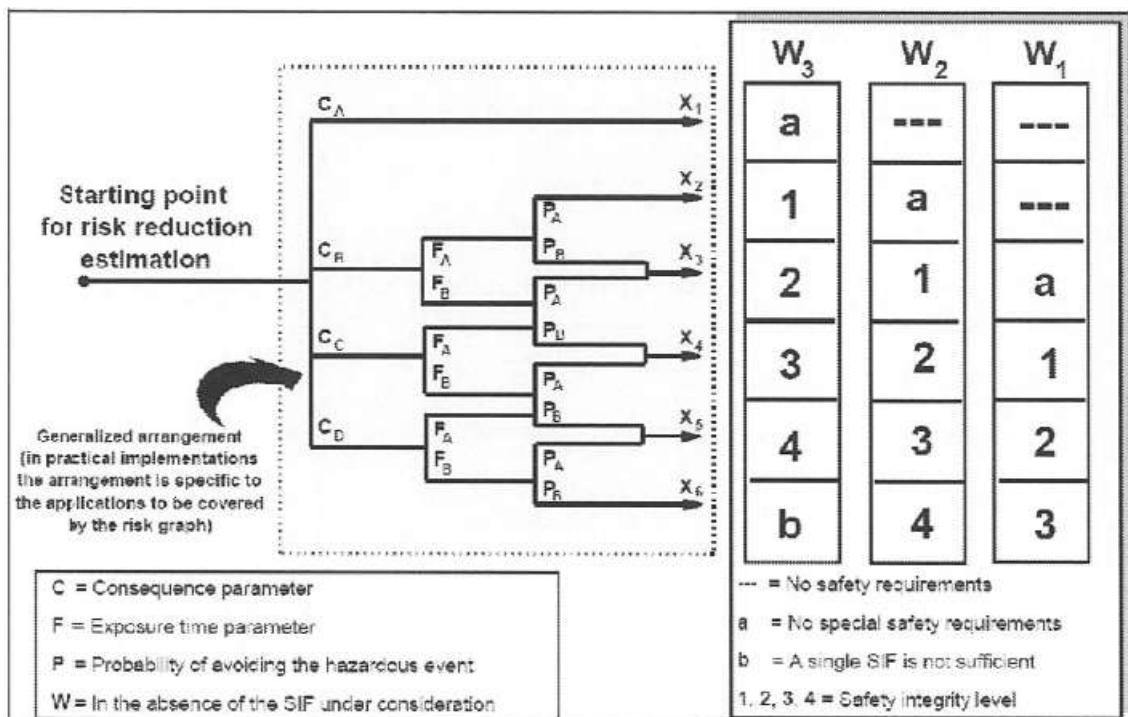


그림4-2. 위험도 그래프를 이용한 SIL 할당

Very frequent 0,5 year	ALARP	2	3	4	forbidden
Frequent D3 0,5 à 4 year	ALARP	1	2	3	4
Rare D2 4 à 20 year		ALARP	1	2	3
very rare D1 > 20 year	-		ALARP	1	2
Health & safety Consequences	care	light injury	irreversible injury	1 to 3 deaths	more than 3 deaths
Loss Consequences	<10 k€	10-100 k€	100-1000 k€	1M-10 M€	>10 M€
Environment Consequences	small 1	Minor 2	significant 3	Major 4	Disastrous 5

그림4-3. 위험도평가매트릭스를 이용한 SIL 할당

그림4-3의 위험도평가매트릭스 방법은 발생빈도(F)와 심각도(S)가 분배된 매트릭스에 해당 안전기능의 실패시 위험도를 대입하여 SIL을 할당하는 방법으로써, 그림4-3과 같이 SIL등급 이외에 허용수준으로 위험도가 제어된 상태인 ALARP적용대상의 선별에도 사용된다. 위험도 평가매트릭스는 위험도 그래프방식과 유사하게 안전기능실패에 대한 매트릭스의 심각도 및 발생 빈도의 정량치를 주관적으로 결정하기 때문에 정성/반정량 방법에 속한다.

Bow Tie모델은 그림4-4와 같이 위험원별 원인에 해당하는 이벤트 발생확률을 결함트리 분석(FTA)을 통해 모델링하고, 발생한 위험원의 심각도(결과)를 이벤트트리분석(ETA)을 통해 모델링하여, 이벤트와 관련된 기능의 SIL을 할당하는 방식이다. 이때 모든 이벤트의 발생 확률 및 위험원으로 인한 사고심각도가 과거의 고장이력 및 통계에 의해 정량적으로 대입되므로 정량적인 SIL 할당 방법에 속한다.

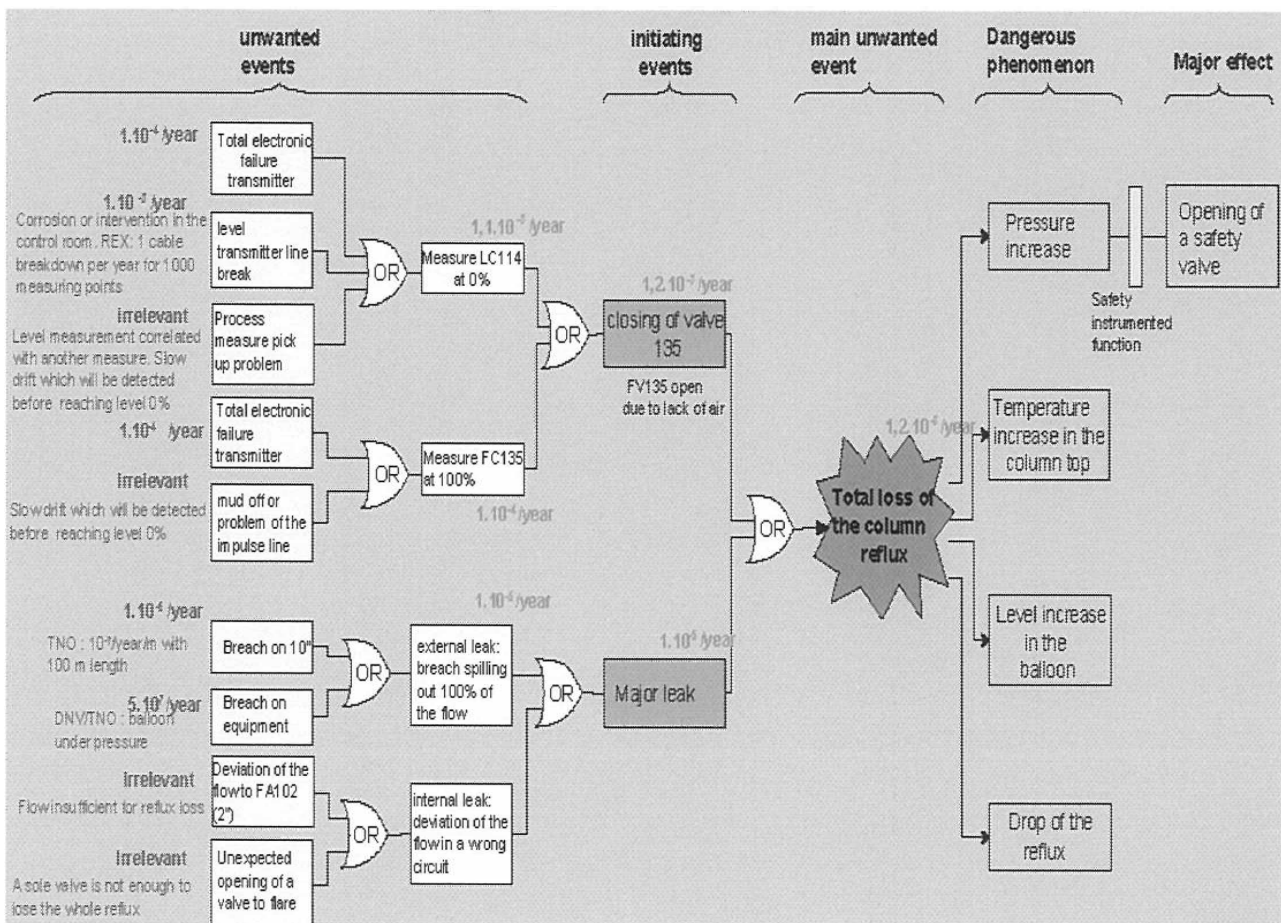


그림4-4. Bow Tie모델을 이용한 SIL 할당

마지막으로 QRA모델은 그림4-4의 Bow Tie모델과 유사하며, Bow Tie모델의 좌변인 FTA부분만을 수행한다. QRA와 Bow Tie모델의 차이점은 Bow Tie모델은 위험원의 심각도를 고려하여 사고발생빈도에 따른 해당 기능의 SIL을 할당하는 반면, QRA는 위험원의 발생빈도를 정량적 목표로 관리하여 해당 위험원에 연관된 기능의 SIL을 할당하는 것이 차별화 된 따라서 QRA는 운영시나리오 분석을 통한 위험원의 사고심각도 정량화가 곤란한 일반응용 (Generic Application)분야의 SIL 할당에 유리하며, Bow Tie모델은 응용시나리오에 의한 사고심각도 정량화가 가능한 특정응용(Specified Application)분야의 SIL 할당에 유리하다.

다. 위험도 요구사항

위험도 요구사항은 위험원별 SIL요구사항, 위험도매트릭스, 목표 사고발생확률 등으로 제시 된다.

위험원별 SIL요구사항은 표4-5의 예와 같이 장치의 위험원을 제시하고 각각의 위험원에 대한 SIL을 요구사항으로 제시하는 방식이다.

표4-5. 위험원과 SIL목표를 제시하는 요구사항의 예

위험원코드	위험원	위험원으로 인한 사고결과	목표 SIL
SSL_PHA_04	이미 채정된 진로와 관련된 진로의 설정 수락	열차충돌	4
SSL_PHA_05	취급된 진로(현장)와 조작반(상위 및 역구내) 정보의 불일치	열차충돌	4
SSL_PHA_06	선로전환기 상태와 SSI메모리 데이터의 불일치	열차충돌	4
SSL_PHA_07	분기부 열차점유시 도중전환 명령발생	열차탈선	4
SSL_PHA_08	정위와 반위가 뒤바뀐 선로전환기 제어명령 발생	열차충돌	4
SSL_PHA_11	입환 및 장내신호기의 위험측(위험측 진행신호)현시	열차충돌	4
SSL_PHA_13	속도제한의 위험측 출력발생(속도제한 처리불능 포함)	열차충돌	4
SSL_PHA_15	작업자 보호요청에 대한 보호출력 실패	사상사고	4
SSL_PHA_19	전유된 궤도회로를 비점유로 인식	열차충돌	4

위험도매트릭스방식은 위험원을 직접 제시하지 않고, 고장모드영향 및 심각도분석(FMECA)등의 방법을 통해 도출된 위험원의 위험도를 표4-6과 같이 허용수준이 표기된 위험도매트릭스에서 모두 안전이 확보되도록 위험원의 발생빈도 또는 심각도를 제어하도록 강제하는 방식이다.

표4-6. 위험도매트릭스를 제시하는 요구사항의 예

위험도 등급	A	B	C	D
1	Intolerable	Intolerable	Intolerable	Undesirable
2	Intolerable	Intolerable	Undesirable	Tolerable
3	Intolerable	Undesirable	Undesirable	Tolerable
4	Undesirable	Undesirable	Tolerable	Negligible
5	Tolerable	Tolerable	Negligible	Negligible
6	Negligible	Negligible	Negligible	Negligible

표4-7. 위험도매트릭스의 정량적 발생빈도 기준표

빈번한 발생 (Frequent)	1	수명주기 동안 빈번하게 발생할 가능성이 있음	10^{-3} 이상
가능성 있는 발생(Probable)	2	수명주기 동안 여러 번 발생할 가능성이 있음	10^{-4} to $\leq 10^{-3}$
종종 발생 가능 (Occasional)	3	수명주기 동안 가끔 발생할 가능성이 있음	10^{-6} to $\leq 10^{-4}$
발생가능성이 미약함 (Remote)	4	수명주기 동안 한두 차례 발생할 가능성이 있음	10^{-8} to $\leq 10^{-6}$
발생 가능성이 거의없음 (Improbable)	5	수명주기 동안 발생 가능성은 있지만, 발생하지 않음	10^{-9} to $\leq 10^{-8}$
발생 가능성이 전혀없음 (Incredible)	6	발생가능성도 희박하며, 절대 발생하지 않음	$\leq 10^{-9}$ 이하

표4-8. 위험도매트릭스의 정량적 심각도 기준표

치명적인 위험 (Catastrophic)	A	인명의 사망, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	3인 이상 사망	열차충돌
중대한 위험 (Critical)	B	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	1인 사망□ to ≤3인 사망	인명사상 열차탈선
중요하지 않은 위험 (Marginal)	C	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	1인 중상□ to ≤1인 사망	대규모 운행지연
사소한 위험 (Insignificant)	D	최소한의 상해, 직업상의 질병보다 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	1인 이하 중상	운행지연
신뢰성 관련 (Reliability Related)	R	인명이나 환경상에 피해를 발생하지 않으나 경제적 손실을 동반하는 위험	유지보수필요	성능저하

주) 1인 사망=10인 중상=100인 경상

대규모운행지연의 정의는 추후개신예정

열차충돌, 열차탈선, 인명사상은 관련법령(철도안전법 등)에 정의.

마지막으로 목표사고발생빈도를 제시하는 방식은 그림4-5의 철도사고에 대한 우리나라의 위험도관리기준과 같이 운영시나리오를 고려한 위험원으로 인한 사고발생빈도의 기준을 요구사항으로 제시하는 방식이다.

본 절에서 제시된 예 이외에도 다양한 유형의 장치 또는 시스템에 대한 안전목표가 공공 및 민간사업의 제안요청사항(RFP)에 활용되고 있으며, 발주자가 제시한 안전목표의 유형에 따라 제한사항 및 범위를 명확히 이해하여 기능별 SIL을 할당하고, 할당된 기능별 SIL의 입증 을 통해 안전확보를 증명하는 것이 중요하다.

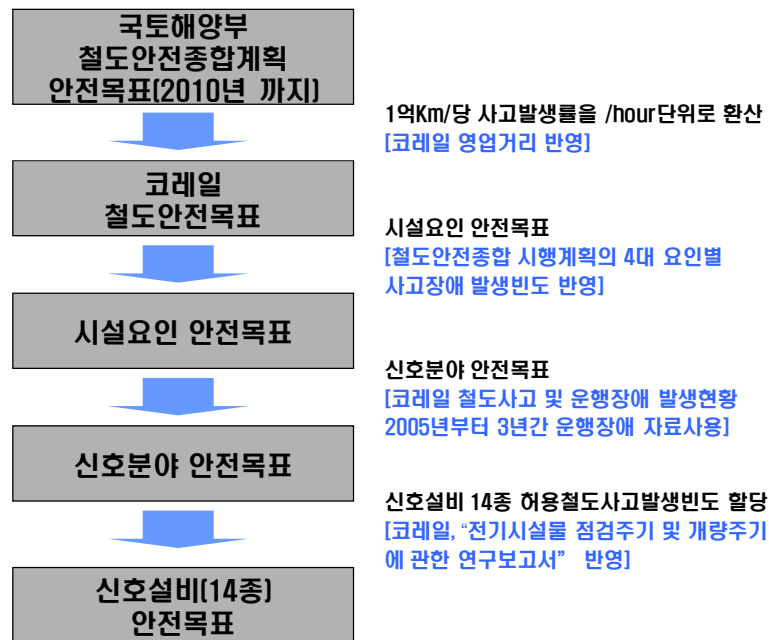


그림4-5. 우리나라 철도분야 국가의 사고억제 안전목표

라. 신뢰성 요구사항

정량적 신뢰도 목표는 표4-9과 같이 분류할 수 있다. 표4-9의 각 목표는 사용자의 경영 및 안전목표와 운영기간 동안 발생한 고장이력을 분석하여 수립하는 것이 최적의 안전확보 및 유지보수계획 수립을 위한 품질확보 방법이다. 그러나 운영기간 동안 발생한 고장이력이 없는 경우에는 신뢰성의 기본 취지에 따라 사용자의 경험을 근거로 구매대상 설비의 RAMS목표를 수립할 수 있다.

따라서 본 문서에서는 철도분야에 사용되는 궤도회로장치에 대한 운영기관의 경험을 설문을 통해 수집하고, 신뢰성이론 관련 수식을 근거로 신뢰도목표를 수립하는 예를 제시한다.

표4-9. 신뢰도목표의 분류

순번	RAMS목표	할당대상	할당목적
1	MTBSF	설비	열차운행지연 관련 고장성분의 정량적 목표로써 운영기관 가용도 목표를 만족하도록 관리하기 위해 할당
2	MTBF	설비의 LRU	LRU단위로 예방유지보수 계획수립 및 교정유지보수 시간관리를 목적으로 할당

궤도회로장치의 신뢰도목표 할당을 위해 표4-10의 정보를 사용자 설문 또는 근거자료를 통해 수집한다.

표4-10. 궤도회로장치 신뢰도목표 할당을 위한 설문

순번	설문내용	설문목적	운영자 답변	단위
TCQ1	분소단위 궤도회로의 평균수량	MTBSF할당		대
TCQ2	궤도회로 고장복구를 위해 소요되는 평균시간(열차운행 지장시간)	MTTSR할당		시간
TCQ3	분소의 궤도회로장치 고장으로 인한 연간 서비스불능의 허용시간	MTBSF할당		시간
TCQ4	궤도회로장치의 LRU구분 및 각각의 교체주기	LRU별 MTBF할당		시간

표4-10의 결과에 따라 궤도회로장치의 정량적 신뢰도목표는 표4-11과 같이 수립될 수 있다.

표4-11. 궤도회로장치의 정량적 신뢰도목표

순번	RAMS목표	산출방식
1	MTBSF	$(1 - \frac{TCQ3}{24 \times 365}) = \frac{TCQ1 \times MTBSF}{TCQ1 \times MTBSF + TCQ2}$
2	MTTSR	TCQ2
3	MTBF	LRU단위의 TCQ4

마. 유지보수성 요구사항

유지보수성은 고장발생의 전후에 따라 고장발생 전에 수행하는 예방유지보수(Preventive Maintenance)와 고장발생 후에 수행하는 교정유지보수(Corrective Maintenance)로 구분된다.

일반적으로 안전필수분야 RFP에 제시되는 요건으로는 고장발생 후 원상태로 복구하는데 소요되는 평균시간인 평균고장시간(MTTR)이 사용되며, MTTR의 산출은 하부구성요소(LRU)단위 고장률에 LRU별 MTTR을 고려하여 산출한다. 이때 산출기준으로는 MIL-HDBK-472가 가장 많이 적용된다.

2. 요구사항의 달성 가이드

본 절에서는 위험원의 관리를 통한 안전입증 절차를 소개하고, 위험원의 발생빈도와 신뢰도의 입력인자인 고장률의 예측과 입증방법을 제시한다.

가. 위험원별 위험도평가에 의한 안전확보 가이드

철도운영에서 열차제어시스템의 고장, 결함은 열차충돌, 탈선 등 파국적인 사고를 초래하기 때문에 열차제어시스템에 대한 위험관리와 안전성 인증의 중요성은 국제적으로 강조되어 왔다.

이를 위해 국제규격인 IEC 62278은 전기/전자/프로그래머블 제어기로서 열차제어시스템의 RAMS(신뢰성, 가용성, 유지보수성 및 안전성) 요구사항을 IEC 62425(EN 50129)는 제어시스템에 적용되는 전자시스템에 대한 안전요건 그리고 열차방호를 위한 열차제어시스템의 신호통신처리 소프트웨어의 안전요건으로서 IEC 62279(EN 50128) 등이 열차제어시스템의 안전성 관련 국제규격으로 제정되어 있다.

국내 철도도 열차제어시스템 대부분이 컴퓨터화된 전자장비로 구성됨에 따라 특별한 징후 없이 발생하는 제어기의 내부고장에 대한 위험측 고장요인을 분석하고, 그 발생빈도와 피해 심각도를 일정수준 이하로 관리하기 위한 위험도(Risk)평가를 핵심으로 하는 안전연구를 지속해 왔다.

현재 한국철도공사(KORAIL) ATP시스템 도입사업의 예와 같이 위험도 평가를 통해 안전 요구사항을 도출하고 이를 근거로 시스템 안전성을 판단하고 있으며, 유럽 각국에서도 철도운영환경에 따라 영국 ALARP(As Low As Reasonably Practicable), 프랑스 GAMAB, 독일 MEM 등 위험도 평가에 기반한 적절한 안전관리 원칙을 적용하고 있다.

특히 영국철도는 국제규격과 유럽규격을 준수하여 열차제어시스템의 개념설계부터 폐기까지 전 수명주기 동안 위험원(Hazard)을 도출하고 위험도를 평가하여 허용수준 이하로 관리하는데 필요한 안전활동의 문서화 및 승인절차를 철도시설관리자(Network-Rail)가 Yellow Book이라는 지침으로써 권고하고 있으며, 여기서 안전성을 판단하는 핵심원칙으로서 ALARP을 적용한다.

본 절에서는 현재 국내 열차제어시스템에 대한 안전성 입증활동 사례로서 한국철도공사의 차상신호시스템 도입사업인 ATP시스템 지상장치에 대한 인터페이스 안전성 활동을 분석하고, ALARP이론을 적용하여 안전성 입증이 가능한지를 검토하였다. 그리고 ALARP 원칙에 따른 위험도 평가를 적용하기 위한 가정 및 요구 데이터를 분석하여 향후 국내 철도시스템의 안전입증에 필요한 요구사항을 도출하고자 한다.

국내 열차제어시스템에 대한 안전성활동은 2001년 철도청(KNR)의 "철도신호제품에 대한 신

뢰성과 안전성 검증기준 제정연구”와 2001년 철도청지시 2001-49호 “열차제어시스템 안전성 확보 기술 권고안”을 시작으로 열차제어시스템의 위험원을 도출(Identification)하고 위험도를 평가하여 허용 가능한 수준으로 완화하기 위한 체계를 수립하였다. 이후 이러한 안전성 활동은 2002년 KORAIL “통합관제실 CTC 소프트웨어의 안전성연구” 및 2004년 KORAIL “차상신호(ATP)시스템 도입사업의 RAMS활동”까지 적용되면서 2005년 철도안전법 제정에도 기여하였다.

이와 같은 위험분석 및 위험도 평가를 기반으로 하는 국내 열차제어시스템 안전성활동체계를 그림4-6에 제시한다. 예비위험원분석을 통해 ATP시스템에 내제된 위험원을 도출하고 이들의 위험도를 완화할 수 있는 안전대책을 시스템설계 단계의 안전요구사항으로 활용한다.

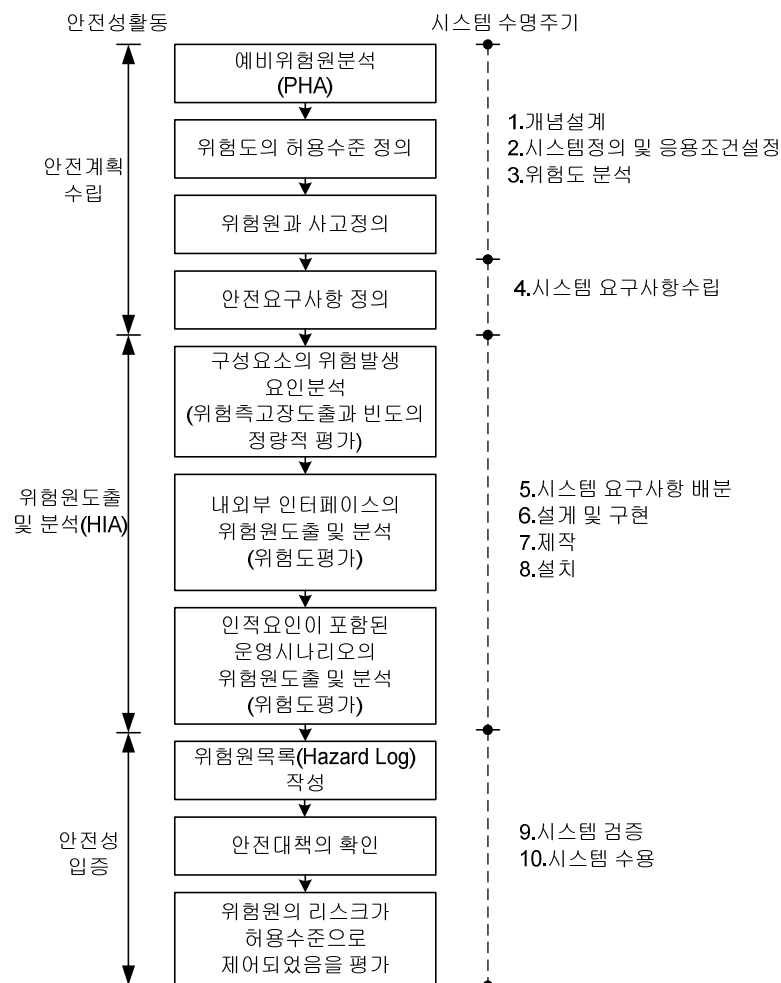


그림4-6. 위험도 평가를 통한 안전성 입증의 업무흐름

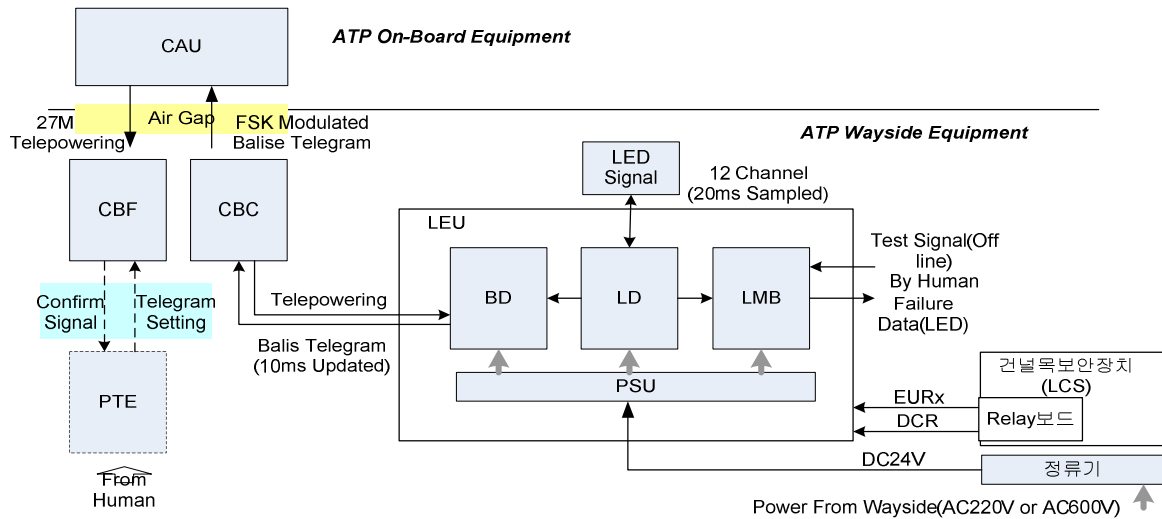
이때 위험도의 허용수준은 앞에서 제시한 ALARP이론과 같은 이론적 평가기준을 사용할 수

있으나, ATP시스템 안전성활동에서는 표4-12와 같은 위험도 허용수준을 안전계획서(Safety Plan)에 설정하여 해당 위험원이 허용할 수 있는 수준으로 제어됨을 입증하는 것으로 수행한다. 따라서 시스템의 모든 위험원에 대해 표4-12의 위험도 허용수준을 적용하여 "Intolerable, Undesirable" 영역의 위험원에 대해서는 안전대책을 검토하여 "Tolerable, Negligible"영역으로 위험도가 완화되었음을 입증하는 종합안전대책기술서(Safety Case)를 작성하고 이를 독립안전성평가자(ISA, Independent Safety Assessment)나 최종사용자가 승인하는 것으로서 안전성입증 활동이 종료된다.

표4-12. ATP시스템의 위험도 허용수준 매트릭스

설 명	치명적인위험 (Catastrophic) 3인이상 사망	중대한 위험 (Critical) 1인이상 사망, 3인미만 사망	경미한 위험 (Marginal) 1인이상 중상, 10인미만 중상	사소한 위험 (Insignificant) 1인이상 경상, 20인미만 중상
빈번한 발생 (Frequent) [10-3/h초과]	Intolerable	Intolerable	Intolerable	Undesirable
가능성 있는 발생 (Probable) [10-4초과, 10-3/h이하]	Intolerable	Intolerable	Undesirable	Tolerable
종종 발생 가능 (Occasional) [10-6초과, 10-4/h이하]	Intolerable	Undesirable	Undesirable	Tolerable
발생가능성이 미약함(Remote) [10-8초과, 10-6/h이하]	Undesirable	Undesirable	Tolerable	Negligible
발생가능성이 거의없음(Improbable) [10-9초과, 10-8/h이하]	Tolerable	Tolerable	Negligible	Negligible
발생가능성이 전혀없음(Incredible) [10-9이하]	Negligible	Negligible	Negligible	Negligible

ATP시스템 지상장치의 내부구성 및 인터페이스는 그림4-7과 같다.



LD : Lamp Detector / BD : Balise Driver / CAU : Compact Antenna Unit
 CBF : Compact Balise Fixed / CBC : Compact Balise Controller
 PSU : Power Supply Unit / LCS : Level Crossing
 LMB : LEU Monitoring Board / LEU : Line-side Electronic Unit
 PTE : Programming Test Equipment

그림4-7. ATP시스템 지상장치 구성도

ATP시스템 지상장치 인터페이스는 ATP지상장치와 기존 KORAIL장치와의 물리적 인터페이스를 범위로 하며, 위험원 도출을 위해 인터페이스별로 Guide Word를 기준으로 이상현상(Deviation)을 예측하여 위험원을 도출하는 HAZOP Study기법을 사용하였다.

ATP지상장치의 인터페이스 요인은 선로변전자유닛(LEU, Line-side Electronic Unit)의 아날로그 전원입력, 신호기상태 검지를 위한 비접촉방식 아날로그 입력, 건널목 제어기와의 인터페이스인 지장물검지계전기와 경보장치 고장검지계전기의 접점입력, ATP차상장치와의 텔레파워링 및 텔레그램신호, LEU의 자기검사기능 등으로 구성된다. 표4-13은 5현시 구간의 신호기 입력에 대한 HAZOP Study의 예이다.

HAZOP Study 워크시트는 국제규격에서 제시하지만 차상신호(ATP)시스템 도입사업의 위험원 도출에서는 FMECA(Failure Mode Effect and Criticality Analysis)의 장점인 위험원별 위험도평가를 HAZOP Study 워크시트에 포함시켜 동시에 수행하도록 별도의 양식을 표4-13과 같이 구성하였다. 따라서 위험원 도출과 함께 사고결과에 따른 위험원의 관리와 안전대책 반영 후의 위험도평가를 통해 안전계획서에 제시된 안전의 허용수준 만족여부를 정량적 기준에 의해 평가할 수 있다.

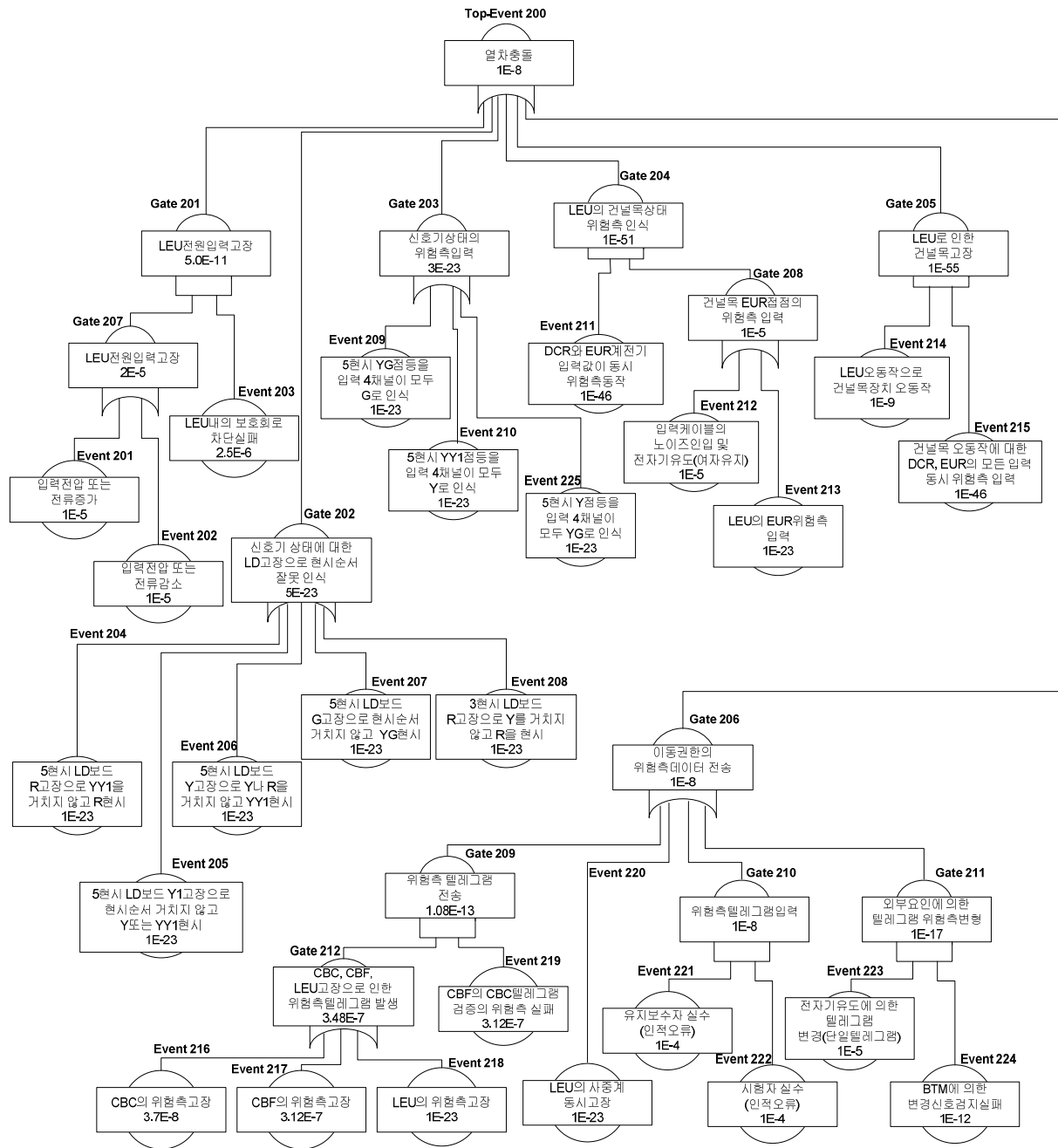


그림4-8. 위험원분석을 위한 FTA 예(ATP시스템 지상장치 IF)

HAZOP Study를 통해 도출된 위험원은 PHA에서 도출된 위험원의 하부 위험원으로써, 위험원을 발생시키는 원인(Casual Effect)에 가까운 형태로 주어진다.

표4-13. ATP지상인터페이스의 HAZOP Study 예(5현시 신호기와 LEU의 인터페이스)

HAZOP Study 대상: LD 입력(5 현시구간 G)																
참조도면번호: 근거 3							갱신번호: V1.0					소요시간: 부록 A 참조				
참여구성원: ATP 시스템 RAMS 컨설팅부서, 시스템 검토그룹(SEG), ATP 지상장치 설계제작사 엔지니어																
기능		Guide Word	이상현상	원인	결과(ATP 지상의 최종상태)	대전 Risk F S R			안전대책	대후 Risk F S R			세부조치내역	조치주체		
LD 입력 (5 현시구간 G)	No		신호기의 상태와 관계없이 단일상태로 고정	LEU의 LD 보드고장	상용제동 (장애 텔레그램 전송)	3	D	3D	다중화 설계	6	D	6D	LEU의 LD 보드 구성을 사중계방식으로 구현	BT		
	More		입력전류의 과다 (허용전류 이상)	LEU-신호기 케이블 이상 신호 유도	상용제동 (장애 텔레그램 전송)	3	D	3D	실드케이블 사용	4	D	4D	LEU-신호기 실드케이블 사용	TJ		
									보호회로 내장				과전류방지회로 (내부전원감시 및 차단회로)	BT		
	Less		입력전류의 미흡 (5W 미만-3W 이상)	LD 내부 전원불량	상용제동 (장애 텔레그램 전송)	3	D	3D	전원감시에 의한 차단	4	D	4D	LD의 전원상태 감시회로 (신호기 상태입력 전송)	BT		
				단선등에 의한 케이블저항증가												
	As well as		해당 없음													
	Part of		충분한 상태입력이 유지되지 않음(20msec 이하)	신호기 점등고장 (ABS EIS 고장)	or	운행지연 (G 신호 전송 실패)	-	-	-	없음	-	-	-	프로젝트의 범위를 벗어남	-	
				LEU의 LD 보드고장		정상동작	-	-	-	안전측설계	-	-	-	20ms 단위의 실시간 신호기상태 감시(신호기 최종 입력상태를 유지)	BT	
	Reverse		신호기 입력(점등) 반대상태 (신호기 소등으로 인식)	LEU의 LD 보드고장	비상제동 (정지 텔레그램 전송)	3	A	3A	고장진단논리	6	A	6A	모든 신호기 정지텔레그램 전송되도록 소등시 BD의 논리를 구현	BT		
			신호기 입력(점등) 반대상태 (신호기 YG 점등을 Y로 인식)	LEU의 LD 보드고장	운행지연 (안전측텔레그램 전송)	-	-	R	다중화 설계	-	-	R	LD와 BD를 사중계로 구성하여 고장률을 SIL4 수준으로 확보	BT		
			신호기 입력(소등) 반대상태 (신호기 YG으로 인식)	LEU의 LD 보드고장	운행지연 (안전측텔레그램 전송)	-	-	R	다중화 설계	-	-	R	LD와 BD를 사중계로 구성하여 고장률을 SIL4 수준으로 확보	BT		
			신호기 입력(소등) 반대상태 (신호기 YY1G로 인식)	LEU의 LD 보드고장	상용제동 (장애 텔레그램 전송)	3	D	3D	고장진단논리	6	D	6D	YY1G가 점등되면 고장으로 인식하는 논리를 BD에 적용 (장애텔레그램 전송)	BT		
			신호기 입력(소등) 반대상태 (신호기 G 소등을 RG로 인식)	LEU의 LD 보드고장	상용제동 (장애 텔레그램 전송)	3	D	3D	다중화 설계	6	D	6D	RG가 점등되면 고장으로 인식하는 논리를 BD에 적용 (장애텔레그램 전송)	BT		
			신호기 입력(소등) 반대상태 (신호기 G 소등을 RG로 인식)	LEU의 LD 보드고장	상용제동 (장애 텔레그램 전송)	3	D	3D	다중화 설계	6	D	6D	RG가 점등되면 고장으로 인식하는 논리를 BD에 적용 (장애텔레그램 전송)	BT		
	Other than		신호현시순서와 상이한 입력	신호기 점등고장 (ABS EIS 고장)	or	열차충돌 (G 신호 전송 실패)	-	-	-	없음	-	-	-	프로젝트의 범위를 벗어남	-	
				LEU의 LD 보드고장		열차충돌 (G 신호 전송 실패)	3	D	3D	고장진단논리	6	D	6D	현시순서를 지키지 않고 YG를 현시(LEU의 상태입력에서 오류가 발생하여 현시순서가 잘못 입력될 확률은 LD 보드 사중화로 인해 SIL4 수준으로 확보. 따라서, 입력 20msec 단위로 샘플링하여 최종 신호기상태에 해당하는 텔레그램 전송)	BT	
	Early		해당 없음													
	Late		해당 없음													
	Before		해당 없음													
After		해당 없음														

LD : Lamp Detector / BD : Balise Driver / LEU : Line-side Electronic Unit / SIL : Safety Integrity Level / ABS : Automatic Block System / EIS : Electronic Interlocking System

따라서 각각의 하부 위험원 결과의 발생빈도는 그림4-8과 같이 결함트리 분석기법을 사용

(FTA분석의 이벤트 발생확률 입증자료의 예는 표4-14와 같다.)하며, 각각의 위험원에 대한 심각도를 표4-15와 같이 가정한 후 위험도를 평가하여 정량적 위험도의 평가결과와 요구사항을 비교한다.

표4-14. FTA이벤트의 산출근거 예

이벤트번호	산출근거	적용빈도[h]
Event 203	LEU의 기능고장 2.5E-6 Reference : 구성요소 기능의 HIA보고서 (CP04011-ETC-0169)	2.5E-6
Event 204	LEU의 위험측고장(LEU기능고장률 2.5E-6의 4배) Reference : 구성요소 기능의 HIA보고서(CP04011-ETC-0169)	1E-23

HAZOP Study를 통해 도출된 위험원은 안전대책이 적용된 최종시스템의 위험도 평가를 위해 그림4-8의 FTA분석에서와 같이 PHA에서 도출된 위험원을 최상위 위험원으로 선정하여 인적오류가 포함된 최종위험원의 발생빈도를 평가한다. 물론 이러한 정량적 발생확률의 표현이 용이하지 않은 이상 현상에 대해서는 표4-16과 같은 가정이 추가되며, 표4-15의 심각도 분류 가정과 마찬가지로 안전계획서 또는 해당 보고서를 통해 최종사용자 또는 독립안전성평가조직의 승인을 받는다.

표4-15. ATP시스템의 심각도 분류에 따른 해당사고의 가정

심각도	등급	설 명	해당사고
치명적인 위험 (Catastrophic)	A	인명의 사상, 시스템의 손실 또는 심각한 환경상의 피해를 유발하는 위험	열차충돌
중대한 위험 (Critical)	B	심각한 인명의 상해, 직업상의 질병 및 중요한 시스템 또는 환경상의 피해를 초래하는 위험	인명사상
중요하지 않은 위험 (Marginal)	C	최소한의 상해, 직업상의 질병 및 최소한 시스템 또는 환경상의 피해를 초래하는 위험	비상제동
사소한 위험 (Insignificant)	D	최소한의 상해, 직업상의 질병보다는 작고, 최소한의 시스템 및 환경상의 피해보다 작은 영향을 초래하는 위험	상용제동
신뢰성관련 (Reliability Related)	R	인명이나 환경상에 피해를 발생하지 않으나 경제적 손실을 동반하는 위험	운행지연

표4-16. 발생빈도 정량화를 위한 가정

이상요인	산출근거	적용빈도[h]
전원 및 신호이상	ATP시스템에 공급되는 전원이나 신호의 이상확률로써, 프로젝트의 범위를 벗어나는 사항에 대하여 일괄 적용한다.	1E-5
인적오류	사용자의 인적오류에 대한 발생빈도를 일괄 적용한다.	1E-4

표4-17. ATP 지상장치 인터페이스 위험원 목록 사례

위험원 ID	위험원 설명	최종 Risk			사고 결과 (영향 분석)	원 인	관련 장치	관련 구성 요소	안전대책	기타사항 (조치주체)	상태
		F	S	R							
HIF-W S002	유지보수 인력 보호실패	4	B	4B	인명 사상	1. 유지보수작업 오류 2. 유지보수관리 절차 실패	ATP 지상 장치	지상장치 유지보수	1.운영기관 관련규정 준수 2.유지보수시 열차방호 및 작업 구간 관리에 대한 절차구축	1.KR 2.KR	완료
HIF-W S003	장애텔레그램 전송에 의한 열차 상용제동 발생	3	D	3D	상용제동	1. 전원계통이상 2. 3현시에 대한 LD보드 고장 3. 5현시에 대한 LD보드 고장	ATP 지상 장치	LEU의 신호기 상태 입력(LD보드)	1.LEU내부의 LD전원감시 기능 포함 2.신호기 비가용상태 안전측 현시시에 장애텔레그램 전송 3.신호기 상태를 실시간 검지하여 고장시 장애텔레그램 송신	1.BT 2.BT 3.BT	완료

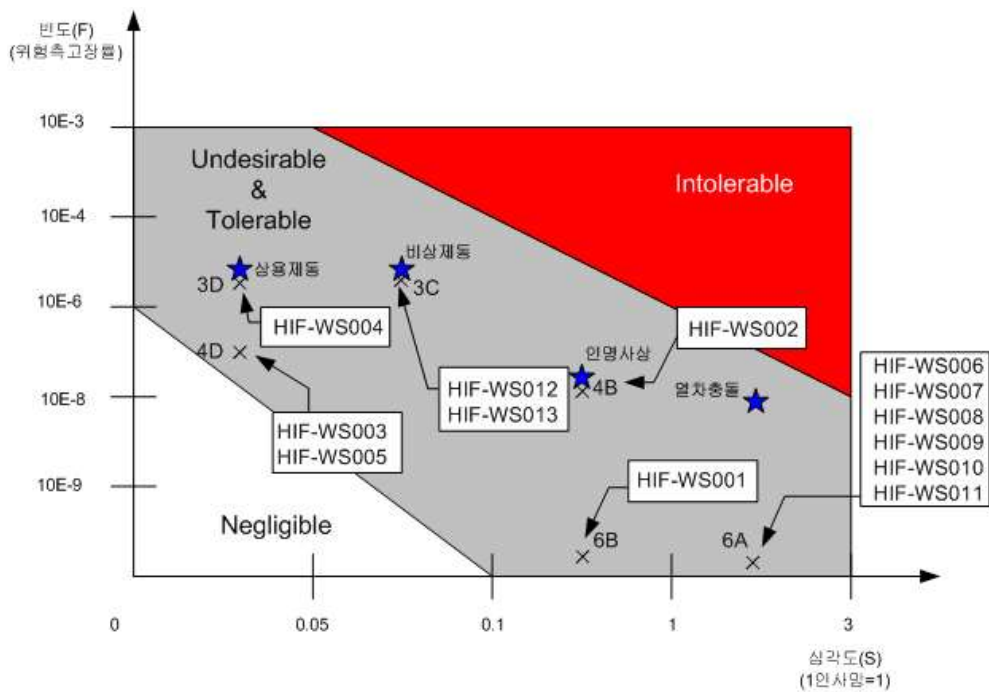


그림4-9. ATP 차상신호시스템 지상인터페이스 안전성 입증

영국철도는 ALARP이론으로 안전성을 입증하기 위해 Yellow Book에서 그림4-10과 같은 7단계의 안전성활동 절차를 제시하고 있다.

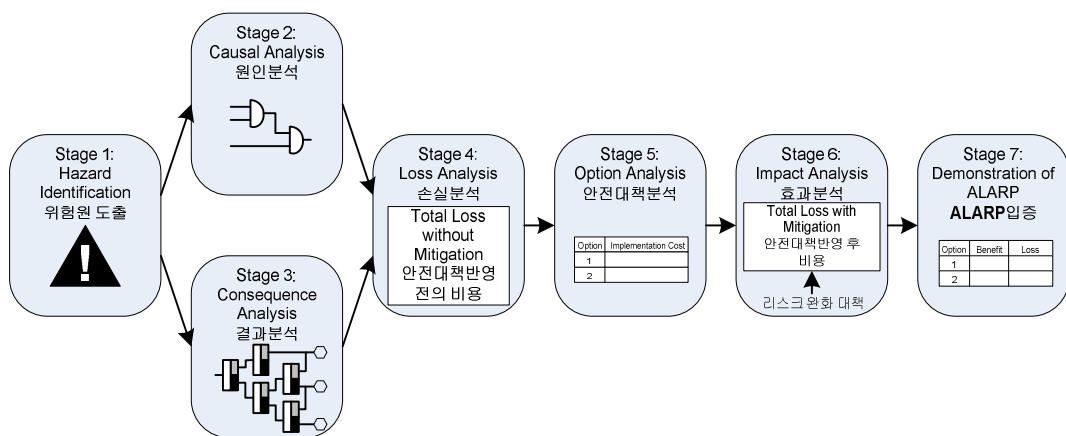


그림4-10. ALARP이론을 적용한 영국철도 안전활동 7단계

7단계 안전성활동 중 1단계와 2단계인 위험원도출 및 분석은 국내 열차제어분야 위험도평가 방식 안전활동의 HIA(Hazard Identification and Analysis)와 동일하게 수행되지만, 3단

계의 결과분석과 4단계의 손실분석은 위험도 평가방식의 빈도분석과 약간의 차이점을 가지고 있다. 국내 위험도 평가방식에서는 위험도의 정량화를 위해 위험원의 발생빈도계산을 안전대책이 모두 반영된 시스템의 최종상태와 인적오류의 발생빈도에 대한 가정을 통해 시스템의 최종상태에 대한 위험도를 평가하는 반면, Yellow Book에서는 안전대책과 인적오류를 빈도분석과 별도로 이벤트트리(ETA, Event Tree Analysis)형태의 결과분석으로 분류하여 수행한다. 이러한 방식은 기존 철도사고의 손실비용을 기반으로 위험원으로 인한 사고의 손실분석을 수행한다.

ATP시스템 지상장치 인터페이스에 대한 안전성활동을 Yellow Book에서 제시하는 7단계 활동으로 수행하면 그림4-8의 결합트리분석결과는 안전활동의 3단계와 4단계에서 그림4-11과 같이 변경된다. ALARP이론은 안전대책의 적용 전과 적용 후의 손실비용을 별도로 산출해야 한다. 그림4-11은 FTA와 ETA를 통한 위험원의 원인 및 결과분석을 안전대책의 적용 전 시스템을 대상으로 계산한 결과이다.

ALARP이론을 만족하기 위한 손실분석을 위해서는 발생한 사고의 사회적 손실비용을 계산해야 한다. 현재 국내에는 위험원의 결과분석으로 도출된 운행지연(상용제동), 비상제동, 열차충돌에 대한 운영환경별 사회적 비용이 제시되어있지 않으므로, 영국의 손실비용을 가정으로 활용한다.

영국 철도에서는 치명적 사상(Fatalities), 심각한 사상(Major Injurers), 경미한 사상(Minor injuries)에 대하여 각각의 비율을 아래와 같이 정의하고 있다.

$$1 \text{ Fatality} = 10 \text{ Major Injury} = 200 \text{ Minor Injury}$$

따라서, 그림4-11의 위험원 결과분석에 따른 상용제동, 비상제동, 열차충돌에 대하여 각각의 인명손실의 크기와 경제적 손실비용을 표4-18과 같이 가정해야 한다.

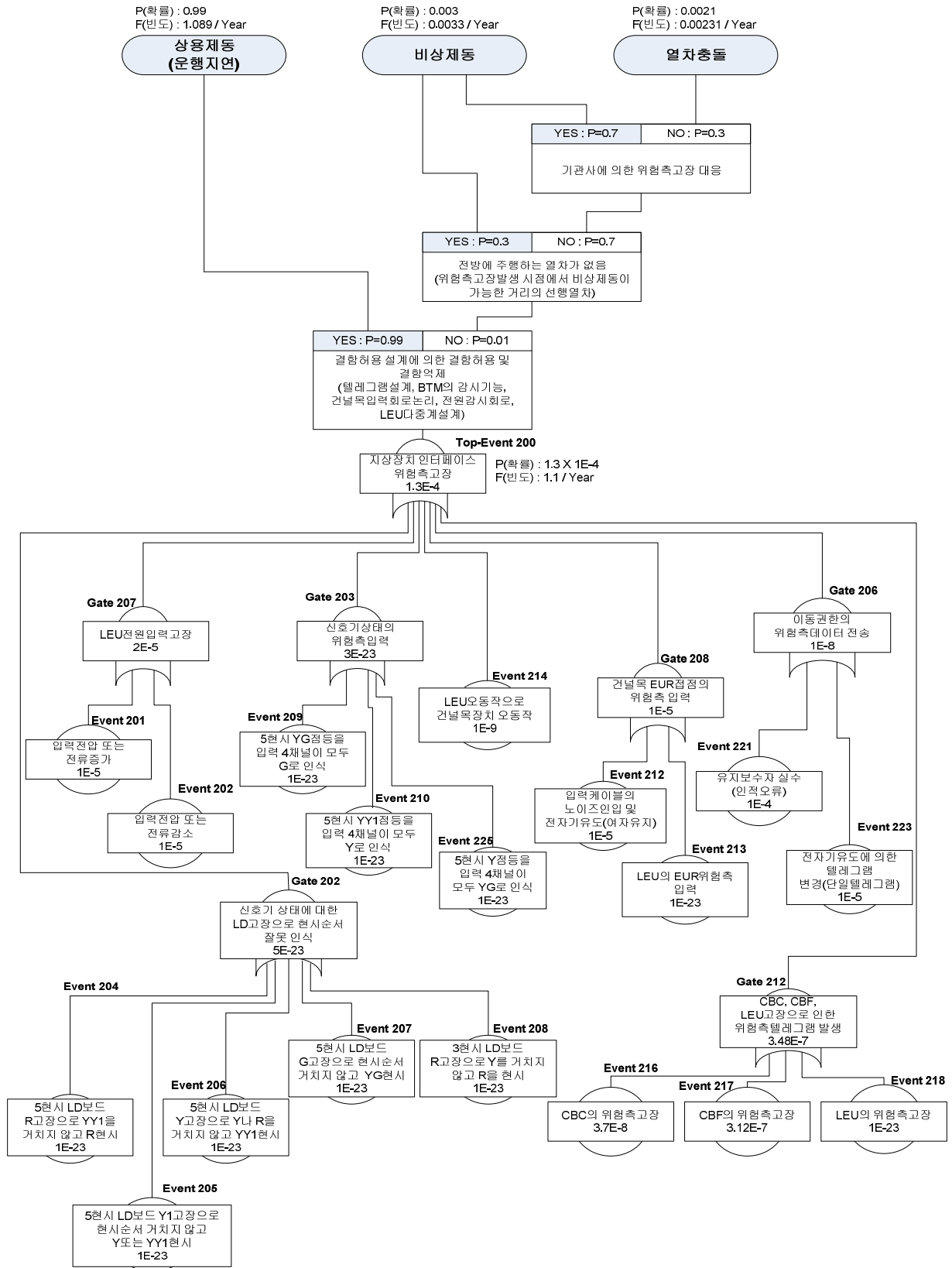


그림4-11. 위험원의 원인과 결과분석 예(ATP 지상장치 IF)

표4-18. 사고결과의 인명손실과 경제적손실의 가정 예

사고결과	인명손실	경제적 손실
열차충돌	30 치명적 사상 50 심각한 사상 200 경미한 사상 합계 36 치명적 사상	720억원
비상제동	2 심각한 사상 6 경미한 사상 합계 0.23 치명적 사상	4.6억원
상용제동 (운행지연)	2 경미한 사상 합계 0.01 치명적 사상	0.2억원

주) 치명적 사상 1건의 경제적 손실은 20억원(1백만 파운드)으로 가정

각각의 사고결과는 가정에 의해 산출된 손실을 정량적인 경제적 가치로 환산하기 위해 그림 4-11에서 도출된 발생확률을 곱하여 연간손실비용을 표4-19와 같이 산출한다.

표4-19. ATP지상장치 인터페이스관련 사고의 손실분석

사고결과	손실분석	연간손실비용
열차충돌	720억원 × 0.00231	1.663억원
비상제동	4.6억원 × 0.0033	0.015억원
상용제동 (운행지연)	0.2억원 × 1.089	0.217억원
	합 계	1.895억원

위험원으로 인한 사고의 손실분석까지 완료되면 그림4-10의 5단계인 안전대책의 비용분석을 수행한다. 안전대책에 소요되는 비용은 설계비용 및 시스템변경비용 그리고 변경된 설계가 반영된 시스템의 유지보수비용을 모두 연간소요비용으로 산출하며, 이를 표4-19의 안전대책 반영 전 연간손실비용과 비교하면 표4-20와 같다.

표4-20의 안전대책 A를 적용한 후 연간 사고의 손실비용 0.11억원과, 안전대책이 적용된 시스템의 안전대책을 위한 연간 추가 유지보수비용 1억은 가정으로써, 실제 안전대책이 수립

된 이후에 소요비용이 정량적으로 산출되어야 한다.

따라서 표4-20의 비교결과 대책A는 안전대책 적용 전후 사고손실비용의 차가 안전대책을 위한 투자비용보다 크므로 대책A는 반영되어야 하며, 대책B는 안전대책 적용 전후 사고손실비용의 차가 안전대책을 위한 투자비용보다 작으므로 반영하지 않는다. ALARP이론은 표4-20과 같이 예측할 수 있는 안전대책에 대하여 모두 손익을 계산하여 위험원목록과 함께 안전승인기관의 승인을 받아야 하며, 이때 모든 안전대책이 고려되었는가의 보장은 종합안전대책기술서의 절차를 토대로 승인기관이 활동의 건전성을 정성적으로 평가하여 시스템의 안전성확보를 승인한다.

표4-20. ALARP이론을 적용한 안전입증 예(ATP지상장치 인터페이스)

	연간손실 (억원/년)	대책으로 인한 연간이득(억)	대책을 위한 연간비용(억원)	대책의 필요성
현재설계	1.895	-	-	-
대책 A	0.11 ¹⁾	1.785 ²⁾	1.00 ³⁾	Yes
대책 B	1.55 ¹⁾	0.345	1.00	No

주1)은 안전대책을 적용한 후 손실분석에 의한 결과

주2)변경 전 손실비용에서 변경 후 손실비용을 제한 값

주3)변경에 소요되는 비용을 연간비용으로 환산한 값

안전성확보를 입증하기 위한 절대적인 방법은 현재까지 존재하지 않는다. 다만, 안전입증을 승인해야 하는 최종사용자는 안전성활동절차의 합리성과 객관성의 향상을 지향한다는 공통의 목표를 갖는다.

ALARP이론은 영국철도에서 반영되어 많은 수행실적과 검증을 거친 방법으로, 경제적 이득이라는 정량적 가치기준을 사용함으로써, 안전성활동의 합리성에는 긍정적인 효과를 주는 것이 자명하다. 하지만 현재 국내철도의 열차제어시스템 안전성분야에 ALARP을 적용하기 위해서는 프로젝트 전주기에 걸쳐서 비용을 예측하고 평가하는 비용기반수명주기관리(LCC, Life Cycle Cost)기법 등이 먼저 전제되어야 한다.

표4-21. 위험도평가방식과 ALARP이론의 가정요인에 대한 분석

	위험도평가방식	ALARP이론
가정요인	1. 허용할 수 있는 위험도수준 2. 인명사상의 심각도에 대한 클래스 화 3. 인적오류에 대한 발생빈도 4. 자연재해의 발생빈도	1. 사고별 손실비용 2. 인적오류 3. 인명사상의 심각도에 대한 클래스 화
가정의 정당화	최종사용자 또는 독립안전인증기관의 승인 취득	과거 사고데이터의 연구로써 손실비용 및 발생빈도의 정량화와 지속적인 관리

또한, 표4-21과 같이 위험도평가방식과 ALARP이론을 적용하기 위한 각각의 가정요인 항목비교에서와 같이 사고에 대한 사회적 손실비용, 인적오류에 대한 정량화기법 그리고 사고의 빈도와 심각도에 대한 기준의 확립이 무엇보다 중요하다. 이러한 가정요인의 최소화는 안전성 활동의 객관성과 비례할 것이다.

나. 고장률 예측에 대한 가이드

열차제어시스템의 신뢰도는 시스템을 구성하는 부품의 고장률예측으로부터 출발한다. 따라서 우발적으로 발생하는 전자부품의 고장률을 정량적으로 예측하기 위해 본 보고서에서 미국 방성 전자부품고장률의 예측지침인 MIL-HDBK-217F를 사용하여 하부시스템단위 고장률을 정량화한다. 예측된 고장률을 토대로 MTBF 만족여부를 판단하고, 시스템 고장률증가의 주요원인을 분석하여 시스템 고장률을 감소시킨다. 또한 가용도는 시스템고장 특성을 지수고장모델로 모델링하여 신뢰도함수를 도출하고 시간에 따른 시스템의 신뢰도를 계산한다.

핵심장치가 전자부품으로 구성된 열차제어시스템의 신뢰도는 하부시스템단위로 고장률을 예측하고, 다중계 특성을 고려한 하부시스템 연관관계를 분석하여 전체시스템의 신뢰도를 예측한다. 따라서 하부시스템의 고장률예측이 전체시스템 고장률예측에 기본이 되므로 하부시스템단위 고장률예측을 먼저 수행한다.

MIL-HDBK-217F에서는 전자부품의 종류를 그림4-12와 같이 분류하고, 고장형태에 따른 고장률예측 방정식을 제공하여, 방정식을 구성하는 Pi값에 사용된 부품의 특성 및 환경조건을 대입하여 부품단위 고장률을 예측한다. 하부시스템 고장률예측을 위해 자동화도구인 Relex7.7을 사용한다. Relex7.7은 다음 식과 같은 메모리소자의 고장률방정식과 같이 하부시스템별 고장률수식을 사용부품관련 정보에 따라 계산하는 자동화 도구이며, 항공우주, 철도,

원자력 등에서 사용하는 MIL규격 외에도 가전에서 사용하는 Telcordia 또는 Bellcore기준을 적용할 수 있다. 또한, 시스템 사용온도조건에 따른 고장률예측 등을 지원하여, 시스템 설계단계에서 고장률의 최소화를 위한 설계보완을 지원한다.

$$\lambda_p = (C_1\pi_T + C_2\pi_E + \lambda_{CUC})\pi_Q\pi_L$$

표4-22는 위 식에 사용된 Pi값의 의미이다.

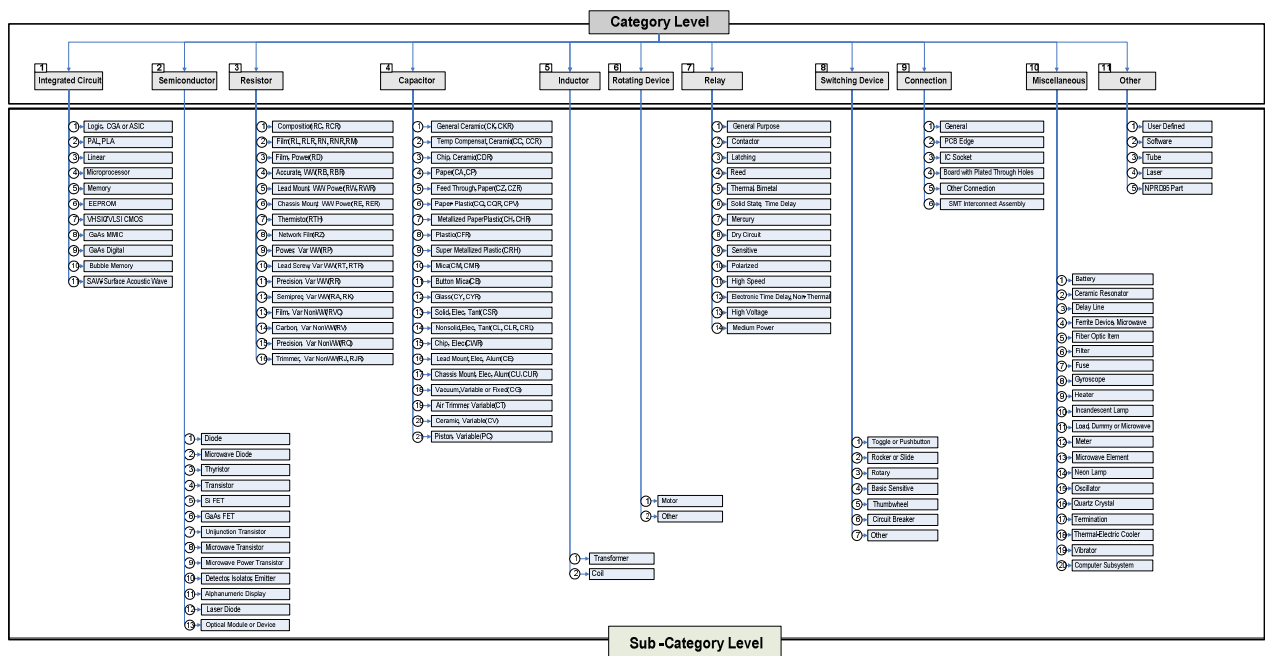


그림4-12. 고장률예측을 위한 전자부품의 분류체계(Relex 7.7)

표4-22. 메모리의 고장률예측을 위한 입력변수

기호	입력변수의 의미
C_1	Die Complexity Failure Rate
π_T	Temperature Factor
C_2	Package Failure Rate
π_E	Environment Factor
λ_{CUC}	EEPROM Read/Write Cycling Induced Failure Rate
π_Q	Quality Factor
π_L	Learning Factor

하부시스템 고장률예측을 위해서는 표4-23과 같이 하부시스템 부품정보(BOM, Bill of Material)를 그림4-13과 같이 자동화도구(Relx7.7)를 사용하여 하부시스템단위로 고장률과 MTBF를 예측한다. 따라서, 고장률의 예측을 위한 BOM의 작성은 설계자와 RAM엔지니어가 함께 작업을 수행해야 한다.

RAM엔지니어는 MIL-HDBK-217의 입력요건에 적합한 설계자의 BOM작성을 지원해야 하며, 작성된 BOM에 의한 하부시스템 또는 전체시스템의 고장률 예측치를 토대로 설계목표 만족을 위한 자문을 수행한다. 표4-23은 열차제어시스템 고장률예측을 위해 RAM엔지니어가 설계자에게 양식을 제공하여 설계자가 작성한 BOM의 예이다.

The screenshot shows the Relx software interface with the title bar 'Relx - [G7_ATC.RPJ]'. The menu bar includes File, Edit, View, Insert, Tools, Project Tree, Window, and Help. The toolbar contains various icons for file operations and analysis. The main window is divided into two panes. The left pane, titled 'System Tree', displays a hierarchical tree structure of the system components. The right pane, titled 'FMEA. Assembly IC', shows a table for FMEA analysis.

System Tree

Name	Part Number	Reference D...	Description	Failure Rate
ATC_system	System		Top-level ass...	427.921694
ATC_onbard				320.604767
불연속신기				15.372306
IC				7.252983
Diode				0.098420
Transistor				7.062581
Resistor				0.045219
Capacitor				0.766294
Inductor				2.72693E-4
Connector				0.046145
Other				0.100391

Assembly IC

Part Number	Category	Subcategory	Reference Designator	Quantity	Failure Rate	Failure Rate, Percentage	Tagged Part
1	Integrated Circuit	VHSIC/WSI CMOS	U1, U6, U10	4.00	0.617275	8.51	
2	Integrated Circuit	VHSIC/WSI CMOS	U2 ~ U5, U	10.00	1.543188	21.28	
3	Integrated Circuit	VHSIC/WSI CMOS	U7, U107	2.00	0.308638	4.26	
4	Integrated Circuit	VHSIC/WSI CMOS	U8, U108	2.00	0.308638	4.26	
5	Integrated Circuit	VHSIC/WSI CMOS	U9, U12, U1	6.00	0.925913	12.77	
6	Integrated Circuit	VHSIC/WSI CMOS	U11, U15, U	4.00	0.617275	8.51	
7	Integrated Circuit	VHSIC/WSI CMOS	U17, U117	2.00	0.308638	4.26	
8	Integrated Circuit	VHSIC/WSI CMOS	U51, U52	2.00	0.308638	4.26	
9	Integrated Circuit	VHSIC/WSI CMOS	U18, U118	2.00	0.308638	4.26	
10	Integrated Circuit	VHSIC/WSI CMOS	U13, U50, U	3.00	0.462956	6.38	
11	Integrated Circuit	VHSIC/WSI CMOS	U10, U110	2.00	0.308638	4.26	
12	Integrated Circuit	VHSIC/WSI CMOS	U14, U114	2.00	0.308638	4.26	
13	Integrated Circuit	VHSIC/WSI CMOS	X1, X101	2.00	0.308638	4.26	
14	Integrated Circuit	VHSIC/WSI CMOS	U53, U54	2.00	0.308638	4.26	

The bottom of the window shows a status bar with the text 'For Help, press F1' and a table of data including 'MIL-HDBK-217 FN2', 'FPMH', and 'Record 0'.

그림4-13. 자동화도구를 사용한 고장률예측

표4-23. ATC 연속수신보드에 사용된 IC의 예

Cat	Sub Cat	Part Num	Description	Qty	Ref	Man	Oper Pow (W)	Power Rat (W)	Case Temp (°C)
1	4	-	TMSP32032PCMA50	2	U 1 0 , U30	TI	0.3	1.95	31.0
1	6	-	AT290010A	2	U 1 1 , U31	ATMEL	0.15	0.27	32.0
1	5	-	K6R4016CID-JC10	4	U 1 2 , U 1 3 , U 3 2 , U33	Samsung	0.5	0.2	29.0

주) Cat-부품의 대분류, Sub Cat-부품의 소분류, Part Num-부품의 개발단계명칭, Description-부품사양, Qty-수량, Ref-PCB상의 번호, Man-제조사, Oper Pow(동작 전력), Power Rat-사용중 소모전력, Case Temp-동작중 표면온도

ATC 하부시스템단위 BOM을 바탕으로 고장률과 MTBF를 예측한 결과는 표4-24와 같다. MTBF는 고장률의 역수인 평균고장수명(MTTF, Mean Time to Failure)과 평균복구시간(MTTR, Mean Time to Repair)의 합이다. 하지만 다중계 시스템으로 구성된 열차제어시스템의 고장검출 및 계절체를 통한 기능복구시간에 해당하는 MTTR이 MTTF에 비하여 매우 작은 시간이므로 MTBF를 고장률의 역수로 계산가능하다. 표4-25의 결과와 같이 ATC 하부구성요소는 모두 목표신뢰도를 만족한다.

하부시스템단위로 예측된 고장률과 MTBF를 기반으로 ATC 지상장치 및 차상장치의 고장률과 MTBF를 계산한 결과를 표4-25에 제시하였다.

표4-24. ATC의 하부시스템별 고장률과 MTBF

분류	순번	구성요소	단위시간당 고장률 (1e-6/h)	MTBF (Hour)
차상 장치	1	연속수신보드	4.829086	207,079
	2	불연속수신보드	7.336311	136,308
	3	디지털입력보드	7.067186	141,499
	4	디지털출력보드	9.335712	107,116
	5	CPU보드	5.29096	190,509
	6	운영자콘솔	9.259259	108,000
지상 장치	7	지상제어모듈	3.978634	251,343
	8	지상연속송신보드	3.872544	258,228
	9	지상불연속송신기	3.566469	280,389

표4-25. ATC 단일계 구성 고장률과 MTBF

구성요소	단위시간당 고장률 (1e-6/h)	MTBF (Hour)	MKBF (km)
차상장치 (단일시스템) (표4-24의 1+2+3+4+5)	33.8593	29,534	128.630
지상장치 (단일시스템) (표4-24의 7+8+9)	11.4176	87,584	-

주) MKBF(Mean Kilometer Between Failure)는 단일계수량 4개, 연간운행일수 365일, 1일 운행시간 7.5h, 1회 435km기준

ATC는 제어기 내부에서 발생된 결함을 실시간으로 검출하는 자기검사알고리즘을 내장하고 있다. 따라서, 단일계에서 결함이 발생하면 결함이 발생된 단일계의 출력을 차단하고 대기계가 제어를 수행하는 능동형여분구조 중 대기이중계구조(Hot-Standby Spring)로 설계하였다. 또한 대기계는 동작계가 정상일 경우 출력을 발생하지 않지만 연산을 동작계와 동일하게 수행하고 있으므로, 이중계구조 시스템의 동작특성을 상태다이어그램으로 모델링하면 그림4-14와 같다.

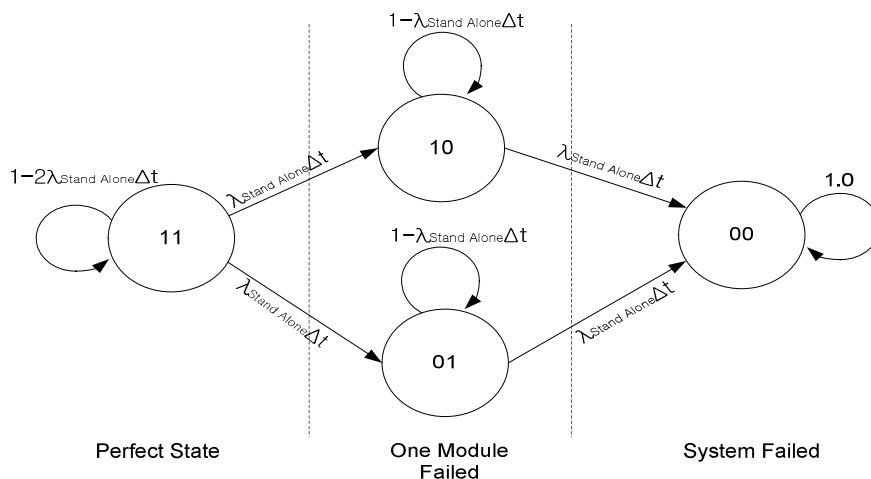


그림4-14 Hot-Standby Sparing 구조 ATC의 상태모델

그림4-14와 같이 시스템의 상태를 결함이 발생할 수 있는 임의시간 Δt 에 따라 마코브모델을 사용하여 시간에 종속된 시스템신뢰도를 계산한다. 따라서 ATC 지상 및 차상장치의 신뢰도는 지수고장특성으로 모델링하면 다음 식과 같이 도출된다.

$$R_{ATC}(t) = 2e^{-\lambda_{stand_alone}} - e^{-2\lambda_{stand_alone}t}$$

위 식에서 λ_{stand_alone} 은 단일모듈의 고장률이며, t 는 시간이다. 따라서, 위 식에 의해 시간에 따른 ATC의 신뢰도를 계산하면 표4-26과 같다.

표4-26. ATC장치의 시간에 따른 신뢰도

시스템 운영시간 (Hour)	시스템 신뢰도(%)	
	차상장치	지상장치
10,000	91.77	98.84
20,000	75.84	95.83
30,000	58.37	91.59
40,000	45.02	86.56
50,000	33.47	81.08
60,000	24.56	75.40
70,000	17.87	69.71
80,000	12.92	64.14
90,000	9.31	58.77
100,000	6.68	53.66

IXL의 하부시스템단위로 제공된 BOM을 바탕으로 고장률과 MTBF를 예측한 결과는 표 4-27과 같다.

표4-27과 같이 하부시스템단위로 예측된 고장률과 MTBF를 기반으로 IXL의 단일계구성 고장률과 MTBF를 계산한 결과를 표4-28에 제시한다. IXL 하부구성요소의 MTBF도 ATC의 하부구성요소와 같이 목표신뢰도를 만족한다.

표4-27. IXL 하부시스템별 고장률과 MTBF

순번	구성요소	단위시간당 고장률 (1e-6/h)	MTBF (Hour)
1	연동논리부 CPU보드	1.119474	898,277
2	연동논리부 통신보드	0.747764	1,337,320
3	현장제어부 입력모듈	3.969599	251,915
4	현장제어부 출력모듈	4.47694	223,374
5	현장제어부 선로전환기모듈	6.082854	164,397
6	현장제어부 신호기제어모듈	6.555135	152,553

표4-28. IXL 단일계구성 고장률과 MTBF

순번	구성요소	단위시간당 고장률 (1e-6/h)	MTBF (Hour)
1	단일계 연동논리부	1.8672	535,550
2	현장제어부 입력모듈	1.9848	503,830
3	현장제어부 출력모듈	2.2384	446,750
4	현장제어부 선로전환기모듈	3.0414	328,790
5	현장제어부 신호기제어모듈	3.2276	305,100

IXL의 연동논리부는 제어기 내부에서 발생된 결함을 실시간으로 검출하는 자기검사회로를 내장하고 있으며, 단일계에서 결함이 발생하면 결함이 발생된 단일계의 출력을 차단하고 대기계가 제어를 수행하는 능동형여분구조 중 대기이중계구조로 설계하였다. 따라서 ATC와 동일한 신뢰도 모델을 사용하여 표4-29과 같이 시간에 따른 신뢰도를 산출하였다.

IXL 현장제어모듈인 TFM_IM, TFM_OM, TFM_PM, TFM_SM의 이중계 구조는 동기방식으로 동작하는 이중계 데이터를 비교기를 사용하여 결함에 따른 데이터의 불일치로 결함을 검출한다.

표4-29. IXL 연동논리부의 시간에 따른 신뢰도

시스템 운영시간 (Hour)	시스템 신뢰도(%)
	전자연동장치 연동논리부
10,000	99.99
20,000	99.87
30,000	99.70
40,000	99.48
50,000	99.21
60,000	98.88
70,000	98.50
80,000	98.70
90,000	97.61
100,000	97.10

따라서, 비교기에서 불일치가 발생하면 불일치가 발생된 모듈은 차단되며, 대기이중계로 구성된 다른 이중계 구조가 동작을 연속적으로 수행하는 듀얼듀플렉스(Dual-Duplex)구조로 구성되어 있다. 듀얼듀플렉스구조 현장제어모듈의 상태다이어그램은 그림4-15와 같다.

그림4-15의 현장제어모듈 상태모델을 마코브모델을 통하여 간소화하여 듀얼듀플렉스 구조의 신뢰도함수를 구하면 다음 식과 같다.

$$R_{TFM}(t) = \frac{2}{3}e^{-\lambda_{s \tan d_alone}t} + 2e^{-3\lambda_{s \tan d_alone}t} - \frac{5}{3}e^{-4\lambda_{s \tan d_alone}t}$$

IXL 현장제어모듈의 신뢰도함수 위 식에 따라 시간에 따른 현장제어모듈의 신뢰도를 구하면 표4-30과 같다.

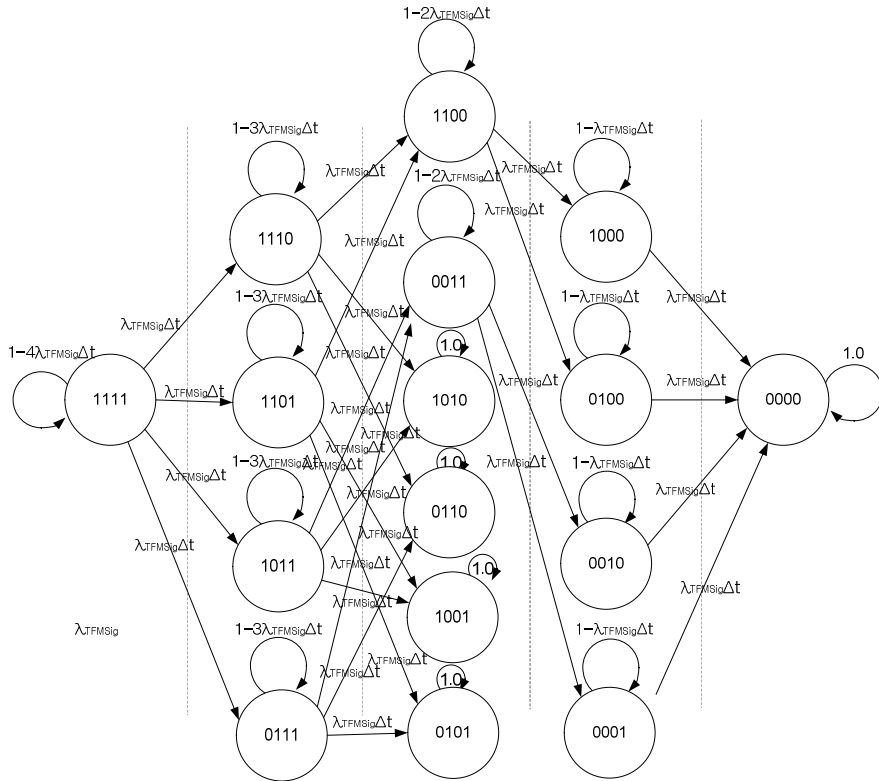


그림4-15. 듀얼듀플렉스구조 IXL 현장제어모듈의 상태모델

표4-30. IXL 현장제어모듈의 시간에 따른 신뢰도

시스템 운영시간 (Hour)	시스템 신뢰도(%)			
	입력모듈	출력모듈	선로전환기 제어모듈	신호기 제어모듈
10,000	99.85	99.81	99.65	99.61
20,000	99.42	99.27	98.70	98.55
30,000	98.75	98.44	97.26	96.95
40,000	97.87	97.35	95.42	94.93
50,000	96.81	96.05	93.28	92.58
60,000	95.59	94.57	90.91	89.99
70,000	94.24	92.94	88.36	87.22
80,000	92.78	91.18	85.68	84.34
90,000	91.22	89.33	82.92	81.38
100,000	89.58	87.41	80.12	78.39

위와 같이 한국형고속철도 열차제어시스템의 신뢰도요구사항인 MTBF 100,000시간을 ATC와 IXL의 하부구성요소가 모두 만족함을 MIL-HDBK-217F를 통한 예측가능하다.

열차제어시스템의 예측신뢰도는 철도신호시스템 RAMS규격인 IEC62278에서 제시하는 바와 같이 예측치의 입증이 수행되어야 한다. 따라서 신뢰도의 입증은 시운전기간동안 발생한 열차제어장치의 고장정보를 분석하여 고장보고분석 및 정정활동시스템인 FRACAS (Failure Reporting, Analysing, Correction Action System)[6]를 그림4-16과 같이 미국방성 규격 MIL-STD-785B를 기준으로 수행하고 있다.

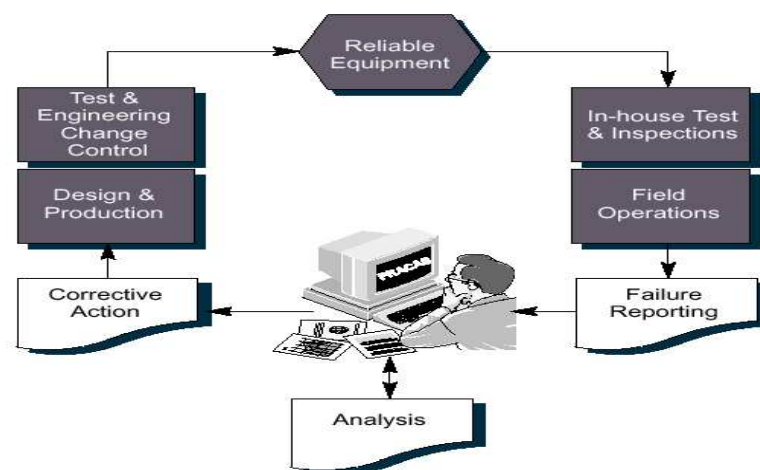


그림4-16. FRACAS의 절차

시운전을 통한 신뢰도의 입증은 데이터수집 범위인 소요시간과 주행거리에 따라 산출된 시스템 신뢰도의 신뢰수준이 결정된다. 따라서, 열차제어시스템 중 ATC 차상장치를 제외한 장치들은 FRACAS를 수행하여 시스템의 신뢰도를 입증하기 위한 충분한 시운전데이터가 확보되어야 한다.

또한 현장시험추진과 병행하여 시스템에 스트레스요인을 가속하여 신뢰도를 입증하는 신뢰성시험을 통해 하부구성요소 단위의 MTBF를 그림4-17과 같은 절차로 추진하여 신뢰도를 입증하고 있다. 신뢰성시험은 시제품의 수명한계에 대한 가속수명시험 보다는 열화스트레스를 사용하여 목표신뢰성의 확보를 확인하는 비파괴방식으로 시험을 추진하고 있다.

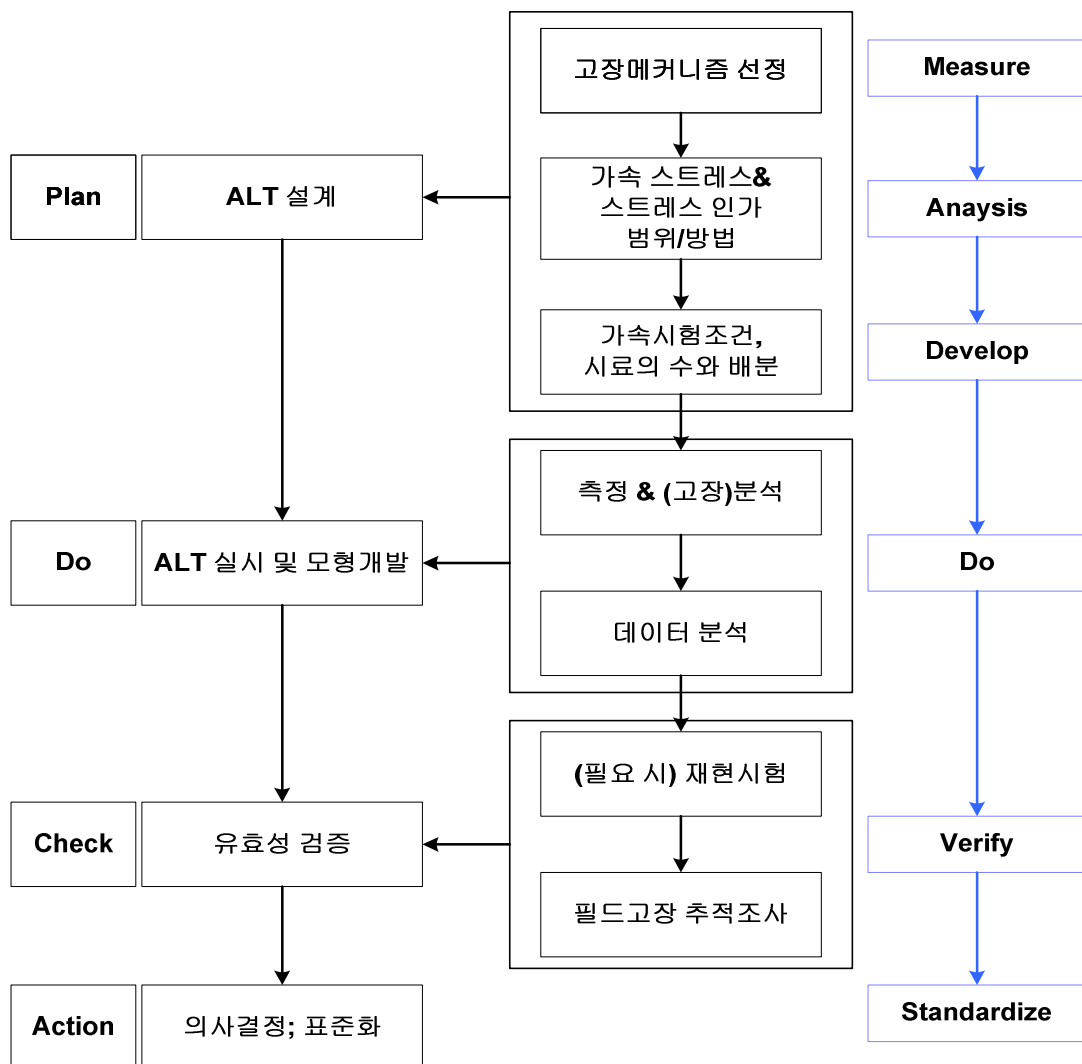


그림4-17. 가속시험 실시절차

제 3 절 IEC 62278의 수명주기 단계별 요구사항 분석

본 절에서는 IEC 62278(KS C IEC 62278)에서 시스템 수명주기별로 제시하는 RAMS 명세 및 입증에 대한 규격인 IEC 62278의 구조에 대한 설명과, IEC 62278에서 제시하는 시스템수명주기 14단계별 요구사항과 검증기준에 대하여 기술한다.

IEC 61508의 Part 1과 2에 해당하는 철도응용 RAMS명세 및 입증에 대한 국제표준 IEC 62278은 시스템의 수명주기를 그림4-18과 같이 개념수립부터 폐기까지 14단계로 구분하여 각각의 수명주기에 대한 목적, 입력요인, 요구사항, 산출문서, 검증방안을 제시하고 있다.

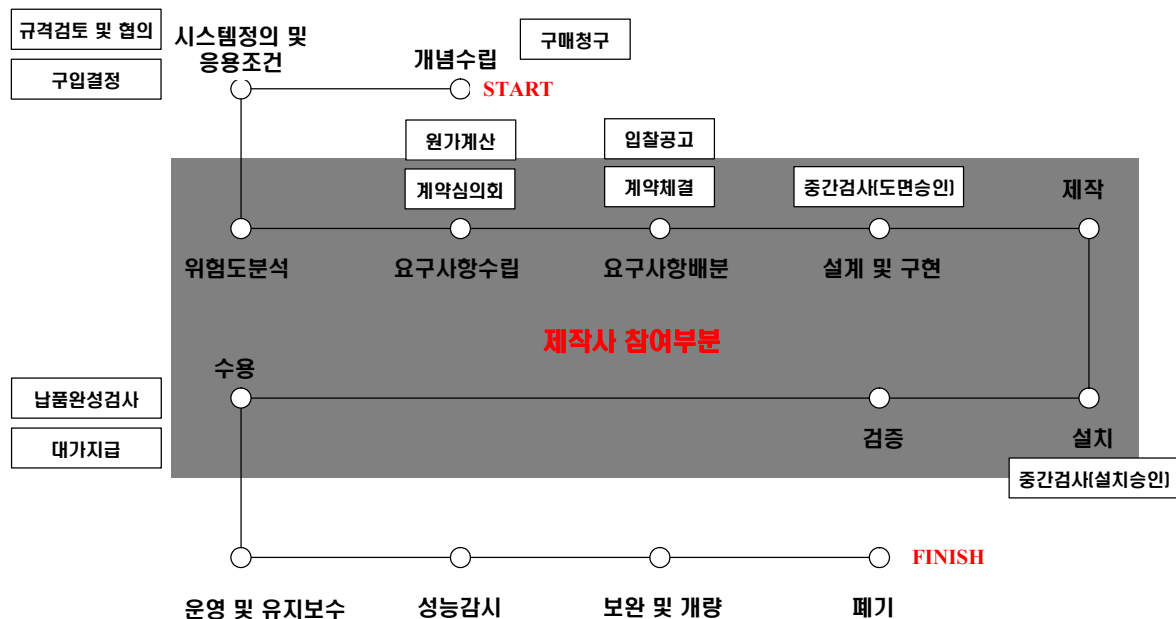


그림4-18. 수명주기 14단계와 코레일 업무주기

그림4-18은 수명주기 14단계에 대한 코레일 업무흐름을 기준으로 수명주기 14단계 중 제작사와 운영기관의 협업이 수행되어야 하는 부분으로 구분하였다.

1. 1단계 : 개념수립

수명주기 14단계 중 1단계에서는 구매를 위한 기본설계를 표4-31과 같이 실시한다.

표4-31. 1단계 개념수립

목적	수명주기 단계별 RAMS관리를 위한 기본설계
입력	사업관련 자료일체(범위, 목적, 사양, 규정, 기준 등) 기존 유사시스템의 RAMS 정보
요구사항	1. 시스템 범위, 내용, 목적 등을 분석한다. 2. RAMS수행의 경제성 및 구현가능성을 분석한다. 3. 다른 시스템 및 인간과의 인터페이스 관련 위험원을 도출한다. 4. 과거시스템 RAMS자료, 위험원, 국가 또는 운영기관의 안전정책, 안전법령을 분석한다. 5. 수명주기 별 RAMS활동 범위를 정의한다.
산출문서	1. 가정 및 제한사항을 명시한 요구사항 분석결과의 문서화 2. Phase 2, 3, 4에 대한 관리조직 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 시스템환경(범위 등)의 적합성 평가 3. 요구사항 '3'의 위험원 적합성 평가 4. 적용된 방법, 도구, 기법의 적절성 평가 5. 수행조직의 능력평가

1단계는 운영기관이 독자적으로 수행한다. 1단계에서 가장 중요한 사항은 시스템의 범위를 결정하는 것이다. 시스템의 물리적 범위와 RAMS관리의 범위(인적오류, 환경요소, EMI 포함 여부 등)가 정의되어야 하며, RAMS활동에 대한 범위의 기준이 되는 시스템 기능요구사항과 과거 유사시스템에 대한 RAMS정보 조사가 실시되어야 한다. 따라서 본 단계에서는 구매대상 시스템의 RAMS적용 유무가 결정되어야 하며, RAMS적용 유무는 운영기관의 경영목표와 국가의 안전목표에 구매대상 시스템의 신뢰성과 안전성이 미치는 영향에 따라 자체적으로 결정한다. 1단계를 통해 운영자는 RAMS요건이 포함된 시스템 요구사항서를 작성하여 자체 또는 전문기관의 검증을 받아야 한다.

2. 2단계 : 시스템정의 및 응용조건

수명주기 14단계 중 2단계에서는 구매를 위한 시스템정의 및 응용조건을 표4-32와 같이 실시한다.

표4-32. 2단계 시스템정의 및 응용조건

목적	시스템 임무, 범위, 적용조건, 위험원분석범위, RAMS관리계획(안전계획 수립)
입력	Phase 1의 산출문서
요구사항	1. 임무, 범위, 적용조건, 위험원분석범위에 대하여 정의한다. 2. 예비RAM분석실시 및 예비위험원도출(위험도 허용기준 포함)을 실시한다. 3. 가용성과 안전성의 Trade-off를 수행하여 RAMS관리방안을 도출한다. 4. 안전계획을 수립한다.(인증구조 설계)
산출문서	1. 가정 및 제한사항을 명시한 요구사항 분석결과의 문서화 2. 시스템 RAMS정책 작성 3. 시스템 안전계획 작성 4. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. Phase 1의 입증 3. 예비RAM분석 및 예비위험원도출 결과의 적합성 평가 4. 안전계획서의 적합성 평가 5. 수행조직의 능력평가 6. 부적합사항 발생시 이전단계 재수행

1단계 시스템의 정의와 RAMS적용 유무를 결정하면, 2단계에서는 세부적인 RAMS관리의 범위를 운영기관이 결정해야 한다. RAMS관리의 범위에서 제외된 고장 및 사고에 대해서는 RAMS활동을 통한 신뢰성과 안전성의 확보가 불가능하므로, 유사시스템의 분석 및 관련 법령이나 운영기관별 규정에 따라 빠짐없이 RAMS활동의 범위와 목표가 정의되어야 한다.

RAMS관리와 관련하여 목표설정의 건전성은 운영기관이 수행하는 사업초기활동에서 가장 중요한 요소이다. 기존에는 도입 또는 구매하고자 하는 시스템과 유사한 국외사례를 바탕으로 평균고장시간(MTBF), 평균서비스고장시간(MTBSF), 평균수리시간(MTTR), 위험요인 발생 빈도의 제어수준인 안전무결성레벨(SIL) 등을 활용하였으나, 유사사례의 운영환경과 국내운영 환경의 차이로 인해 의도되지 않은 효율 및 안전성의 저하와 같은 문제점이 끊임없이 발생되었다.

평균고장시간과 평균서비스고장시간의 차이는 고장의 결과가 서비스에 미치는 영향의 차이이다. 만약 열차지연10분 이상을 서비스고장으로 정의하는 경우, 열차운행에 지장을 주지 않는 고장이나 고장으로 인한 열차지연이 10분 미만인 고장에 대해서는 평균고장시간 산출에 있

어서 고장요소에는 포함되지만, 평균서비스고장시간 산출에 대한 고장요소에는 포함되지 않는다. 운영기관 관점에서는 평균고장시간은 예방 및 유지보수절차를 수립하는 데이터로 활용하며, 평균서비스고장시간은 시스템의 운영가용성을 평가하는 데이터로 활용한다. 그러므로 고장 발생의 영향이 서비스불능 또는 사고의 원인이 되는지의 여부를 분류하는 방법으로 고장모드 영향분석(FMEA) 등의 기법을 사용하며, 고장모드영향분석을 통해 분류된 고장의 발생확률을 통합하기 위해 신뢰도블럭다이어그램(RBD) 및 결합트리분석(FTA) 등의 기법을 사용한다. 각 기법에 대한 구체적인 설명은 4단계인 요구사항수립에서 설명한다.

2단계에서 정의해야 할 중요한 사항 중 하나가 인증구조의 결정이다. 유럽의 경우 국가가 안전을 승인할 수 있는 전문기관으로 공인안전승인기관(NoBo)을 지정하여 관리하고 있으나, 국내의 경우 현재까지 국가가 지정하는 안전승인기관이 없으며, 운영기관이 사업 또는 구매건별 안전승인 전문기관을 지정하여 관리하고 있다. 안전승인을 운영기관에서 직접 수행 또는 전문기관에 위탁수행 여부를 결정함에 따라 사업에 소요되는 시간 및 비용이 연동되므로 사업 또는 구매계획 초기에 운영기관의 안전승인에 대한 전략 및 계약구조가 정의되어야 한다.

3. 3단계 : 위험도분석

수명주기 14단계 중 3단계에서는 구매를 위한 시스템에 해당하는 위험도를 표4-33과 같이 분석한다.

기존(1990년대)에는 안전무결성레벨을 시스템 또는 설비의 안전목표로 할당하였다. 예를 들어, 전자연동장치 SIL4, 열차집중제어장치(CTC)는 SIL2를 만족해야 한다는 식으로 안전목표를 할당하였으나, 이는 시스템 또는 설비에 포함된 위험원 중 어떤 위험원에 대하여 SIL을 적용해야 하는지와, SIL4를 적용하면 모든 위험요인이 안전하게 되는지에 대한 문제가 국제적으로 제기되었다. 따라서 SIL로 안전목표를 할당하는 것은 운영환경에 대한 결과분석이 용이하지 않은 범용시스템 등의 경우에 한하여 제한적으로 사용되고 있으며, 관련 규격인 EN 50126-2에서도 SIL에 의한 안전목표의 할당은 부적절함을 권고하고 있다.

따라서, 최근(2000년대)에는 국가별 안전목표를 근거로 해당 시스템 또는 설비의 위험요인을 도출하고, 도출된 위험요인의 위험도를 결과분석(Consequence Analysis)을 통해 정량적으로 평가하여 사상인원·백억km당 안전목표(국내의 경우 1억km당 사고발생빈도)의 만족여부를 평가하고 있다.

표4-33. 3단계 위험도분석

목적	시스템관련 위험원도출, 위험원의 결과 및 위험도 평가, 위험도관리 절차 수립
입력	Phase 2의 산출문서
요구사항	1. 시스템응용조건에서 발생할 수 있는 위험원을 도출한다. 2. 위험도의 허용여부를 가용도와 LCC를 고려하여 결정한다. 3. 위험원목록(Hazard Log)을 작성하고, 변경사항 발생시 갱신 등의 유지관리를 수행한다.
산출문서	1. 가정 및 제한사항을 명시한 요구사항 분석결과의 문서화 2. 위험도분석결과가 기록된 위험원 목록 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. Phase 2의 입증 3. 위험도평가결과의 건전성 평가 4. 허용위험도 등급의 건전성 평가 5. 위험원목록의 적합성 평가 6. 적용된 방법, 도구, 기법의 적절성 평가 7. 부적합사항 발생시 이전단계 재수행

시스템 또는 설비에 대한 구체적 사양(다중계 사용여부, 입출력회로의 구성 등)이 결정되지 않은 본 3단계에서는 개념적인 시스템(입력, 출력, 기능요구사항 정의 수준) 또는 설비의 기능요구사항만을 참고로 하여 운영기관이 시스템에 필수적으로 적용해야 하는 위험요인을 선별하는 예비위험요인분석(PHA)을 실시해야 한다.

예비위험요인분석의 목적은 시스템으로 인한 사고의 원인(위험요인)을 분석하여 안전확보를 위한 필수위험요인을 정의하고, 정의된 위험요인의 위험도를 제어하기 위한 수명주기별 안전요구사항을 도출하기 위해 수행한다.

4. 4단계 : 시스템 요구사항 수립

수명주기 14단계 중 4단계에서는 구매를 위한 시스템의 요구사항을 표4-34와 같이 수립한다.

2단계에서 기술한 바와 같이 운영기관은 정의된 고장, 서비스고장, 복구, 서비스복구, 사고에 따른 정량적 목표할당을 본 4단계에서 실시해야 한다.

표4-34. 4단계 시스템 요구사항 수립

목적	RAMS요구사항, 입증계획, 수용기준을 작성하고 RAM프로그램을 수립한다.
입력	Phase 2와 Phase 3의 산출문서
요구사항	1. RAMS요구사항을 작성한다. 2. 입증계획, 수용기준, 부적합시 대책, 인증을 위한 조직구성을 수립한다. 3. 상세 RAM프로그램을 작성한다.(사용자의 승인취득) 4. Phase 2에서 작성된 안전계획을 보완한다.
산출문서	1. 가정 및 제한사항을 명시한 요구사항 분석결과의 문서화 2. 안전계획 및 수용계획 보완 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. Phase 2와 Phase 3의 산출물을 근거로 LCC를 고려한 요구사항의 평가 3. 안전요구사항의 국가 및 운영기관 안전정책 부합여부 평가 4. RAM요구사항의 운영기관 경영목표와의 부합여부 평가 5. 입증 및 수용계획의 적합성 평가 6. RAM프로그램의 적합성 평가 7. 적용된 방법, 도구, 기법의 적절성 평가 8. 수행조직의 능력평가 9. 부적합사항 발생시 이전단계 재수행

운영기관의 유지보수주기 최적화와 연동되는 목표는 평균고장시간 및 평균수리시간이다. 대부분 전자부품으로 구성된 제어기를 사용하고, 고장영향이 서비스지연 및 사고발생으로 귀결되는 신호시스템과 같이 신뢰도함수를 지수고장모델로 평가하는 시스템의 경우, 일반적으로 예방유지보수주기는 하부시스템의 평균고장시간과 동일하게 된다. 이러한 시스템의 고장영향 및 발생빈도를 고려하여 예방유지보수임무 및 점검주기를 최적으로 할당하는 방법이 신뢰도기반유지보수(RCM)이며, 위에서 설명한 바와 같이 신호설비는 대부분 예방유지보수임무가 하부시스템의 교체에 해당된다.

운영기관은 각각의 정시율목표 또는 가용도 목표를 경영지표로 할당하여 관리하고 있다. 따라서 열차의 정시율에 해당하는 신뢰성목표는 평균서비스고장시간 및 평균서비스복구시간이다. 해당 시스템 또는 설비의 가용도와 평균서비스고장시간 및 평균서비스복구시간의 관계는 다음 식과 같다.

$$Ass = \frac{MTBSF}{MTBSF + MTTSR}$$

일반적으로 운영기관은 가용도에 대한 운영목표와 해당 시스템 또는 설비의 수량 및 단품에 대한 평균서비스복구시간을 설정하고 있다. 따라서 위 식에 의해 시스템 또는 설비의 평균서비스고장시간을 산출하기 위해서는 위 식을 다음 식의 형태로 응용하여 활용하는 것이 편리하다. 다음 식에서 Ass는 가용도이며, n은 해당 시스템 또는 설비의 수량이다.

$$MTBSF = \frac{n \cdot MTTSR}{\frac{1}{Ass} - 1}$$

예를 들어, 궤도회로의 평균서비스고장시간을 할당하는 경우에 궤도회로의 수량이 1,000개이며, 각 궤도회로에서 고장이 발생한 후 가용한 상태로 복구시키는데 소요되는 평균서비스복구시간이 1시간이라고 가정하면, 운영기관의 정상상태가용도 목표가 99.8%(1년에 17시간 사용불능)이면 궤도회로 1식의 평균서비스고장시간은 499,000시간이 되고, 정상상태가용도 목표가 99.98%(1년에 1.7시간)이라면 궤도회로 1식의 평균서비스고장시간은 4,999,000시간이 되어 운영목표에 따라 대상시스템의 평균서비스고장 목표가 크게 상이함을 알 수 있다. 이러한 논리에 의해 국외 유사시스템의 평균서비스고장시간이나 평균고장시간 등의 운영조건을 구분하지 않고 신뢰도목표를 국내 철도환경에 적용하게 되면 시스템 또는 설비의 수량으로 인해 요구되지 않은 가용도의 저하가 발생할 수 있다.

안전목표는 2단계와 3단계에서 실시한 예비위험요인분석결과인 필수위험요인에 대하여 제작사가 수명주기별로 안전요구사항을 준수하여 정부의 철도안전목표를 만족할 수 있도록 할당해야 한다. 앞에서 기술한 바와 같이 최근에는 SIL에 의한 안전목표 할당을 지양하며, 위험요인을 모두 도출하고 위험도를 평가하여 해당 위험요인으로 인한 사고발생빈도를 근거로 안전확보의 유무를 평가한다.

따라서 본 단계를 수행하는 운영기관은 제작사가 안전목표의 달성을 입증할 수 있도록 해당 시스템 또는 설비로 인한 위험요인의 사고발생빈도 산출(일반적으로 ETA(Event Tree Analysis)기법이 적용됨)에 필요한 결과분석 목적의 운영조건 및 환경요인이나 인적오류 발생빈도를 제작사에 제시해야 한다. 예를 들어 구매대상이 전자연동장치인 경우에는 일반화된

필수위험요인인 “선로전환기 도중전환”에 대하여 도중전환이 발생하는 순간에 분기부에 열차가 존재할 확률이나 필요 시 여객열차와 화물열차의 통과비율 그리고 환경요인으로 인한 노이즈, 낙뢰 등의 발생빈도, 선로전환기의 유지보수와 전자연동장치의 선로전환기 단독취급과 관련된 운영인력의 인적오류 발생빈도 등을 안전목표와 함께 제작사에 제시해야 한다. 표4-35는 전자연동장치 전체에 대한 RAMS목표할당의 예이다.

표4-35. 전자연동장치 RAMS목표 할당 예

순번	분류	목표
1	신뢰도목표	MTBSF = 1,000,000시간 이상 하부시스템 MTBF목표
		하부시스템
		전원모듈
		프로세서모듈
		통신모듈
		입력모듈
		출력모듈
		계전기랙
2	가용도목표	하부시스템 1식으로 구성된 전자연동장치의 평균서비스고장에 대한 가용도는 99.98%(1.7시간/1년)이내
3	유지보수도	평균서비스복구시간 1시간 이내
		하부시스템
		전원모듈
		프로세서모듈
		통신모듈
		입력모듈
		출력모듈
		계전기랙
4	안전성	IEC 62278에 근거한 안전관리활동 필수위험요인으로 인한 사고발생빈도 $9.30 \times 10^{-8}/\text{hour}$ 이내

5. 5단계 : 시스템 요구사항 배분

수명주기 14단계 중 5단계에서는 납품을 희망하는 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 단계로써 표3-36과 같이 진행한다.

5단계는 제작사가 운영기관이 제공하는 시스템 또는 설비별 RAMS목표 달성을 위한 관리 계획을 수립하여 운영기관의 승인을 받는 단계로써 구매업무의 제안서 제출단계에서 이루어져

야 한다.

표4-36. 5단계 시스템 요구사항 배분

목적	RAMS요구사항을 하부시스템, 부품, 외부장치에 할당하고 수용기준을 수립
입력	Phase 4의 산출문서
요구사항	1. RAMS요구사항을 배분하고, 시스템구성을 구체화하며, RAM프로그램을 재검토한다. 2. 할당된 RAMS요구사항의 수용기준 및 방법을 수립한다. 3. 인적요인을 포함하여 안전계획과 입증계획을 갱신한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 안전계획서 갱신 3. 설계된 하부시스템, 부품, 외부장치에 배분된 요구사항 문서화 4. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. LCC와 Phase 4의 산출물을 고려한 RAMS요구사항 배분 적합성 평가 3. 배분된 RAMS요구사항이 전체 RAMS요구사항을 만족하는지에 대한 평가(추적성 평가 포함) 4. 안전계획서 및 입증계획서 갱신의 평가 5. 적용된 방법, 도구, 기법의 적절성 평가 6. 수행조직의 능력평가 7. 부적합사항 발생시 이전단계 재수행

제작사는 운영기관의 RAMS목표를 달성하기 위한 수명주기별 예측, 입증, 위험요인도출 및 분석, 위험도평가에 대한 각 단계별 적용기법을 포함한 활동계획을 조직구성과 함께 제작사가 공급하는 시스템에 따라서 작성해야 한다.

위 4단계 까지가 일반화된 시스템 또는 설비에 대한 요구사항이라면 5단계부터는 제작사가 공급하는 실제 시스템에 대한 목표의 배분 및 요구사항 달성을 위한 세부계획이 포함되어야 한다. 예를 들어 4단계의 수명주기에 예로 든 전자연동장치의 경우에 프로세서모듈, 입력모듈, 출력모듈로 운영기관이 하부시스템을 정의하여도, 제작사의 시스템이 선로전환기제어모듈, 신호기제어모듈, 연동처리모듈 등의 분산제어구조로 구성되어 운영자가 제시한 요구사항 항목에 일치되지 않는 경우라 하더라도 전체시스템 RAMS목표를 재분배하여 운영기관이 제시한 최종목표에 만족되도록 요구사항을 분배해야 한다.

또한, 2단계에서 운영기관이 제안한 안전승인을 위한 조직구성에 따라 수행조직을 편성하고, 각 수행조직을 구성하는 인적자원의 능력을 검증해야 한다.

운영기관이 제시한 RAMS목표를 달성하기 위해 적용되는 신뢰도예측 및 입증, 위험요인도출 및 분석을 위한 구체적인 적용기법도 본 단계에서 운영기관에 제출되어야 하며, 수행도중 사업일정에 영향을 미치는 인증기관, 고장률 입증자료, 기 취득 성적서 또는 인정서의 인정여부도 본 단계에서 운영기관과 조율되어야 한다.

6. 6단계 : 설계 및 구현

수명주기 14단계 중 6단계에서는 구매계약이 결정된 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 단계로써 표4-37과 같이 진행한다.

표4-37. 6단계 설계 및 구현

목적	설계단계에서의 RAMS요구사항 만족을 입증하고, 다음 단계들을 위한 계획수립
입력	Phase 4와 Phase 5의 산출문서
요구사항	1. RAMS요구사항을 만족하도록 시스템을 설계한다. 2. RAMS요구사항을 만족하는 시스템설계를 준수하여 제작한다. 3. 설치, 시운전, 운영(데이터 수집방법 포함), 유지보수에 대한 계획을 수립한다. 4. RAMS요구사항을 만족시키기 위한 제작절차를 수립한다. 5. 승인을 고려한 안전보고서(Safety Case)를 준비한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. RAMS검증자료의 문서화 3. 다음 단계들에 대한 구체적 계획수립 4. 운영 및 유지보수 절차(안전관련) 작성 5. 안전보고서 초안생성 6. 응용안전보고서 생성(선택) 7. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 분석과 시험에 의한 하부시스템 설계의 RAMS요구사항 만족여부 확인 3. 분석과 시험에 의한 하부시스템 제작의 설계준수여부 확인 4. 분석과 시험에 의한 제작체계 평가 5. 다음 단계의 구체적 계획을 LCC를 고려하여 평가 6. 안전보고서 초안의 평가 7. RAMS검증계획서의 갱신확인 8. 적용된 방법, 도구, 기법의 적절성 평가 9. 수행조직의 능력평가 10. 부적합사항 발생시 이전단계 재수행

6단계는 제작사가 공급하는 시스템의 실체가 아직 없는 상태에서 운영기관이 설계승인 여부를 판단할 수 있도록 예측 등의 방법에 의해 설계된 시스템 또는 설비가 RAMS목표에 만족함을 입증하는 단계이다.

이미 제작이 완료된 시스템 또는 설비를 구매하는 경우에는 본 단계를 건너뛰고 9단계의 검증에서 수행하는 RAMS관련 지표의 입증치를 대체하여 적용할 수 있다.

신호설비 RAMS지표는 시스템 또는 설비의 고장률로부터 산출된다. 6단계에서는 설계단계에 있는 시스템 또는 설비의 고장률예측에 의한 목표만족여부를 평가하며, 이때 일반적으로 사용되는 방법이 미국방지침인 MIL-HDBK-217과 같은 규격에 근거한 고장률예측이다.

규격에 근거한 고장률예측, 신뢰성시험에 의한 신뢰도입증, 시운전을 통한 신뢰도입증에 포함되는 고장요인들은 표4-38과 같다. 따라서 시운전을 통한 RAMS지표의 입증이 가장 우선하지만, 시운전을 위해 대규모의 인프라가 요구되는 철도의 특성에 따라 6단계에서는 규격에 의한 예측을 활용하며, 필요시 시스템 또는 설비를 인수하기 전단계인 9단계에서 신뢰성시험을 통한 입증이나 시운전을 통한 입증치를 평가해야 한다.

표4-38. 고장요인에 따른 예측, 신뢰성시험, 시운전시험의 포함여부

적용방법	온도요인	습도요인	진동요인	전자기요인	설계오류	S/W오류
고장률예측 (MIL-HDBK-217)	○	×	×	×	○	×
신뢰성시험	○	×	×	×	○	○
시운전시험	○	○	○	○	○	○

고장률예측, 신뢰성시험, 시운전시험을 통해 신뢰도, 가용도, 유지보수도 산출을 위한 고장률 데이터가 산출되면, 제작사는 표4-39와 같이 하부시스템단위 고장률을 산출근거와 함께 운영기관에 제시해야 하며, 운영기관은 제출된 자료를 5단계에서 제작사가 제출한 RAMS계획서와 비교하여 산출근거의 인정여부 및 고장률 산출과정에서의 건전성을 평가한다.

평균고장시간은 시스템 또는 설비를 구성하는 하부시스템, 하부시스템을 구성하는 모듈, 모듈을 구성하는 부품의 고장률을 모두 합한 값인 고장률(λ)을 역수로 근사화한다. 따라서 평균 고장시간에는 일반적으로 고장이 발생해도 시스템의 서비스제공에는 영향을 미치지 않는 냉각팬, 전면 LED 등이 포함된다.

평균고장시간은 다중계구조, 병렬구조, 직렬구조 등의 부품, 모듈, 하부시스템 구조에 따라

표4-39와 같은 부품목록에 대하여 그림4-19와 같이 신뢰도 블럭다이어그램을 통해 제시될 수 있다

표4-39. 하부시스템의 고장률평가 예(차상신호(ATP)구축사업의 KTX차량 차상장치의 예)

순번	RBD 분류	수량	하부요소	제작사	기 호	고장률(/hour)	산출근거
1	Loud Speaker	1	-	YK	λ_{SPK}	1.00E-09	가정
2	MMI	1	-	DEUTA-WERKE	λ_{MMI}	9.26E-06	근거13
3	RU/JRU	1	-	FAIVELEY	λ_{JRU}	8.62E-06	근거20
4	DX-K	1	-	BT	λ_{DXK}	1.25E-06	근거11
5	DX-K I/F	1	ASDR1	BT	N/A	1.00E-09	가정
			ASDR2	BT	N/A	1.00E-09	가정
			ASDR3	MORS SMITT	N/A	1.00E-06	가정
			CRR1	MORS SMITT	N/A	1.00E-06	가정
			CRR2	MORS SMITT	N/A	1.00E-06	가정
			COR	MORS SMITT	N/A	1.00E-06	가정
			CFR	MORS SMITT	N/A	1.00E-06	가정
			ARM RELAY	MORS SMITT	N/A	1.00E-06	가정
			합 계		λ_{DXKIF}	6.00E-06	N/A
6	DX-L	1	-	BT	λ_{DXL}	1.25E-06	근거11
7	DX-L I/F	1	ATCARM	TJ	N/A	1.00E-09	가정
			ATCDRM	TJ	N/A	1.00E-09	가정
			합 계		λ_{DXLIF}	2.00E-09	N/A
8	Odometer	2	SDU	BT	N/A	3.31E-06	근거11
			ASIG BOARD	FAIVELEY	N/A	8.33E-06	근거20
			WIEGAND SENSOR	FAIVELEY	N/A	5.08E-07	근거19
			합 계		λ_{ODO}	1.21E-05	N/A
9	VCU For STM	1	-	BT	λ_{VCUSTM}	5.56E-07	근거11
10	DR	1	-	DEUTA-WERKE	λ_{DR}	6.01E-06	근거11

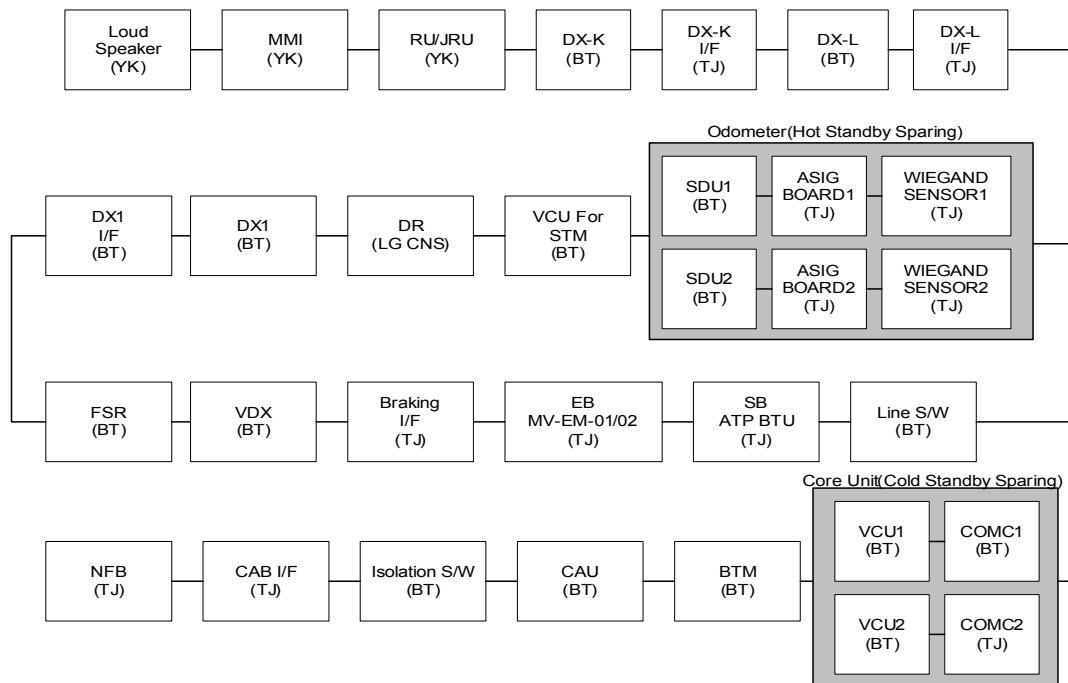


그림4-19. 표4-39의 신뢰도 블럭다이어그램(차상신호(ATP)구축사업의 KTX차량 차상장치의 예)

평균서비스고장시간은 앞에서 설명한 바와 같이 시스템 또는 설비의 고장발생에 대한 영향 평가를 고장모드영향분석, 고장모드영향 및 심각도분석, HAZOP Study등의 기법을 사용하여 표4-40과 같이 고장모드별로 식별하여 그림4-19과 같이 평균서비스고장에 대한 신뢰도 블럭 다이어그램 또는 결함트리분석을 통해 제시한다.

표4-40. 고장모드영향분석 사례(차상신호(ATP)구축사업의 KTX차량 차상장치의 예)

HAZOP Study 대상: KTX제동출력(SB출력)												
참조도면번호: 근거3					개정번호: V1.0					소요시간: 부록A 참조		
참여구성원: ATP시스템 RAMS컨설팅부서, 시스템 검토그룹(SEG), ATP차상장치 설계제작사 엔지니어												
기능	Guide Word	이상현상	원인	결과(ATP차상장치의 최종상태)	대체 전 Risk F S R			안전대책	대체 후 Risk F S R			세부조치내역
KTX제동출력(SB출력)	No	출력이 발생되지 않음	1.케이블 탈거 2.케이블 결손 3.입력포트 소손 4.소프트웨어 오류 5.결선오류	비상제동	4	C	4 C	1.잠금장치 사용 2.보호차재사용 3.자기전단기능 4.시운전을 통한 검증 5.특수커넥터 6.기관사의 수동 제동가능	5	C	5 C	1.특수도구(6각렌치)를 사용한 체결 2.보호차재를 사용한 보강 및 고정시공 3.VDX/DX내부 전단기능 4.우선 및 확대설치시 시운 전시험 성적서 5.코딩핀을 사용한 결선오류방지 6.이상발생시 경고음에 의한 기관사의 수동제동 가능
	More	해당 없음										
	Less	해당 없음										
	As well as	해당 없음										
	Part of	해당 없음										
	Reverse	제어조건과 반대정보의 출력	1.결선오류 2.설계오류 3.출력장치 고장	상용제동	4	D	4 D	1.특수커넥터 2.검증시험 수행 3.바이탈 제어	5	D	5 D	1.특수도구(6각렌치)를 사용한 체결 2.우선 및 확대설치시 시운 전시험 성적서 3.SIL4를 만족하는 VDX로 제어
Other than	해당 없음											

7. 7단계 : 제 작

수명주기 14단계 중 7단계에서는 구매계약이 결정된 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 단계로써 표4-41과 같이 진행한다.

표4-41. 7단계 제작

목적	RAMS검증이 가능하도록 제작을 수행하고 RAMS절차보증 및 하부시스템 RAMS 지원체계 수립
입력	Phase 6의 산출문서
요구사항	1. 제작공정을 검증한다. 2. 하부시스템 및 부품의 지원체계가 수립되어야 한다. 3. 제작 동안 RAMS요구사항 만족을 입증하기 위한 계획을 수립한다.(선택)
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 제작관련RAMS검증 업무기록 문서화 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. RAMS요구사항과 LCC를 고려한 RAMS지원문서의 적절성 평가 3. 제작되는 시스템의 RAMS요구사항 만족여부 평가 4. 적용된 방법, 도구, 기법의 적절성 평가 5. 수행조직의 능력평가 6. 부적합사항 발생시 이전단계 재수행

7단계에서는 6단계까지 제작사에서 제출한 RAMS관리계획서, RAM예측보고서 및 안전확보를 위한 안전대책이 시스템 또는 설비의 제작에 모두 반영되었는지 여부를 운영기관이 검토하는 단계이다.

정해진 시운전시간을 통해 입증이 곤란한 하부시스템의 경우, 운영기관은 신뢰성시험을 통해 제작사가 예측신뢰도를 입증하도록 할 수 있으나, 신뢰성시험의 대상 하부시스템 정의 및 시험방법에 대하여 5단계의 제작사와 운영기관 RAMS관리계획서 제출 및 승인단계에서 확인된 사항에 대해서만 실시가 가능하다.

또한 시스템 또는 설비가 단순 구매일 경우, 본 단계는 9단계인 검증단계에서 한번에 실시할 수 있다.

8. 8단계 : 설 치

수명주기 14단계 중 8단계에서는 구매계약이 결정된 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 단계로써 표4-42와 같이 진행한다.

표4-42. 8단계 설치

목적	RAMS검증이 가능하도록 제작을 수행하고 RAMS절차보증 및 하부시스템 RAMS지원체계 수립
입력	Phase 6(설치계획) 및 Phase 7(RAMS지원문서)
요구사항	1. 설치계획에 따라 하부시스템을 조립하고 설치한다. 2. 설치과정을 문서화한다. 3. 설치종료 후를 고려하여 안전계획을 갱신한다. 4. 교육시작 및 지원시스템(예비품 및 공구 공급)계획을 수립한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 설치과정의 RAMS검증업무기록을 문서화 3. 안전계획서 갱신 4. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 설치계획의 준수여부 평가 3. 설치된 시스템의 RAMS요구사항 만족여부 평가 4. 적용된 방법, 도구, 기법의 적절성 평가 5. 수행조직의 능력평가 6. 부적합사항 발생시 이전단계 재수행

8단계 설치에서는 시스템 또는 설비를 제작사가 현장에 설치하는 과정에 있어서 RAMS관리계획서에 명시된 운영조건 또는 안전대책을 적절하게 반영하였는지를 운영기관이 평가하는 단계이다.

안전확보를 위한 안전대책에서는 설치인력 인적오류에 의한 사상도 포함하는 것이 일반적이며, 4단계에서운영기관이 승인한 안전대책 중에 설치관련 안전요구사항이 있는 경우, 안전요구사항의 반영여부를 평가할 수 있도록 제작사는 입증자료를 문서화 하여야 하며, 운영기관은 현장검토 및 입증문서를 심사하여 적합성을 평가한다.

9. 9단계 : 시스템 검증(안전성수용 및 시운전포함)

수명주기 14단계 중 9단계에서는 구매계약이 결정된 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 단계로써 표4-43과 같이 진행한다.

표4-43. 9단계 시스템 검증

목적	시스템 RAMS요구사항 만족여부를 검증하고, 시운전을 통해 안전입증을 실시한다. (시운전시 데이터수집 및 평가방안 포함)
입력	Phase 6(시운전계획) 및 Phase 7(교육자료)
요구사항	1. 입증계획을 근거로 시스템을 검증한다. 2. 시운전계획에 따라 시운전을 실시하고 과정을 문서화한다. 3. 안전보고서를 준비한다. 4. 운영데이터수집 및 평가(FRACAS)방안을 수립한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 시운전 및 RAMS검증업무의 기록을 문서화 3. 응용안전보고서 작성 4. 시스템 수용관련 기록의 문서화 5. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 시운전자료에 의한 RAMS요구사항 만족여부 평가 3. 시운전계획서의 준수여부 평가 4. 시운전 데이터 수집방법의 건전성 평가 5. 적용된 방법, 도구, 기법의 적절성 평가 6. 수행조직의 능력평가 7. 부적합사항 발생시 이전단계 재수행

시스템검증은 6단계에서 제작사가 제시한 RAM예측데이터가 4단계에서 운영기관이 제시한 RAM목표와 일치하는지의 여부를 시운전 또는 시험을 통해 검증하는 과정이다.

시운전을 실시하는 경우에는 시스템 평균고장시간에 따라 시운전시간을 산출해야 하며, 시운전실시로 인해 확보되는 신뢰도를 시운전시간 결정시에 고려해야 한다.

신뢰도 입증을 위한 시운전시간 결정은 다음 식과 같은 카이자승공식을 일반적으로 활용한다.

$$\hat{\theta} \geq \frac{2nh}{\chi^2(\alpha, 2r+2)}$$

$\hat{\theta}$: 평균수명

α : 유의수준(계산결과의 신뢰수준)

r : 고장 개수

n : 시료 수

h : 시험 시간

위 식을 활용하여 평균고장시간이 13,600시간으로 제시된 차상장치에 대한 시운전시간을 산출할 수 있다. 시운전시간 동안 고장이 한번도 발생하지 않을 경우, 위 식을 활용하여 필요한 시운전시간을 도출하면 표4-44와 같다.

표4-44. 평균고장시간에 의한 시운전시간 결정의 예(KTX 15호차 차상장치 시운전의 예)

항목	목 표	최소 시험시간	최소 시험거리
상용제동관련 고장	MTBF 13,600 시간	20,370 시간	2,037,000 km

최소 시험거리는 시간당 평균 100km의 주행을 가정.

표4-44의 결과는 위 식에 고장개수는 “0”, 시료 수는 2개, 유의수준은 95%의 정밀도를 갖도록 산출한 예로써, 95% 무고장에 대한 $\chi^2(\alpha, 2r+2) = 5.991$ 는 카이제곱 통계표를 활용한다.

표4-44의 결과와 같이 예측신뢰도를 위해서는 상당량의 피시험체와 시험기간이 소요된다. 따라서 운영기관은 단계5에서 제작사의 신뢰도입증을 위한 시운전시간 결정이 어느 정도의 예측신뢰도 입증의 효과를 갖는 지를 사전에 검토해야 한다.

시스템 검증에 해당하는 고장률입증 및 교정유지보수도평가의 건전성과 관련하여 가장 중요한 요소는 고장정보의 기록이다. 고장정보 기록의 분류체계와 기록의 성실도에 따라 입증된 RAMS지표에는 많은 차이가 발생된다.

따라서 시운전으로 인한 발생고정의 기록 및 분석에 대한 건전성확보 및 체계적 관리를 위해 일반적으로 고장보고, 분석 및 정정시스템(FRACAS)가 많이 사용되고 있다.

고장보고, 분석 및 정정시스템은 표4-45와 같이 발생고장을 기록하는 양식과 고장의 원인분석

및 누락 방지를 위한 고장검토위원회(FRB)의 운영이 핵심사항이다.

표4-45. 고장보고, 분석 및 정정시스템을 위한 고장입력지(차상신호(ATP)시스템의 예)

고장 정보데이터 보고서							
1. 문서번호:		2. 프로젝트 명:		3. 고장 발생 일시: ____/____/____ :__			
4. 고장 발생 장치	차상장치			지상장치			
	☐ 차상안테나 유니트 ☐ 차상변환모듈 ☐ 속도/거리연산장치 ☐ 타코미터 ☐ 도플러센서 ☐ 차량제어유니트 ☐ 통신유니트 ☐ 표시장치 ☐ 바이탈 입출력장치 ☐ 입출력장치 ☐ 자료기록유니트 ☐ ATS용 특정전송모 들			☐ 가변정보전송장치 ☐ 고정정보전송장치 ☐ 선로변제어유니트 ☐ 정류기 ☐ 서지보호회로 ☐ 건널목IF			
5. 누적 운영 시간 또는 누적 운행 거리: ____:____ ~ ____:____ / ____Km ~ ____Km							
6. 환경 조건: ☐ 온도 ____℃ ☐ 습도 ____% ☐ 기타_____							
7. 보고 시간: ____/____/____ :__		8. 고장 발생 위치 :		9. 보고자 :		10. 서명:	
11. 내용 요약 및 조치내역:							
12. 고장 장치	A. 시스템	B. 고장 장치 고유 코드	C. 분류	D. 장치 고유 번호	E. 제작사	F. 고장 영향 분류	G. 고장 영향설명
			☐ LRU ☐ 장치 ☐ 시스템			☐ LRU ☐ 장치 ☐ 시스템	
13. 고장 내용 설명:							
14. 고장 범위: ☐ 하드웨어 ☐ 소프트웨어 ☐ 운영절차 ☐ 검수절차 ☐ 기타 (인적 요인 포함)							
15. 현장 조치 내역:							

특히 고장검토위원회는 제작사, 운영기관, 고장발견자, 유지보수자, 신뢰성전문가가 함께 참여하여 고장이 발생한 하부시스템을 정확하게 진단하여 신뢰도를 입증해야 한다.

또한 8단계까지 제작사가 운영기관에 제출한 교정유지보수시간 및 안전확보를 위한 유지보수관련 안전대책 실시의 적절성도 본 단계에서 평가되어야 한다.

대부분의 경우, 시운전시간 동안 시스템 또는 설비에 대한 RAMS의 입증이 충분하게 이루어지지 못한다. 이는 시운전을 위해 막대한 시간 및 인프라가 소요되기 때문에 정해진 시운전 시간 동안 운영기관이 제시한 목표 RAMS를 제작사가 달성하지 못했을 경우의 처리절차에 대해서도 4단계의 운영기관 요구사항에 포함시키고, 5단계의 제작사 RAMS관리계획을 통해 상호 합의되어야 한다.

10. 10단계 : 시스템 수용

수명주기 14단계 중 9단계에서는 구매계약이 결정된 제작사가 운영기관의 요구사항에 따라 RAMS관리를 실시하는 마지막 단계로써 표4-46과 같이 진행한다.

표4-46. 10단계 시스템 수용

목적	전체시스템의 RAMS요구사항 만족을 평가하여 영업운전을 위한 시스템 수용
입력	Phase 4(시스템 요구사항, 확인 및 검증계획, 수용계획) 및 Phase 9(시스템 검증업무 기록)
요구사항	1. 시스템의 RAM입증 및 안전보고서를 평가한다. 2. 영업운전은 시스템 수용 후에 시작한다. 3. 시스템 검증기간 동안 발생된 데이터가 반영된 위험원목록이 관리되어야 한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 시스템 수용업무 기록의 문서화 3. 변경사항을 반영한 위험원 목록 갱신 4. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. LCC관점에서의 RAMS요구사항만족여부 평가 3. 시스템 수용계획의 준수여부 평가 4. 안전계획의 갱신 및 준수여부 평가 5. 위험원의 관리상태 평가 6. 안전보고서의 적합성 및 완전성 평가 7. 적용된 방법, 도구, 기법의 적절성 평가 8. 수행조직의 능력평가 9. 부적합사항 발생시 이전단계 재수행

10단계는 제작사와 운영기관이 공동으로 작업하는 마지막 단계로써 운영기관이 4단계에서 제시한 RAMS목표가 달성되었음을 제작사가 입증하는 마지막 단계이다.

제작사는 운영기관의 RAMS목표달성에 대한 입증자료 뿐만 아니라, 목표달성을 위해 수행된 활동의 건전성 또한 증거문서를 통해 입증한다. 이러한 증거문서로서 일반적으로 최종안전보고서(Safety Case)가 해당되며, 최종안전보고서에는 사업과 관련된 모든 산출물의 요약, 특히 운영기관이 인수단계 이후에도 시스템 또는 설비에 대한 지속적인 유지보수와 개량시의 RAMS지표 유지를 위한 위험요인 목록(Hazard Log)이 포함되어야 한다.

11. 11단계 : 운영 및 유지보수

수명주기 14단계 중 11단계에서는 운영기관이 도입 또는 구매된 시스템 및 설비의 운영 및 유지보수와 관련된 RAMS를 표4-47과 같이 관리한다.

표4-47. 11단계 운영 및 유지보수

목적	RAMS요구사항을 지속적으로 만족하도록 유지관리
입력	Phase 6(운영 및 유지보수 계획)
요구사항	1. 시스템의 성능 및 LCC를 주기적으로 검토한다. 2. RAMS요구사항 유지를 위한 교육훈련, FRACAS 등을 실시한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 시스템 관련문서 갱신 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 지원체계 변경사항에 대하여 RAMS요구사항과 LCC관점에서 적절성 평가 3. 수행조직의 능력평가

11단계에서는 9단계 시운전에서 실시한 바와 같이 고장보고, 분석 및 정정시스템을 사용하여 시스템 또는 설비의 RAMS변화를 관찰해야 한다. 이러한 관찰결과를 근거로 운영기관은 제한된 비용을 유지보수 및 개량에 효율적으로 투자할 수 있다.

12. 12단계 : 성능감시

수명주기 14단계 중 12단계에서는 운영기관이 도입 또는 구매된 시스템 및 설비의 성능 감시를 통해 RAMS활동을 표4-48과 같이 관리한다.

표4-48. 12단계 성능감시

목적	시스템의 RAMS성능을 유지
입력	시스템 RAMS유지 및 지원과 관련된 정보
요구사항	1. RAMS데이터의 수집, 분석, 통계, 평가 및 안전보고서 등을 지속적으로 관리한다. 2. 운영, 유지보수, 지원시스템 변경사항에 대한 RAMS데이터를 분석한다.

산출문서	1. 성능감시업무기록의 문서화 및 유지 2. 시스템 지원문서 갱신 3. 다음 수명주기의 입력요소로 활용
검증기준	1. 사용된 자료의 건전성 평가 2. 지원체계의 변경 사항에 대하여 RAMS요구사항과 LCC관점에서 적절성 평가 3. 적용된 방법, 도구, 기법의 적절성 평가 4. 수행조직의 능력평가

본 12단계는 11단계와 연동하여 운영 및 유지보수 동안 발생하는 시스템의 RAMS변동을 추적하여 시스템의 현재상태를 파악하는 단계이다.

전자부품으로 구성된 신호설비의 고장률은 예측 및 입증단계에서 일정한 것으로 가정하고 있으나, 실제 시스템 또는 설비의 고장률은 장시간 운영으로 인한 누적스트레스와 적절하지 못한 유지보수로 인해 시간에 따라 증가추이를 보인다. 따라서 운영기관은 주기적으로 시스템의 RAMS변동추이를 분석할 수 있도록 고장 및 유지보수정보를 분석해야 한다.

13. 13단계 : 보완 및 개량

수명주기 14단계 중 13단계에서는 운영기관이 도입이나 구매한 시스템 및 설비의 보완 및 개량과 관련된 RAMS활동을 표4-49와 같이 관리한다.

표4-49. 13단계 보완 및 개량

목적	시스템의 보완 및 개량에 대한 RAMS요구사항의 유지
입력	관련정보
요구사항	1. 안전계획을 수립한다. 2. 보완 및 개량에 대하여 RAMS요구사항이 유지되도록 관리하며, 관련문서를 모두 갱신한다.
산출문서	1. 보완된 시스템의 검증기록 2. 가정 및 제한사항을 명시한 문서화 3. 확인, 검증, 수용과 관련된 기록의 문서화 4. 위험원 목록 갱신 5. 안전보고서 갱신 6. RAM관련 문서의 갱신(해당항목에 대하여) 7. 다음 수명주기의 입력요소로 활용

검증기준	1. 사용된 자료의 건전성 평가 2. 보완 및 개량이 RAMS요구사항과 LCC관점에서 적절성 평가 3. 갱신된 문서의 적절성 및 완전성 평가(안전보고서는 필수) 4. 적용된 방법, 도구, 기법의 적절성 평가 5. 수행조직의 능력평가
------	---

13단계는 11단계 운영 및 유지보수와 12단계 성능감시를 통해 보완이 요구되는 시스템 및 설비의 전부 또는 일부를 개량하는 과정이다.

이때 보완 및 개량을 통해 변경되는 신뢰도데이터, 유지보수도데이터 및 위험요인과 위험도에 대한 데이터는 최신의 것으로 갱신되어야 한다.

14. 14단계 : 폐 기

수명주기 14단계 중 마지막 단계에서는 운영기관의 시스템 또는 설비의 폐기와 관련된 RAMS활동을 표4-50과 같이 관리한다.

표4-50. 14단계 폐기

목적	시스템의 폐기업무 통제
입력	관련정보
요구사항	1. 시스템 폐기로 인한 관련 시스템의 영향을 평가한다. 2. 폐기업무의 안전 및 관련시스템의 RAMS요구사항이 고려된 폐기계획이 수립되어야 한다. 3. Phase 1(개념)부터 Phase 14(폐기)까지의 LCC가 분석되어야 한다.
산출문서	1. 가정 및 제한사항을 명시한 문서화 2. 폐기업무에 대한 기록의 문서화 및 유지 3. 위험원 목록 갱신 4. 안전계획서 갱신 5. 안전보고서 갱신 6. RAMS요구사항의 유지와 관련된 문서의 갱신
검증기준	1. 사용된 자료의 건전성 평가 2. 폐기와 관련된 문서의 적절성 평가 3. 적용된 방법, 도구, 기법의 적절성 평가 4. 수행조직의 능력평가

시스템 또는 설비의 수명주기 마지막 단계인 폐기는 제작사에 의해 5단계에서 제시된 폐기 관련 안전요구사항과, 운영, 유지보수, 성능감시, 보완 및 개량을 통해 운영기관에 의해 교정된 폐기 관련 안전요구사항을 준수하여 폐기를 실시하고 입증자료를 첨부한다.

제 5 장 연구개발과제 구성 및 추진전략

제 1 절 비전 및 목표

1. 국내 현황

- 철도신호제어시스템의 안전성을 확보하기 위한 노력(요구사항)은 해외에서 시작되어 점차 국내에 적극적으로 도입되고 있는 실정이다. 해외 메이저 철도신호제어시스템 공급업체들은 국제공인인증기관으로부터 SIL인증을 획득한 제어시스템을 기반으로 전세계적인 Market을 형성하여 공급하고 있지만, 현재 국내 철도신호 공급업체의 실적은 전무한 상태이다.
- 최근 발주되는 해외프로젝트는 상기 장치에 대한 SIL인증을 반드시 요구하고 있기에 국내 공급업체의 수주는 현실적으로 불가능한 상황이며, 국내 발주 프로젝트 또한 거의 유사한 형태로서 핵심장치는 대부분 해외 시스템이 적용되고 있는 상황으로 많은 문제점이 발생되고 있다.
- 가장 큰 문제점은 해외시스템의 도입으로 인한 투입금액의 증가를 가져오며, 두 번째로는 핵심시스템(해외)에 따라 국내 공급자가 공급하는 주변 타 시스템의 변경(인터페이스, 프로토콜 등)이 발생하게 되어 고유의 기능과 성능을 보장하지 못하는 점이다. 마지막으로 운영상 발생하는 문제점(오류, 결함 등)에 대한 유지보수의 어려움과 지연 등으로 인해 원활한 서비스가 어려워질 수 있다.

2. 과제 비전

- 해외 메이저 급 철도신호제어시스템 공급사에 대항하기 위해 국내 철도신호제어 시스템의 개발과 안전인증은 반드시 수행되어야 하며 매우 시급한 상황이다. 이러한 핵심 제어시스템의 개발을 위해서는 이를 뒷받침 할 수 있는 제어처리 플랫폼이 우선되어야 한다.
- 본 연구과제에서는 다양한 제어시스템에 적용할 수 있는 공통 플랫폼을 단기간에 개발하여 국내 공급사에서 신속하게 공급하여 국내뿐만 아니라 해외 프로젝트에 적용할 수 있기에 매우 중요한 과제이며, 더욱이 철도분야 이외의 다양한 산업분야(원자력, 화학플랜트, 선박, 의료기 등의 안전필수분야)에 적용하여 활용성이 높다고 볼 수 있다.
- 경제성 분석 결과, 현재 국내 일반철도의 전자연동장치의 수는 약 500여개이며, SIL인증 전자연동장치로 전면 교체할 경우 외산 보드를 적용하는 것에 비해 250억원을 절감할 수

있다. 도시철도 1개 구간을 사례로 들었을 경우 외산(탈레스)시스템에 비해 37억원을 절감할 수 있다. 국내 도시철도 5개소에 적용될 경우, 약 175억원의 경제적 효과를 볼 수 있을 것으로 예상된다.

3. 과제 목표

- 일반 산업의 공통 플랫폼 시장은 성숙단계이나, 관련 안전규격에 의해 고도의 안전성 확보 및 입증되어야 할 철도신호설비에 대해서는 유럽을 중심으로 시장이 형성되는 단계에 있다. 이에 공통 플랫폼의 개발이 시급한 상황이다. 그러므로 본 연구과제의 목표는 연구과제를 통해 국제표준에 부합하는 신호 및 제어 분야의 인증 체계를 수립하고, 최종적으로 국제적 경쟁력을 갖춘 신호설비를 개발하여 SIL 인증을 획득하는 것이다.
- 공통플랫폼은 신호설비에 적용할 수 있는 내장형제어기(Embedded Controller) 형태로써 실시간 운영체제를 바탕으로 접점방식의 입출력, 고속 신호처리가 가능한 아날로그 입출력, 직렬통신 입출력 등 다양한 입출력카드가 확장슬롯을 통해 조합되며 각각의 입출력은 안전 무결성수준(SIL) 4등급의 위험측고장률이 확보되도록 개발
- 공통플랫폼의 소프트웨어(운영체제 및 디바이스드라이버)와 하드웨어는 철도안전국제표준인 IEC 62278(철도응용-철도시스템 RAMS)의 일반응용(Generic Application) 수준의 제3자 보증을 취득하여 안전인증이 필수로 요구되는 철도신호분야에 즉시 실용화 될 수 있는 수준의 전문기관 안전인증서를 포함한다.
- 철도안전법의 형식승인 대상품목 및 국가연구과제 개발 장치를 우선 적용 대상으로 선정하여 실용화 단계에서 적극적으로 활용이 기대된다.

제 2 절 핵심기술요소 선정 및 TRL목표

1. 핵심기술요소(CTE) 도출

가. 핵심기술요소(CTE) 후보

핵심기술요소의 구분을 위해 신호설비의 플랫폼관련 다음의 국가연구개발사업을 대상으로 조사분석하였다.

- 전기신호시스템 엔지니어링 기술개발
- 경량전철 시스템 신호제어시스템 기술개발
- 고속철도 열차제어시스템 안정화 기술개발
- 텀팅열차 시험선 신호보안설비 성능평가연구
- 열차제어시스템 안전성 평가 및 사고방지 기술개발
- 통합 차상신호시스템 시험절차 개발
- 철도차량용 급전 및 신호시스템 핵심부품 개발
- 디지털 송수신기 RAMS 향상 연구
- 열차제어시스템 표준체계 구축 및 안전성평가

위 과제의 분석결과 내장형제어기를 사용한 신호장치 개발 및 안전성향상을 위한 기반연구라는 공통점이 도출되었으나, 적용대상을 위한 맞춤형 기술개발을 목적으로 플랫폼의 공동활용을 위한 연구는 체계적으로 독립수행되지 않았음을 확인하였다.

또한, 내장형 제어기 플랫폼을 공동활용할 수 있도록 개발하고, 관련 국제표준 등에서 요구하는 안전요구사항을 만족하기 위해 필요한 기술로 결합허용 제어기 개발, SIL4 수준인 입출력장치, 철도신호 제어기용 운영체제 개발, 원거리 진단 및 원격유지보수라는 핵심기술을 도출할 수 있었으며, 이에 따라 도출된 핵심기술을 대상으로 우선순위를 분석하였다.

No.	CTE명
후보1	신호설비용 결합허용 제어기 개발
후보2	안전무결성수준(SIL) 4등급의 병렬, 직렬, 아날로그 입출력카드 개발
후보3	철도안전 국제표준의 일반적용(GA)안전인증 취득
후보4	철도신호 내장형제어기용 실시간 운영체제 개발
후보5	원거리 진단 및 원격수리를 위한 자기치유 네트워크형 분산시스템 개발

나. 핵심기술요소(CTE) 선정

핵심기술 후보과제의 우선순위 및 연구개발 필요성을 평가하기 위해 다음과 같이 기술개발의 적절성, 개발위험요인, 독창성, 신규성, 범용성을 기준으로 후보과제별 평가를 시행하였으며, 그 결과 다음과 같이 후보과제 1, 2, 3이 우선순위가 높게 평가되어 기술개발대상으로 선정하였다.

- 신호설비용 결합허용 제어기 개발(핵심기술 후보1)
- SIL4급의 명령, 직렬, 아날로그 입출력카드 개발(핵심기술 후보2)
- 철도안전 국제표준에 따른 안전인증(핵심기술 후보3)

체크리스트	후보 1	후보 2	후보 3	후보 4	후보 5	비고
1. 이 기술이 사용요구조건, 비용, 일정 등에 직접적으로 영향을 미치는가?	○	○	○			반드시 충족
2. 해당기술을 개발하거나 시연하는데 중대한 (실패)위험이 예상되는가?	○	○		○		하나 이상 충족
3. 해당기술이 새롭거나 독창적인가					○	
4. 기존에 성공적으로 적용된 이후에, 이번에 개발시 변경된 기술인가?	○	○				
5. 해당기술이 유사환경에서 실현되도록 재 개발되는가?	○	○	○	○		
6. 이 기술이 임의의 환경에서 작동할 것으로 기대되거나 당초의 설계 의도 혹은 규정된 성능을 뛰어넘는 성능을 달성할 것으로 기대 되는가?	○	○			○	
핵심기술요소(CTE) 선정여부	○	○	○	×	×	

다. 핵심기술요소(CTE) 목록

핵심기술 후보과제별로 연구개발 수행 후의 기술성숙도(TRL)을 추정하였다. 먼저 후보과제 1인 신호설비용 결합허용 제어기, 후보과제 2인 고안전 입출력카드, 내장형제어기 실시간 운영체제의 경우 연구개발 완료 후에 관련 국제표준인 IEC 62278, 62425에 따른 전문기관 안전성평가(인증)취득이 최종성으로 예측되었으며, 후보과제 3인 국제표준기반의 안전인증 취득 기법과 관련해서는 연구개발 된 체계를 통해 신호설비의 안전성을 확보하기 위한 결과가 현재 신호설비 건설 및 개량사업에 요구사항으로 제시하는 국제표준에 따른 RAMS활동에 부합하여 사업화 수준인 TRL9까지 가능할 것으로 평가된다.

또한, 후보과제 5인 자기검사 및 원거리 유지보수 기술과 관련해서는 현재 기술개발의 필요성은 확장되고 있으나, 적용대상 및 구체적인 실용화 방안의 예측이 어려워 TRL5인 시제품 제작 수준에 그칠것으로 평가된다.

CTE	유형	CTE명	최종 TRL
1	장비·장치	신호설비용 결합허용 제어기 개발	TRL8 (시제품 인증)
2	장비·장치	안전무결성수준(SIL) 4등급의 병렬, 직렬, 아날로그 입출력카드 개발	TRL8 (시제품 인증)
3	공법·기법	철도안전 국제표준의 일반적용(GA)안전인증 취득	TRL9 (사업화)
4	소프트웨어	철도신호 내장형제어기용 실시간 운영체제 개발	TRL8 (시제품 인증)
5	시스템	원거리 진단 및 원격수리를 위한 자기치유 네트워크형 분산시스템 개발	TRL5 (시제품 제작)

2. 기술성숙도(TRL) 단계별 목표

앞에서의 후보과제 중 우선순위가 높은 후보과제 1, 2, 3에 대한 연구개발을 가정하여 연차별 TRL을 예측한 결과 다음과 같이 평가되었으며, 각각의 기술을 기획연구결과인 RFP에 반영하였다.

연구과제명		신호설비 안전필수 공통플랫폼		유형		장비·장치	
프레임워크			선행단계		시제품 제작 및 시연	현장적용	제품화/실용화
마일스톤			현재 TRL	마일스톤 목표 TRL			
				1차년도		2차년도	3차년도(종료)
마일스톤 일정			'15.01	'16.01	'17.01	'18.01	
CTE No.	기술명						
CTE 1	신호설비용 결합허용 제어기 개발		3	4		6	8
CTE 2	안전무결성수준(SIL) 4등급의 병렬, 직렬, 아날로그 입출력카드 개발		3	4		6	8
CTE 3	철도안전 국제표준의 일반적용(GA)안전인증 취득		5	6		8	9

제 3 절 연구개발과제 구성

1. 과제 구성

- 연구과제는 핵심기술요소 선정을 통해 철도안전 국제표준에 따라 공통플랫폼 개발 전주기의 위험원분석과 관리를 통해 전문기관의 안전인증(GA)을 취득하기 위한 과제, 상용 실시간 운영체제 기반의 공통플랫폼을 구성하는 결합허용구조 내장형제어기와 입출력카드 개발 과제, 마지막으로 운영체제와 응용프로그램이 일체화된 단순 구조 고안전 공통플랫폼 개발의 총 3개의 과제로 구성
- 다음 그림과 같이 개발단계별 신뢰성 및 안전성을 평가하여 설계를 보완하고 안전인증 취득을 위한 문서화를 수행하는 과제를 중심으로 고성능과 보급형의 고안전 공통플랫폼 개발로 과제를 구성

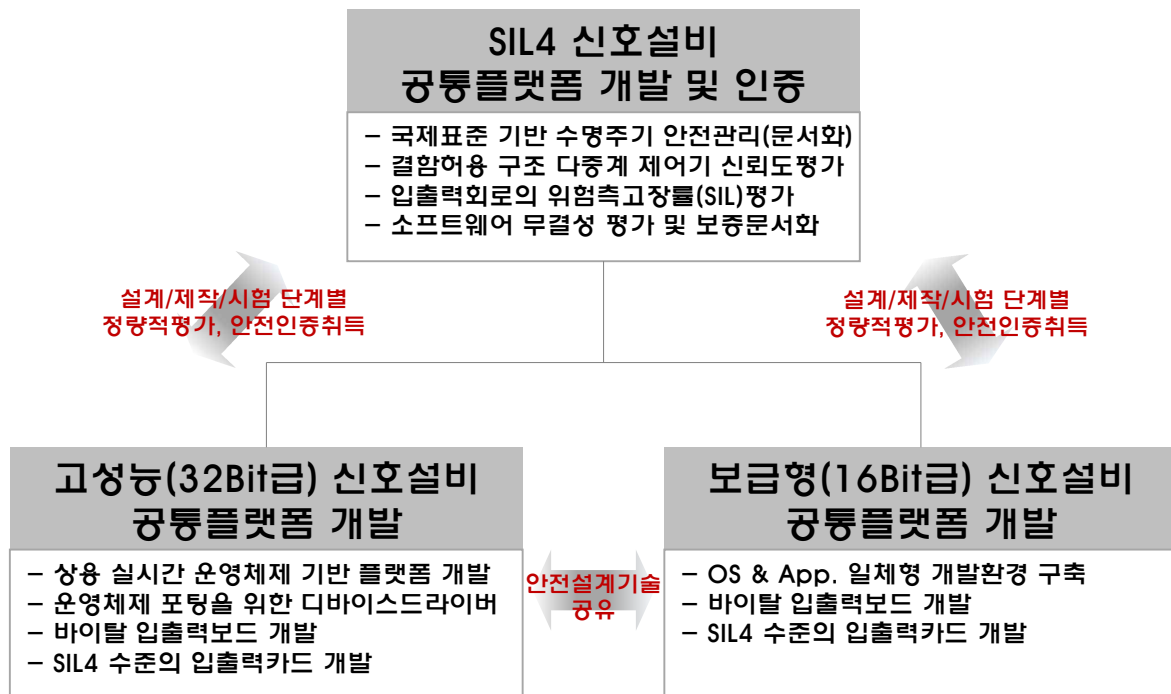


그림. 연구개발과제 구성 및 상호연계방안

- 위 연구개발과제 구성에 대하여 건설운영, 산업(제조), 인증, 연구기관의 전문가 8명 대상으로 심층인터뷰를 진행, 자문결과 다음과 같은 자문을 통해 연구개발과제 구성에 대한 검증 및 실용화를 위한 의견을 수렴

자문실시	분야	전문가 소속	자문의견요약
2014.12.11.	건설운영	한국철도시설공단	필요성 공감, 개발기술의 공개필요
2014.12.11.	건설운영	한국철도공사	개발필요, 신호기업 대상 공개필요
2014.12.08.	건설운영	신분당선(주)	개발필요, 성능구분 없이 양산필요
2014.12.10.	산업(제조)	(주)테크빌	성능검증 중요, 신호업체 다수참여 필요
2014.12.09.	연구	전자부품연구원	공통플랫폼이 산업의 대세임, 기술공개는IoT사례 참조
2014.12.09.	인증기관	TUV라인란드	성능구분 없이 양산이 효과적, 참여기업 SIL인증 후 기술실시 필요
2015.01.09.	산업(제조)	(주)혁신전공사	인증인프라 비용절감 절실, 개발기술의 공개가 중요
2015.12.17.	인증기관	Lloyd's Register	소프트웨어 인증을 위해서는 참여기업이 인증취득 후 기술실시가 효과적

- 또한, 본 보고서의 제3장 2절에서와 같이 공통플랫폼은 고성능과 보급형으로 구분하여 개발하는 것이 실용화에 유리함을 전문가 자문을 통해 확인
- 후보과제별 주요내용, 성과물, 기대효과 등에 대한 사항을 다음과 같이 분석하였으며, 각각의 우선순위는 핵심과제 분석결과를 반영

과제명	주요내용	기존 기술과의 차별성	최종 성과물	기대효과	우선순위
SIL4 신호설비 공통플랫폼 개발 및 인증	• SIL4 신호설비 공통플랫폼 개발 및 인증 -공통플랫폼 성능별 적용대상 선정 -성능별 공통플랫폼 인증활동 -철도신호시스템 인증절차 체계화 -공통플랫폼 실용화를 위한 인증체계 개발	• 사고와 장애 경험을 통해 축적된 설계는 물론 국제표준에 따른 안전설계 방법도출	• 신호설비 주요장치별 및 공통플랫폼 RAMS목표 • 철도안전 국제표준기반 일반응용(GA)인증취득 가이드 • 공통플랫폼 인증서 갱신 및 SA인증취득 가이드	• 철도신호 안전인증관련 국외전문기관 의존 체제를 협력체제로 전환하여 국내기술의 국외진출 및 국내철도 안전확보에 기여	3
고성능 (32bit급) 신호설비 공통플랫폼 개발	• 32bit급 고성능 공통플랫폼 개발 -메인MCU보드 개발 -확장용 I/O보드 개발 -공통플랫폼 개발 -Generic Product SIL4인증 • 공통플랫폼 적용 장치 개발 -공통플랫폼 적용 장치 개발 -Generic Application SIL인증	• 기존 장치위주의 기술개발을 초월하여 안전성이 확보된 핵심처리장치(공통플랫폼) 개발 및 SIL인증 • SIL인증 공통플랫폼을 적용한 핵심처리장치 개발 및 SIL인증	• 메인CPU보드 • 확장용 I/O보드 • 공통플랫폼 • 사용자 사용매뉴얼 • 유지보수 매뉴얼 • 공통플랫폼 표준사양서 • GP SIL4인증서 • 공통플랫폼 적용장치 • GA SIL인증서	• 기존 철도신호 핵심장치의 고도화 및 안전성 확보 • 핵심장치 개발 비용 절감 • 국내 철도신호 핵심장치의 해외수출 기반 마련	1

보급형 (16bit급 이하)신호 설비 공통플랫폼 개발	16bit급 보급형 공통플랫폼 개발 -운영체제와 응용프로그램 일체형 개발환경 구축 -자기검사회로 내장형 Fail-Safe 플랫폼 개발 -공통플랫폼 고안전 입출력카드 및 확장모듈 개발 -보급형 공통플랫폼 운영 및 유지보수 시나리오 도출	상동	- 신호설비 보급형 공통플랫폼 운영체제 및 어플리케이션 개발환경 - 보급형 공통플랫폼 - 보급형 공통플랫폼 입출력카드 및 확장모듈 - 보급형 공통플랫폼 실용화 매뉴얼	- 기존 철도신호 핵심장치의 고도화 및 안전성 확보 - 핵심장치 개발 비용 절감 - 국내 철도신호 핵심장치의 해외수출 기반 마련	2
--	--	--	---	---	---

2. 연구 목표

- 고성능과 보급형 신호설비 공통플랫폼 개발 분야는 각각의 개발목표에 따라 내장형제어기와 입출력카드를 개발
- 공통플랫폼의 신호설비 실용화를 위한 현실적인 신뢰도 및 안전성목표 설정, 신뢰도목표는 성능별 공통플랫폼 각각의 평균고장시간(MTBF), 안전성목표는 각각의 입출력 정보의 위험측 고장률을 $1e-8/h$ 미만이 되도록 설정
- 내장형제어기의 결함허용구조에 따른 안전성과 신뢰성의 정량적 평가 및 입출력카드의 위험측고장발생빈도 평가를 국제표준에 따라 단계별로 수행하여 설정된 목표에 만족함을 입증
- 개발된 성능별 신호설비 공통플랫폼에 대하여 「SIL4 신호설비 공통플랫폼 개발 및 인증」 과제를 중심으로 제3의 전문기관으로부터 국제표준 기반의 안전인증 취득을 통해 실용화 추진

[세부과제1의 주요연구목표]

- 공통플랫폼 성능별 요구사항 수립
- 성능별 공통플랫폼 인증활동
- 철도신호시스템 인증절차 체계화
- 공통플랫폼 실용화를 위한 인증체계 개발

[세부과제2의 주요연구목표]

상용 실시간 운영체제 포팅

다중계구조 결함허용 플랫폼 개발

공통플랫폼 고안전 입출력카드 및 확장모듈 개발

고성능 공통플랫폼 운영 및 유지보수 시나리오 도출

[세부과제3의 주요연구목표]

운영체제와 응용프로그램 일체형 개발환경 구축

자기검사회로 내장형 Fail-safe 플랫폼 개발

공통플랫폼 고안전 입출력카드 및 확장모듈 개발

보급형 공통플랫폼 운영 및 유지보수 시나리오 도출

[연구개발 최종성과]

- 철도안전 국제표준(IEC 62278)에 적합한 신호설비 공통플랫폼을 고성능(32bit급)과 보급형(16bit급 이하)으로 구분하여 개발

공통플랫폼 평균고장시간(MTBF)은 카드단위 100,000시간 이상, 플랫폼 전체 50,000시간 이상, 평균유지보수시간 플랫폼단위 0.5시간 이내

- 신호설비 공통플랫폼 적용을 위한 기능안전국제표준(IEC 61508)기준 안전무결성수준(SIL4)급 입출력카드 및 호환모듈 개발

입출력카드는 접점형식 DIO(16채널/카드 이상), 직렬통신(4채널/카드 이상), 고속신호처리 가능한 DSP내장형 필수

- 입출력카드를 포함한 공통플랫폼의 국제표준기반 일반응용(GA) 안전인증서 및 실용화 시 상세응용(SA) 안전인증을 위한 가이드

제 4 절 세부과제 주요내용 및 추진전략

국제표준에 따라 안전인증을 취득한 신호설비 공통플랫폼의 개발은 다음의 3가지의 후보과제로 구분하여 추진한다.

후보과제 1은 신호설비 공통플랫폼의 요구사항 도출과 개발단계의 국제표준기반 인증을 위한 활동을 수행한다. 후보과제 2와 3은 후보과제 1에서 도출한 요구사항을 바탕으로 결합허용 및 안전설계를 반영한 공통플랫폼을 개발하고, 국제표준기반의 안전인증 취득을 위한 RAMS 문서화를 핵심활동으로 한다. 후보과제 2는 전자연동장치, 차상신호장치 등 고성능 플랫폼을 개발하고, 후보과제 3은 자동폐색장치, 궤도회로 등 저비용 플랫폼을 개발한다. 32bit와 16bit는 프로세서의 데이터 버스 사이즈를 기준으로 한다.

연구목표	주요 연구내용
후보과제 1 SIL4 신호설비 공통플랫폼 개발 및 인증	- 제어 성능별 공통 플랫폼 요구사항 도출 - 신호제어 설비의 시장조사분석 - 신호제어 설비에 대한 제어 용량 기준 제시 - 제어 용량에 따른 표준 플랫폼 구축 방안 마련 - 공통 플랫폼이 적용 가능한 신호제어 설비 도출 - 성능별 공통플랫폼의 인증활동 - 고장, 품질 및 안전목표, 적용규격 정의 - 인증활동계획 수립 및 수명주기별 산출물 작성 - 성능별 표준플랫폼의 전문기관 인증취득(일반제품, GP) - 철도신호시스템 인증절차 체계 정리 - 적용표준의 수명주기별 요건 정리 - 일반제품(GP), 일반응용(GA), 상세응용(SA) 인증별 요건과 문서화 가이드, 체크리스트 개발 - 공통플랫폼 활성화를 위한 인증체계 개발 - 공통플랫폼의 인증(공개된 방법에 따라 제작된 공통플랫폼의 건전성 확인, SRAC에 포함)주체 정립 - 공통플랫폼의 GP를 포함한 GA와 SA 인증취득 체계

연구목표	주요 연구내용
후보과제 2 고성능(32bit급) 신호설비 공통플랫폼 개발	- 공통 플랫폼에 대한 실시간 운영체제 선정 방안 확립 - 상용 리얼타임 OS에 대한 신호 플랫폼 적용 연구 - 리얼타임 OS와 BSP간 응용 기술 개발 - 철도신호 공통 플랫폼(32bit급) 시스템 다중화 구성 연구 - 신뢰성과 가용성을 고려한 CPU 다중화 방안 확립 - 적용 설비별 I/O 다중화 방안 도출 - 기존 시설물과의 인터페이스 기술 연구 - 제어 용량별 다중화 기준 작성 - 철도신호 공통 플랫폼(32bit급) 개발 - 안전성과 신뢰성이 확보된 제어 용량별 공통 하드웨어 플랫폼 개발 - 어플리케이션 레이어 포팅 기술 개발 - 적용 설비별 I/O 카드 및 확장 모듈 개발 - 철도신호 공통 플랫폼(32bit급) 운영 및 유지보수 시나리오 도출 - 표준 플랫폼에 대한 유지보수 매뉴얼 개발 - 표준 플랫폼에 대한 운영기술 개발 - 어플리케이션 레이어 포팅 매뉴얼 개발
후보과제 3 보급형(16bit급 이하) 신호설비 공통플랫폼 개발	- 철도신호 공통 플랫폼(16bit급 이하) 시스템 고안전 구성 연구 - OS와 응용소프트웨어 일체형 개발환경 구축 - 신뢰성과 가용성을 고려한 CPU 자기검사 방안 확립 - 적용 설비별 I/O 자기검사 방안 도출 - 기존 시설물과의 인터페이스 기술 연구 - 제어 용량별 다중화 기준 작성 - 운영체제 건전성 확보방안 도출 - 철도신호 공통 플랫폼(16bit급 이하) 개발 - 안전성과 신뢰성이 확보된 제어 용량별 공통 하드웨어 플랫폼 개발 - 어플리케이션 레이어 포팅 기술 개발 - 적용 설비별 I/O 카드 및 확장 모듈 개발 - 철도신호 공통 플랫폼(16bit급 이하) 운영 및 유지보수 시나리오 도출 - 표준 플랫폼에 대한 유지보수 매뉴얼 개발 - 표준 플랫폼에 대한 운영기술 개발 - 어플리케이션 레이어 포팅 매뉴얼 개발

제 5 절 과제별, 연차별 기술로드맵 및 성과로드맵

국제표준에 근거한 안전인증을 취득한 신호설비 공통플랫폼의 성능별 개발은 총 3년의 연구를 통해 도출될 것으로 예상되며, 후보과제 각각에 대한 연차별 세부사항은 다음의 로드맵에 따라 수행한다.

1. 후보과제 1 「SIL4 신호설비 공통플랫폼 개발 및 인증」의 기술 및 성과 로드맵

주요내용	1차년				2차년				3차년				최종성과
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	
성능별 공통플랫폼 요구사항 수립	공통플랫폼 적용대상 선정			정량적 RAMS 목표설정									신호설비 주요장치별 및 공통플랫폼 RAMS목표
성능별 공통플랫폼 인증활동			공통플랫폼 RAMS Plan		공통플랫폼 RAM분석 및 설계향상			공통플랫폼 신뢰성 및 안전성 설계보완			철도안전 국제표준기반 일반응용 (GA)인증서		
					위험원 도출(PHA)	위험도관리 SSA/HW O&SA	위험도관리 V&V	RAMS인증 (가속시험)					
					소프트웨어 보증활동								
					국외전문기관 1단계 ISA				국외전문기관 2단계 ISA				인증취득
철도신호시스템 인증절차 체계화	철도안전 국제표준 요구사항 가이드 작성				전문기관 안전인증 취득을 위한 상세 가이드 작성				공통플랫폼활용 상세응용(SA) 인증취득 가이드작성				안전인증 취득가이드
공통플랫폼 활성화를 위한 인증체계 개발	공통플랫폼 활용 협의체 구성				공통플랫폼 공개범위 설정			성능별 공통플랫폼 안전전제조건(SRAC) 문서화					공통플랫폼 인증서갱신 및 SA인증취득 가이드
					공개기술 안전인증 갱신방안 수립								
TRL	6				8				9				

성능별 공통플랫폼 요구사항 수립을 1차년에 수행하여 적용대상 선정과 정량적 RAMS목표 수립을 통해 신호설비 주요장치별 공통플랫폼의 RAMS목표를 수립하고, 성능별 공통플랫폼 인증활동을 2차년과 3차년에 관련 국제표준(IEC 62278)에 따라 수행

또한, 일반응용 인증서를 전문기관으로 취득. 또한 3개년의 연구기간에 걸쳐 국제표준에 따른 안전인증 취득을 위한 요구사항 가이드를 작성하여 향후 신호설비 안전인증 취득을 위한 체계를 구축하고, 특정 사업에 따라 상세응용 안전인증 취득을 위한 전략수립과 단계별 수행 체계를 정립

2. 후보과제 2 「고성능(32bit급) 신호설비 공통플랫폼 개발」의 기술 및 성과 로드맵

주요내용	1차년				2차년				3차년				최종성과
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	
상용 실시간 운영체제 포팅	OS선정 및 개발환경 구축				다중계구조 CPU모듈 BSP개발	고안전 IO모듈 BSP 개발	응용프로그램 포팅검증						신호설비 고성능 공통플랫폼 운영체제 및 App. 개발환경
다중계구조 결함허용 플랫폼 개발		N out of M 플랫폼 설계 및 시작품 제작	디바이스 드라이버 개발		N out of M 공통플랫폼 OS 포팅 및 디버깅	결함허용 시험 및 설계보안			3차 시작품 제작		공인기관 환경시험		고성능 공통플랫폼 다중계 CPU 모듈
공통플랫폼 고안전 입출력카드 및 확장모듈 개발	IO종류, 사양, 채널등 선정				DIO,AO,COM등 모듈개발 및 디버깅	결함허용 시험 및 설계보안			2차 시작품 제작		공인기관 환경시험		고성능 공통플랫폼 입출력카드 및 확장모듈
고성능 공통플랫폼 운영 및 유지보수 시나리오 도출					고성능 공통플랫폼 기술매뉴얼 작성	성능별 공통플랫폼 인터페이스, 운영, 유지보수 매뉴얼 작성							고성능 공통플랫폼 실용화 매뉴얼
TRL	4				6				8				

고성능 공통플랫폼의 개발을 위해서는 상용 실시간운영체제의 포팅을 위해 1차년에 운영체제 선정 및 하드웨어와의 연계를 위한 드라이버 소프트웨어를 개발하고, 2차년에 다중계구조로 플랫폼을 설계하여 3차년까지 호환되는 입출력카드의 개발 및 응용프로그램 포팅을 통해 성능을 검증토록 구성. 이를 통해 개발환경구축과 다중계구조의 CPU모듈을 개발

향후의 확장모듈 및 안전성을 지속적으로 확보하기 위한 유지보수 시나리오를 도출하여 매뉴얼화를 진행하며, 후보과제 1과의 연계를 통해 국제표준에 따른 SIL인증 참고문헌을 개발하여 유사 사업의 전문기관 안전인증 취득을 위한 체계를 구축

3. 후보과제 3 「보급형(16bit급 이하) 신호설비 공통플랫폼 개발」의 기술 및 성과 로드맵

주요내용	1차년				2차년				3차년				최종성과
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	
운영체제와 응용프로그램 일체형 개발환경 구축	컴파일러선정 및 개발환경 구축				부트와 App.영역 구분	응용프로그램 포팅검증							신호설비 보급형 공통플랫폼 운영체제 및 App. 개발환경
자기검사회로 내장형 Fail-safe 플랫폼 개발		자기검사회로 설계 및 시작품 제작	보급형 플랫폼 기대성능 설정		자기검사회로 성능시험 환경 구축 및 시험	Fail-safe 시험 및 설계보안			3차 시작품 제작		공인기관 환경시험		보급형 공통플랫폼
공통플랫폼 고안전 입출력카드 및 확장모듈 개발	IO종류, 사양, 채널등 선정				DIO,AO,COM등 모듈개발 및 디버깅	Fail-safe 시험 및 설계보안			2차 시작품 제작		공인기관 환경시험		보급형 공통플랫폼 입출력카드 및 확장모듈
보급형 공통플랫폼 운영 및 유지보수 시나리오 도출					보급형 공통플랫폼 기술매뉴얼 작성	성능별 공통플랫폼 인터페이스, 운영, 유지보수 매뉴얼 작성							보급형 공통플랫폼 실용화 매뉴얼
TRL	4				6				8				

보급형 공통플랫폼은 운영체제와 응용프로그램을 일체화하여 개발하기 위한 개발환경 구축을 위해 1차년도에는 SIL4 취득을 위한 컴파일러 선정 및 안전구조에 대하여 IEC 62425의 SIL별 요구사항을 반영하여 개발

보급형 공통플랫폼의 핵심기능인 자기검사기능을 개발을 위해 고장모드영향분석(FMEA)을 통해 결함검출대상을 선별하고, 결함검출을 위한 회로구성 및 발생한 결함을 격리하고 허용하기 위한 하드웨어 및 소프트웨어 설계기술을 개발

입출력카드 및 확장모듈의 설계와 관련하여 허용할 수 없는 결함이 발생하는 경우에 안전측으로 동작시키기 위한 Fail-Safe회로를 하드웨어적으로 구성하고, 개발된 플랫폼을 대상으로 적용대상의 설치환경(실내, 선로변, 차량 등)조건에 따라 관련 표준에 따른 환경시험 수행

각각의 후보과제의 연차별 로드맵과 관련하여 세부 연구내용의 수행에 필요한 예산을 다음과 같이 추정

[단위 : 천원]

세부과제명	1차년도	2차년도	3차년도	합 계
1. SIL4 신호설비 공통플랫폼 개발 및 인증	567,570	517,272	415,157	1,500,000
2. 고성능(32bit급) 신호설비 공통플랫폼 개발	1,043,550	1,271,291	1,720,030	4,034,872
3. 보급형(16bit급 이하) 신호설비 공통플랫폼 개발	604,096	731,547	775,162	2,110,806
합계	2,215,216	2,520,110	2,910,349	7,645,678

제 6 절 성과활용 방안

가. 연구결과의 활용방안

- 단기 및 중·장기적인 연구개발계획의 수립 및 시행에 활용
 - 본 과제는 기획과제로 연구완료시, 연구결과를 바탕으로 철도신호 플랫폼 표준화 및 인증체계 수립의 중·장기적인 연구개발계획의 수립 및 이의 시행에 필요한 재원확보에 활용
 - 핵심과제 발굴 및 투자우선순위 설정에 활용
 - 정부 및 관련기관에 정기/비정기적인 보고 및 홍보를 통하여 사업추진의 공감대를 형성
- 성능별(고급형과 보급형)의 구분개발에 대한 검토
 - 32bit와 16bit급 이하의 성능기준을 통합하여 공통플랫폼을 개발하는 경우 연구개발기간 및 재원에 대한 절약과 대량생산으로 인한 실용화가능성은 높아지나, 현장설치 후 부품의 개수가 상대적으로 많을수록 고장발생빈도와 유지보수 비용이 발생하여, 장치의 기능요구사항에 적합하도록 성능기준을 고성능과 보급형으로 구분하여 개발하는 것이 효과적

나. 기대성과 및 파급효과

- 신호설비 표준플랫폼으로 국제표준에서 강제하는 안전성과 신뢰성을 확보한 성능별(고성능, 중하성능) 제어기의 하드웨어 구조 및 소프트웨어 운영체제표준화를 위한 개발범위, 안전 인증을 위한 수명주기별 절차 기획
- 상대적으로 영세한 국내 제조사별로 국제표준의 안전인증에 중복 투자되는 비용을 절감하고, 신호설비 플랫폼 표준화를 통해 구성품단위 호환성을 확보하여 운영 및 유지보수 비용 절감 기대
- 자체 개발한 표준플랫폼의 활용으로 기존 전자연동장치 등에서 사용된 외산 플랫폼의 OS 라이선스 비용이 절감되는 효과

다. 외산 플랫폼에 대한 독립성

- 공통플랫폼의 필요성이 강조됨에 따라 해외 플랫폼 제작사에서 이미 개발을 시작하여 국내 진입을 시도하고 있으며, 안전인증(SIL)이 완료되었거나 현재 진행 중임
- 본 과제를 통해 개발되는 자체 제작 플랫폼에 대한 예측 데이터와 외산 플랫폼을 도입할 경우에 대해 비교 조사한 결과를 제시한다. 본 과제에서 제작될 플랫폼의 경우를 A, 최근 적용되고 있는 외산 플랫폼B 그리고 C에 대해 분석한 결과는 아래와 같다.

(1) 플랫폼 도입 및 순수 제작비 비교

- 각 사의 플랫폼 도입비용은 투입되는 인건비를 제외한 기자재 비용만 고려되었다. B사의 CPU 플랫폼은 구입(도입)비용이 1ea당 70,000,000원의 비용으로 가장 높으며, C사의 CPU 플랫폼이 1ea당 9,000,000원으로 두 번째로 높다. A사의 CPU 플랫폼은 자체 개발에 의한 제작비용은 1ea당 2,500,000원이다.

(2) 플랫폼 적용 Application 개발 비용

- 각 사의 플랫폼을 전자연동장치(SIL4인증) 개발에 적용할 경우 투입되는 비용에 대해 비교 분석하였다. 또한, Application 개발 비용을 예측하기 위해 대형역인 서울역의 전자연동장치를 대상으로 계산되었다.

서울역 전자연동장치 I/O Point	
Input Point	928 Point
Output Point	307 Point

	국산 A사(가정)		외산 B사		외산 C사	
	Cost (원)	Remark	Cost (원)	Remark	Cost (원)	Remark
CPU 플랫폼	20,000,000	8ea (2,500,000원) 이중계 구성	70,000,000	1ea (이중계구성) CSC x 2 + Relay box	18,000,000	2ea (9,000,000원) 이중계 구성 적용
IL Subsystem	3,000,000	2ea (1,500,000원) 이중계 구성				
Output Board	10,000,000	20ea (500,000원) 307point/32ch = 9.6 = 10ea 이중계 구성 = 20ea	10,000,000	20ea 307point / 32ch = 9.6 = 10ea 이중계 구성 = 20ea	59,280,000	78ea (760,000원) 307point/8ch = 38.3 = 39ea 이중계 구성 = 78ea
Input Board	23,200,000	58ea (400,000원) 928point/32ch = 29ea 이중계 구성 = 58ea	23,200,000	58ea 928point / 32ch = 29ea 이중계 구성 = 58ea	74,240,000	116ea (640,000원) 928point/16ch = 58ea 이중계 구성 = 116ea
I/O Subsystem	9,000,000	6ea (1,500,000원) (10장 + 29장) / 16 = 2.4ea 이중계 구성 = 6ea	120,000,000	8ea (15,000,000원) (10장 + 29장) / 12 = 3.25ea 이중계 구성 = 8ea	39,600,000	33ea (1,200,000원) (78장 + 116장)/6 = 33대
합계	65,200,000		223,200,000		191,120,000	

전자연동장치를 개발하기 위해 아래와 같은 구성으로 분석하였다.

〈IL Subsystem〉

전자연동장치의 IL Subsystem은 핵심 처리모듈로서 CPU플랫폼의 이중계 구성을 위해 제작되는 Shelf형태의 모듈이다. 외산 플랫폼인 B, C사는 CPU플랫폼 1set 비용에 포함되어 있으며, A사의 국산 플랫폼은 CPU플랫폼을 기반으로 IL Subsystem을 구성할 경우 3,000,000원이 투입된다.

〈Output 보드〉

Output보드의 경우, C사는 Output 307point에 대하여 8ch씩 구성됨으로써 총 39ea(이중계 구성 78ea)가 필요하다. 이는 A사와 B사의 20ea(이중계)에 비해 훨씬 많은 양이며 ea당 가격도 260,000원이 더 요구된다. 전체 비용에서는 59,280,000원으로 6배 가량의 큰 금액 차이가 난다.

〈Input 보드〉

Input 보드 또한 C사의 경우 Input 928point에 대하여 16ch씩 구성됨으로써 총 58ea(이중계 구성 116ea)가 필요하다. A사와 B사는 절반인 58ea(이중계)이며 ea당 가격도 240,000원이 적게 든다. 전체 비용에서는 C사가 74,240,000원의 금액으로 A, B사보다 약 3배 정도 큰 금액이다.

〈I/O Subsystem〉

I/O Subsystem은 Output 보드와 Input 보드 수 총합에서 장착 가능한 I/O 모듈 수만큼 나누어서 필요한 수량을 파악하는데 C사가 33ea로 A사의 6ea, B사의 8ea보다 많이 요구된다. 그러나 ea당 가격이 B사가 15,000,000원으로 크게 비싸므로 금액적인 차이가 많이 난다.

〈구성품목별 제작비〉

공통플랫폼을 적용한 전자연동장치의 개발에 지출되는 각 부품의 비용을 보여준다. B사의 제작비가 플랫폼과 I/O 서브시스템에서 다른 제품보다 크게 지출됨을 알 수 있다.

(3) 외산 플랫폼에 대한 독립성 제시

상기의 내용에서와 같이 외산 플랫폼을 적용하게 될 경우 최대 3배가량 비용이 투입됨을 실제 데이터(비용)를 적용한 결과를 확인할 수 있다. 이에 본 과제에서 기획된 공통플랫폼의 국산화를 통해 외산에 대한 의존성을 탈피하고 독립성을 가져야 하며, 이에 따라 자체적인 기술력 확보와 시스템의 확장성 및 유지보수성을 확보할 수 있다.

(4) 실시간 운영체제

실시간 운영체제의 쉬운 해석으로는 ‘시스템의 하드웨어와 어플리케이션을 이어주는 역할’이라 볼 수 있으며 임베디드 시스템에 적용할 수 있도록 TASK 관리, 메모리 관리, 커널, 기타 I/O통신 관리 등을 수행한다. RTOS(Real Time Operating System)으로 칭하며, 종류로는 VxWorks, PikeOS, QNX, SafeRTOS 등이 존재한다.

이러한 실시간 운영체제는 바이탈 임베디드 시스템에 적용하기 위해 국제표준규격에 따른 SIL인증을 획득함으로써 안전성을 확보하였다.

본 과제를 통해 국내 자체적인 공통 플랫폼에 탑재될 실시간 운영체제는 32bit급과 16bit급으로 구분되어 적용에 따른 시간적, 비용적 효과를 증대시키고자 한다.

32bit급 공통 플랫폼은 철도신호장치 중에서 안전과 직결되는 Vital 장치에 적용되기에 국제적으로 안전성이 입증된 상기의 SIL인증 RTOS가 적용된다. 우선적으로 철도안전법에서 추진하고 있는 형식승인 대상품목인 전자연동장치, AF궤도회로, 자동폐색제어장치 등이 있으며, 열차자동방호장치(ATP)등에 적용될 수 있다.

모든 철도신호 처리 및 제어장치에 32bit급 처리 플랫폼이 장착될 필요가 없으며, 32bit급 장치보다 수량 및 공급량이 더 높은 16bit급 플랫폼 또한 개발되어 이에 대한 안전성을 확보할 필요가 있다. 16bit급 플랫폼의 운영체제는 자체OS 또는 상용OS가 적용될 수 있지만, 32bit급 플랫폼에 적용된 SIL인증 OS를 적용하게 될 경우 16bit급 플랫폼이 적용된 소형, Non-Vital 장치의 개발 기간과 비용의 상승으로 경쟁력을 잃을 수 있다.

라. 공통플랫폼 실용화 및 공유 방안

국내 철도신호분야는 오래전부터 핵심장치의 국산화를 추진해오고 있다. 또한 이러한 핵심장치의 안전성을 확보하기 위한 다각적인 노력을 운영기관 및 공급업체에서 기울여 왔다. 그 결과 국산화 비중은 매우 높은 단계까지 증가하였으며, 국제적인 SIL인증을 획득하는 경우도

점차 증가하고 있다. 이러한 추세는 가까운 중국에서 더 가파른 증가 추세를 보이고 있는 실정이다.

그러나 이러한 국내의 핵심장치에서 처리장치는 대부분 외산제품을 도입하고 이에 따른 기술 지원을 받아 진행된 경우가 대부분인 것으로 확인되었다. 이 경우, 핵심장치의 공급량 증가에 따른 처리장치 비용이 가중될 수 있으며, 공급 이후 신속한 유지보수 및 개선이 어려운 단점을 가지고 있다.

이에 본 과제에서 개발되는 공통플랫폼은 개발과 동시에 대상시스템에 적용함으로써 국내 철도안전법 및 표준규격을 만족할 수 있는 장치를 개발하고자 한다. 또한 철도신호시스템은 다양한 처리방법과 어플리케이션 그리고 인터페이스 환경을 가지고 있기에 이러한 사항에 대해 포괄할 수 있는 범용적인 플랫폼이 반드시 필요한 요구사항으로 볼 수 있다.

개발된 공통플랫폼은 다음과 같은 방법으로 적극적인 홍보 및 공유를 할 예정이다.

- 국가연구과제 적극 활용 - 연구과제 적용을 위한 RFP 및 기술 지원
- 철도안전법 형식승인 대상품목 우선 적용 - 공통플랫폼 및 기술 지원
- 핵심장치 개량 지원

제 7 절 연구수행 체계

- 다음 그림과 같이 개발단계별 신뢰성 및 안전성을 평가하여 설계를 보완하고 안전인증 취득을 위한 문서화를 수행하는 과제를 중심으로 고성능과 보급형의 고안전 공통플랫폼 개발로 과제를 구성

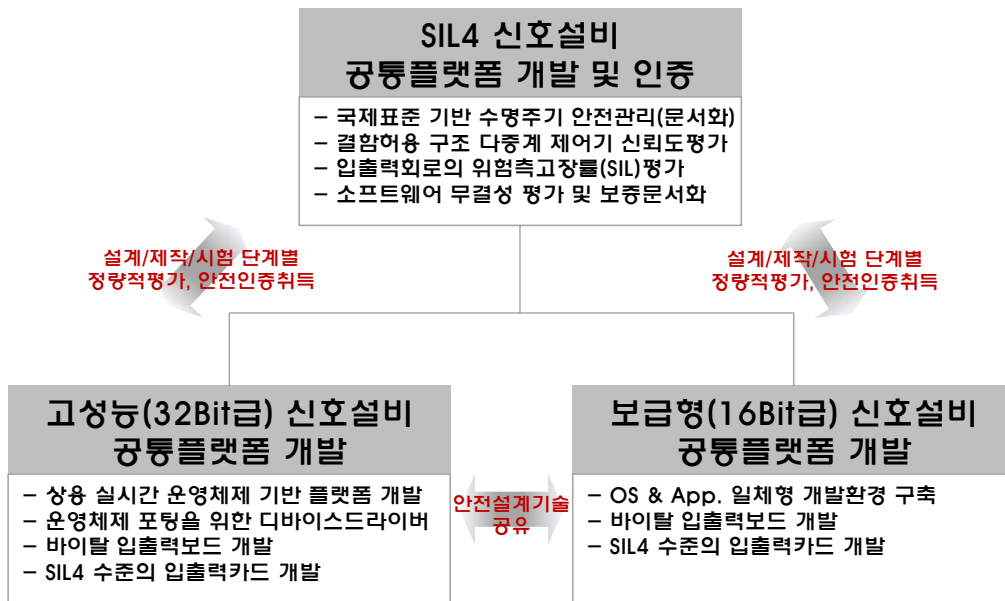


그림. 연구개발과제 구성 및 상호연계방안

- 공통플랫폼 실용화를 위해 다양한 분야(산·학·연)로 참여기관 구성하고 국내 철도신호기업의 공통플랫폼 활용 촉진에 위한 철도신호협회 및 철도신호연구조합 등 기존 협의체 참여
- 성능별 공통플랫폼의 연구결과는 실용화를 위해 하드웨어(PCB 도면 및 부품리스트), 소프트웨어(실행코드), 안전인증서를 협의체에 참여한 기업을 대상으로 공개
- 참여기관은 공통플랫폼의 소프트웨어(소스코드)와 안전인증 취득을 위한 평가문서에 대한 소유권을 가짐
- 참여기관은 세부과제 별로 안전인증취득 또는 컨설팅, 신호설비 개발 및 제조실적이 있는 기관으로 구성

제 6 장 과제 제안요구서

제 1 절 과제 제안요구서

연구과제명	고안전 신호설비 공통플랫폼개발 연구
1. 최종 목표	○ 철도안전 국제표준기반 안전인증된 신호설비 공통플랫폼 개발
2. 최종 성과물	○ 철도안전 국제표준(IEC 62278)에 적합한 신호설비 공통플랫폼을 고성능(32bit급)과 보급형(16bit급 이하)으로 구분하여 개발 - 공통플랫폼 평균고장시간(MTBF)은 카드단위 100,000시간 이상, 플랫폼 전체 50,000시간 이상, 평균유지보수시간 플랫폼단위 0.5시간 이내 - 개발 프로세스는 IEC 62278을 준수, 공통플랫폼의 기능안전은 IEC 62425 기준 SIL4 요구사항 적용 - 평균고장시간은 MIL-DHBK-217FN2(상온, 지상설치 조건) 기준 예측치와 신뢰성시험 결과를 바탕으로 요구사항만족 확인 - 평균유지보수시간은 MIL-STD-472 기준 예측치와 현장평가 결과를 바탕으로 요구사항만족 확인 ○ 신호설비 공통플랫폼 적용을 위한 기능안전국제표준(IEC 61508)기준 안전무결성수준(SIL4)급 입출력카드 및 호환모듈 개발 - 입출력카드는 접점형식 DIO(16채널/카드 이상), 직렬통신(4채널/카드 이상), 고속신호처리 가능한 DSP내장형 필수 - 접점방식은 DC24V, Switching Time 1ms이내, 직렬통신은 RS 232, 422, 485를 모두 적용 ○ 입출력카드를 포함한 공통플랫폼의 국제표준기반 일반응용(GA) 안전인증서 및 실용화 시 상세응용(SA) 안전인증을 위한 가이드 - IEC 62278, 62425, 62279의 SIL4관련 요구사항을 명세하고, 각각의 요구사항 만족을 위한 방안과 참고데이터 제시 - 예비위험원분석(PHA), 고장모드영향 및 심각도분석(FMECA), 위험원목록(Hazard Log)관련 템플릿 제시 - 전문기관 일반응용 및 상세응용 안전평가 준비를 위한 각각의 자체검사 체크리스트 제시

3. 추진 필요성	○ 현재 국내에서 운영 중인 차상 및 지상 신호 플랫폼이 각기 상이하고, 상호 호환성이 결여되어 효율성이 낮으며, 대부분 수입됨에 따라 운영 및 유지보수에 외국업체에 많이 의존하고 있어 관련 비용이 많이 소요됨 ○ 국제표준의 신호설비 안전성 표준강화로 인해 제작사별로 신뢰성, 안전성 개발환경 구축, 안전인증취득을 위한 컨설팅 및 인증비용의 중복발생으로 제조기업의 국내외 경쟁력 악화로 인한 제품의 품질과 안전부실화 우려 ○ 세계적으로 신호안전설비의 전문화 및 안전비용 절감을 위해 독일의 MEN사와 미국의 Artesyn사가 공통플랫폼을 개발하여 국내외 철도신호시장에 빠르게 확산. 이로 인한 국내 신호업체의 핵심기술 해외 의존도가 급격히 상승우려 ○ 따라서, 일반응용(GA)수준의 안전인증된 공통플랫폼을 국산화 하여 해외 기술의 국내시장 잠식을 견제하고, 국제 철도신호 제조기업 제품의 품질안전 고도화에 집중토록 시장환경 조성이 요구됨
4. 연구개발 내용	☐ 세부과제1 : SIL4 신호설비 공통플랫폼 개발 및 인증 ○ 공통플랫폼 성능별 요구사항 수립 - 신호설비 공통플랫폼 적용대상 선정 - 주요 신호설비 각각에 대한 예비위험원분석 실시 및 정량적 RAMS 목표 설정 - 공통플랫폼의 신뢰도(MTBF), 가용도(Ass), 유지보수도(MTTR), 기능별 안전요구사항(SIL) 할당 ※ MTBF(Mean Time Between Failure), Ass(Steady State Availability), MTTR (Mean Time To Repair), SiL(Safety Integrity Level) ○ 성능별 공통플랫폼 인증활동 - 공통플랫폼 RAMS Plan 및 시스템위험원분석(SHA) - 성능별 위험원분석(SSHA), 인터페이스 위험원분석(IHA), 운영 및 유지보수 위험원분석(O&SHA) 수행 - IEC 62279(철도응용 소프트웨어)기반 소프트웨어 보증활동 - 시스템 확인 및 검증(V&V), 예측 신뢰도에 대한 가속수명시험을 통한 입증 - 국내외 실용화를 위한 국외전문기관 ISA선정 및 안전인증 취득 ○ 철도신호시스템 인증절차 체계화 - 관련 국제표준 준수를 위한 가이드 개발 - 전문기관 안전인증 취득을 위한 가이드 개발

- 공통플랫폼을 적용한 상세응용(SA) 안전취득을 위한 가이드 개발
- 공통플랫폼 실용화를 위한 인증체계 개발
 - 공통플랫폼 실용화를 위한 협의체 구성
 - 공통플랫폼 기술공개범위 설정 및 안전인증의 갱신환경 구축
 - 공통플랫폼 안전전제조건(SRAC) 문서화

□ 세부과제2 : 고성능(32bit급) 신호설비 공통플랫폼 개발

- 상용 실시간 운영체제 포팅
 - 실시간 운영체제 선정 및 개발환경 구축
 - 결함허용 다중계구조 공통플랫폼(고안전 입출력카드 포함) 디바이스 드라이버 개발 및 드라이버 안전인증
- 다중계구조 결함허용 플랫폼 개발
 - N out of M 플랫폼 설계(FMECA 포함) 및 시작품 개발
 - ※ FMECA(Failure Mode Effect & Criticality Analysis)
 - 공통플랫폼의 결함허용 및 안전측동작 시험환경 구축
 - KRS 및 ETCS기준 환경시험 실시
- 공통플랫폼 고안전 입출력카드 및 확장모듈 개발
 - 공통플랫폼 입출력의 종류, 사양, 채널(용량) 등 기술사양 선정
 - 확장 인터페이스(BUS Type) 선정 및 기술문서화
 - 입출력카드 및 확장모듈별 SIL4 안전설계
 - KRS 및 ETCS기준 환경시험 실시
- 고성능 공통플랫폼 운영 및 유지보수 시나리오 도출
 - 고성능 공통플랫폼 기술메뉴얼 작성
 - 고성능 공통플랫폼 인터페이스, 운영, 유지보수 매뉴얼 작성

□ 세부과제3 : 보급형(16bit급 이하) 신호설비 공통플랫폼 개발

- 운영체제와 응용프로그램 일체형 개발환경 구축
 - 컴파일러선정 및 개발환경 구축
 - 보급형 플랫폼 기대성능 설정
 - 부트와 응용프로그램 영역구분 및 부트영역 소프트웨어 안전인증
 - 응용프로그램 포팅을 통한 무결성 검증
- 자기검사회로 내장형 Fail-safe 플랫폼 개발
 - 자기검사회로 설계 및 시작품 제작
 - 보급형 플랫폼 FMECA 및 기능별 SIL할당
 - 자기검사회로 및 Fail-safe동작 성능시험 환경구축 및 시험실시
 - KRS 및 ETCS기준 환경시험 실시

	○ 공통플랫폼 고안전 입출력카드 및 확장모듈 개발 - 공통플랫폼 입출력의 종류, 사양, 채널(용량) 등 기술사양 선정 - 확장 인터페이스(BUS Type) 선정 및 기술문서화 - 입출력카드 및 확장모듈별 SIL4 안전설계 및 검증 - KRS 및 ETCS기준 환경시험 실시 ○ 보급형 공통플랫폼 운영 및 유지보수 시나리오 도출 - 보급형 공통플랫폼 기술메뉴얼 작성 - 보급형 공통플랫폼 인터페이스, 운영, 유지보수 매뉴얼 작성
5. 연구기획 추진방법	
	○ 공통플랫폼 실용화를 위해 다양한 분야(산·학·연)로 참여기관 구성하고 국내 철도신호기업의 공통플랫폼 활용 촉진에 위한 철도신호협회 및 철도신호연구조합 등 기존 협의체 참여 ○ 성능별 공통플랫폼의 연구결과는 실용화를 위해 하드웨어(PCB 도면 및 부품리스트), 소프트웨어(실행코드), 안전인증서를 협의체에 참여한 기업을 대상으로 공개 ○ 참여기관은 공통플랫폼의 소프트웨어(소스코드)와 안전인증 취득을 위한 평가문서에 대한 소유권을 가짐 ○ 참여기관은 세부과제 별로 안전인증취득 또는 컨설팅, 신호설비 개발 및 제조실적이 있는 기관으로 구성
6. 연구개발기간 및 소요예산	
	○ 연구기간 : 협약일로부터 36개월 ○ 연구예산 : 6,000백만원(정부지원) 이내
7. 기타	

제 2 절 평가기준 설정

- 본 연구개발사업을 통해 개발될 공통플랫폼의 성능 및 요구사항대비 평가기준을 다음과 같이 설정하였다.

순번	요구사항	평가지표	평가방법
1	신호설비 공통플랫폼 적용대상 선정 및 예비위험원분석과 정량적 RAMS 목표 설정	장치별 MTBF, MTTR, Ass, SIL할당 여부	대상장치 선별유무 IEC 62278기준 MTBF, MTTR, Ass할당여부 장치의 기능별 SIL할당여부
2	공통플랫폼 인증활동	IEC 62278기준 산출물 작성 - RAMS Plan - SHA - SSHA - IHA - O&SHA - SQAP - V&V - Safety Case	관련 국제표준의 요구사항대비 산출물 점검표 - IEC 62278 - IEC 62279(SW) - IEC 62425(SIL)
3	안전인증활동 가이드 작성	일반응용(GA) 안전인증 취득을 위한 절차개발 상세응용(SA) 안전인증 취득을 위한 절차개발	IEC 62278의 GA관련 요구사항대비 성과품 점검표 SA인증취득을 위한 가이드라인 작성유무
4	고성능(32bit급) 공통플랫폼 개발	실시간 운영체제 포팅 다중계구조 설계 디바이스 드라이버개발 입출력카드 성능검증 환경시험 실시	실시간 운영체제 환경확인 결함허용 시험을 통한 다중계구조 및 디바이스 드라이버 확인 입출력카드 성능시험 성적서 확인 환경시험 성적서 확인
5	보급형(16bit급) 공통플랫폼 개발	운영체제 개발 자기검사회로 설계 입출력카드 성능검증 환경시험 실시	운영체제 환경확인 결함허용 시험을 통한 자기검사기능 확인 입출력카드 성능시험 성적서 확인 환경시험 성적서 확인

주 의

1. 이 보고서는 국토교통부에서 시행한 국토교통연구기획사업의 연구보고서입니다.
2. 이 보고서 내용을 발표하는 때에는 반드시 국토교통부에서 시행한 사업의 연구 결과임을 밝혀야 합니다.
3. 국가과학기술 기밀유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 아니됩니다.