미래철도기술개발사업 중간보고서

R&D/05철도안전C03

열차제어시스템 안전성능 평가 및 사고방지기술 개발 연구보고서

2010. 06.

핵심주관기관 / 한국철도기술연구원

세부연구기관 / 대아티아이(주)

LS산전(주)

(주)에이알텍

RP05086

국 토 해 양 부

한국건설교통기술평가원

Land Transpot and Maritime R&D Report

미래철도기술개발사업 중간보고서

R&D / 05철도안전003

열차제어시스템 안전성능 평가 및 사고방지기술 개발 연구보고서

2010. 06.

핵심주관기관 / 한국철도기술연구원
세부연구기관 / 대아티아이(주)
LS산전(주)
(주)에이알텍

국 토 해 양 부
한국건설교통기술평가원

Land Transport and Maritime R&D Report

제 출 문

국토해양부장관(한국건설교통기술평가원장) 귀하

본 보고서를 "열차제어시스템 안전성능 평가 및 사고방지기술 개발"의 중간보고서로 제출합니다.

2010 . 06. 30.

핵심주관기관 : 한국철도기술연구원
원 장 최 성 규
세부연구기관 : 대아티아이(주)
대표이사 최 진 우
세부연구기관 : LS산전(주)
대표이사 김 정 만
세부연구기관 : (주)에이알텍
대표이사 이 상 남

■ 핵 심 연 구 책 임 자 / 책임연구원 황 종 규 총 괄

■ 핵심연구기관 참여연구원 / 책임연구원 김 용 규 평가기술
/ 책임연구원 이 재 호 사상사고
/ 책임연구원 정 락 교 사상사고
/ 선임연구원 윤 용 기 정형기법
/ 선임연구원 김 백 현 S/W기술
/ 선임연구원 신 승 권 사고방지
/ 선임연구원 신 경 호 사고방지
/ 주임연구원 조 현 정 평가기술

■ 세 부 연 구 책 임 자 / (LS산전㈜)
책임연구원 조 용 기 고안전성 연산처리장치 개발
/ (대이타이아㈜)
상무 안 진 안전성 활동 적용성 기술
/ (㈜에이알텍)
부사장 김 유 호 사상사고 저감 안전설비 개발

요 약 문

I. 제목

◦ 열차제어시스템 안전성능 평가 및 사고방지기술 개발

II. 연구개발의 목적 및 필요성

1. 연구개발의 목적

◦ 열차제어시스템의 안전성 평가기술 및 사고방지를 위한 안전성 향상기술 개발

2. 주요 연구개발 내용

◦ 열차제어시스템의 안전성 평가기술 개발

◦ 열차제어시스템 안전성 향상 기술 개발

◦ 열차제어 측면의 사상사고 저감 기술 개발

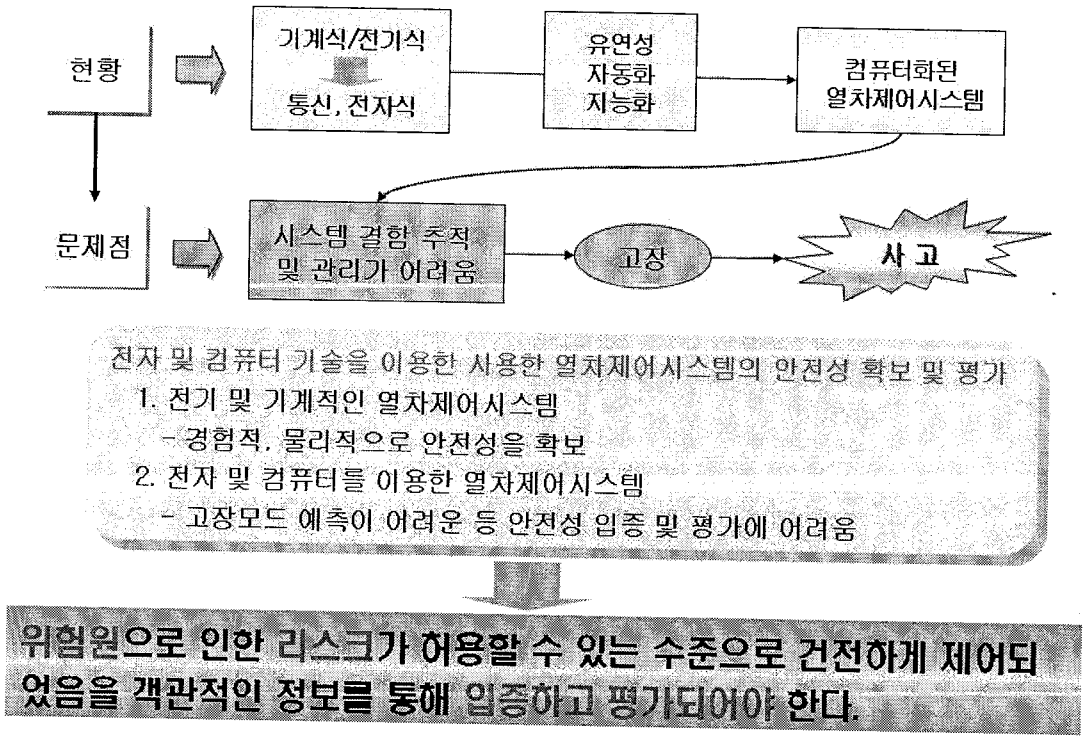
3. 연구개발의 필요성

가. 기술적 측면

◦ 컴퓨터 및 통신 기술의 발달로 인해 컴퓨터를 이용한 열차제어장치 사용의 증가에 따라 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 열차제어시스템의 특성상 시스템에 엄격한 안전성 관리 및 제어가 필요함.

◦ 기존의 전기 및 기계적인 방식에 의한 열차제어시스템은 경험적으로 나 물리적인 기술에 의해 안전성 확보 및 입증이 가능하였지만, 컴퓨터화된 열차제어시스템은 고장모드 예측이 어려운 등 제어시스템의 안전성 입증과 평가에 어려움이 있음.

◦ 열차제어시스템에 의한 사고억제 및 방지를 위한 결함허용 시스템 기술과 같은 시스템측면과 정형기법에 의한 바이탈 소프트웨어 설계기술과 같은 소프트웨어 측면에서의 안전성 향상을 위한 기술의 개발을 필요로 함.



나. 경제 · 산업적 측면

◦ 열차제어시스템을 위한 안전성관련 규격들이 IEC 61508/62278/62279/62425 등으로 국제 규격화됨으로 인해 안전성 활동과 이를 바탕으로 한 평가 및 인증이 요구되고 있으며, 국내 열차제어시스템으로 이러한 국제규격에 의해 안전성 활동 및 평가가 이루어지도록 요구되고 있음.

◦ 이러한 안전성 관련 국제규격들로 인해 안전성 활동 및 평가를 수행하지 않은 국내 열차제어시스템의 국내 운용과 해외진출에 어려움이 있음.

◦ 따라서 열차제어시스템의 안전성 확보를 위한 수명주기별 기술의 안전성 활동, 안전성 평가 기술, 하드웨어와 소프트웨어 측면에서의 안전성 향상 기술 개발이 필요함.

◦ 열차제어시스템의 결함에 따른 열차사고는 사회적으로 매우 큰 파장을 발생시키므로, 열차제어시스템의 안전성 활동을 통한 안전성 입증을 위한 세부수행 기술과 안전성 평가기술의 개발은 상당한 시급성이 요구됨.

Ⅲ. 연구개발의 내용 및 범위

구 분	연구개발 목표	연구개발내용 및 범위
2차년도 (2005)	열차제어시스템 안전성 평가 및 사고방지를 위한 기반기술 연구	- 철도안전SE과제와의 연계사항 관리 및 조정 · 과제총괄 및 SE과제와 연계 · 최신연구동향 조사 및 분석 - 열차제어시스템 안전성 평가기술 개발 · IEC 61508/62278/62279 조사분석 · 관련 국내외 선행 연구 조사분석 · 열차제어시스템 안전성 활동 체계 및 평가 관련 기술조사연구 · 바이탈 열차제어시스템 소프트웨어 안전성 평가 기술 조사연구 · 열차제어시스템 주요 위험원 조사분석 -열차제어시스템 사고억제 및 안전성 향상을 위한 기반기술 연구 · 열차제어시스템 운용현황 및 사고발생현황 조사 분석 · 열차제어시스템 기능별 사고사례 조사 · 열차제어시스템에 적용된 사고방지기술 조사분석 · 안전성 향상을 위한 고안전성 연산처리 장치 기술 및 정형명세기술 조사연구
3차년도 (2006)	안전성 평가기술 연구 및 평가대상 시스템 선정	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(1) · 열차제어시스템을 위한 고안전성 연산처리 장치 개발방향 정립 및 기본설계 · 열차제어시스템 안전핵심 소프트웨어 개발 절차 및 방법 연구 · 열차제어시스템을 위한 정형기법 검토 -열차제어시스템 안전성 평가기술 개발(1) · 안전성 활동 및 평가를 위한 세부수행기술 연구 · 열차제어시스템 안전성 평가기술관련 템플릿 작성 · 열차제어시스템 안전핵심 소프트웨어의 테스트 항목 및 방법 도출 · 열차제어시스템 안전성 평가기술 적용성 연구를

		위한 평가대상 시스템 검토 및 선정 · 평가대상 열차제어시스템 기본설계 · 열차제어시스템 바이탈 소프트웨어 안전성평가를 위한 테스트 도구 개발사양 작성 · 열차제어시스템 통신 안전성 평가방법 및 검증 요구사항 분석
4차년도 (2007)	평가대상시스템 제작 및 시험기 설계	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(2) · 열차제어시스템에 적용을 위한 정형화 요구명세 방법 제시 · 열차제어시스템을 위한 고안전성 연산처리 장치 상세설계 및 일부 모듈 시제품 제작 -열차제어시스템 안전성 평가기술 개발(2) · 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 상세설계 및 일부모듈 제작 · 평가대상 시스템 시험을 위한 시뮬레이터 설계 · 열차제어시스템 S/W 테스팅 도구 설계 및 시제품 제작(1) -열차제어측면의 사상사고 저감기술 개발(1) · 국내외 적용기술 조사분석 · 사상사고 저감을 위한 열차제어 측면의 기술 조사분석
5차년도 (2008)	평가대상시스템 제작 및 시험기 제작	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(3) · 열차제어시스템에 적용을 위한 정형검증기술 연구 · 열차제어시스템을 위한 고안전성 연산처리 장치 시제품 제작 · 열차제어장치에 의한 열차분리 검지기술 분석 및 요구사항 제시 -열차제어시스템 안전성 평가기술 개발(3) · 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 제작 · 열차제어시스템 S/W 테스팅 도구 시제품 제작

		(2) · mock-up 시스템 시험을 위한 시뮬레이터 제작(1) · 열차제어시스템 안전성 평가 가이드라인 작성 - 열차제어 측면의 사상사고 저감기술 개발(2) · 사상사고 저감을 위한 기술 설계
6차년도 (2009, 당해년도)	열차제어시스템 안전성 평가 및 향상기술의 보완	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(4) · 열차제어시스템을 위한 정형기법 적용방안 제시 · 열차제어시스템을 위한 고안전성 연산처리장치 시제품 보완제작 및 성능시험 · 선로전환결함 방지기술 조사분석 -열차제어시스템 안전성 평가기술 개발(4) · 열차제어시스템 안전성 평가가이드라인(안) 보완 · 열차제어시스템 S/W 테스팅 자동화도구 시제품 제작(3) · 평가대상시스템 제작보완 및 시험을 위한 시뮬레이터 제작(2) · 평가대상시스템 Safety Case 작성(1) - 열차제어 측면의 사상사고 저감기술 개발(2) · 열차제어측면의 사상사고 저감을 위한 안전설비 상세설계 및 제작 .
7차년도 (2010)	개발기술의 확립 및 실용화	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(5) · 선로전환결함 요구사항 제시 -열차제어시스템 안전성 평가기술 개발(5) · 열차제어시스템 안전성 평가가이드라인 최종안 제시 · 열차제어시스템 S/W 테스팅 자동화도구 시제품 통합제작 및 성능 확인(4) · 평가대상시스템 안전성 평가 및 분석 · 평가대상시스템 시험을 위한 시뮬레이터 보완 및 적용시험 - 열차제어 측면의 사상사고 저감기술 개발(3)

		· 열차제어측면의 사상사고 저감을 위한 안전설비 보완 제작 및 성능시험

Ⅳ. 당해연도 주요 연구개발 결과

6차년도인 당해 연도에는 열차제어시스템 안전성 평가기술 연구, 안전성 평가기술 적용성 연구를 위한 평가대상 열차제어시스템 제작 보완 및 소프트웨어 테스팅 자동화 도구 제작, 플랫폼 사상사고 저감 안전설비 시제품 제작, 작업자 사상사고 저감 안전설비 시제품 보완제작을 목표로 하였으며, 이에 따른 당해 연도 주요 연구내용은 다음과 같다.

연구내용	연구결과
◦ **열차제어시스템 안전성 향상 핵심기술 개발 (4)** - 열차제어시스템을 위한 고안전성 연산처리 장치 시제품 보완제작	◦ **열차제어시스템 안전성 향상 핵심기술 개발 (4)** **① 열차제어용 고안전성 연산처리장치 시제품 보완제작** -고안전성 연산처리 장치 시제품 보완제작 통합시험 수행 -시제품 인터페이스를 위한 바이탈 I/O 보드 제작 -열차제어용 고안전성 연산처리장치 평가메트릭 제시 -시제품 Safety Case 작성 -열차제어용 고안전성 연산처리장치 설치 및 운용을 위한 기술지침(안) 작성
- 열차제어시스템을 위한 정형기법 적용방안 제시	**② 열차제어시스템을 위한 정형기법 적용방안 제시** -열차제어시스템을 위한 정형명세 작성 및 검증 절차 제시

- 선로전환 결함 방지기술 분석 및 요구사항 제시	-Zed와 Statechart를 이용한 정형명세 작성 및 검증 절차 적용 예 제시 **③ 선로전환 결함방지기술 조사분석** -선로전환 결함관련 장애사례 조사분석 -선로전환 결함 방지관련 각종 설비 및 요구사항 분석
◦ **열차제어시스템 안전성 평가기술 개발(4)** - 안전성 평가활동 및 평가 적용성 기술 개발	◦ **열차제어시스템 안전성 평가기술 개발(4)** **① 안전성 평가기술 적용성 연구를 위한 대상시스템 보완제작** - 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 시제품(CRD 시스템) 보완제작 및 시험 **② 평가대상 시스템 안전성 활동 수행** -대상 시스템 안전성 활동 수행(Consequence Analysis, Causal Analysis, SIL 결정 및 할당) -대상시스템 Safety Case 작성(1) -열차제어시스템 안전성 활동 기술지침 초안 작성
- 평가대상 시스템 시험을 위한 시뮬레이터 제작(2)	**③ 평가대상 시스템 시험을 위한 시뮬레이터 제작** -대상 시스템 시뮬레이터 보완제작(ATS 시뮬레이터, 차상 시뮬레이터, 신호시뮬레이터) -대상 시스템 안전측 동작 검증 시뮬레이터 제작 -평가대상 시스템과 인터페이스 시험 수행
- 열차제어시스템 안전성 평가 가이드라인 수정안 작성	**④ 열차제어시스템 안전성 평가 가이드라인 보완작성** -열차제어시스템 안전성 활동 기술체계 보완작성 -열차제어시스템 안전성 평가 가이드라인 보완작성 -리스크 분석기법(HAZOP-KR) 정리 -열차제어시스템 안전성 평가를 위한 체크리

- 열차제어시스템 SW 테스팅 자동화도구 시제품 제작(3)	스트 작성 **⑤ 열차제어시스템 S/W 안전성 테스트 툴 설계 및 시제품 제작** -열차제어시스템 S/W 테스팅 자동화도구 설계 및 3차 시제품 제작(3개 하부모듈) -개발도구를 통한 평가대상시스템 소프트웨어의 테스팅 수행 -열차제어시스템 SW 테스팅 기술지침 초안 작성
◦열차제어측면의 사상사고 저감기술 개발(2) - 플랫폼 공중사상사고 저감 안전설비 상세설계 및 시제품 제작	**◦열차제어측면의 사상사고 저감기술 기본설계** **① 플랫폼 공중사상사고 저감 안전설비 상세설계 및 시제품 제작** -플랫폼 공중사상사고 저감을 위한 3D 레이저레이더를 이용한 안전설비 상세설계 -시제품 제작 및 시험
- 선로변 작업자 사상사고 저감 안전설비 시제품 보완제작 및 시험	**② 선로변 작성자 사상사고 저감 안전설비 시제품 제작 및 현장시험** -무선을 이용한 작업자 사상사고 저감 안전설비 시제품 보완 제작 및 현장시험 -작업자 사상사고 저감 안전설비 시제품 철도운영기관 대상 시연회 개최 및 시범설치 운용 중(서울메트로 군자/창동/수서 차량기기)

V. 연구개발결과의 활용계획

1. 기대효과

◦기술적 측면

- 열차제어시스템 안전성 평가기술의 개발로 열차제어시스템의 안전성 확보 및 평가가 가능
- 안전성 향상을 위한 고안전성 연산처리 장치 기술 및 정형기법에 의한 바이탈한 열차제어시스템의 소프트웨어 설계기술의 개발로 열차제어시스템의 안전성 향상이 기대됨
- 국내기술로 열차제어시스템 안전성 향상 및 평가기술의 개발로 철도선진국과 동등한 안전성 관리가 가능

◦ 경제·산업적 측면
- 열차제어시스템 안전성활동 체계에 실행기술과 이의 평가기술 확보를 통한 안전성 관련 국제규격에 따른 시스템의 개발 및 운용이 가능하며, 또한 국내 열차제어시스템의 수입대체효과 기대
- 열차제어시스템의 안전성 평가기술의 국산화를 통해 국내 시스템이 기술 및 가격 경쟁력을 갖추게 되면 독자적인 세계시장 진출이 가능
- 열차제어시스템을 위한 안전성 활동 및 평가관련 전문인력 확보가능

2. 활용방안

◦ 본 연구를 통해 확보할 열차제어시스템 안전성 활동 수행기술과 평가기술은 국내 운용기관, 제작사 등에 활용이 가능함

◦ 사고억제 및 안전성 향상을 위한 고안전성 연산처리 시스템 기술 및 정형기법에 의한 열차제어시스템 소프트웨어 설계 기술은 국내 열차제어시스템의 신뢰성 및 안전성 향상에 기여할 것으로 예상됨

◦ 열차제어시스템 안전성 평가기술과 평가대상 시스템의 평가를 위해 개발하는 시험기는 국내의 열차제어시스템의 평가 및 인증을 위한 기반 인프라 설비 및 체계로 활용되어, 국내에서 개발되는 열차제어시스템의 안전성 향상에 기여할 것으로 기대됨

SUMMARY

(영문요약문)

Ⅰ. Title

◦ Safety Assessment of Railway Signalling System & Development of Technologies for Accident Prevention

Ⅱ. Objective & Needs of Research and Development

1. Objective of Research and Development

◦ To describe safety assessment of railway signalling system, and to develop safety improvement technologies for accident prevention

2. Main Subjects of Research and Development

◦ To develop safety assessment technologies of railway signalling system

◦ To develop safety improvement technologies of railway signalling system

◦ To develop mock-up of trailway signalling system, and safety assessment simulator to research applicability of the assessment technologies

3. Needs of Research and Development

a. Technical Aspect

◦ Rigorous safety management and control is required because of the unique feature of railway signalling system, which have huge potential failures of equipments, are directly link to extensive damages of human lives, or financial loses, following the increasing uses of railway signalling equipments utilizing computers as the advances in computers and communication technologies

◦ Although existing railway signalling systems, operated by electrical and mechanical methods, could secure and demonstrate safety on the basis of experiences and physical technologies, computer-based signalling systems have difficulties in demonstrating and assessing train control systems, for instance those in predicting failure modes.

◦ It is required to develop technologies for safety improvement in terms of software aspect (e.g. vital software design technologies by formal methods) and system aspect(e.g. failure acceptance systems for accident control and prevention by train control systems)

b. Economical · Industrial Aspect

◦ As safety-related regulations for signalling systems are standardized to IEC 61508/62278/62279/62425, and others at the international level, safety activity and its assessment and certification followed is required to be performed. The activity and assessment of domestic signalling systems need to be done by those international standards.

◦ Those safety-related international standards limit domestic/internal operation and international export of domestic signalling systems which safety activities and assessments are not performed.

◦ Therefore, there is need to develop technologies for safety improvement to secure safety of signalling systems in terms of technologies for safety activities on each life-cycle, technologies for safety assessment, H/W and S/W aspects.

◦ Accidents from signalling system faults causes a great impact on society. There is an urgent need to develop technologies of specific performances and those for safety assessment to certify safety through safety activities of signalling systems.

Ⅲ. Subjects and Scope of Research & Development

Divisions	Objectives of Research & Development	Subjects and Scope of Research & Development
2nd year (2005)	Research on Infra-technologies for safety assessment of TCS and accident prevention	- Management and Coordination of subjects connecting to railway safety SE project · Generalization of the project and Connection with the SE project · Examination and Analysis in current trends of relevant studies - Development of safety assessment technologies of signalling systems · Examination and Analysis in IEC 61508/62278/62279 · Research and Analysis of relevant studies internally and externally preceded · Research and Study of safety activity systems and assessment of TCS - Study of Infra-technologies for TCS accident prevention and safety improvement · Research and Analysis in current operational situation of signalling systems and accident occurrences · Research of accidents cases for each signalling function · Research and Analysis in hazards of signalling · Research and Analysis in accident prevention technologies applied to signalling · Research and Analysis in fault-tolerant system technologies and formal specification technologies for safety improvement
3rd year (2006)	The general planning of mock-up system for establishing	- Management and Coordination of subjects connecting to railway safety SE project - Development key technologies for safety improvement of signalling systems

	the safety-assessment technologies	· Identification and preliminary design for fault-tolerant system development of signalling systems · Study of development procedures and methods of signalling systems safety-critical S/W · Examination of development and applicability of signalling systems vital S/W by means of formal methods - Development of safety assessment technologies of signalling systems(1) · Study of specific performance technologies for safety activity and assessment · Establishment of templates relevant to assessment technologies of signalling systems · Derivation of item to be tested and methods of signalling systems safety-critical S/W · Examination and Adoption of mock-up systems to study applicability of signalling systems safety assessment technologies · Preliminary design of mock-up signalling systems · Drawing development specifications of test tools for safety assessment of signalling systems vital S/W · Analysis in safety assessment methods and verification requirements of signalling systems communication safety
4th year (2007)	Design of the mock-up for study on the applicability of safety assessment technologies	- Managing and Coordinating the matters relevant to railway safety SE project - Developing key technology for improving TCS safety(2) · Suggestion of TCS safety critical S/W formal requirement specification method · Detailed design of FT system for TCS and making a module sample

		- Developing TCS safety assessment methodology(2) · Designing mock-up system and making module sample for the studies on applicability of safety assessment methodology · Designing a simulator for moçk-up system test · Designing TCS S/W safety assessment tester and making a sample - Developing accident reduction technology with aspect of train control(1) · Performing inspection and analysis on national/international application technologies · Performing inspection and analysis on accident reduction technology with aspect of train control
5th year (2008)	Manufacturing of the mock-up for study on the applicability of safety assessment technologies	- Managing and Coordinating the matters relevant to railway safety SE project - Developing key technology for improving TCS safety(3) · Researching formal verification technology for TCS safety critical S/W · Making a sample FT system for TCS · Performing an analysis on train separation detecting technology via TCS and suggesting related requirements - Developing TCS safety assessment methodology(3) · Making mock-up system for the studies on applicability of safety assessment methodology · Making TCS S/W safety assessment tester sample(2) · Making a simulator for mock-up system test(1) · Establishing a guideline for TCS safety assessment

		- Developing accident reduction technology with aspect of train control(2) · Designing accident reduction technology
6th year (2009, This Year)	Midification of developed technologies	- Managing and Coordinating the matters relevant to railway safety SE project - Developing key technology for improving TCS safety(4) · Suggesting application plan on formal method for TCS safety critical S/W · Performing a performance verification test for TCS FT system · Analyzing track switch error prevention technology and suggesting related requirements - Developing TCS safety assessment methodology(4) · Suggesting final TCS safety assessment guideline · Supplementing mock-up system made and performing safety assessment · Making a simulator for mock-up system test(2) - Developing accident reduction technology with aspect of train control(3) · Designing accident reduction technology
7th year (2010	Establishment of Development Technology and the Practicalization	- Managing and coordinating related details with the railway safety SE project - TCS Safety Improvement Core Technology Development(5) · Proposing requirements on faults in track switching - TCS Safety Assessment Technology Development(5) · Proposing the final plan on the TCS safety assessment guidelines · Integrated manufacturing and performance verification of the prototypes of TCS S/W testing automation tools(4) · Mock-up system safety assessment and

		analysis · Simulation complement and the application test for Mock-up system test - Casuality lowering technology development in terms of train control(3) · Manufacturing with the complement of safety facilities and performance test for lowering casuality in terms of train control

Ⅳ. Results of Main Research & Development of This Year

Subjects	Results
▫ TCS Safety Improvement Core Technology Development(4) -Complementary production of FT system prototypes for TCS	▫ TCS Safety Improvement Core Technology Development(4) ① Complementary production of FT system prototypes for TCS -Carrying out the integrated test for the complementary manufacturing of FT system prototypes -Manufacturing a vital I/O board for the interface of prototpyes -Proposal of the assessment metrics of FT systems for TCS -Preparing for Safety Case of prototypes -Installation of FT systems for TCS and preparation for technology guidelines for the operation
-Suggesting the application to formal methods for TCS	② Suggesting the application to formal methods for TCS -Preparing for formal specification and suggesting the verification procedure

	-with the use of Zed and Statechard, preparing for formal specifications and suggesting examples on the application to verification procedure
-Technology analysis on the prevention of switching faults and requirement suggestion	③ Inspection & Analysis on prevention of track switching faults -Inspection & Analysis on the exmaples on track switching faults -Analysis on various facilities and requirements related to the prevention of track switching faults
▫ Developing TCS safety assessment methodology (4) -Safety assessment activities and assessment applicability technology development	▫ Developing TCS safety assessment methodology (4) ① Detailed design and manufacture of mock-up system for the study on applicability of safety assessment methodology -Complementary manufacturing and test of the mock-up system prototypes(CRD system) for the study on applicability of safety assessment methodology ② Performing safety activities for mock-up system -Performing safety activities for mock-up system(Consequence Analysis, Causal Analysis, SIL decision and allocation) -Preparing for Safety Case of mock-up systems(1) -Preparing for a draft of TCS safety assessment guideline

-Development a simulator for mock-up system test(2) -Preparing for the correction of TCS safety assessment guidelines	③ Design a simulator for mock-up system test(2) -Complementary manufacting of mock-up system simulator(ATS simulator, Onboard simulator, Signal simulator) -Manufacturing the simulator for the verification of the fail-safe in mock-up systems -Performing interface tests with mock-up system ④ Complementary preparation for TCS safety assessment guideline -Complementary preparation for the technology systems on TCS safety activities
· Developing accident reduction technology with aspect of TCS (2) -Design and Development on accident reduction technology with aspect of TCS	· Inspection and analysis on accident reduction technology with aspect of TCS -Prototype development on accident reduction technology for applying platform -Complementary manufacturing and test of trackside safety equipment and the tested on applicability at real trackside.

The objective of 2009, the 6th year of project, is to develop the Mock-up TCS for the studies on TCS safety assessment methodology and its applicability, to develop and test the two safety facilities.Main contents of

studies performed for the objectives are as follow.

V. Research & Development Results and Application Plan

1. Expected Effects

◦ Technical Aspect

- Enable to ensure and assess safety of train control systems, by development of signalling systems safety assessment technologies
- Enable to expect safety improvement of signalling systems by developing design technologies for vital signalling systems S/W by means of Fault-tolerant system technologies and formal methods to improve safety
- Enable to manage safety, equivalent to advanced railway countries, by means of developing assessment technologies and improving signalling systems safety by domestic our own technologies

◦ Economical · Industrial Aspect

- Enable to develop and operate systems according to safety-related international standards, by securing assessment and implementation technologies into the system of signalling systems safety activities, and to achieve an alternative effect of import from domestic signalling systems
- Enable to make an independent inroads into international market in the case of producing competitive domestic systems in terms of technical and price aspects through localization of signalling systems safety assessment
- Enable to secure professional experts related to safety activities and assessment for signalling systems

2. Application Plan

◦ As for implementation and assessment technologies of signalling systems

safety activities secured by this research: Enable to apply it to domestic operation organizations and manufacturers

- As for design technologies of signalling systems S/W by Fault-tolerant system technologies and formal methods for accident prevention and safety improvement: It is expected to contribute to reliability and safety improvement of domestic signalling systems
- As for the testers being developed to assess Mock-up signalling systems, and assessment technologies of signalling systems safety: enable to be applied as infrastructure facilities and system to assess and certify domestic signalling systems, and expected to contribute to safety improvement of signalling systems developed domestically

목 차

제 출 문 ····· i

요 약 문 ····· ii

SUMMARY ····· xi

CONTENTS ····· xlv

제 1 장 연구개발과제의 개요 ····· 1

제1절 연구개발의 필요성 ····· 1

1. 기술적 측면 ····· 1

2. 경제·산업적 측면 ····· 2

제2절 연구개발의 목표 및 범위 ····· 3

1. 연구개발의 최종목표 ····· 3

2. 연도별 연구개발 목표 및 내용 ····· 3

제3절 기술개발 추진체계 ····· 7

1. 추진전략 및 방법 ····· 7

2. 당해 연도 업무역할 체계 ····· 9

3. 연구개발 추진체계 ····· 10

제 2 장 국내외 기술동향 ····· 11

제1절 국내기술 동향 ····· 11

제2절 국외기술 동향 ····· 12

제3절 기술동향 분석 결론 ····· 13

제 3 장 연구개발 수행내용 및 결과 ····· 15

제1절 열차제어시스템 안전성 평가기술 개발 ····· 15
1. 기능 아키텍처 ····· 17
2. 물리 아키텍처 ····· 17
3. 설계분석보고서 ····· 18
가. 요구사항과의 적합성 ····· 18
나. 설계기준 ····· 18
다. 검증 방법에 따른 증거 자료 ····· 18
라. 성과물의 내용 및 결과 ····· 19
(1) 열차제어시스템 안전성 활동 기술체계 ····· 19
(2) 위험원 분석 방법(HAZOP-KR) ····· 35
(3) 열차제어시스템 안전성 평가 가이드라인 ····· 47

제2절 열차제어시스템 S/W 안전성 평가기술 개발 ····· 79
1. 기능 아키텍처 ····· 81
2. 물리 아키텍처 ····· 81
3. 설계분석보고서 ····· 82
가. 요구사항과의 적합성 ····· 82
나. 설계기준 ····· 82
다. 검증 방법에 따른 증거 자료 ····· 82
라. 성과물의 내용 및 결과 ····· 83
(1) 국내외 SW 안전성 평가관련 개발현황 ····· 83
(2) 열차제어시스템 SW 안전성 평가 체크리스트 ····· 87

제3절 열차제어시스템 바이탈 소프트웨어 테스팅 자동화 도구의 개발 ····· 109
1. 기능 아키텍처 ····· 111
2. 물리 아키텍처 ····· 111
3. 설계분석보고서 ····· 112
가. 요구사항과의 적합성 ····· 112
나. 설계기준 ····· 112

다. 검증 방법에 따른 증거 자료 ····· 112
라. 성과물의 내용 및 결과 ····· 113
(1) 개요 ····· 113
(2) Boundary Value Analysis / Equivalence Classes Testing 모듈 ····· 115
(3) Fault Tree Analysis모듈 ····· 146
(4) 평가 대상시스템 소프트웨어에 적용 결과 ····· 199
(5) 열차제어시스템 소프트웨어 테스팅 기술지침(안) 구성 제안 ····· 209

제4절 안전성 평가기술 적용을 위한 안전성 평가용 대상 열차제어시스템 보완 제작 ····· 217
1. 기능 아키텍처 ····· 219
2. 물리 아키텍처 ····· 219
3. 설계분석보고서 ····· 220
가. 요구사항과의 적합성 ····· 220
나. 설계기준 ····· 220
다. 검증 방법에 따른 증거 자료 ····· 220
라. 성과물의 내용 및 결과 ····· 221
(1) 안전성 평가용 대상 열차제어시스템 ····· 221
(2) 안전성 평가용 대상 열차제어시스템 설계내용 보완 ····· 226
(3) 안전성 평가용 대상 열차제어시스템 보완제작 ····· 234
(4) 안전성 평가용 대상 열차제어시스템 시험 방법 및 결과 ····· 243

제5절 평가대상시스템을 통한 적용성 기술 개발 ····· 271
1. 기능 아키텍처 ····· 273
2. 물리 아키텍처 ····· 273
3. 설계분석보고서 ····· 274
가. 요구사항과의 적합성 ····· 274
나. 설계기준 ····· 274
다. 검증 방법에 따른 증거 자료 ····· 275
라. 성과물의 내용 및 결과 ····· 276
(1) 평가대상시스템 SIL 결정 ····· 276

(2) 평가대상시스템 SIL 할당 ····· 289
(3) Verification & Validation ····· 301
(4) 평가대상시스템 Safety Case ····· 307
(5) 열차제어시스템 안전성 활동 기술 지침서 ····· 308

제6절 평가대상 시스템 시뮬레이터 제작 및 시험 ····· 405
1. 기능 아키텍처 ····· 407
2. 물리 아키텍처 ····· 407
3. 설계분석보고서 ····· 408
가. 요구사항과의 적합성 ····· 408
나. 설계기준 ····· 408
다. 검증 방법에 따른 증거 자료 ····· 408
라. 성과물의 내용 및 결과 ····· 408
(1) 개요 ····· 408
(2) 제작 ····· 409
(3) 인터페이스 ····· 450
(4) 인터페이스 시험 ····· 458

제7절 고안전성 연산제어 시스템 개발 ····· 463
1. 기능 아키텍처 ····· 465
2. 물리 아키텍처 ····· 465
3. 설계분석보고서 ····· 466
가. 요구사항과의 적합성 ····· 466
나. 설계기준 ····· 466
다. 검증 방법에 따른 증거 자료 ····· 468
라. 성과물의 내용 및 결과 ····· 468
(1) 고안전성 연산제어 시스템의 보완 제작 ····· 468
(2) 고안전성 연산제어 시스템 평가 Metric ····· 482
(3) 보안된 고안전성 연산제어 시스템의 안전성 활동 ····· 503
(4) 고안전성 연산제어 시스템의 특징 및 장점 ····· 520

제8절 열차제어시스템을 위한 정형기법 적용기술 개발 ····· 527
1. 기능 아키텍처 ····· 529
2. 물리 아키텍처 ····· 529
3. 설계분석보고서 ····· 530
가. 요구사항과의 적합성 ····· 530
나. 설계기준 ····· 530
다. 검증 방법에 따른 증거 자료 ····· 531
라. 성과물의 내용 및 결과 ····· 531
(1) 열차제어시스템의 정형명세 작성 절차 연구 ····· 531
(2) 열차제어시스템의 정형 검증 절차 연구 ····· 534
(3) 예제 시스템 정형명세와 정형 검증 절차서 적용 예 제시 ····· 535

제9절 선로전환 결함방지 기술 분석 및 요구사항 제시 ····· 577
1. 설계분석보고서 ····· 579
가. 요구사항과의 적합성 ····· 579
나. 성과물의 내용 및 결과 ····· 579
(1) 선로전환 결함 사고사례 ····· 579
(2) 선로전환 결함 방지를 위한 설비 조사분석 ····· 585
(3) 선로전환기 요구사항 ····· 607

제10절 열차제어측면의 사상사고 저감기술개발 ····· 625
1. 기능 아키텍처 ····· 627
2. 물리 아키텍처 ····· 627
3. 설계분석보고서 ····· 628
가. 요구사항과의 적합성 ····· 628
나. 설계기준 ····· 628
다. 검증방법에 따른 증거 자료 ····· 629
라. 성과물의 내용 및 결과 ····· 629
(1) 국내·외 철도안전설비 기술현황 조사 ····· 630

(2) 선행기술조사 및 차별화 방안 ····· 635
(3) 플랫폼 공중사상사고 저감 안전설비 상세 설계 ····· 648
(4) 3D 레이저레이더를 이용한 안전설비 시제품 제작 ····· 683
(5) 선로변 작업자를 위한 안전설비 시제품 보완제작 ····· 691

제 4 장 연구개발 목표달성도 및 관련분야 기여도 ····· 707

1. 목표 달성도 ····· 707
가. 당해 연도 목표 및 평가의 착안점 ····· 707
2. 연구개발의 활용계획 ····· 714
가. 기대효과 ····· 714
나. 활용방안 ····· 715
다. 실용화 방안 ····· 715

제 5 장 참고문헌 ····· 717

표 차 례

표 3.1.1 시스템 수명주기에 따른 주요 안전성 활동 ····· 20
표 3.1.2 IEC 62425에서의 위험원 분석 방법 ····· 25
표 3.1.3 위험원 분석 방법 및 타입에 따른 관계 ····· 26
표 3.1.4 단계별 위험원 분석 방법의 적용 ····· 29
표 3.1.5 PHL 결과 예 ····· 30
표 3.1.6 PHA 결과 예 ····· 31
표 3.1.7 HAZOP-KR 결과 예 ····· 31
표 3.1.8 EIM 모듈의 SSHA 결과 예 ····· 32
표 3.1.9 HAZOP-KR 파라메터 ····· 41
표 3.1.10 기존 HAZOP Study의 Guide word ····· 42
표 3.1.11 HAZOP-KR의 Guide word ····· 42
표 3.1.12 HAZOP-KR의 Deviation ····· 43
표 3.1.13 HAZARD-1의 HAZOP-KR 분석 결과 ····· 44
표 3.1.14 HAZARD-2의 HAZOP-KR 분석 결과 ····· 45
표 3.1.15 HAZARD-3의 HAZOP-KR 분석 결과 ····· 46
표 3.2.1 SW 안전성 평가기술 국내외 동향 ····· 84
표 3.3.1 목표시스템의 하부모듈 구성 ····· 113
표 3.3.2 Boundary Value Analysis/Equivalence Classes Testing 모듈 기능 리스트 ····· 117
표 3.3.3 기능별 세부 모듈 ····· 130
표 3.3.4 Equivalence Classes/Boundary Value Analysis Testing 모듈 기능 리스트 ····· 132
표 3.3.5 Equivalence Classes Analyzer의 자료구조 ····· 134
표 3.3.6 Boudary Value Analyzer의 자료구조 ····· 136
표 3.3.7 Testcase Generator의 자료구조 ····· 137
표 3.3.8 Execution Engine의 자료구조 ····· 138
표 3.3.9 Test Report Generator의 자료구조 ····· 139

표 3.3.10 Fault Tree Analyzer 주요 기능 리스트 ····· 149
표 3.3.11 FaultTreeElement Class 설계 사항 ····· 157
표 3.3.12 FaultTreeEvent Class 설계 사항 ····· 157
표 3.3.13 FaultTreeGate Class 설계 사항 ····· 158
표 3.3.14 FaultTreeTransfer Class 설계 사항 ····· 158
표 3.3.15 FaultTreeConnection Class 설계 사항 ····· 159
표 3.3.16 FaultTreeModel Class 설계 사항 ····· 160
표 3.3.17 PageElement Class 설계 사항 ····· 160
표 3.3.18 PageElementEditorInput Class 설계 사항 ····· 161
표 3.3.19 CCPActionGroup Class 설계 사항 ····· 162
표 3.3.20 SelectionDispatchAction Class 설계 사항 ····· 162
표 3.3.21 DeleteAction Class 설계 사항 ····· 162
표 3.3.22 OpenAction Class 설계 사항 ····· 163
표 3.3.23 OpenEditorActionGroup Class 설계 사항 ····· 163
표 3.3.24 RenameAction Class 설계 사항 ····· 163
표 3.3.25 ReportGenerationAction Class 설계 사항 ····· 164
표 3.3.26 FaultTreePageContentProvider Class 설계 사항 ····· 165
표 3.3.27 RenamePageDialog Class 설계 사항 ····· 165
표 3.3.28 ReortGeneration Class 설계 사항 ····· 165
표 3.3.29 EditorContextMenuProvider Class 설계 사항 ····· 166
표 3.3.30 EditorPaletteFactory Class 설계 사항 ····· 166
표 3.3.31 EditorUtility Class 설계 사항 ····· 167
표 3.3.32 FaultTreeUIEditor Class 설계 사항 ····· 167
표 3.3.33 FaultTreeUIPlugin Class 설계 사항 ····· 167
표 3.3.34 FTCalcProbsAction Class 설계 사항 ····· 168
표 3.3.35 FTLayoutAction Class 설계 사항 ····· 168
표 3.3.36 GraphicalEditorActionBarcontributor Class 설계 사항 ····· 168
표 3.3.37 ModelElement class 설계 사항 ····· 169
표 3.3.38 Shape class 설계 사항 ····· 170
표 3.3.39 connection class 설계 사항 ····· 170

표 3.3.40 FaultTreeDiagram class 설계 사항 ····· 170
표 3.3.41 Position class 설계 사항 ····· 171
표 3.3.42 PropertyShape class 설계 사항 ····· 171
표 3.3.43 EventShape class 설계 사항 ····· 172
표 3.3.44 GateShape class 설계 사항 ····· 172
표 3.3.45 AndGateShape class 설계 사항 ····· 173
표 3.3.46 PrimaryEvent class 설계 사항 ····· 173
표 3.3.47 TransferInshape class 설계 사항 ····· 174
표 3.3.48 ShapeEditPart class 설계 사항 ····· 175
표 3.3.49 ShapeEditPartFactory class 설계 사항 ····· 175
표 3.3.50 DiagramEditPart class 설계 사항 ····· 175
표 3.3.51 ShapeComponentEditPolicy class 설계 사항 ····· 176
표 3.3.52 ShapeConnectionEditPart class 설계 사항 ····· 176
표 3.3.53 ShapeConnectionEditPolicy class 설계 사항 ····· 176
표 3.3.54 ShapeCreateCommand class 설계 사항 ····· 177
표 3.3.55 ShapeDeleteCommand class 설계 사항 ····· 178
표 3.3.56 ShapeSetConstraintCommand class 설계 사항 ····· 178
표 3.3.57 ConnectionCreateCommand class 설계 사항 ····· 178
표 3.3.58 ConnectionDeleteCommand class 설계 사항 ····· 179
표 3.3.59 ConnectionReconnectCommand class 설계 사항 ····· 179
표 3.3.60 FaultTreeFigure class 설계 사항 ····· 180
표 3.3.61 FaultTreeAndGateFigure class 설계 사항 ····· 181
표 3.3.62 FTAPerspective class 설계 사항 ····· 182
표 3.3.63 DiagramProbabilityContectProvider class 설계 사항 ····· 183
표 3.3.64 DiagramProbabilityLabelProvider class 설계 사항 ····· 183
표 3.3.65 ProbabilityPage class 설계 사항 ····· 183
표 3.3.66 Attribute class 설계 사항 ····· 184
표 3.3.67 Attributes class 설계 사항 ····· 185
표 3.3.68 HtmlUtil class 설계 사항 ····· 185
표 3.3.69 Tag class 설계 사항 ····· 185

표 3.3.70 Project Element ····· 186
표 3.3.71 Page Element ····· 186
표 3.3.72 Gate Element ····· 187
표 3.3.73 Event Element ····· 187
표 3.3.74 Transfer Element ····· 187
표 3.3.75 Connection Element ····· 188
표 3.3.76 Fault Tree Diagram 구성 예 ····· 188
표 3.3.77 FTStructure Code ····· 189
표 3.3.78 오류 분석 보고서 ····· 190
표 3.3.79 개발 환경 및 테스트 환경 정보 ····· 200
표 3.3.80 제어기 시뮬레이터(Mock-up)의 기본 정보 ····· 201
표 3.3.81 주요 검출 규칙 및 심각도 ····· 202
표 3.4.1 CRD 주요 기능 ····· 223
표 3.4.2 시스템 요구 사양서 구조 ····· 227
표 3.4.3 광케이블 절손상태에서 광통신 계통 ····· 238
표 3.4.4 무정전전원장치 사양 ····· 239
표 3.4.5 장치별 기능시험 분류 내용 ····· 243
표 3.4.6 인터페이스 시험 분류 내용 ····· 244
표 3.4.7 ICM시험 기준 ····· 245
표 3.4.8 DCM시험 기준 ····· 246
표 3.4.9 ATS시뮬레이터 표시기능 시험 기준 ····· 247
표 3.4.10 ATS시뮬레이터 제어기능 시험 기준 ····· 247
표 3.4.11 차상시뮬레이터(ATP) 시험 기준 ····· 248
표 3.4.12 차상시뮬레이터(ATO) 시험 기준 ····· 248
표 3.4.13 장치별 통신개시 시험 기준 ····· 248
표 3.4.14 장치별 통신개시 시험 기준 ····· 251
표 3.5.1 CRD시스템 사고 분류 ····· 277
표 3.5.2 CRD 시스템 위험원 도출 ····· 277
표 3.5.3 BP-risk 장점 ····· 283
표 3.5.4 BP-risk S 결정 파라메터 ····· 285

표 3.5.5 BP-risk D 결정 파라메터 ····· 285
표 3.5.6 BP-risk U 파라메터 ····· 285
표 3.5.7 BP-risk 파라메터 정의 ····· 286
표 3.5.8 BP-risk THR에 따른 SIL ····· 286
표 3.5.9 연구대상 열차제어시스템 SIL결정 ····· 286
표 3.5.10 Functional Safety Requirements ····· 287
표 3.5.11 Technical Safety Requirements ····· 289
표 3.5.12 연구대상 열차제어시스템 SSHA 결과 ····· 295
표 3.5.13 연구대상 열차제어시스템 하드웨어 구성 및 데이터 ····· 296
표 3.5.14 Subsystem별 FTA결과 ····· 296
표 3.5.15 Subsystem별 가용도 ····· 297
표 3.5.16 연구대상 열차제어시스템 PHA 결과 ····· 297
표 3.5.17 연구대상 열차제어시스템 SSHA결과 ····· 297
표 3.5.18 연구대상 열차제어시스템 FTA결과 ····· 298
표 3.5.19 연구대상 열차제어시스템 Subsystem별 SIL ····· 298
표 3.5.20 위험원별 Subsystem 가용도 ····· 298
표 3.5.21 연구대상 열차제어시스템 기법 및 수단 요구사항 ····· 299
표 3.5.22 연구내용 및 연구결과 ····· 300
표 3.5.23 Verification 업무 ····· 305
표 3.5.24 Validation 업무 ····· 307
표 3.6.1 역 구분 표시 ····· 410
표 3.6.2 열차 기본 표시 ····· 411
표 3.6.3 열차 Label 표시 ····· 411
표 3.6.4 열차 출입문상태 표시 ····· 411
표 3.6.5 열차 대기상태 표시 ····· 412
표 3.6.6 열차 비상제동상태 표시 ····· 412
표 3.6.7 열차 이동상태 표시 ····· 412
표 3.6.8 블록 점유 표시 ····· 413
표 3.6.9 블록 개방/폐쇄/검지손실 표시 ····· 413
표 3.6.10 진로 표시 ····· 413

표 3.6.11. 임시속도제한 표시 ····· 414
표 3.6.12 PMA 표시 ····· 414
표 3.6.13 플랫폼 개방/폐쇄 표시 ····· 414
표 3.6.14 Dwell Time 표시 ····· 414
표 3.6.15 선로전환기 쇄정 표시 ····· 415
표 3.6.16 명령 메뉴 표시부 구성 ····· 416
표 3.6.17 PMA설정 확인 버튼 ····· 420
표 3.6.18 선로전환기 상태 표시 ····· 424
표 3.6.19 선로전환기 상태 표시 ····· 425
표 3.6.20 선로전환기 고장 설정 표시 ····· 425
표 3.6.21 시스템 장치간 인터페이스 방식 ····· 430
표 3.6.22 mock-up시스템간 인터페이스 방식 ····· 431
표 3.6.23 검증 항목 ····· 432
표 3.6.24 네트워크 통신 메시지 구조 ····· 451
표 3.6.25 시리얼 통신 메시지 구조 ····· 452
표 3.6.26 ICM ⇔ ATS 시뮬레이터간 메시지 종류 ····· 453
표 3.6.27 DCM-ATS시뮬레이터간 메시지 종류 ····· 453
표 3.6.28 DCM-차상시뮬레이터(ATP)간 메시지 종류 ····· 454
표 3.6.29 ATS시뮬레이터-차상시뮬레이터(ATO)간 메시지 종류 ····· 454
표 3.6.30 ICM-신호설비제어시뮬레이터간 메시지 종류 ····· 455
표 3.6.31 시스템간 통신개시에 따른 장치/메시지 구분과 Polling주기 ····· 456
표 3.7.1 평가 Metric 시험 결과 ····· 488
표 3.7.2 챔버 테스트 ····· 488
표 3.7.3 시간별대 온도 설정 ····· 489
표 3.7.4 시간별 온도 설정 ····· 490
표 3.7.5 테스트 명령어 리스트 ····· 493
표 3.7.6 적용규격과 문서화 기준 ····· 503
표 3.7.7 안전성 활동 조직 ····· 504
표 3.7.8 위험원 도출 1단계 ····· 518
표 3.7.9 대상시스템 위험원 도출 Sheet ····· 519

표 3.7.10 도출된 위험원 ····· 520
표 3.8.1 제안하는 디자인 패턴 항목과 기술 내용 ····· 532
표 3.9.1 이상현상 원인분석 및 조치결과 ····· 581
표 3.9.2 제어부의 계전기 성능 ····· 600
표 3.9.2 검지센서의 성능 ····· 601
표 3.9.3 장애 시 점검 사항 ····· 601
표 3.9.4 선로전환기 구성부품 ····· 604
표 3.9.5 NS형 선로전환기 ····· 607
표 3.9.6 NS-AM형 선로전환기 ····· 608
표 3.9.7 NS형 선로전환기 간류 ····· 608
표 3.9.8 전환시간 및 동작전류 ····· 611
표 3.9.9 전환시간 및 운전전류 ····· 612
표 3.9.10 전자클러치 토크 및 공극 ····· 614
표 3.9.11 제어계전기, 회로제어기 형식 ····· 615
표 3.9.12 체결장치 ····· 616
표 3.9.13 연결간 및 첨단간의 절연체 성능 ····· 618
표 3.9.14 접속간 및 유동방지간 절연체의 성능 ····· 618
표 3.9.15 MJ81 선로전환기 성능 ····· 619
표 3.9.16 MJ81 선로전환기 제원 ····· 620
표 3.9.17 MJ81 선로전환기 최장 전환시간 ····· 620
표 3.9.18 MJ81 선로전환기 최단 전환시간 ····· 620
표 3.9.19 MJ81 선로전환기 최대 소비전류 ····· 621
표 3.10.1 국내 철도사상사고 현황 (관련자료: 국토해양부 보도자료, 2009.4) ····· 631
표 3.10.2 철도시스템 안전설비 설치현황 ····· 632
표 3.10.3 이미지 센서 검지방법 ····· 636
표 3.10.4 영상처리기술의 주요 기능 ····· 636
표 3.10.5 승강장 낙하물 검지범위 ····· 637
표 3.10.6 승강장 낙하물 검지 주요 기능 ····· 638
표 3.10.7 선로차단 지원시스템 구축방안 ····· 639
표 3.10.8 승강장 안전 시스템 구축방안 ····· 639

표 3.10.9 안전시스템의 비교 ····· 641
표 3.10.10 승강장 제원 ····· 664
표 3.10.11 파일형식 ····· 679
표 3.10.12 저장구조 특징 ····· 680
표 3.10.13 시제품 제작 사양 ····· 683
표 4.1.1 사업계획서의 정량적 성과지표 ····· 708

그 림 차 례

그림 1.1.1 연구개발의 필요성 ····· 2
그림 1.3.1 과제 추진전략 ····· 8
그림 3.1.1 열차제어시스템 안전성 활동 절차 ····· 22
그림 3.1.2 시스템 수명주기에서의 열차제어시스템 안전성 활동 체계(안) ····· 23
그림 3.1.3 시스템 수명주기에 따른 위험원 분석 타입의 분류 ····· 25
그림 3.1.4 리스크 분석 방법의 분류 ····· 28
그림 3.1.5 Top 레벨에서의 FTA 분석 결과 예 ····· 33
그림 3.1.6 열차제어시스템 안전성 활동 체계에 따른 적용기술 ····· 34
그림 3.1.7 위험원과 사고와의 관계 ····· 36
그림 3.1.8 위험원 관리 절차 ····· 37
그림 3.1.9 FMEA(From cause to results)의 수행 방향 ····· 38
그림 3.1.10 HAZOP Study(Bidirectional analysis)의 수행 방향 ····· 38
그림 3.1.11 일반 HAZOP Study 템플릿 ····· 39
그림 3.1.12 해외 기술자문 결론 부분 ····· 48
그림 3.2.1 IEC 61508에 기반한 각 분야별 활용 규격 ····· 86
그림 3.3.1 목표 시스템 개발계획 개요 ····· 114
그림 3.3.2 전체 시스템 구조 ····· 114
그림 3.3.3 Equivalence Classes Testing 기능구성도 ····· 116
그림 3.3.4 Boundary Value Analysis Testing 기능구성도 ····· 117
그림 3.3.5 동치영역 대표값을 이용한 테스트 수행 시나리오 ····· 119
그림 3.3.6 경계값을 이용한 테스트 수행 시나리오 ····· 121
그림 3.3.7 프로젝트 설정 입력 화면 ····· 122
그림 3.3.8 시나리오 정보 입력 화면 ····· 123
그림 3.3.9 동치영역 자동 분할 및 수정 화면 ····· 124
그림 3.3.10 경계값 자동 분석 및 수정 화면 ····· 125
그림 3.3.11 동치영역 대표값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면 ····· 126

그림 3.3.12 경계값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면 ····· 127
그림 3.3.13 테스트 수행 화면 ····· 128
그림 3.3.14 보고서 생성 화면 ····· 129
그림 3.3.15 ASP 수행 개념 ····· 129
그림 3.3.16 각 모듈과의 관계도 ····· 131
그림 3.3.17 Execution Engine 수행 구조도 ····· 138
그림 3.3.18 프로그램 초기 화면 ····· 140
그림 3.3.19 프로젝트 설정 입력 ····· 141
그림 3.3.20 시나리오 정보 입력 ····· 141
그림 3.3.21 동치영역 자동 분할 및 수정 ····· 142
그림 3.3.22 경계값 자동 분석 및 수정 ····· 143
그림 3.3.23 동치영역 대표값 테스트케이스 생성 및 예상 출력값 입력 ····· 143
그림 3.3.24 경계값 테스트케이스 생성 및 예상 출력값 입력 ····· 144
그림 3.3.25 테스트 수행 ····· 144
그림 3.3.26 보고서 생성 ····· 145
그림 3.3.27 Fault Tree Analysis Steps ····· 146
그림 3.3.28 Fault Tree Analyzer system interface ····· 151
그림 3.3.29 FTA 화면 구성 ····· 152
그림 3.3.30 Project Explorer 화면 ····· 154
그림 3.3.31 Properties View 화면 ····· 154
그림 3.3.32 Probability Viewer 화면 ····· 155
그림 3.3.33 Editor View ····· 155
그림 3.3.34 FTA package class diagram ····· 156
그림 3.3.35 UI package class diagram ····· 159
그림 3.3.36 action package class diagram ····· 161
그림 3.3.37 dialog package class diagram ····· 164
그림 3.3.38 editor package class diagram ····· 166
그림 3.3.39 model package class diagram ····· 169
그림 3.3.40 editpart package class diagram ····· 174
그림 3.3.41 command package class diagram ····· 177

그림 3.3.42 figure package class diagram ····· 180
그림 3.3.43 perspective package class diagram ····· 181
그림 3.3.44 views package class diagram ····· 182
그림 3.3.45 html package class diagram ····· 184
그림 3.3.46 오류분석 보고서 ····· 191
그림 3.3.47 Fault Tree Analysis Project 생성 ····· 192
그림 3.3.48 Projec Explorer 화면 ····· 193
그림 3.3.49 Fault Tree Page 추가 ····· 193
그림 3.3.50 Create Fault Tree Page Dialog ····· 194
그림 3.3.51 Fault Tree Diagram 예제 ····· 194
그림 3.3,52 Layout ····· 195
그림 3.3.53 Probability 계산 결과 ····· 196
그림 3.3.54 Report Generation ····· 197
그림 3.3.55 Report Generation Dialog ····· 197
그림 3.3.56 오류 보고서 파일 생성 ····· 198
그림 3.3.57 Fault Tree Analysis Report ····· 198
그림 3.3.58 테스트 적용 절차 ····· 201
그림 3.3.59 IEC61508-7 검출 사례 ····· 203
그림 3.3.60 IEC62279-2 검출 사례 ····· 203
그림 3.3.61 IEC62279-5 검출 사례 ····· 203
그림 3.3.62 IEC62279-6 검출 사례 ····· 204
그림 3.3.63 IEC62279-8 검출 사례 ····· 204
그림 3.3.64 IEC62279-9 검출 사례 ····· 204
그림 3.3.65 SURE_BASIC-02 검출 사례 ····· 205
그림 3.3.66 SURE_BASIC-08 검출 사례 ····· 205
그림 3.3.67 SURE_BASIC-09 검출 사례 ····· 205
그림 3.3.68 SURE_BASIC-10 검출 사례 ····· 206
그림 3.3.69 SURE_BASIC-11 검출 사례 ····· 206
그림 3.3.70 SURE_BASIC-16 검출 사례 ····· 206
그림 3.3.71 SURE_BASIC-22 검출 사례 ····· 207

그림 3.3.72 SURE_BASIC-31 검출 사례 ····· 207
그림 3.3.73 SURE_BASIC-40 검출 사례 ····· 208
그림 3.3.74 Control Flow / Data Flow Testing 주요 검출 사례 ····· 208
그림 3.4.1 안전성 평가용 열차제어시스템 구성도 ····· 222
그림 3.4.2 제작된 안전성 평가용 열차제어시스템 ····· 234
그림 3.4.3 이중계 구성 ····· 236
그림 3.4.4 데이터 비교 처리 흐름도 ····· 237
그림 3.4.5 광통신을 이용한 네트워크 구성도 ····· 238
그림 3.4.6 무정전전원장치 장착 ····· 240
그림 3.4.7 최초 소스코드 분석 결과 ····· 242
그림 3.4.8 1차 수정 후 소스코드 분석 결과 ····· 242
그림 3.5.1 결과분석 개념 ····· 278
그림 3.5.2 연구대상 시스템 Hazard-1 Consequence Analysis ····· 279
그림 3.5.3 연구대상 시스템 Hazard-2 Consequence Analysis ····· 279
그림 3.5.4 연구대상 시스템 Hazard-3 Consequence Analysis ····· 280
그림 3.5.5 연구대상 시스템 Hazard-4 Consequence Analysis ····· 280
그림 3.5.6 BP-risk 개념도 ····· 283
그림 3.5.7 BP-risk 수행절차 ····· 284
그림 3.5.8 Failure 정의 ····· 289
그림 3.5.9 Safety Integrity Requirement 정의 ····· 290
그림 3.5.10 SSHA 절차 ····· 292
그림 3.5.11 SSHA 방법 ····· 293
그림 3.5.12 연구 프로세스 도식 ····· 300
그림 3.6.1 L/S 화면 ····· 410
그림 3.6.2 MMI 화면 ····· 415
그림 3.6.3 Overview 화면 ····· 417
그림 3.6.4 제어명령 표시부 ····· 417
그림 3.6.5 차상시뮬레이터 초기 화면 ····· 418
그림 3.6.6 차상시뮬레이터 시뮬레이션 화면 ····· 419
그림 3.6.7 차상시뮬레이터(ATP) 송·수신정보 표시 화면 ····· 422

그림 3.6.8 차상시뮬레이터(ATO) 송·수신정보 표시 화면 ····· 423
그림 3.6.9 선로전환기 수동 조작 화면 ····· 424
그림 3.6.10 신호설비제어시뮬레이터 초기 화면 ····· 426
그림 3.6.11 신호설비제어시뮬레이터 실행 전 선로전환기 상태 ····· 426
그림 3.6.12 신호설비제어시뮬레이터 실행 화면 ····· 427
그림 3.6.13 선로전환기 반위 전환 실행 화면 ····· 428
그림 3.6.14 선로전환기 S-Sw21 반위 전환 상태 표시 ····· 428
그림 3.6.15 시스템 구성도 ····· 430
그림 3.6.16 데이터 수집 방안 ····· 431
그림 3.6.17 검증 시뮬레이터 초기 화면 ····· 434
그림 3.6.18 CMI와 CMR 사이의 시컨스 번호 관리 ····· 457
그림 3.7.1 시제품의 전체 구성 ····· 469
그림 3.7.2 시제품 시험을 위한 화면 구성 예시 ····· 469
그림 3.7.3 고안전성 연산제어 장치 시제품 ····· 470
그림 3.7.4 고안전성 연산제어 시스템의 구조 ····· 472
그림 3.7.5 DSV 보드 ····· 473
그림 3.7.6 DSV 보드의 하드웨어 구조 ····· 474
그림 3.7.7 3중화 구성도 ····· 475
그림 3.7.8 VDI 보드 블록 다이어그램 ····· 476
그림 3.7.9 VDI ····· 477
그림 3.7.10 VDO 블록 다이어그램 ····· 478
그림 3.7.11 VDO ····· 479
그림 3.7.12 CPU ····· 480
그림 3.7.13 CPU 블록 다이어그램 ····· 480
그림 3.7.14 SIO 보드 ····· 481
그림 3.7.15 SIO 보드 블록 다이어그램 ····· 481
그림 3.7.16 LVDS 신호 전송 지연 시간 ····· 483
그림 3.7.17 LVDS 신호 전송 지연 시간 ····· 483
그림 3.7.18 LVDS Link Port Serial 통신 Timing Diagram ····· 484
그림 3.7.19 LVDS 전송속도 ····· 484

그림 3.7.20 보팅기능 테스트 환경 ····· 486
그림 3.7.21 1Kbytes 공유시간 ····· 486
그림 3.7.22 공유 보팅 시험 ····· 487
그림 3.7.23 시간별도 온도 설정 그래프 ····· 489
그림 3.7.24 시간별도 온도 설정 그래프 ····· 490
그림 3.7.25 DSV 보드 시험 환경 ····· 492
그림 3.7.26 보팅기능 테스트 환경 ····· 493
그림 3.7.27 시험용 시스템 구성 ····· 494
그림 3.7.28 시험 수행 순서 ····· 495
그림 3.7.29 시험용 프로그램 ····· 496
그림 3.7.30 세 개의 CPU 정상 시 결과 ····· 497
그림 3.7.31 하나의 CPU 고장 시 ····· 497
그림 3.7.32 2개 이상의 CPU 보드 고장 발생시 ····· 498
그림 3.7.33 기본 열차제어시스템 고장 분류 ····· 509
그림 3.7.34 시스템 고장에 대한 책임 트리 ····· 510
그림 3.7.35 Controller subsystem의 고장 트리 ····· 511
그림 3.7.36 VDI/VOD의 고장 트리 ····· 511
그림 3.7.37 CPU를 위한 Semi-Markov 모델 ····· 512
그림 3.7.38 SIO을 위한 신뢰성, 안정성 모델 ····· 513
그림 3.7.39 VDI을 위한 신뢰성, 안정성 모델 ····· 513
그림 3.7.40 VDO을 위한 신뢰성, 안정성 모델 ····· 514
그림 3.8.1 Z 명세 작성 프로세스 ····· 533
그림 3.8.2 패턴을 이용한 DCM의 statechart 및 Z명세 작성절차 ····· 536
그림 3.9.1 이상현상 발생 현황 ····· 580
그림 3.9.2 개소별 이상현상 발생 현황 ····· 580
그림 3.9.3 선로전환기 상판결빙 사고 ····· 582
그림 3.9.4 휴즈 삽입부 체결볼트 이완으로 접촉불량 ····· 583
그림 3.9.5 선로전환기 정위 상태에서 명령(정보) 송출 개요 ····· 584
그림 3.9.6 제어 및 표시정보 전송체계도 ····· 587
그림 3.9.7 선로전환기 제어모듈 블록도 ····· 587

그림 3.9.8 표시출력 ····· 589
그림 3.9.9 표시 입력부 1 ····· 589
그림 3.9.10 표시 입력부 2 ····· 590
그림 3.9.11 제어전압 감시 ····· 591
그림 3.9.12 모터전원 감시 ····· 592
그림 3.9.13 제어부 논리회로 ····· 593
그림 3.9.14 표시부(출력)논리 회로도 ····· 593
그림 3.9.15 표시부(입력)논리 회로도 ····· 594
그림 3.9.16 감시설비 전면 판넬부의 고장상태 표충 현황 ····· 594
그림 3.9.17 밀착검지기 구조 ····· 595
그림 3.9.18 근접센서 발진파형 ····· 596
그림 3.9.19 설치도 ····· 597
그림 3.9.20 현장 설치도 ····· 597
그림 3.9.21 단동기 밀착검지기 결선도 ····· 598
그림 3.9.22 단동 밀착검지기 제어부 회로도 ····· 599
그림 3.9.23 PR realy전원 변환 경우1 ····· 600
그림 3.9.24 PR realy전원 변환 경우2 ····· 600
그림 3.9.25 고속분기기용 밀착검지기 구성품 ····· 602
그림 3.9.26 첨단부 설치도 ····· 603
그림 3.9.27 크로싱부 설치도 ····· 603
그림 3.9.28 NS형 선로전환기 구조 ····· 604
그림 3.9.29 밀봉형 클러치 구조 ····· 606
그림 3.9.30 기존 클러치 구성품 ····· 607
그림 3.9.31 밀봉형 클러치 구성품 ····· 607
그림 3.9.32 NS형 선로전환기 구조 ····· 609
그림 3.9.33 NS-AM형 선로전환기 구조 ····· 610
그림 3.9.34 동작계수기 ····· 617
그림 3.9.35 MJ81형 전기선로전환기 내부 상세도 ····· 622
그림 3.9.36 MJ81형 전기선로전환기 외부 상세도 ····· 623
그림 3.10.1 ITS/HRI 시스템 구성도 ····· 633

그림 3.10.2 카메라를 이용한 승강장 추락검지 시스템 ····· 634
그림 3.10.3 철도건널목 장애물 검지시스템 ····· 635
그림 3.10.4 영상기반 승강장 안전시스템 구성 일례 ····· 637
그림 3.10.5 선로차단 지원 시스템 구성 일례 ····· 638
그림 3.10.7 화상처리식 검지시스템 구성 일례 ····· 642
그림 3.10.8 개발된 스테레오 카메라 ····· 643
그림 3.10.9 전체적인 시스템 구성도 ····· 644
그림 3.10.10 3D 레이저 레이더를 이용한 장애물 검지시스템의 구성도 ····· 646
그림 3.10.11 장애물 검지 데이터 흐름도 ····· 652
그림 3.10.12 레이저 스캐너 구조 일례(1) ····· 654
그림 3.10.13 레이저 스캐너 구조 일례(2) ····· 654
그림 3.10.14 펄스식 비행시간 레이저 센서의 작동 ····· 655
그림 3.10.15 침투력이 높은 레이저 사용 ····· 656
그림 3.10.16 FMCW 레이저의 맥놀이 주파수 및 대표적인 첩(chirped) 파형 ···· 657
그림 3.10.17 수신된 레이저 신호의 페이저(phasor) 다이어그램 ····· 659
그림 3.10.18 다른 2개의 변조 주파수 ····· 660
그림 3.10.19 3D 레이저 레이더의 장애물 검출 시스템 구조(1) ····· 661
그림 3.10.20 3D 레이저 레이더의 장애물 검출 시스템 구조(2) ····· 661
그림 3.10.21 승강장 유형 ····· 663
그림 3.10.22 낙하물 검지 ····· 665
그림 3.10.23 레이저 센서의 감시영역 ····· 665
그림 3.10.24 레이저 센서의 감시영역 동작 계통도 ····· 666
그림 3.10.25 설치 모형도(승강장 하부) ····· 667
그림 3.10.26 설치 모형도(승강장 외측) ····· 667
그림 3.10.27 3D 레이저 레이더 스캔(승강장 외측) ····· 668
그림 3.10.28 승강장 선로 장애물 검출시스템 구성도 ····· 668
그림 3.10.29 일반적인 디지털 영상처리 단계 ····· 672
그림 3.10.30 영상장치 흐름도 ····· 673
그림 3.10.31 영상처리 과정 ····· 674
그림 3.10.32 영상 파일 포맷 ····· 674

그림 3.10.33 차이연산을 통한 물체감지 ····· 676
그림 3.10.34 승강장 감시영역 설정 ····· 676
그림 3.10.35 인덱스를 이용한 자료분할 ····· 681
그림 3.10.36 범위에 따른 데이터 처리 방법 ····· 682
그림 3.10.37 영상자료관리 ····· 683
그림 3.10.38 3D 레이저 레이더 시제품 모델링 ····· 685
그림 3.10.39 3D 레이저레이더 센서 제어부 시제품 사진 ····· 685
그림 3.10.40 개발 시제품 사진 ····· 686
그림 3.10.41 레이저 레이더를 이용한 물체 스캔 데이터(1) ····· 687
그림 3.10.42 센서부 시험을 위한 실제 전경 ····· 688
그림 3.10.43 분석 소프트웨어를 거친 스캔 데이터 ····· 688
그림 3.10.44 센서부 시험을 위한 실제 전경(150m) ····· 690
그림 3.10.45 분석 소프트웨어를 거친 스캔 데이터(150m) ····· 690
그림 3.10.46 개발 안전설비 개요 ····· 691
그림 3.10.47 차상 단말기의 구성도 ····· 694
그림 3.10.48 작업자 단말기의 구성도 ····· 694
그림 3.10.49 차상용 및 작업자용 단말기의 주요 구성 ····· 695
그림 3.10.50 차상제어장치 송신용 프레임 구조 ····· 696
그림 3.10.51 기본 경보동작 메커니즘 ····· 698
그림 3.10.52 모터카가 전파수신 영역 벗어난 후 후진하는 경우 ····· 699
그림 3.10.53 모터카가 전파수신 영역 내에서 후진할 경우 ····· 700
그림 3.10.54 모터카↔작업자 및 모터카 사이의 경보 동작 메커니즘 ····· 701
그림 3.10.55 작업자용 단말기 시제품 ····· 702
그림 3.10.56 차상용 단말기 시제품 ····· 702
그림 3.10.57 차상 안전설비 출력신호 ····· 703
그림 3.10.58 현장시험 사진 ····· 704
그림 3.10.59 개발시제품의 서울메트로 시연회 사진 ····· 704
그림 3.10.60 시제품 시범설치 및 운용방법 교육 사진 ····· 705

CONTENTS

(영문목차)

Chapter 1 SUMMARY of Research & Development 1

Section 1 Needs of Research & Development 1
1. Technical Aspect 1
2. Economical · Industrial Aspect 2

Section 2 Subjects and Scope of Research & Development 3
1. Ultimate goal of research & development 3
2. Objectives & Contents for each year of research & development 3

Section 3. Technology Development Implementation Scheme 7
1. Implementation Strategy and Method 7
2. Annual Task System 9
3. Research & Development Implementation Scheme 10

Chapter 2. National/International Technical Trends 11

Section 1. National Technical Trends 11
Section 2. International Technical Trends 12
Section 3. Technical Trends Analysis 13

Chapter 3. R&D Achievements and Results 15

Section 1. TCS Safety Evaluation Technology Development 15
1. Functional Architecture 17
2. Physical Architecture 17

3. Design Analysis Report ····· 18
A. Requirement and Conformance ····· 18
B. Design Criteria ····· 18
C. Evidence for Verification Methods ····· 18
D. Achievements and Results ····· 19
(1) Safety Activity Technology Scheme and its Application Technology ····· 19
(2) Hazard Analysis Method(HAZO-KR) ····· 35
(2) Safety Evaluation Guideline Documentation ····· 47

Section 2. TCS S/W Safety Evaluation Technology Development ····· 79
1. Functional Architecture ····· 81
2. Physical Architecture ····· 81
3. Design Analysis Report ····· 82
A. Requirement and Conformance ····· 82
B. Design Criteria ····· 82
C. Evidence for Verification Methods ····· 82
D. Achievements and Results ····· 83
(1) Development Status of National/International SW Safety Evaluation ····· 83
(2) TCS S/W Safety Evaluation Checklist ····· 87

Section 3. TCS S/W Testing Technology Development ····· 109
1. Functional Architecture ····· 111
2. Physical Architecture ····· 111
3. Design Analysis Report ····· 112
A. Requirement and Conformance ····· 112
B. Design Criteria ····· 112
C. Evidence for Verification Methods ····· 112
D. Achievements and Results ····· 113
(1) Outlines ····· 113
(2) Boundary Value Analysis / Equivalence Classes Testing module ····· 115

(3) Fault Tree Analysis module ····· 146
(4) Results Applying Testing Module to Safety Evaluation Object TCS ···· 199
(5) Proposal of Contents for Railway SW Testing Guide ····· 209

Section 4. Safety Evaluation Object TCS Design & Manufacture for Applicability of Safety Assessment Technology ····· 217
1. Functional Architecture ····· 219
2. Physical Architecture ····· 219
3. Design Analysis Report ····· 220
A. Requirement and Conformance ····· 220
B. Design Criteria ····· 220
C. Evidence for Verification Methods ····· 220
D. Achievements and Results ····· 221
(1) Safety Evaluation Object TCS ····· 221
(2) Supplement Design of Safety Evaluation Object TCS ····· 226
(3) Supplement Manufacture of Safety Evaluation Object TCS ····· 234
(4) Testing & Results Safety Evaluation Object TCS ····· 243

Section 5. Applicability Technology Development through Mock-up system ··· 271
1. Functional Architecture ····· 273
2. Physical Architecture ····· 273
3. Design Analysis Report ····· 274
A. Requirement and Conformance ····· 274
B. Design Criteria ····· 274
C. Evidence for Verification Methods ····· 275
D. Achievements and Results ····· 276
(1) Mock-up system SIL Decision ····· 276
(2) Mock-up system SIL Assignment ····· 289
(3) Verification & Validation ····· 301
(4) Mock-up system Safety Case ····· 307

(5) Safety Activity Technology Scheme and its Application Technology Guidelines ····· 308

Section 6. Mock-up system simulator manufacture and test ····· 405
1. Functional Architecture ····· 407
2. Physical Architecture ····· 407
3. Design Analysis Report ····· 408
A. Requirement and Conformance ····· 408
B. Design Criteria ····· 408
C. Evidence for Verification Methods ····· 408
D. Achievements and Results ····· 408
(1) Outlines ····· 408
(2) manufacture ····· 409
(3) Interfaces ····· 450
(4) Interface test ····· 458

Section 7. Development on a sample for Fault-tolerant system ····· 463
1. Functional Architecture ····· 465
2. Physical Architecture ····· 465
3. Design Analysis Report ····· 466
A. Requirement and Conformance ····· 466
B. Design Criteria ····· 466
C. Evidence for Verification Methods ····· 468
D. Achievements and Results ····· 468
(1) Supplement Manufacture of Fault-tolerant System ····· 468
(2) Fault-tolerant system evaluation matrix ····· 482
(3) Supplement Safety Activities of Fault-tolerant System ····· 503
(4) Fault-tolerant system features and merits ····· 520

Section 8. Formal Applicability technology development for TCS ····· 527

1. Functional Architecture ····· 529
2. Physical Architecture ····· 529
3. Design Analysis Report ····· 530
A. Requirement and Conformance ····· 530
B. Design Criteria ····· 530
C. Evidence for Verification Methods ····· 531
D. Achievements and Results ····· 531
(1) Study on Formal Specification Procedure for Train Control Systems ···· 531
(2) Study on Formal Verification Procedure for Train Control Systems ····· 534
(3) Application of DCM Formal Specification & Formal Verification ····· 535

Section 9. Research & Analysis on Track Switch Defect Prevention Technology ····· 577
1. Design Analysis Report ····· 579
A. Requirement and Conformance ····· 579
B. Achievements and Results ····· 579
(1) Track Switch Defect Accident Cases ····· 579
(2) Reseach & Analysis on Prevention Devices for Track Switch Defect ··· 585
(3) Requirements of Track Switch ····· 607

Section 10. Development on Accident Reduction in view of Train Control ····· 625
1. Functional Architecture ····· 627
2. Physical Architecture ····· 627
3. Design Analysis Report ····· 628
A. Requirement and Conformance ····· 628
B. Design Criteria ····· 628
C. Evidence for Verification Methods ····· 629
D. Achievements and Results ····· 629
(1) Domestic/International Railroad Safety Facilities Technology Status ··· 630
(2) Pre-research on Technology Investigation & Differentiation Method ···· 635

(3) Detail Design of Development Object Platform Safety Facilities ····· 648
(4) Manufacture of Safety Facilities Prototype using 3D Laser-rader ····· 683
(5) Supplement Manufacture of Safety Facilities for Trackside Maintenace workers ··· 691

Chapter 4. R&D Accomplishment and Contribution ····· 707

1. Accomplishment of R&D objective ····· 707
A. Annual objective and evaluation criteria ····· 707
2. Plan to use R&D ····· 714
A. Expectation Effect ····· 714
B. Application Scheme ····· 715
C. Practical Using Scheme ····· 715

Chapter 5. Reference ····· 717

제 1 장 연구개발과제의 개요

제1절 연구개발의 필요성

1. 기술적 측면

◦ 최근에 들어 전자, 컴퓨터, 통신 기술의 발달에 따라 열차제어장치들도 전자화 및 컴퓨터화 되어감에 따라 열차제어시스템의 안전성 확보에 어려움이 있음

◦ 하드웨어와 소프트웨어가 결합되어 작동되는 열차제어장치는 결함이 발생되었을 때 결함발생 원인을 파악하여 대처하기에 어려움이 있음

◦ 이러한 컴퓨터를 이용한 열차제어장치 사용의 증가에 따라 장치들의 고장이 대규모 인명피해나 경제적 손실과 직결되는 열차제어시스템의 특성상 시스템에 엄격한 안전성 관리, 검증 및 평가가 필요함

◦ 컴퓨터를 사용한 열차제어시스템이 급격하게 기존의 기계 및 전기적인 열차제어시스템을 대체하고 있으나 대규모 인명피해나 경제적 손실과 직결되는 열차제어시스템의 특성상 시스템의 엄격한 안전성 활동 및 평가기술이 요구되고 있음

◦ 따라서 열차제어시스템의 안전성 확보를 위한 절차를 수행하는 체계인 안전성 활동이 시스템의 수명주기 전반에 걸쳐 진행되어야 하며, 이러한 안전성 활동을 통한 안전성 평가기술의 확보가 매우 중요함

◦ 열차제어시스템에 의한 사고억제 및 방지를 위한 결함허용 시스템 기술과 같은 시스템측면과 정형기법에 의한 바이탈 소프트웨어 설계기술과 같은 소프트웨어 측면에서의 안전성능 향상을 위한 기술의 개발을 필요로 함

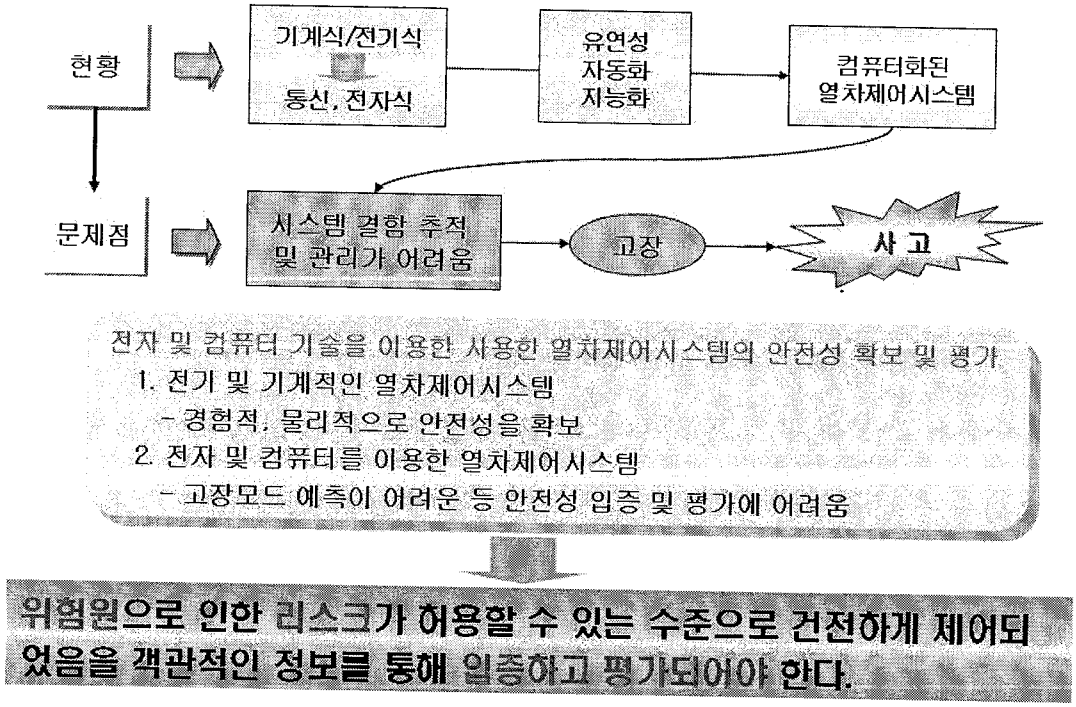


그림 1.1.1 연구개발의 필요성

2. 경제·산업적 측면

◦ 열차제어시스템을 위한 RAMS관련 규격들이 IEC61508/62278/62425 등에 의해 국제규격화 됨에 따라, 열차제어시스템의 적용에 있어서 안전성 활동 절차의 적용을 통한 열차제어시스템의 안전성 관리 및 평가를 요구하고 있음

◦ 이처럼 열차제어시스템의 안전성 평가 및 인증이 국제규격에 의해 규제되어감에 따라 국내 열차제어시스템도 이에 따른 안전성 활동 및 평가가 이루어져야 함

◦ 이러한 국제규격화로 안전성 활동 및 평가를 수행하지 않은 국내 열차제어시스템의 국내 운용과 해외진출에 어려움이 있음

◦ 따라서 열차제어시스템의 안전성 확보를 위한 수명주기별 기술의 안전성 활동, 안전성 평가 기술, 하드웨어와 소프트웨어 측면에서의 안전성 향상 기술 개발이 필요

◦ 열차제어시스템의 결함에 따른 열차사고는 사회적으로 매우 큰 파장을 발생시키므로, 열차제어시스템의 안전성 활동을 위한 세부수행 기술과 평가기술의 개발은 상당한 시급성이 요구됨

제2절 연구개발의 목표 및 범위

1. 연구개발의 최종목표

◦ 열차제어시스템의 안전성 평가기술 개발

◦ 열차제어시스템 안전성 향상기술 개발

◦ 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 및 시뮬레이터 제작

◦ 열차제어측면의 사상사고 저감을 위한 안전설비 시제품 제작

2. 연도별 연구개발 목표 및 내용

구 분	연구개발 목표	연구개발내용 및 범위
2차년도 (2005)	열차제어시스템 안전성 평가 및 사고방지를 위한 기반기술 연구	- 철도안전SE과제와의 연계사항 관리 및 조정 · 과제총괄 및 SE과제와 연계 · 최신연구동향 조사 및 분석 - 열차제어시스템 안전성 평가기술 개발 · IEC 61508/62278/62279 조사분석 · 관련 국내외 선행 연구 조사분석 · 열차제어시스템 안전성 활동 체계 및 평가 관련 기술조사연구 · 바이탈 열차제어시스템 소프트웨어 안전성 평가 기술 조사연구 · 열차제어시스템 주요 위험원 조사분석 -열차제어시스템 사고억제 및 안전성 향상을 위한 기반기술 연구 · 열차제어시스템 운용현황 및 사고발생현황 조사 분석 · 열차제어시스템 기능별 사고사례 조사 · 열차제어시스템에 적용된 사고방지기술 조사분석 · 안전성 향상을 위한 고안전성 연산처리 장치 기술 및 정형명세기술 조사연구
3차년도 (2006)	안전성 평가기술 연구 및 평가대상 시스템	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(1) · 열차제어시스템을 위한 고안전성 연산처리 장치

	선정	개발방향 정립 및 기본설계 · 열차제어시스템 안전핵심 소프트웨어 개발 절차 및 방법 연구 · 정형기법에 의한 열차제어시스템 바이탈 소프트웨어 개발 적용성 검토 -열차제어시스템 안전성 평가기술 개발(1) · 안전성 활동 및 평가를 위한 세부수행기술 연구 · 열차제어시스템 안전성 평가기술관련 템플릿 작성 · 열차제어시스템 안전핵심 소프트웨어의 테스트 항목 및 방법 도출 · 열차제어시스템 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 검토 및 선정 · 평가대상 열차제어시스템 기본설계 · 열차제어시스템 바이탈 소프트웨어 안전성평가를 위한 테스트 도구 개발사양 작성 · 열차제어시스템 통신 안전성 평가방법 및 검증 요구사항 분석
4차년도 (2007)	평가대상시스템 제작 및 시험기 설계	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(2) · 열차제어시스템 안전핵심 소프트웨어 정형화 요구명세 방법 제시 · 열차제어시스템을 위한 고안전성 연산처리 장치 상세설계 및 일부 모듈 시제품 제작 -열차제어시스템 안전성 평가기술 개발(2) · 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 상세설계 및 일부모듈 제작 · 평가대상 시스템 시험을 위한 시뮬레이터 설계 · 열차제어시스템 S/W 안전성 평가 시험기 설계 및 시제품 제작(1) -열차제어측면의 사상사고 저감기술 개발(1) · 국내외 적용기술 조사분석 · 사상사고 저감을 위한 열차제어 측면의 기술 조사분석
5차년도 (2008)	평가대상시스템 제작 및 시험기	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(3)

	제작	· 열차제어시스템 안전핵심 소프트웨어를 위한 정형검증기술 연구 · 열차제어시스템을 위한 고안전성 연산처리 장치 시제품 제작 · 열차제어장치에 의한 열차분리 검지기술 분석 및 요구사항 제시 -열차제어시스템 안전성 평가기술 개발(3) · 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 제작 · 열차제어시스템 S/W 안전성 평가 시험기 시제품 제작(2) · mock-up 시스템 시험을 위한 시뮬레이터 제작(1) · 열차제어시스템 안전성 평가 가이드라인 작성 - 열차제어 측면의 사상사고 저감기술 개발(2) · 사상사고 저감을 위한 기술 설계
6차년도 (2009, 당해년도)	열차제어시스템 안전성 평가 및 향상기술의 보완	-철도안전SE과제와의 연계사항 관리 및 조정 -열차제어시스템 안전향상 핵심기술 개발(4) · 열차제어시스템 안전핵심 소프트웨어를 위한 정형기법 적용방안 제시 · 열차제어시스템을 위한 고안전성 연산처리장치 시제품 보완제작 및 성능시험 · 선로전환결함 방지기술 조사분석 -열차제어시스템 안전성 평가기술 개발(4) · 열차제어시스템 안전성 평가가이드라인(안) 보완 · 열차제어시스템 S/W 테스팅 자동화도구 시제품 제작(3) · 평가대상시스템 제작보완 및 시험을 위한 시뮬레이터 제작(2) · 평가대상시스템 Safety Case 작성(1) - 열차제어 측면의 사상사고 저감기술 개발(2) · 열차제어측면의 사상사고 저감을 위한 안전설비 상세설계 및 제작
7차년도	개발기술의 확립	-철도안전SE과제와의 연계사항 관리 및 조정

(2010)	및 실용화	-열차제어시스템 안전향상 핵심기술 개발(5) · 선로전환결함 요구사항 제시 -열차제어시스템 안전성 평가기술 개발(5) · 열차제어시스템 안전성 평가가이드라인 최종안 제시 · 열차제어시스템 S/W 테스팅 자동화도구 시제품 통합제작 및 성능 확인(4) · 평가대상시스템 안전성 평가 및 분석 · 평가대상시스템 시험을 위한 시뮬레이터 보완 및 적용시험 - 열차제어 측면의 사상사고 저감기술 개발(3) · 열차제어측면의 사상사고 저감을 위한 안전설비 보완 제작 및 성능시험

제3절 기술개발 추진체계

1. 추진전략 및 방법

연구개발 목표달성을 위한 관련 기술정보의 수집 및 분석, 국내외 전문가 확보, 타 기관과의 협조 방안 강구 및 기술개발 방법 등은 다음과 같다.

◦ 철도운영기관의 협조를 통한 열차제어시스템의 운영현황 분석
  - 철도공사나 도시철도 운영기관 등 현재 운행 중인 열차제어시스템의 운영현황과 사고발생현황을 조사 분석한다.

◦ 국제규격, 외국의 사례, 선행 연구들의 분석을 통한 기본방향 설정
  - 현재 국제적으로 적용하고 있는 IEC 규격, 유럽 EN 규격, IEEE 규격, 기타 철도관련 각국의 규격 또는 규정들, 국내외 관련 선행연구들의 분석을 통하여 열차제어시스템의 안전성 평가 및 안전성 활동 세부수행 기술 기본방향을 설정한다.
  - 설정된 기본 방향을 바탕으로 외국의 철도시스템에서 안전성 확보를 위한 경향과 활동사항, 규격의 적용사례들을 검토한다.

◦ 본 연구과제의 지금까지의 자료분석과 연구결과를 통해 열차제어시스템에 적용할 안전성 평가기술을 도출하고, 그 이후에는 이를 바탕으로 모의 열차제어시스템의 제작, 모의 열차제어시스템을 통한 적용성 연구 등을 통해 최종적인 (안) 도출 및 제시한다.

◦ 관련규격 및 적용사례의 정확한 정보와 전략을 획득하기 위해 TÜV, Network Rail 등 관련분야 전문가를 초청 또는 방문하여 교육훈련 및 자문을 수행한다.

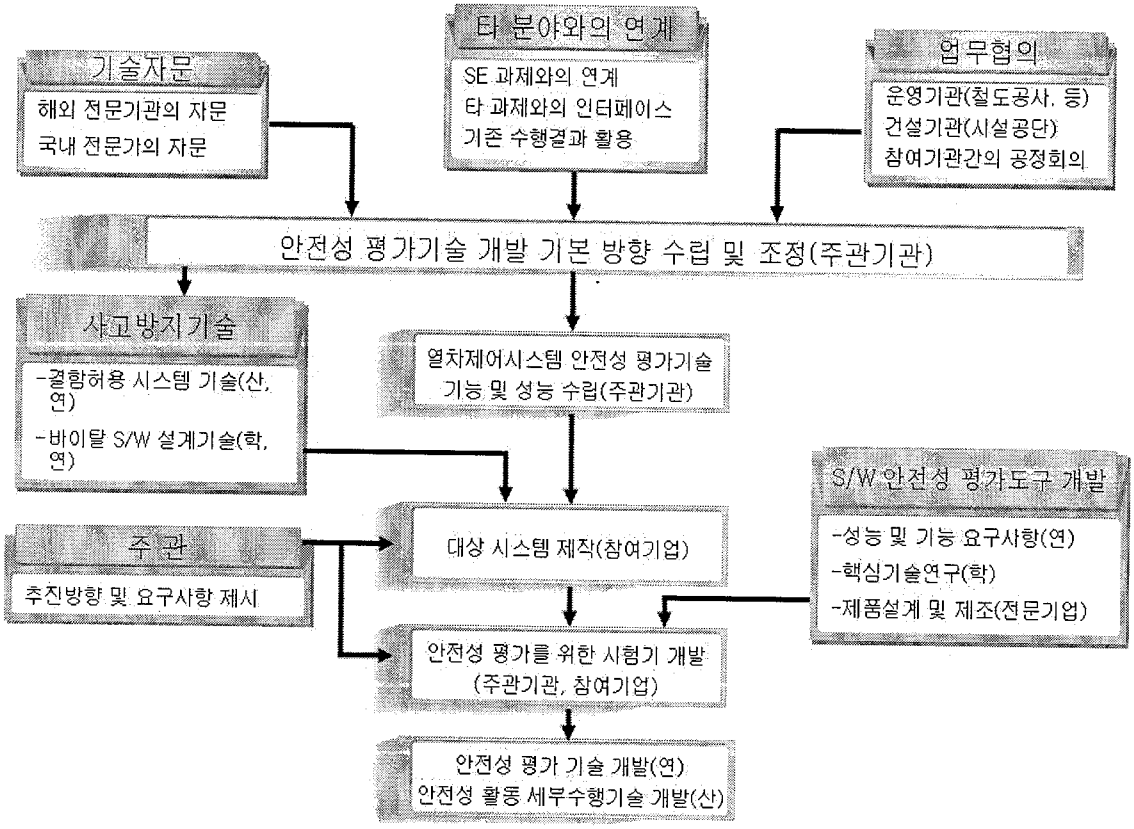
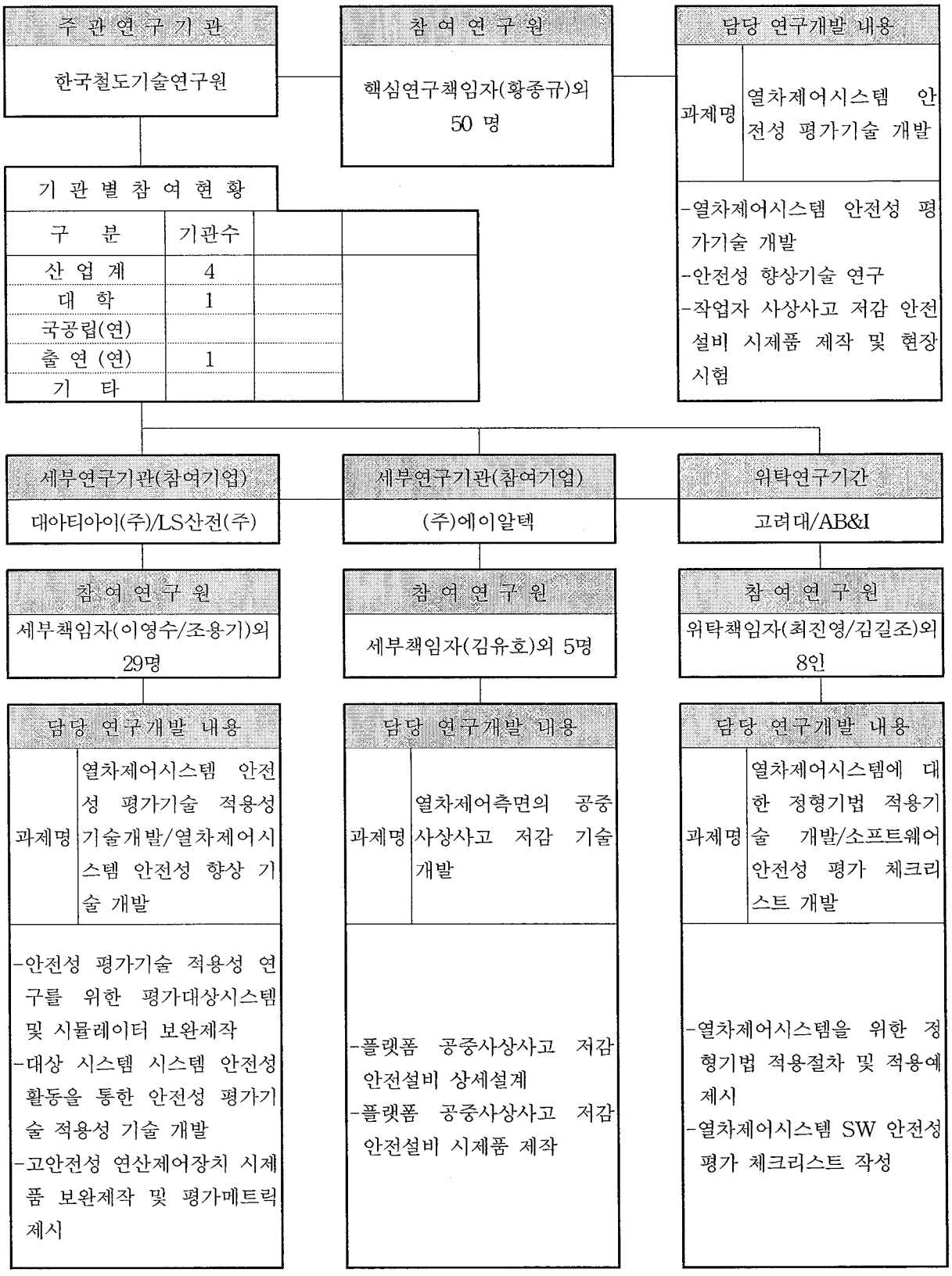
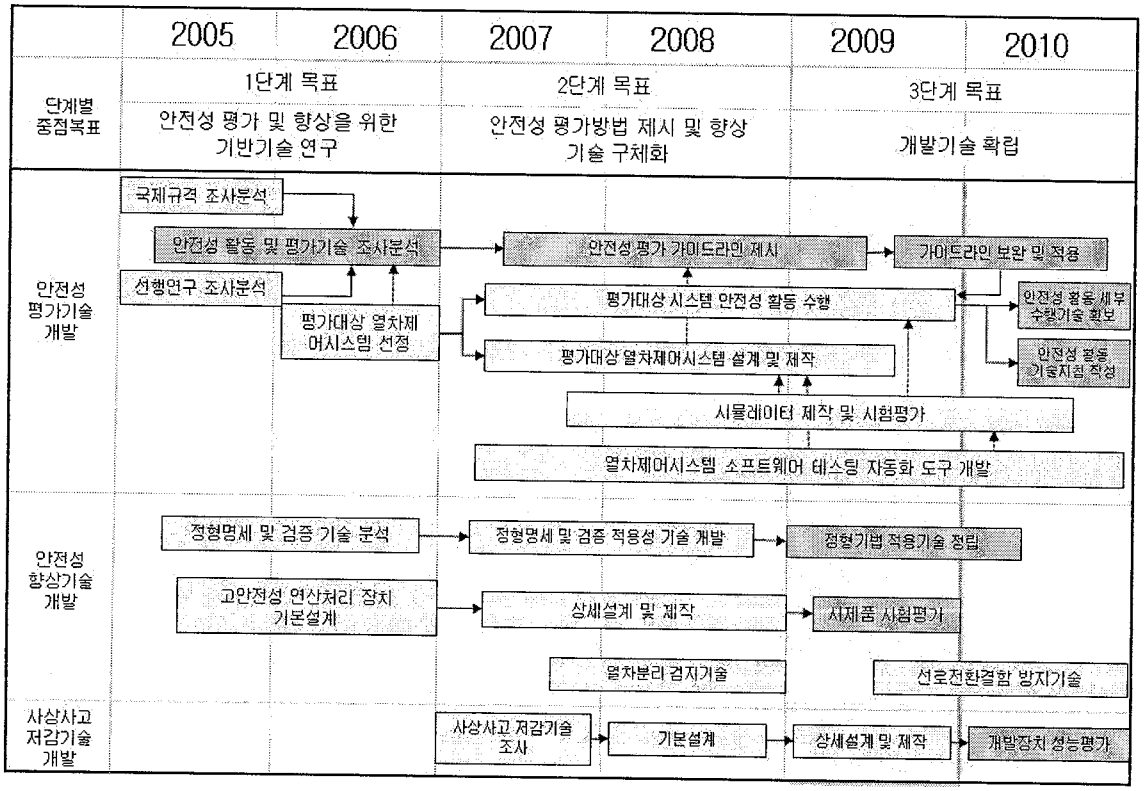


그림 1.3.1 과제 추진전략

2. 당해 연도 업무역할 체계



3. 연구개발 추진체계


2005
2006
2007
2008
2009
2010
단계별 중점목표
1단계 목표
안전성 평가 및 향상을 위한 기반기술 연구
2단계 목표
안전성 평가방법 제시 및 향상 기술 구체화
3단계 목표
개발기술 확립
안전성 평가기술 개발
국제규격 조사분석
안전성 활동 및 평가기술 조사분석
선행연구 조사분석
평가대상 열차제어시스템 선정
안전성평가 가이드라인 제시
가이드라인 보완 및 적용
평가대상 시스템 안전성 활동 수행
안전성 활동 세부 수행기술 확보
평가대상 열차제어시스템 설계 및 제작
안전성 활동 기술지침 작성
시뮬레이터 제작 및 시험평가
열차제어시스템 소프트웨어 테스팅 자동화 도구 개발
안전성 향상기술 개발
정형명세 및 검증 기술 분석
정형명세 및 검증 적용성 기술 개발
정형기법 적용기술 정립
고안전성 연산처리 장치 기본설계
상세설계 및 제작
시제품 시험평가
열차분리 검지기술
선로전환결함 방지기술
사상사고 저감기술 개발
사상사고 저감기술 조사
기본설계
상세설계 및 제작
개발장치 성능평가

제 2 장 국내외 기술동향

제1절 국내기술 동향

◦ 국내의 경우 한국철도기술연구원에서 수년 전부터 철도의 안전관련 시스템에 대한 조사연구가 수행되었으나, 열차제어시스템의 안전성 활동을 위한 세부수행 기술과 평가기술에 대한 연구가 거의 이루어지고 있지 않고 있음

◦ 하지만 철도공사에 의해 철도신호제품의 안전성 검증 및 평가를 위한 활동이 요구되고 또한 해외 수출을 위해 IEC61508 등 국제규격에 의해 요구됨에 따라 이 분야의 기술에 대한 연구개발의 필요성을 인식하고 있는 단계

◦ 열차제어시스템에 의한 사고억제 및 방지기술로서 시스템 및 하드웨어적인 측면에서 결함허용 시스템 기술 등 일부 기술들이 개발 및 적용되고 있으나, 대부분 국내에서 운용되고 있는 열차제어시스템의 기술들은 외국의 시스템이 그대로 도입 및 운용되고 있는 등 이 분야 기술들이 체계적으로 정리 및 개발되어지고 있지 않고 있음

◦ 또한 바이탈 소프트웨어의 경우 정형기법에 의한 설계 및 검증 기술이 학계차원에서는 일부 연구가 진행되고 있으나 열차제어시스템의 소프트웨어 설계 및 검증을 위한 적용성 연구는 전혀 이루어지고 있지 않음

◦ 열차제어시스템을 위한 통신분야로는 한국철도기술연구원에서는 정형기법을 이용하여 열차제어시스템을 위한 통신프로토콜을 설계 및 검증하였으며, 그 연구결과 제시된 프로토콜이 철도공사에 의해 표준으로 채택되어 적용되었으나,

◦ 아직 열차제어시스템을 위한 네트워크 적용기술 및 이에 따른 안전성 확보 및 평가기술 등에 대한 연구는 이루어지고 있지 않음

◦ 일반 상업용 소프트웨어나 정보통신 기기용 임베디드 소프트웨어의 경우 한국정보통신기술협회(TTA)에서 소프트웨어의 품질시험을 통한 인증을 하는 등 신뢰성 시험이 일부 이루어지고 있음

◦ 열차제어시스템 소프트웨어 시험의 경우 국내에서는 지금까지 개발과정 중에서 안전성활동 문서를 통해 안전성 평가가 이루어지고 있음

◦ 국내에서도 최근 내장형 소프트웨어의 동적시험도구가 상용화 되어 대기업들에

서 호평을 받고 있음

◦ 본 연구에서 제안하고자 하는 열차제어시스템 소프트웨어와 같은 내장형 소프트웨어의 안전성을 평가하는 연구는 수행된 사례가 없음

제2절 국외기술 동향

◦ 열차제어시스템 안전성 활동 체계는 유럽을 중심으로 규격화가 이루어졌으며, 또한 이 규격이 국제규격인 IEC 규격으로 제정되어 적용되고 있고, 일본의 경우도 IEC 국제 규격을 바탕으로 안전성 기술지침을 제정하여 적용을 권고하고 있음

◦ 또한 열차제어시스템에 대한 안전성 활동 세부수행 기술과 평가기술은 시스템 제작사나 인증기관들이 고유의 기술을 확보하고 있고 이를 적용하고 있으나 이 기술의 공개가 이루어지고 있지 않음

- 유럽에서는 철도의 하드웨어 및 소프트웨어의 안전성을 확보하기 위해 EN 50126, 50128, 50129 등을 제정하여 그것에 맞게 안전성 인증을 하고 있으며, 철도신호시스템의 안전성확보를 위한 절차를 제정 사용하고 있음
- 국제규격인 IEC 규격에서는 다음과 같은 규격을 제정하여 안전성 활동을 하고 있음

·IEC 61882 : HAZOP application
·IEC 60812 : 고장모드영향분석(FMEA)
·IEC 61025 : Fault Tree Analysis
·IEC 61511 : 프로세서 산업을 위한 계측시스템의 기능안전 규격
·IEC 61508 : 안전관련 전자제어시스템의 RAMS
·IEC 62278 : 철도신호분야 제어시스템의 RAMS
·IEC 62279 : 철도신호분야 안전관련 제어시스템의 소프트웨어 RAMS
·IEC 62280 : 철도신호분야 안전관련 통신시스템 RAMS

◦ 사고억제 및 방지를 위한 기술로서 하드웨어 및 시스템 측면에서 결함허용시스템과 Fail-safe 기술은 철도선진국의 대부분의 열차제어시스템에 적용 및 운용되고 있으며, 정형기법에 의한 설계 및 검증 등 소프트웨어 측면에서의 안전성

향상 기술은 많은 연구개발이 이루어졌으나, 일부 시스템을 제외하고는 아직 상용화된 제품에 적용이 이루어지고 있지 않음

◦ 소프트웨어의 안전성을 평가하는 자동화 도구는 소프트웨어의 품질평가 도구가 주류를 이루고 있으며, 위험도를 평가하는 도구는 없는 실정임

◦ 내장형 소프트웨어의 자동화된 평가도구들이 최근에 이용되고 있음

제3절 기술동향 분석 결론

◦ 선진각국은 열차제어시스템과 관련된 규격에 따른 안전성 활동의 수행을 통해 시스템을 설계 및 개발하고 있으며, 규격에 의한 안전성 활동 체계에 따른 세부수행기술은 각 기관이 독자적으로 확보하여 적용하는 등 열차제어시스템을 위한 안전성 활동이 정착된 것으로 판단함

◦ 점차적으로 국외뿐만 아니라 국내의 운용기관에서도 열차제어시스템의 국제규격에 따르도록 요구되어질 것으로 예상되며, 그 결과로 국내기관이나 기업이 정확한 대비를 하지 못하면 국내의 열차제어시스템이 외국으로의 수출이 불가능할 뿐만 아니라, 국내에서도 적용되기 어려울 것으로 예상됨

◦ 안전과 관련된 열차제어시스템은 정해진 규격에 따라서 정확한 안전성 활동 및 평가가 필수적으로 요구될 것으로 예측됨

◦ 또한 안전성 향상을 위한 시스템 및 소프트웨어 측면에서의 기술은 철도선진국에서는 시스템 측면의 기술들은 많이 연구개발 및 적용이 되고 있으며, 국내에서는 운용되고 있는 대부분의 열차제어시스템이 외국의 시스템과 기술이 그대로 도입 및 운용되고 있어 결함허용 기술 등에 대한 연구가 체계적으로 이루어지고 있지 않음

◦ 열차제어시스템을 위한 소프트웨어의 설계 및 검증 등 소프트웨어 측면의 기술은 유럽을 중심으로 열차제어시스템에 점차 적용이 확대되고 있는 추세이나 국내에서는 아직 일부 학술적인 차원에서만 연구가 이루어지고 있음

분야	선진국	국내	기술격차
안전성	IEC	규격분석 및 일부 적용 중	소

관련규격		61508/62278/62279/ 62280 등 국제규격으로 제정되어 적용 중		
열차제어시스템 Hazard		열차제어시스템 Hazard DB화되어 있음	일부 장치에 대한 Hazard 도출작업이 이루어지고 있음	중
열차 제어 시스템	안전성 활동체계	국제 규격화 되어있음	국제 규격의 국내 적용성 연구가 진행 중	중
	안전성 활동 세부수행 기술	각 기관별 확보하고 있음, 철도에서 적용으로 풍부한 경험확보	필요성 인식 단계	대
	문서화	제작사별로 풍부한 경험을 확보한 것으로 발표	필요성 인식단계	대
	시험평가	시험평가활용	일부 진행 중	대
	소프트웨어 시험도구	임베디드 소프트웨어 시험 도구 사용 판매	일부 제작사에서 임베디드 소프트웨어 시험도구 개발 및 판매	중
	인증기관	TÜV, Lloyd, 등	-	대
	관련회사	자문기관, 관련 소프트웨어 툴 개발 사 등 다수 존재	-	대

제 3 장 연구개발 수행내용 및 결과

제1절 열차제어시스템 안전성 평가기술 개발

	검증계획서 **(Verification Plan)**	**ID No :** **TC - SR02 - SSR02 - 2010** 작성일 : 2010. 06. 18 수정일 :

2. 프로젝트는 열차제어시스템 안전성 평가기술을 개발해야 한다.

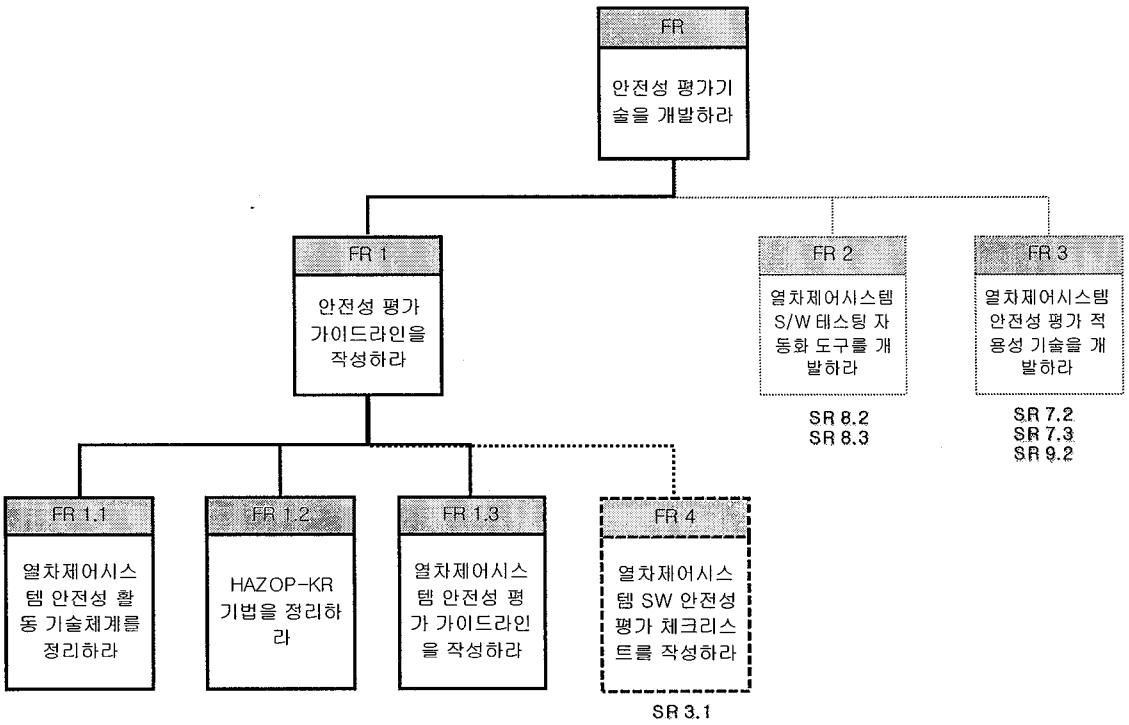
2.2 프로젝트는 열차제어시스템 안전성 평가기술을 개발하여야 한다.

입력물 :	**업무 :**	**출력물 :**
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 안전성 평가 가이드라인, SW 안전성 평가 체크리스트 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 1.2 외국자료와 비교, - 3.1 국제규격 부합 - 3.3 전문가 검토	- SE 검증	- 수정 VRTM - 검증결과표

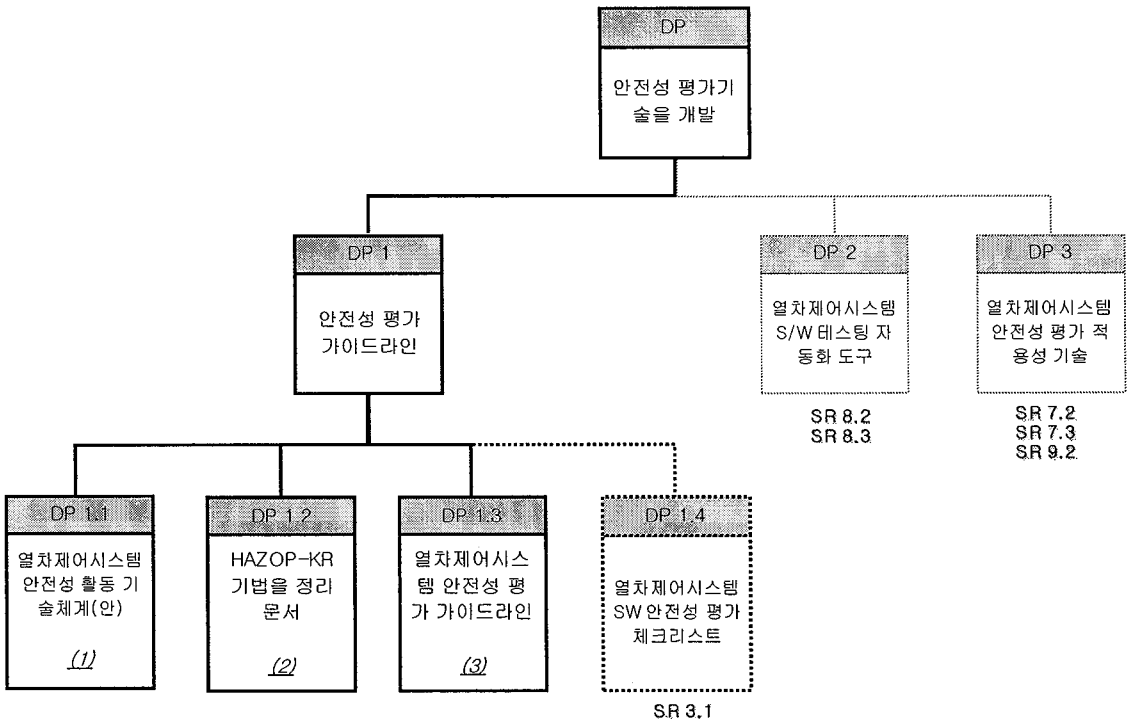
Verification Specification (검증기준) :

1. 열차제어시스템 안전성 평가 가이드라인의 작성 근거가 적합한가?
2. 국제규격의 요구사항을 반영하고 있는가?
3. 전문가 자문을 수행하였는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

열차제어시스템 안전성 활동 기술체계 및 평가 가이드라인 제시 요구사항 『SR 2. 프로젝트는 열차제어시스템 안전성 평가기술을 개발하여야 한다.』 중 「SSR. 2.2. 프로젝트는 열차제어시스템 안전성 평가기술을 개발하여야 한다.」에 해당하는 내용이다. 본 연구에서는 전년도에 제시한 '열차제어시스템 안전성 평가 가이드라인 초안'과 당해연도의 대상시스템을 통한 적용성 연구, 국내 전문기관 및 해외 전문기관의 기술자문 등을 통해 안전성 평가 가이드라인을 보완하였다. 이 가이드라인은 열차제어시스템 안전성 승인 및 수용 조건을 나타내는 IEC 62425 규격을 기본으로 하였으며, 독일의 안전성 평가 전문기관의 기술자문 결과를 바탕으로 보완되었다. 또한 당해연도에 적용성 연구를 통해 열차제어시스템 안전성 활동을 위한 기술체계와 리스크 예측 및 분석 기법인 HAZOP-KR 기법을 보완 제시하였다.

나. 설계기준

○ 열차제어시스템 안전성 평가업무 분석을 위해서 전기전자 시스템들의 안전성 활동에 대한 국제규격인 IEC62278과 IEC62425 규격을 참고하였으며, 영국 Network Rail의 "Engineering Safety Management, Yellow Book"의 자료를 참고하였다.

○ 철도통신 안전성관련 규격인 IEC 62280("Safety-related communication in closed transmission systems" - EN 50159-1, "Safety-related communication in open transmission systems" - EN 50159-2)을 참고하였다.

○ 당해 연도에는 열차제어시스템 안전성 평가 가이드라인 제시하기 위해 해외의 안전성 평가 전문기관(TÜV SÜD)으로부터의 기술자문을 수행하였으며, 그 결과를 반영하였으며, 소프트웨어 안전성 평가 체크리스트는 국내 전문기관을 통한 기술자문을 통해 작성하였다.

다. 검증 방법에 따른 증거 자료

열차제어시스템 안전성 평가기술 개발을 위해 본 절에서는 전년도 연구결과와 당해연도의 평가대상시스템의 제작과 안전성 활동 수행을 통한 적용성 연구를 바탕으로 안전성 평가 가이드라인 초안을 작성하였다. 또한 이 가이드라인 작성을 위해 기본적으로 열차제어시스템 안전성 입증관련 국제규격인 IEC 62425 규격과 독일의 안전성 평가 전문기관인 TÜV SÜD 기관으로부터 수개월 간의 자문을 통해 가이드라인 초안을 작성하였다. 또한 당해연도에 적용성 연구를 통해 열차제어시스템 안전성 활동을 위한 기술체계와 리스크 예측 및 분석 기법인 HAZOP-KR 기법을 보완 및 정리하였으며, 이와 관련된 내용을 2개의 학술지 논문으로 게재되었다.

라. 성과물의 내용 및 결과

(1) 열차제어시스템 안전성 활동 기술체계

열차제어시스템의 안전성 평가는 시스템에 대한 안전성 활동 과정과 결과의 분석을 통해 이루어진다. 따라서 열차제어시스템의 안전성 평가기술의 정립을 위해서는 열차제어시스템에 적용하기 적합한 안전성 활동 기술체계 및 이에 따른 수행기술에 대한 분석이 필수적으로 요구된다. 전년도까지 연구에서 통해 열차제어시스템의 안전성 활동 기술체계와 각 단계별 적용할 수 있는 다양한 기법들에 대해 분석하였으며, 당해연도에는 전년도까지의 연구결과를 바탕으로 평가대상 시스템을 통한 적용성 연구를 통해 전년도에 제시한 기술체계를 보완 제시하였다.

(가) 개요

열차제어시스템의 안전성 활동은 개발되는 열차제어시스템이 내재하고 있는 잠재적 위험원이나 결함을 찾아 제거하거나 그 발생확률을 줄일 수 있도록 하드웨어, 소프트웨어, 설비, 환경, 운영, 문서를 고려한 모든 일련의 활동을 의미한다. 즉, 안전성 활동은 시스템 수명주기 동안 열차제어시스템 위험원의 도출 및 도출된 위험원의 제어하거나 일정 수준 이하로 제어하는 일련의 과정을 말한다.

이러한 위험원 제어 측면에서의 열차제어시스템 안전성 활동 체계는 IEC 62278에서 제시하는 시스템 수명주기를 기본으로 하는 안전성 확보를 위한 안전성 활동의 체계를 의미한다. 전년도에 이러한 IEC 62278에서 제시하는 시스템의 수명주기

에 따른 열차제어시스템에 적용하기 적합한 안전성 활동 기술체계를 제시하였으며, 당해연도에는 평가 대상시스템의 적용성 연구와 해외 안전성 평가 전문기관의 기술자문을 통해 일부 수정 및 보완하였다.

(나) 안전성 활동 기술체계의 제시

국제규격에서 요구하는 열차제어시스템의 안전성 활동은 개발되는 열차제어시스템이 내재하고 있는 잠재적 위험원(Hazard)이나 결함을 찾아 제거하거나 그 발생확률을 허용수준 이하로 줄일 수 있도록 하드웨어, 소프트웨어, 설비, 환경, 운영, 문서를 고려한 모든 일련의 활동을 의미한다. 즉, 안전성 활동은 시스템의 안전성 확보를 위해 시스템 수명주기 동안 열차제어시스템 위험원을 도출 하고 이 도출된 위험원을 제거하거나 일정 수준 이하로 제어하는 일련의 과정을 말한다.

관련규격, 선행연구, 미 국방성 안전성 활동체계 등의 조사 분석, 해외 안전성 평가 전문기관의 기술자문 등을 토대로 열차제어시스템을 위한 안전성 활동 단계와 각 단계별 주요한 활동을 분석하였으며, IEC 62278에 제시된 수명주기 내에서의 안전성 활동과 비교하여 표 3.1.1에 나타내었다. 즉, 안전성 활동은 표 3.1.1과 같이 시스템 수명주기 내에서 프로젝트 시스템의 안전성 향상 및 입증을 위해 수명주기 각 단계에서 수행되어진다. 그림 3.1.1은 시스템 수명주기 단계와 비교 없이 국제규격에 따른 안전성 활동 중심으로 해서 표현한 블록도로서 안전성 평가에 필요한 안전성 활동 절차를 나타낸 것이다.

표 3.1.1 시스템 수명주기에 따른 주요 안전성 활동

안전성 활동 단계	주요 안전성 활동	IEC 62278 수명주기 단계
시스템 분석 및 위험도 분석	-시스템 기능요구사항, 인터페이스 요구사항, 운영시나리오를 토대로 리스크 분석 -과거 유사시스템을 통한 위험원 리스트 작성 -PHA기법을 통한 위험원에 대한 리스크 예측	수명주기 1, 2 단계

시스템 HIA(위험원 도출 및 분석)	-세부 설계자료를 토대로 시스템으로 인한 사고를 예측 -FMEA, HAZOP 기법 등을 통한 위험원 확인 -위험측고장률을 산출하기 위한 위험원 분석	수명주기 3 단계
리스크 분석 및 안전성 목표수립	-정량적 또는 정성적 방법을 통한 리스크 분석 -분석된 리스크를 통해 기능 또는 위험원별 SIL 및 THR 할당 -시스템의 안전요구사항 작성	수명주기 4, 5 단계
안전대책수립 및 활동	-안전성측면의 위험측고장률은 SIL등급별 위험측고장률에 위험측 고장관련 기능 및 소자를 모델링하여 관리	수명주기 6, 7, 8 단계
안전성 확인 및 검증	-시스템의 기능 및 성능요구사항의 준수여부 확인 -시스템의 시스템요구사항 및 안전요구사항의 준수여부를 검증	수명주기 9 단계
안전성 인증	-안전성 활동의 완성도의 판단을 위임하는 기관에서 작성하는 평가보고서에 따라 안전성 인증 진행	수명주기 10 단계
안전성 관리	-시스템이 운영을 시작한 이후에 적용하는 신뢰성 및 안전성 측면의 유지보수 및 철거 프로그램으로써, 유지보수는 신뢰성과 안전성을 모두 고려하여 주기적 보수 및 고장에 의한 유지보수를 실시	수명주기 11, 12, 13, 14 단계

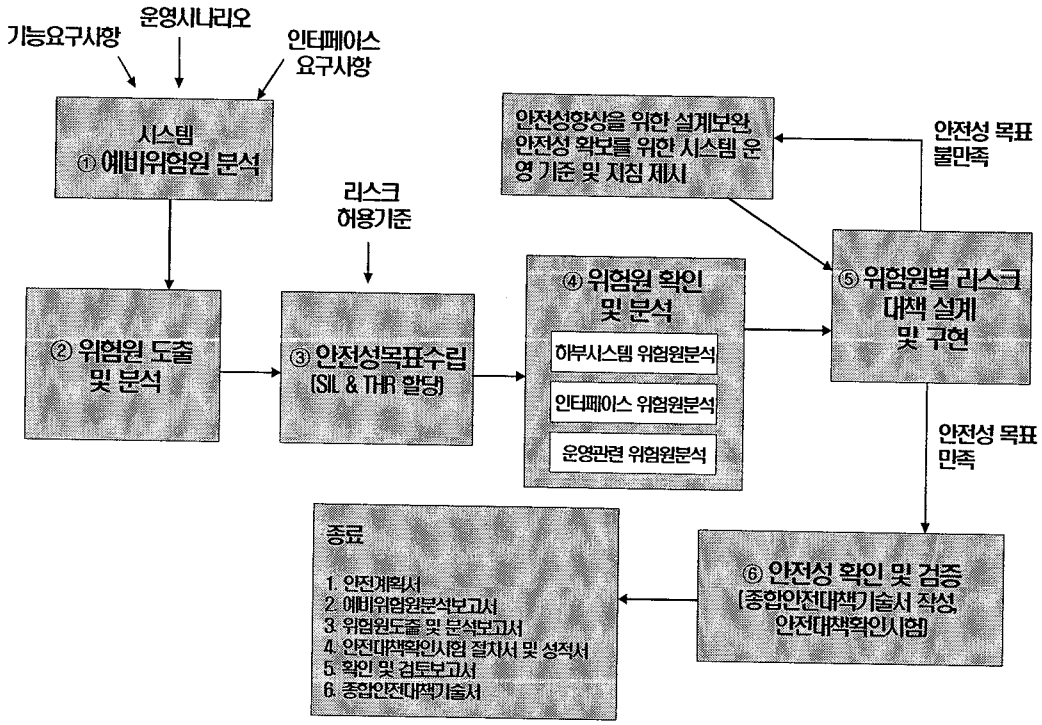


그림 3.1.1 열차제어시스템 안전성 활동 절차

표 3.1.1의 마지막 단계인 "안전성 관리" 단계는 시스템에 대한 안전성 승인 이후 운용과정에서의 안전성 활동 단계이며, 시스템을 인도하기 직적의 안전성 평가 시에는 이 부분은 안전측면에서 운용 및 유지보수를 위한 계획에 대한 평가만 수행된다. 즉, 열차제어시스템의 안전성 확보 및 입증을 위한 안전성 활동체계는 우선적으로 열차제어시스템의 잠재적인 위험원을 도출하고 이의 분석 및 평가를 수행하고, 최종적으로는 이 도출된 위험원 이 안전성 활동을 통해 허용수준 이하로 제어되었는지를 입증함으로써 안전성 입증이 이루어지도록 하고 있다. 즉, ① 예비위험원 분석 단계, ② 위험원 도출 및 분석 단계, ③ 안전성 목표수립 단계, ④ 위험원 확인 및 분석 단계, ⑤ 위험원별 리스트 대책설계 및 구현 단계, 그리고 ⑥ 최종적인 안전성 확인 및 검증 단계로 구성된다. 안전성 활동은 열차제어시스템의 위험원을 시스템 수명주기를 통해 관리 및 제어하여 최종적으로 허용수준 이하로 제어되도록 하고 이를 입증하는 단계로 구성된다.

표 3.1.1과 그림 3.1.1에서의 분석결과를 바탕으로 국내의 열차제어시스템 안전성 활동을 위한 절차를 그림 3.1.2와 같이 나타내었다. 이 안전성 활동 절차는 그림 3.1.2에서 나타낸 기본적인 절차와 유사하지만 안전성 활동을 수행하기 위한 구체

적인 기술단계들과 각 단계별 주요한 입출력 문서들을 함께 표현한 것으로 실제 열차제어시스템에 적용하기 쉽도록 보다 구체화한 절차라 할 수 있다. 이러한 안전성 활동 절차는 위험원 도출 및 리스크 분석과정을 통해 시작되어지게 되고, 이 활동을 통해 위험원 목록(Hazard Log)과 안전요구사항(Safety Requirement)이 도출되게 된다. 안전성 활동의 결과물로서 가장 중요한 문서 중의 하나인 위험원 목록은 두 번째 단계인 위험원 도출 단계에서 생성되며, 안전성 활동 각 단계에서 지속적으로 업데이트 되어야 하는 문서이다.

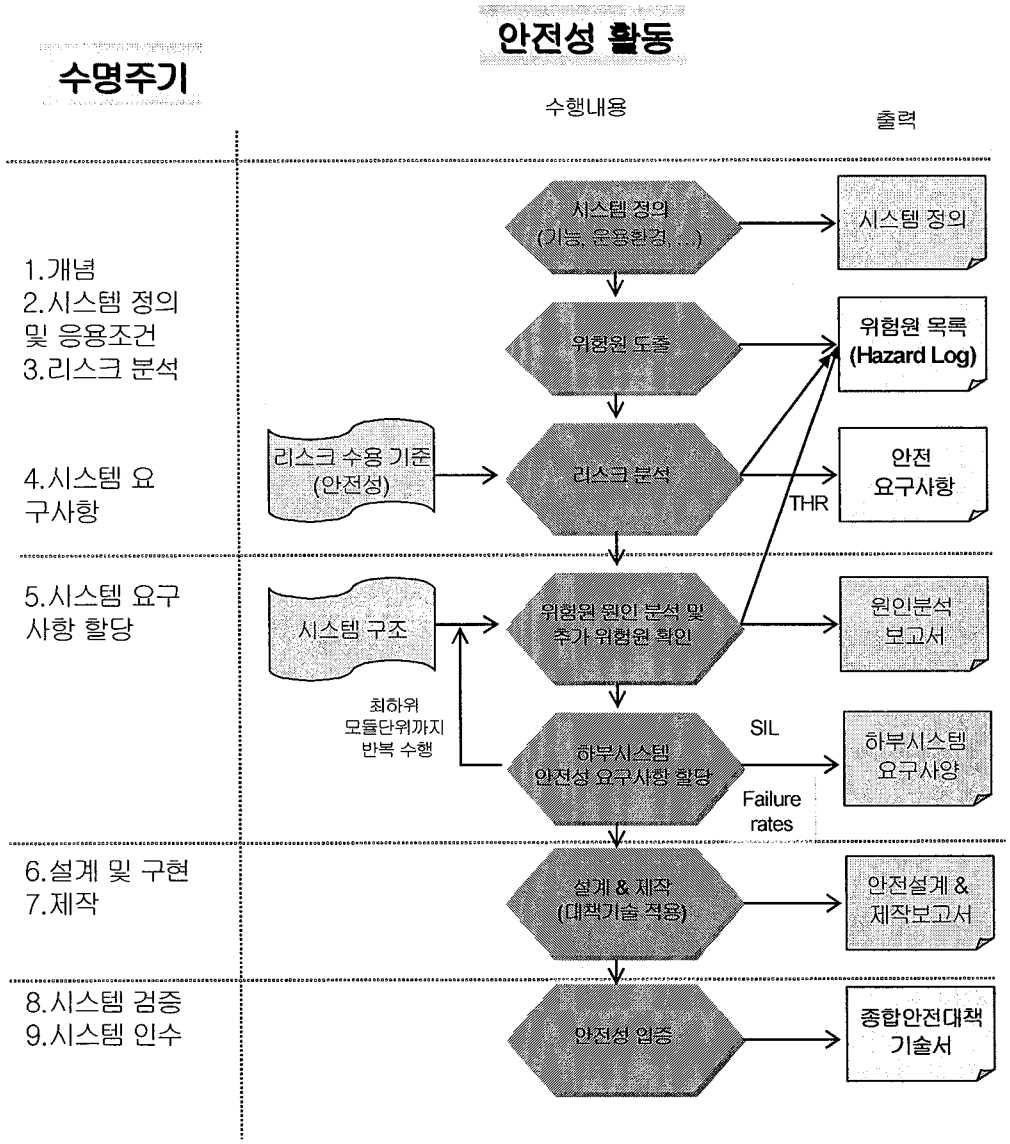


그림 3.1.2 시스템 수명주기에서의 열차제어시스템 안전성 활동 체계(안)

또한 세 번째 단계인 리스크 분석 단계에서는 위험원별 리스크를 예측 및 분석하고, 동시에 수용 가능한 리스크 기준(Tolerable Risk Criteria) 입력과과 비교를 통해 수용가능한 리스크 기준을 초과하는 위험원에 대해서는 이를 제거 또는 기준 이하로 줄일 수 있는 안전요구사항이 도출되게 된다. 작성된 안전요구사항은 개발하는 시스템의 구조에 따라 하부시스템으로 각각 할당하게 되며, 이때 하부 시스템별로 안전무결성 등급(SIL : Safety Integrity Level)과 허용가능 위험측 고장률(THR : Tolerable Hazard Rate)로 표현되는 안전요구사항이 각각 할당되며, 이러한 할당된 안전요구사항을 바탕으로 시스템의 설계 및 제작이 이루어지게 된다. 시스템의 설계 및 제작 단계에서는 할당된 안전요구사항이 만족되도록 다양한 형태의 대책기술이 수립되어 반영되어야 한다.

최종적으로 이러한 일련의 안전성 활동을 통해 프로젝트 시스템이 안전한지에 대한 최종적인 안전성 입증을 위한 문서인 종합안전대책기술서(Safety Case)는 최종단계에서 작성하게 되고, 이 문서를 통해 시스템의 안전성을 평가 및 인증 받게 된다. 종합안전대책기술서에서는 기본적으로 안전성 활동 과정에서 생성된 위험원 목록에서 모든 위험원이 제거되었거나 리스크 수용수준 이하로 제어되었음이 확인 및 입증되어야 한다.

(다) 안전성 활동 기술체계 단계별 적용기술 제시

① 위험원 분석 기술

안전성 활동의 첫 번째 단계인 위험원 분석을 위한 기술에는 여러 가지 방법들이 있다. 이러한 방법들 중 앞 장에서 제시한 열차제어시스템을 위한 안전성 활동 절차에 적합한 방법의 도출하기 위해 본 논문에서는 위험원 분석 타입에 따라 분류하였다. 다음은 위험원 분석 타입을 나타낸 것이다.

- CD : Conceptual Design hazard analysis type
- PD : Preliminary Design hazard analysis type
- DD : Detailed Design hazard analysis type
- SD : System Design hazard analysis type
- OD : Operations Design hazard analysis type
- HD : Health Design hazard analysis type
- RD : Requirements Design hazard analysis type

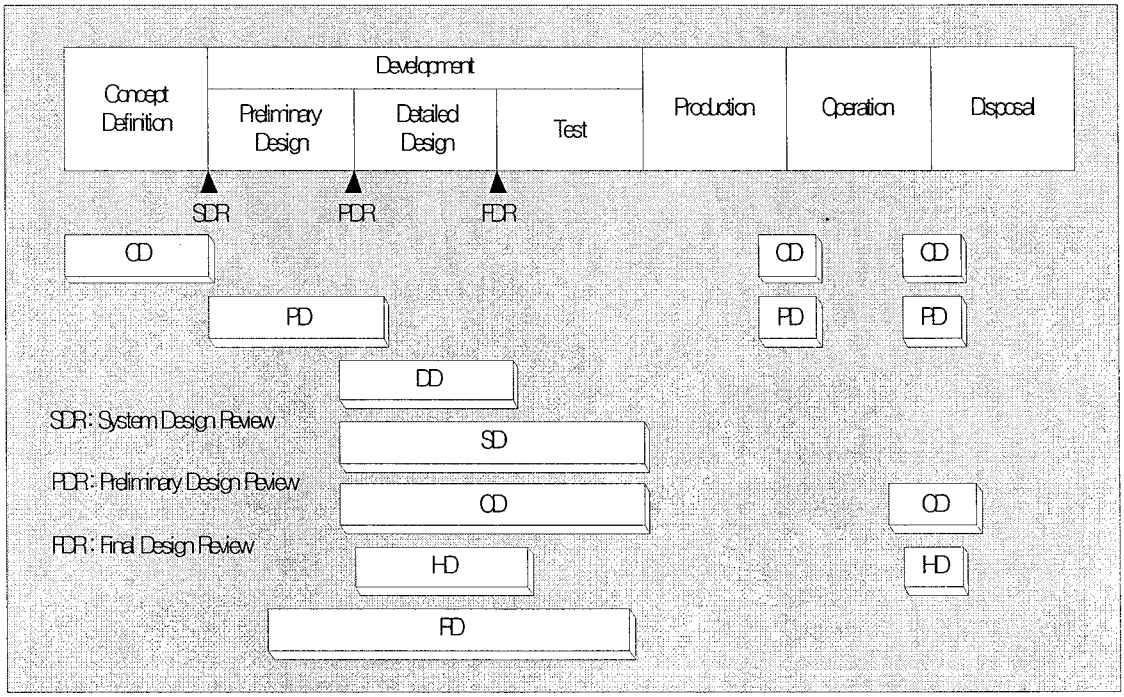


그림 3.1.3 시스템 수명주기에 따른 위험원 분석 타입의 분류

위험원 분석 타입은 전체 시스템 개발 수명주기에서 그림 3.1.3과 같이 배치되어 질 수 있다. 이처럼 수명주기 각 단계별 위험원 분석 타입이 조금씩 다르며, 이에 따라 수명주기별 또는 타입별 각각 다른 위험원 분석기술이 적용되는 것이 바람직한 접근 방법이다. 이러한 위험원 분석을 위한 방법에는 매우 다양한 방법들이 있으며 관련 국제 규격에서도 위험원 분석을 위해 표 3.1.2와 같이 다양한 방법들을 권고하고 있다.

표 3.1.2 IEC 62425에서의 위험원 분석 방법

기법/수단	SIL 1	SIL 2	SIL 3	SIL 4
PHA	HR	HR	HR	HR
FTA	R	R	HR	HR
FMECA	R	R	HR	HR
HAZOP	R	R	HR	HR

원인-결과 블럭도	R	R	HR	HR
ETA	R	R	R	R
인터페이스 위험원 분석	R	R	HR	HR

위험원 분석 기술은 표 3.1.2에서 제시한 방법 이외에도 매우 다양하며, 각각 고유의 특성을 지니고 있다. 그렇게 때문에 열차제어시스템에는 모든 기법들이 적용될 필요가 없으며, 특성에 맞게 적합한 기술을 선정되어야 한다. 표에서 제시한 방법 이외에 다음과 같은 방법들이 있다.

- PHL : Preliminary Hazard List
- SSHA : Subsystem Hazard Analysis
- SHA : System Hazard Analysis
- O&SHA : Operation & Support Hazard Analysis
- HHA : Health Hazard Analysis
- FaHA : Fault Hazard Analysis
- FuHA : Functional Hazard Analysis

앞에서 설명한 위험원 분석 타입과 분석 기술들 간의 비교분석 결과를 표 3.1.3과 같이 나타낸 것이다. 각 분석기법이 수행되는 수명주기의 단계를 그림 3.1.3을 활용하여 분석 타입으로 구분하였으며, 위험원을 도출할 수 있는지의 여부와 정량적·정성적 분석인지를 분석하여 제시하였다.

표 3.1.3 위험원 분석 방법 및 타입에 따른 관계

Technique	Type	Identify Hazard	Identify Root Causes	Lifecycle Phase	Qualitative/ Quantitative	Level of Detail
PHL	CD	Y	N	CD~PD	Qualitative	Minimal
PHA	PD	Y	P	CD~PD	Qualitative	Moderate to in-depth
SSHA	DD	Y	Y	DD	Qualitative	In-depth

SHA	SD	Y	Y	PD~DD~Test	Qualitative	In-depth
O&SHA	OD	Y	Y	PD~DD~Test	Qualitative	In-depth
HHA	HD	Y	Y	PD~DD~Test	Qualitative	In-depth
FTA	SD, DD	P	Y	PD~DD	Qualitative/quantitative	Moderate to in-depth
ETA	SD	P	P	PD~DD	Qualitative/quantitative	Moderate to in-depth
FMEA	DD	P	P	PD~DD	Qualitative/quantitative	In-depth
HAZOP	SD	Y	P	PD~DD	Qualitative	Moderate to in-depth
FaHA	DD	P	P	PD~DD	Qualitative	In-depth
FuHA	SD	P	P	CD~PD~DD	Qualitative	Moderate to in-depth

수명주기의 단계와 분석 타입에 따라 위험원 분석 활동이 수행되어지는데, 이때 같은 분석 타입에 중복되는 기법이 적용되는 것을 피하는 것이 적절하지만, DD 단계에서 적용할 수 있는 SSHA와 FMECA는 같이 적용하는 것이 더 효과적일 수 있다. 이유는 SSHA는 위험원을 추가적으로 도출할 수 있지만 정성적인 분석이 이루어질 수밖에 없고, FMECA는 위험원에 대한 정량적인 분석이 가능하기 때문에 SSHA와 상호 보완적으로 적용할 수 있기 때문이다. HAZOP 기법은 바이탈 제어 시스템의 위험원 분석을 위해 가장 많이 활용되는 기법 등의 하나이다. SHA, SSHA, O&SHA는 위험원 분석 기법으로 적용대상의 범위에 따라 분류되는 방법이다. 따라서 이러한 세 가지의 위험원 분석을 위해서는 FMECA나 HAZOP 기술들이 적용되어 질수도 있다.

이러한 검토를 바탕으로 본 논문에서는 열차제어시스템의 위험원 분석을 위해서

FMECA와 HAZOP 기법을 선정하였다. 이 중 HAZOP 기법은 화학공정 분야에서 개발되어 적용되어 온 방법으로, 입출력이 디지털이고 컴퓨터에 의해 제어되는 열차제어시스템에 적용하기에 다소 어려움이 있다. 당해연도에는 선행연구를 통해 철도의 열차제어시스템에 적합하도록 가이드워드를 보완하는 등 기존 방법을 변경한 새로운 방법을 HAZOP-KR(HAZOP for Korean Railway)을 적용하였다.

② 리스크 분석 기술

안전성 활동의 두 번째 단계인 리스크 분석은 앞 절에서 설명한 각종 방법에 의해 도출된 위험원들을 정량적으로 평가하여 리스크를 예측 및 분석하는 단계이다. 이러한 리스크 분석을 통해 다음 단계인 목표 THR과 SIL 등급의 할당되고, 이 후 목표 THR과 SIL 등급을 만족시키기 위한 리스크 제어 활동이 수행되게 된다.

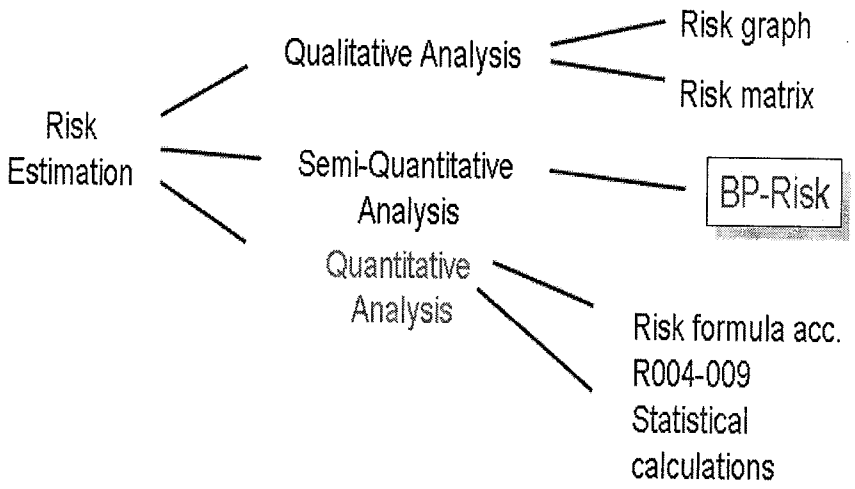


그림 3.1.4 리스크 분석 방법의 분류

이러한 리스크 분석 기법에는 그림 3.1.4와 같이 정량적인 방법과 정성적인 방법이 있으며, 일반적으로 정성적인 방법의 하나인 리스크 매트릭스(Risk Matrix) 기법이 널리 사용되고 있으며, 이 기법보다 좀 더 구체화한 방법인 리스크 그래프(Risk Graph) 기법 등이 유럽의 일부에서 사용되고 있다. 일반적으로 리스크 매트릭스 기법은 적용하기가 편리해 많은 프로젝트에 적용되고 있지만, 사고의 발생빈도와 심각도 두 가지 요소만을 가지고 리스크를 분석하며, 또한 이 두 가지 요소들도 전문가들의 자의적인

판단에 따라 결정되는 경우가 많다. 이러한 문제점으로 인해 본 논문의 연구에서는 준정량화된 방법의 하나로 BP-risk 방법을 적용하였다.

BP-risk 기법 또한 전문가들에 의한 자의적인 판단이 많지만 위험에 노출된 사람의 수, 열차의 속도, 사고유형, 위험원 지속시간, 운영조건 등 보다 많은 요소들을 고려함으로써 리스크 매트릭스 기법의 문제점을 다소 보완할 수 있는 장점이 있다. 이 BP-risk 기법과 적용방법은 선행연구 결과에 자세히 설명되어져 있다.

③ 안전성 활동 수행기술 및 적용 결과

앞에서 설명한 바와 같이 안전성 활동을 수행하기 위한 다양한 기법 및 기술들이 존재하지만, 각 기법별 고유한 특성들이 있다. 당해연도에는 앞에서 제시한 각 기법들을 본 과제에서 제작한 안전성 평가 대상시스템에 적용을 통해 열차제어시스템에 적합한 안전성 활동 절차와 각 단계별 적용기술을 포괄하는 안전성 활동 기술체계를 제시하였다.

앞에서 제시한 안전성 활동 절차 및 기술들을 적용하기 위한 대상시스템은 열차제어시스템의 주요한 기능인 간격제어 모듈(DCM :Distance Control Module), 진로제어 모듈(EIM : Electronic Interlocking Module) 그리고 현장설비와의 인터페이스를 위한 모듈(ICM : Interface Control Module)로 구성되어 있다. 이 대상 시스템을 통해 앞에서 제시한 안전성 활동 체계 및 이에 따른 단계별 수행기술에 대한 적용성 연구를 수행하였다.

표 3.1.4 단계별 위험원 분석 방법의 적용

Analysis Type	Coverage	Hazard Focus	Primary Analysis Tech.
CD	Conceptual design	System hazards	PHL
PD	Preliminary design	Systems hazards	PHA
DD	Detailed subsystem design	Subsystem hazards	FMECA, SSHA, IHA
DD, SD	Detailed subsystem design/ Integrated system design	Subsystem hazards/ Integrated system hazards	FTA

SD	Integrated system design	Integrated system hazards	SHA, HAZOP-KR
OD	Operational design	Operational hazards	O&SHA

표 3.1.5 PHL 결과 예

Preliminary Hazard List			
System Element Type : CRD system/CRD Interface			
No.	Hazard	Hazard Effects	Comments
PHL-1	현장신호설비 제어명령 처리 실패	오진로 설정 시 열차충돌, 진로설정 실패 시 열차지연, 진로취소 실패 시 열차충돌, 선로전환기 전환 실패 시 열차지연, 선로전환기 잘못된 방향으로 전환 시 열차충돌	현장신호설비 제어명령 -진로요청명령 -진로취소명령 -전체진로취소명령 -선로전환기 전환명령
PHL-2	블록제어명령 처리 실패	블록개방 실패 시 열차지연, 블록폐쇄 실패 시 유지보수자 인명사고	블록제어명령 -개방, 폐쇄
PHL-3	임시속도제한명령 처리 실패	임시속도제한 초과운행 시 열차탈선	
. . .	. . .	. . .	. . .

표 3.1.4는 위험원 분석 타입별 선정한 위험원 분석 기법을 나타낸 것이다. 이 표에서와 같이 적용되는 기술 중 분석타입이 중복되는 사항이 발견되지만 이는 보다 명확한 분석을 위해서 중복 적용이 가능할 수 있다. 위험원 도출 단계인 예비위험원 분석 활동(CD, PD)에서는 표 3.1.3과 표 3.1.4의 분석결과와 같이 PHL과 PHA 활동을 수행하도록 하였으며, 그 결과의 일부분을 표 3.1.5와 3.1.6에 나타내었다. 이러한 PHL과 PHA를 통해 도출된 위험원을 바탕으로 다음 단계(DD, SD)에서 SSHA, IHA를 수행하였다.

표 3.1.6 PHA 결과 예

No.	Hazard	Causes	Effects	R(B)	Recommended Action	R(A)
PHA-1	현장신호설비 제어명령 처리 실패	ATS로부터 비정상적인 진로설정 명령 입력	열차지연	2D	-진로제어명령에 대한 유효성 판단	4E
		선로전환기 상태 오류	열차지연, 열차충돌	1D	-연동처리 검증 -선로전환기 전환 검증 -선로전환기 상태 오류시 메시지 출력	3E
		진로-큐(DB) 오류	열차지연	3C	-진로-큐 에러시 메시지 출력	4E
		CRD 소프트웨어 내부적 오류	열차지연, 열차충돌	1C	-시스템 이중계 -운영 전 테스트 수행	2D
PHA-2	블록제어명령 처리 실패	열차위치 분실정보 누락	열차충돌	1D	-열차위치검지 실패시 운영 매뉴얼 적용	2D
		ATS로부터 비정상적인 블록폐쇄 명령 입력	열차지연	2D	-블록폐쇄명령 유효성 판단	4E
		⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

표 3.1.7 HAZOP-KR 결과 예

Hazard5	안전속도를 초과하여 운행 중인 열차				
Parameter	Guideword	Deviation	Causes	Consequences	Mitigation
Interface	No	차상 인터페이스 불가	차상 무선 안테나 고장	열차간 충돌	안테나 이중계 구성
	Other	차상과 간헐적 인터페이스	환경요인으로 인한 무선통신 방해	열차간 충돌	차상과 3초간 인터페이스 두절시 열차정지
Action	No	열차제동 안함	운전자 해이	열차탈선/충돌	경고음 발생
	Early	구간최고속도전에 가속	운전자 정보 오류	열차탈선	경고음 발생, 운전자 교육
	Late	늦은 열차제동	운전자 정보 오류	열차탈선	경고음 발생,

					운전자 교육
Limit	More	열차최고속도 초과	열차제동장치 고장	열차탈선/충돌	관제사 열차고장정보 확인
	Less	제동력 미달	열차제동장치 고장	열차탈선	관제사 열차고장저보 확인
Outside	Other	강풍에 의한 과속	강풍에 의한 과속	열차탈선	날씨에 따른 열차간격 및 속도제어
Data	No	차상제어정보 없음	ATS 속도제어 명령 없음	열차탈선/충돌	경보 이벤트 출력

표 3.1.8 EIM 모듈의 SSHA 결과 예

Subsystem	EIM																							
Failure Identification			Failure Effect		S=E+V+A						D=T+C+H							U		S	THR	Recommended Action
Hazard	Failure mode	Cause	Subsystem	System	E	E 설명	V	V 설명	A	A 설명	T	T 설명	C	C 설명	H	H 설명	U	U 설명	DU		
Hazard-1	열차위치 확인 실패	EIM 처리 오류	열차진로 및 허용이동권한 설정 불가	열차충돌	5	충돌로 인한 다수 사상	4	최대운행속도	5	열차간 충돌	1	유효성 검사	3	평균적인 수준	4	인적조정조건 필요	-1	중앙제어설비	21	10^{-9}	EIM 이중계 구성
		└ EIM 처리 모듈 오류			5	충돌로 인한 다수 사상	4	최대운행속도	5	열차간 충돌	1	DCM에서 검지	3	평균수준	4	충분한 시간 필요	-1	중앙제어설비	21	$4x10^{-9}$	ICM이중계구성 무중단계절체
		└ EIM 서브랙 고장			5	충돌로 인한 다수 사상	4	최대운행속도	5	열차간 충돌	1	DCM에서 검지	3	평균수준	1	계절체	-1	중앙제어설비	18	10^{-9}	ICM이중계구성 무중단계절체
		IHA에서 분석함																				
	열차속도 정보 획인실패	EIM 처리 오류	DCM 열차속도정보 처리 불가	열차충돌 및 탈선	5	충돌로 인한 다수 사상	5	최대운행속도 초과	5	열차간 충돌	1	유효정 검사	3	평균적인 수준	4	인적조정조건 필요	-1	중앙제어설비	22	$4x10^{-9}$	EIM 이중계 구성
		└ EIM 처리 모듈 오류			5	충돌로 인한 다수 사상	5	최대운행속도 초과	5	열차간 충돌	1	DCM에서 검지	3	평균수준	4	충분한 시간 필요	-1	중앙제어설비	22	$4x10^{-9}$	ICM이중계구성 무중단계절체
		└ EIM 서브랙 고장			5	충돌로 인한 다수 사상	5	최대운행속도 초과	5	열차간 충돌	1	DCM에서 검지	3	평균수준	1	계절체	-1	중앙제어설비	19	10^{-9}	ICM이중계구성 무중단계절체

앞에서도 설명하였듯이 SSHA와 IHA를 위해서는 FMECA 방법을 적용하였고, 또한 시스템의 상세한 위험원 도출 및 분석을 위해 HAZOP-KR을 적용하였으며 그 결과는 표 3.1.7과 같다. SSHA와 IHA는 기본적으로 FMECA 기법을 적용하였으며, 실제 본 연구에서는 앞에서 설명한 BP-risk 기법과 결합한 형태의 템플릿을 적용하였다. 표 3.1.8은 CRD 시스템의 하부 모듈인 EIM 모듈에 대한 SSHA 결과

로서, 전체적으로는 FMECA를 수행하면서 리스크 분석을 위해 을 적용하였다. 표 3.1.8에서와 같이 BP-risk를 위한 각종 매개변수(S, D, U)를 도출하고, 이 매개변수를 합한 값(S+D+U)을 가지고 이 값과 THR과의 변환 표를 통해 각 위험원별 THR이 최종적으로 계산되어지게 된다. IHA는 SSHA와 동일한 방법으로 분석을 수행하는 기법으로 분석대상이 인터페이스 관련 위험원이 된다.

BP-risk 방법에 의해 리스크 분석이 이루어지게 되면, 위험원별 THR이 도출되게 된다. 그 이후 발생 가능한 모든 가능한 위험요인들을 결정하기 위해 FTA 기법을 적용하였다. 그림 3.1.5는 CRD 시스템의 최상위 위험원에 대한 FTA 결과를 나타낸 것으로, 앞 단계에서 도출된 위험원별 각각 FTA를 수행하였다. 이 FTA 수행을 통해 위험요인에 대한 분석 뿐 아니라 리스크 분석을 통해 도출된 THR을 하부 위험요인이나 하부 모듈들로 할당이 가능하게 된다. 즉, 리스크 분석을 통한 위험원별 THR이 FTA 과정을 통해 하부 기능모듈별로 각각 할당되게 되며, 이러한 과정을 통해 하부 시스템별 THR 및 SIL 등급이 할당되어지게 된다.

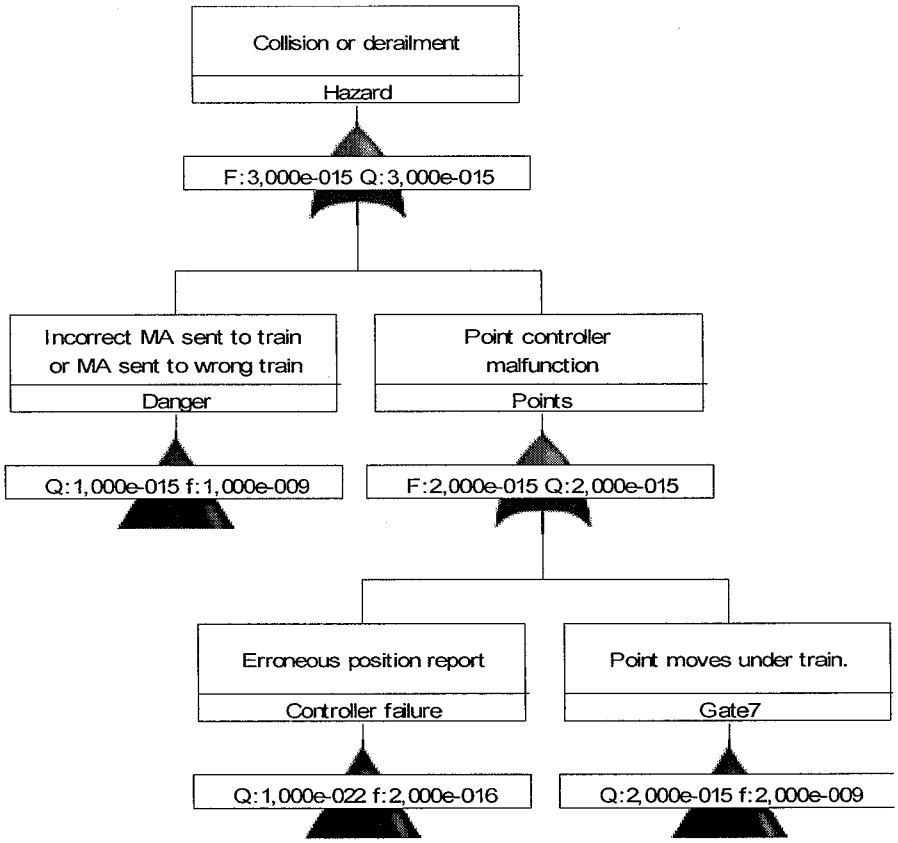


그림 3.1.5 Top 레벨에서의 FTA 분석 결과 예

철도시스템 안전성 활동 관련하여 각 단계별 적용 가능한 많은 기법들이 있지만, 각 기법별 특징들이 있고 또한 적용하기에 적합한 대상이 별도로 있는 경우도 있다. 이러한 특징으로 인해 각 기법이나 기술들을 상호 보완적으로 적용해야 하는 방법들도 있다. 본 연구에서는 관련된 국제규격 및 선행연구의 분석 등을 통해 국제규격의 요구사항을 준수하면서 열차제어시스템에 적합한 안전성 활동 절차 및 이에 따른 적용 기술 및 기법들을 제시하였다. 또한 CRD라는 대상 시스템에 적용을 통해 제시한 절차 및 기법들의 적합성을 확인하였다.

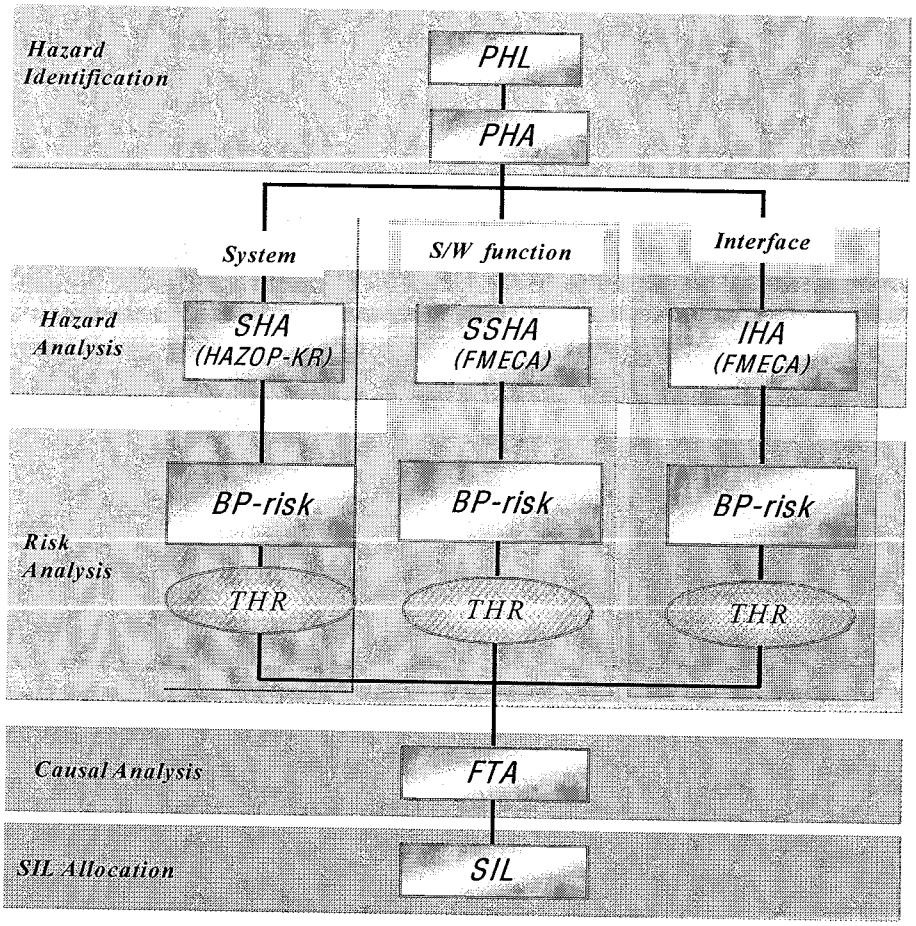


그림 3.1.6 열차제어시스템 안전성 활동 체계에 따른 적용기술

이를 통해 본 연구에서는 국내 열차제어시스템을 국제규격에 적합한 안전성 활동 절차 및 이에 따른 기술을 포괄하는 안전성 활동 기술체계를 그림 3.1.6과 같이 제시하였다. 그림 3.1.6은 본 연구에서 제시하는 열차제어시스템을 위한 안전성 활

동 절차 및 각 단계별 적용기술과 기법들을 나타낸 것으로, 위험원 도출에서부터 SIL 할당까지를 나타내고 있다. 그림에서와 같이 PHL과 PHA 템플릿을 적용하여 위험원 도출을 하고, 또한 이 단계에서 도출된 기본 위험원을 바탕으로 상세한 위험원 도출 및 분석을 위해 HAZOP-KR과 FMEA 기법을 병행하여 적용하는 것으로 제시하였다. HAZOP-KR은 열차제어시스템에 적합하도록 변경한 기법으로 시스템 측면의 상세 위험원 도출 및 분석에 적용하고, 시스템의 기능 및 인터페이스관련 위험원은 FMECA 기법을 적용하였다. 이처럼 HAZOP-KR과 FMECA 기법은 그 특성에 따라 위험원 분석을 위해 상호 보완적으로 활용하도록 하였다. 이 단계 이후에서는 BP-Risk를 통한 위험원별 THR 도출 및 이를 통한 SIL 할당을 하도록 하였다. 이 이후에는 할당된 SIL 및 THR을 바탕으로 이를 만족하기 위한 시스템의 안전대책 설계 및 제작이 이루어지게 된다.

(2) 위험원 분석 방법(HAZOP-KR)

국제규격에 의해 요구되는 안전성 확보를 위해서는 시스템 수명주기에 따른 안전성 활동이 필요하다. 이러한 안전성 활동은 예비 위험원 분석 단계, 리스크 분석(Risk Analysis) 단계와 이러한 위험원 및 리스크 분석 결과를 바탕으로 설계에 반영하는 위험원 제어 단계 등 여러 단계로 구성되어진다. 이러한 여러 단계 중 전체 안전성 활동의 기본이 되는 위험원 도출을 위해서는 국제 규격인 IEC 62425에서는 철도시스템의 위험원 분석을 위해 HAZOP(Hazard and Operability Studies) 기법의 적용을 권고(HR : Highly Recommend)하고 있다. 또한 영국의 철도시스템 안전성 활동 지침서에 해당하는 Yellow Book에서도 HAZOP 방법을 권고하고 있다. 이러한 HAZOP 기법은 위험원의 도출을 위한 형식화된 기술로서, 국내의 일부 선행연구에서는 열차제어시스템의 위험원 도출을 위해 HAZOP 방법이 적용된 사례가 있다.

하지만 국제 규격화된 HAZOP 방법은 화학 플랜트 산업에서 처음 고안되어 발전되어 왔기 때문에 기존의 매개변수(Parameter)와 안내어(Guide word)를 열차제어시스템에 그대로 적용하기에는 적합하지 않은 요소로 인해 그 적용효과 및 효율이 떨어진다. 따라서 본 논문에서는 기존의 HAZOP 방법을 유지하면서 열차제어시스템의 위험원 분석에 효과적으로 적용할 수 있는 매개변수와 안내어를 제안하였으며, 이를 본 연구에서는 HAZOP-KR(HAZOP for Korean Railway)로 명명하였다.

(가) 위험원 분석 기술

① 시스템 위험원

시스템의 위험원은 인명의 사상, 시스템의 손상 및 손실 등을 유발시킬 수 있는 잠재적인 위험요소들을 의미한다. 즉 위험원은 사고를 발생시킬 수 있는 시스템 내부의 결함 또는 외부적인 요인들을 나타낸 것으로, 사고에 직접적인 관련이 있다. 그림 3.1.7은 위험원과 사고의 관계를 나타낸 것으로, 각 구성요소들(HE : Hazardous Element, IM : Initiating Mechanism, T/T : Target and Threat)의 바퀴 구멍들이 모두 정확하게 정렬하게 될 경우 위험원은 잠재적인 사고에서 실제의 사고로 발전하게 된다.

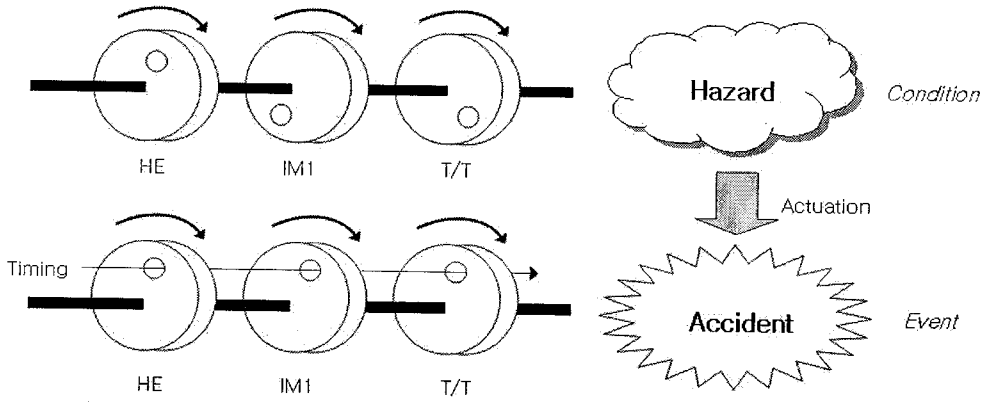


그림 3.1.7 위험원과 사고와의 관계

시스템은 의도된 기능이나 역할을 수행하기 위한 목적을 위해 설계되고 제작된 것이다. 그러나 시스템은 의도하지 않거나 바람직하지 못한 기능을 수행할 수 있는 원천적인 설계 결함 또는 외부환경이나 인적인 운용상의 결함들을 포함할 수 있다. 이러한 결함들이 그림 3.1.7처럼 사고로 발전하여 위험원이 될 수 있고, 이 위험원들은 시스템 설계자가 확인하기가 쉽지 않으며, 안전성 활동의 하나인 위험원 도출 및 분석과정을 통해 식별 될 수 있다. 철도 관련된 국제 규격에서는 안전성 확보 및 입증을 위해 기본적으로 위험원의 도출 및 분석을 기본으로 하는 안전성 활동을 요구하고 있다. 따라서 이러한 위험원의 도출 및 분석이 열차제어시스템의 안전성 확보에 필수적이다.

② 위험원 분석 기술

국제규격에서 정의하는 열차제어시스템의 안전성 활동은 개발되는 열차제어시스템이 내재하고 있는 잠재적 위험원을 찾아 제거하거나 허용수준 이하로 줄일 수 있도록 대책을 수립하고 이를 시스템의 설계 및 개발에 반영하는 모든 일련의 활동을 의미한다.

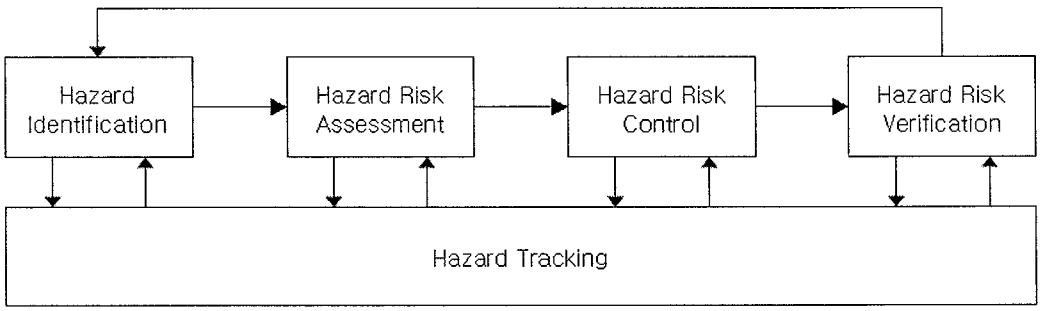


그림 3.1.8 위험원 관리 절차

그림 3.1.8은 이러한 위험원 관리 측면에서의 안전성 활동 과정을 간략하게 나타낸 것이다. 즉, 시스템의 안전성 활동은 위험원 도출, 리스크 평가, 그리고 위험원이 나타내는 허용 가능한 수준으로 관리하기 위한 리스크 제어, 그리고 이의 확인 과정이 필요하다. 이 절차는 각 단계가 항상 피드백 되어 위험원이 도출, 허용 가능한 수준이 되도록 제어하고 검증될 때까지 반복 수행되게 된다.

앞에서 설명한 바와 같이 열차제어시스템의 안전성 활동은 위험원 도출을 기본으로 하며, 도출된 위험원의 분석 및 제어하는 과정이다. 이러한 위험원을 도출하기 위한 활동 및 방법에는 PHL(Preliminary Hazard List), PHA(Preliminary Hazard Analysis), HAZOP, FMEA(Failure Mode Effect Analysis) 등과 같은 매우 많은 기법들이 있다. 이러한 기법들 중 PHL과 PHA는 초기 위험원 확인을 위한 방법들이며, 이 초기 단계의 도출된 위험원을 바탕으로 한 상세한 위험원 도출방법으로 FMEA, HAZOP이 사용된다. 이 두 가지 기법은 위험원 도출을 위한 이상현상의 분석기준을 FMEA에서는 고장모드(Failure Mode), HAZOP에서는 안내어를 사용한다는 점에서 차이가 있다. 일반적으로 시스템 내부의 위험원은 완벽하게 식별될 수 없다. 따라서 여러 가지 방법들을 고루 사용하는 것이 최선이며, HAZOP과 FMEA는 서로 상이한 관점으로써 상호보완적으로 사용되어질 수 있다. FMEA를 위해

서는 초기에 구성요소의 고장모드와 이로 인한 영향에 대한 분석을 기초로 하는 방법으로 그림 3.1.9와 같이 표현할 수 있다. HAZOP은 설계개념으로부터 벗어난 상황(결함)에서부터 시작하여, 이 결함에 대하여 가능한 원인과 결과를 분석하는 방법으로 그림 3.1.10와 같다.

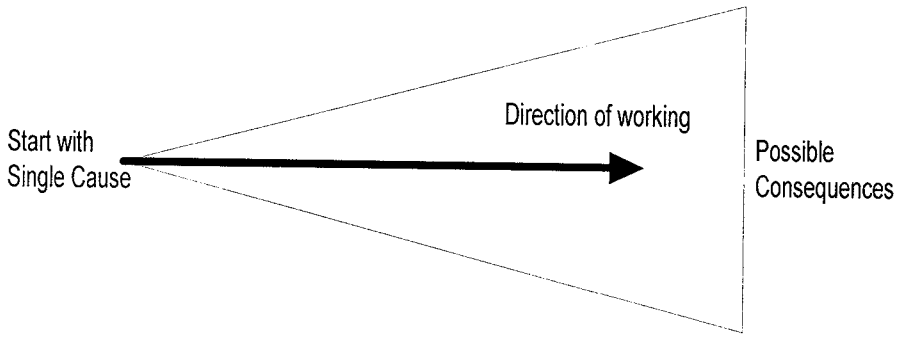


그림 3.1.9 FMEA(From cause to results)의 수행 방향

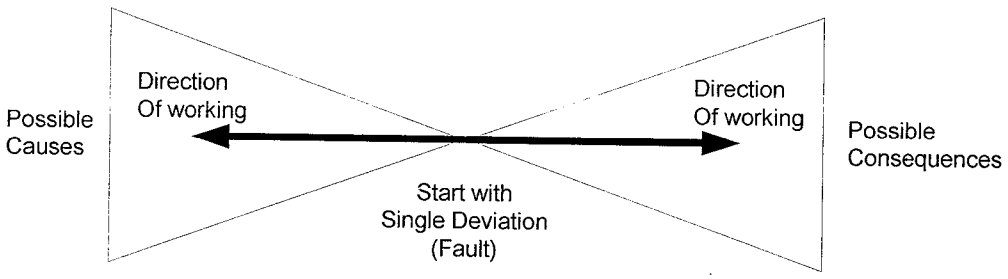


그림 3.1.10 HAZOP Study(Bidirectional analysis)의 수행 방향

이 두 기법 중에서 HAZOP 기법은 위험원의 식별을 위한 형식화된 방법으로서 열차제어시스템 안전관련 국제규격인 IEC 62425와 영국철도의 Yellow Book 에서 HAZOP 기법을 위험원 분석을 수단으로 활용할 것을 권고하고 있다. 본 논문은 안전성 활동에서 가장 기본이 되는 단계인 위험원 도출을 위한 HAZOP 기법의 열차제어시스템 적용기술을 대상으로 연구하였다.

(나) 일반 HAZOP 기법

HAZOP 기법은 앞에서 설명한바와 같이 위험원 도출을 위한 형식화된 시스템적 기법으로서 특정 파라미터가 안내어에 따라 벗어났을 경우에 대한 결과와 원인의 분석한다. 위험원 도출에서 가장 중요한 기술은 위험원의 원인과 결과를 분석하는

것으로, 이러한 단계에서 HAZOP을 이용하면 안전성 분석절차 초기에 유용하게 위험원을 도출할 수 있다. HAZOP은 시스템의 위험원들을 도출하기 위해 안내어(Guideword)라는 개념을 사용한다. More, No, Less 등과 같은 안내어들은 위험원을 도출하는 과정에서 시스템의 여러 상태와 결합되어 설계의도에서 벗어날 수 있는 이상현상(Deviation)들을 식별하여 위험원의 발생을 찾게 된다. HAZOP의 목적은 계획된 운영 의도부터 안내어의 특수한 사용에 이르기까지 일어날 수 있는 시스템의 이상현상들을 분석하고 확인하는 것이다. 이런 잠재적인 시스템 이상현상이 사고로 발전할 수 있다.

HAZOP study 대상:								
참조도면번호:				경신번호:			소요시간:	
참여구성원:							회의일시:	
기능	Guide Word	이상현상	원인	결과	안전대책	기타사항	세부조치내역	조치의 주체
	No							
	More							
	Less							
	As well as							
	Part of							
	Reverse							
	Other than							
	Early							
	Late							
	Before							
	After							

이상현상 유형	안내어 (Guide word)	의미
부정	No	명령이 실행되지 않는 상태
정량적 변형	More	수량의 비정상증가
	Less	수량의 비정상 감소
정성적변형	As well as	기대하지 않은 동작수행
	Part of	완전한 수행을 하지 못함
대체	Reverse	목적과 반대되는 결과도출
	Other than	목적과 다른 결과도출
시간	Early	예상시간보다 일찍 발생
	Late	예상시간보다 늦게 발생
명령 또는 흐름	Before	예상순서보다 일찍 발생
	After	예상순서보다 늦게 발생

그림 3.1.11 일반 HAZOP Study 템플릿

HAZOP은 설계 의도로부터 어떻게 이상현상이 발생할 수 있는지 입증하기 위해 시스템에 대해 충분히 설명하고, 그에 대한 모든 부분을 체계적으로 조사하는 것을 포함한다. 일단 확인이 되고나면, 분석은 그러한 이상현상과 이에 따른 결과들이 시스템의 안전하고 효율적인 운영에 부정적인 영향을 줄 수 있는지에 관하여 행해진다. 앞에서 언급하였듯이 HAZOP 기법은 그림 3.1.11과 같은 매개변수(Parameter, 이상현상 유형)와 안내어를 사용한다. 매개변수는 적용대상 시스템의 기능이 기대하지 않는 동작이 수행되는지와 이의 원인 및 결과를 체계적으로 분석하기 위한 기능으로서 6가지로 분류되어 있고, 이 매개변수는 다시 11가지의 세부

적인 안내어로 분류되어 있다. 일반적인 안내어는 적용대상에 대한 11가지 상태에 대하여 세분화되어 있다. 이상현상이 파악되면 우선적으로 예측되는 원인과, 이상현상으로 인해 발생되는 최종사고를 '결과'에 기록하고, 파악된 원인의 발생을 억제하기 위한 안전대책 및 안전대책의 실시주체와 확인여부를 정리한다.

이러한 일반적인 HAZOP 기법은 최초에 화학공정에서 개발되어 발전되어 온 기법으로서, 그림 3.1.11에서 나타낸 바와 같이 매개변수와 안내어들이 정성적인 변형량의 변화 등과 같은 항목들로 구성되어 있다. 그림에 나타낸 파라메터와 이에 따른 안내어는 액체나 가스 등의 제어가 일반적인 화학공정에는 적합하지만, 제어출력이 거의 대부분 디지털 신호이고 제어대상도 디지털 값들로 대부분 이루어진 열차제어시스템의 경우 이러한 일반적인 매개변수와 안내어를 적용하기에는 적합하지 않은 부분이 있다. 이러한 적절하지 않은 매개변수와 안내어로 인해 열차제어시스템의 위험원 분석에 있어서 HAZOP 기법의 장점을 잘 살리지 못하거나, 안내어의 일부분을 임의로 해석해서 적용하는 등의 문제점을 가지고 있다.

(다) HAZOP-KR

① HAZOP-KR 개요

앞에서 설명하였듯이, 기존의 화학공정의 위험원 분석에 적합하도록 제시되어 있는 파라미터와 안내어를 기반으로 하는 HAZOP 기법은 열차제어시스템의 위험원 분석에 바로 적용하기에는 부적합한 부분이 있다. 즉, 디지털 제어기반의 열차제어시스템은 온도, 압력, 액체 등에 기반을 둔 More, Less 등과 같은 정량적인 변화에 따른 이상현상의 분석으로는 정확한 위험원 분석에 한계가 있다. 즉, 열차제어시스템은 선로변, 차상, 제어센터 등 다양한 위치에 많은 설비들이 인터페이스를 통해 종합적으로 운영되어지고 있고, 입출력신호가 거의 대부분 디지털 신호로 구성되어 있다. 또한 열차제어시스템은 열차 안전운전을 담당하는 설비로서 비상시 대응절차와 이에 따른 시스템에의 반영내용 등에서 위험원이 중요한 문제가 되는 등 일반적인 화학공정 시스템과는 다른 특성을 가지고 있다.

본 연구에서는 기존의 HAZOP 개념 및 절차를 그대로 활용하면서, 열차제어시스템에 적용하기 적합하도록 새로운 매개변수와 안내어를 제안하였으며, 이를 HAZOP-KR이라 하였다. 이에 따라 실제 열차제어시스템의 위험원 한 가지에 대한 적용 사례를 기술할 것이다.

② 매개변수의 정의

HAZOP 기법에서의 매개변수는 안내어를 적용할 수 있는 물리적, 시간적, 운영적인 변수들을 의미하며, 플랜트 산업에서는 다음과 같이 특정 매개변수와 일반 매개변수로 구분하여 적용하고 있지만, 이러한 매개변수들은 열차제어시스템에는 적합하지 않은 부분들이다. HAZOP-KR에 적용하기 위한 매개변수를 표3.1.9과 같이 제안하였다.

표 3.1.9 HAZOP-KR 파라메터

No.	Parameter	Description
1	Interface	· 지상설비와 차상설비 간 데이터 인터페이스 · 지상 운영자와 차량 운전자간 통신 인터페이스 · 서브시스템 간 데이터 인터페이스 · 관련 시스템 간 데이터 인터페이스 · 지상 운영자(시스템)와 유지보수자간 통신 인터페이스
2	Time	· 열차스케줄에 의한 열차운행 시간 · 현장설비의 동작 시간 · 소프트웨어 데이터 처리 시간 · 일반적으로 정의된 시간
3	Action	· 운영자, 운전자, 유지보수자 조작 · 현장설비의 동작 · 차상설비의 동작
4	Limit	· 열차 속도 한계 · 선로 용량 한계 · 소프트웨어적 데이터 처리 한계 · 인적 노동 한계 · 설비의 가용성 및 신뢰성 한계
5	Procedure	· 운영, 운전, 유지보수 절차 · 비상시 대응 절차
6	Outside	· 자연현상 (지진, 태풍, 눈, 비, 바람 등) · 승객 행동 · 의도적인 외부 장애요건

7	Data	· 제어명령 (열차제어, 현장설비제어 등) · 현장정보 · Database 정보

③ 안내어의 정의

일반적인 HAZOP 안내어는 표 3.1.10와 같다. 표와 같이 가스나 액체의 양적 변화량 등이 주요한 안내어로 구성되어 있어, 이러한 안내어를 열차제어시스템에 바로 적용하기가 어렵다. 이러한 안내어를 바로 적용할 경우 안내어의 기능을 열차제어시스템에 맞게 임의로 변경하여 적용할 수 있는데 이럴 경우 열차제어시스템의 특성을 반영하고 있지 않기 때문에 체계적인 위험원 분석이 이루어질 수 없다. 따라서 표 3.1.11과 같은 열차제어시스템에 적합한 안내어를 제안하였다.

표 3.1.10 기존 HAZOP Study의 Guide word

Guide word	Description
No, Not, None	매개변수가 없거나, 동작이 없음
More	어떤 특정 매개변수가 양적으로 증가함
Less	어떤 특정 매개변수가 양적으로 감소함
Reverse	설계의도와 반대로 수행됨
As well as	설계의도 외의 매개변수가 부가됨
Parts of	설계의도대로 완전히 이루어지지 않음
Other than	설계의도가 완전히 바뀜

표 3.1.11 HAZOP-KR의 Guide word

Guide word	Description	관련 Parameter
No, Not, None	정의된 매개변수가 없음.	Interface, Time, Action, Limit, Procedure,

		Data
Part of	일부만 수행되거나, 고려됨	Action, Procedure, Outside, Data
Early	정의된 시간보다 일찍 수행됨	Time, Action, Data
Late	정의된 시간보다 늦게 수행됨	Time, Action, Data
More	변수의 초과 및 증가	Limit, Data
Less	변수의 미달 및 감소	Limit
Other than	비정상적인 매개변수	Interface, Action, Limit, Procedure, Outside, Data

④ 이상현상(Deviation)

앞에서 정의한 매개변수와 안내어의 조합으로 열차제어시스템에서의 이상현상을 정의하면 표 3.1.12과 같다.

표 3.1.12 HAZOP-KR의 Deviation

Deviation	No	Part of	Early	Late	More	Less	Other
Interface	Interface 불가						비정상적인 Interface
Time	정의된 시간이 없음		정의된 시간보다 빠름	정의된 시간보다 늦음			
Action	동작하지 않음	일부만 동작	빠른 조작 및 동작	늦은 조작 및 동작			기타 비정상적인 조작 및 동작
Limit	정의된 한계 없음				정의된 한계를 초과함	정의된 한계에 미달됨	기타 비정상적인 한계
Procedure	절차없음	절차 일부만 존재함					비정상적인 절차
Outside		외부요인이 일부작용함					비정상적인 외부 요인
Data	Data 없음	Data 일부만 생성 송신 수신	빠른 Data 생성 송신 수신	늦은 Data 생성 송신 수신	Data 생성, 송신 초과함		기타 비정상적인 Data

(라) HAZOP-KR의 적용

앞에서 설명한 새로운 HAZOP-KR 기법을 국내 열차제어시스템의 위험원 분석에 적용을 통한 연구를 위한 대상 시스템은 다양한 철도시스템 중 신호관련 열차제어시스템으로써 하드웨어와 소프트웨어 모두에 대해 안전성 활동을 수행할 수 있다. 연구 대상시스템은 연동로직을 통한 열차진로제어와 열차간격제어를 수행하는 CRD(Control Route & Distance)으로 하였다. CRD 시스템을 대상으로 위험원 분석을 위한 다음과 같은 최상위 위험원을 도출하였다.

- 정의된 최소 열차간격 이하로 열차 간 접근 : 이 위험원은 CRD 시스템의 열차간격제어 기능의 실패로 인해 발생할 수 있는 상황으로 열차간 충돌의 가능성이 높다.
- 열차의 안전속도를 초과하는 열차 : 이 위험원은 CRD시스템의 열차간격제어와 관련되어 CRD시스템의 열차 속도제어 실패 시, 열차 간 충돌의 가능성이 높다.
- 정의된 진로가 아닌 진로/방향으로 운행하는 열차 : 이 위험원은 CRD 시스템의 열차진로제어 기능의 실패로 인해 발생할 수 있는 상황으로 열차 간 충돌이나 탈선의 가능성이 높다.

HAZOP-KR Study는 앞에서 설명한 위험원에 대해 그 원인을 파악하고 그에 대한 대책을 수립하는 분석기법으로 CRD 시스템의 구성단계에서 수행되었다. 이를 위해 앞 장에서 설명한 열차제어시스템에 적합한 새로운 매개변수와 안내어를 적용하여 HAZOP을 수행하였다.

표 3.1.13 HAZARD-1의 HAZOP-KR 분석 결과

Hazard-1	정의된 최소 열차간격 이하로 열차 간 접근					
매개변수	Guide word	Deviation	Causes	Description	Consequences	Mitigation
Interface	No	Interface 불가	열차의 위치 확인 실패	열차의 위치확인 불가로 열차 간 접근을 확인할 수 없음.	열차충돌	열차와의 인터페이스 불가시, 열차 비상정지
			열차 속도정보 확인 실패	열차와의 인터페이스 불가로 열차의 속도를 확인할 수 없음	열차충돌	열차와의 인터페이스 불가시, 열차 비상정지
			열차 고장정보 확인 실패	열차의 고장정보 확인 불가로 열차의 고장유무를 확인할 수 없음	열차충돌	열차와의 인터페이스 불가시, 열차 비상정지
			열차 이동권한 전송	열차이동권한 차상으로	열차충돌	열차와의 인터페이스 불가

			실패	전달하지 못함		시, 열차 비상정지
Action	No	동작하지 않음	선로전환기 전환 실패	선로전환기가 작동하지 않아 안전하지 못한 방향으로 열차 진입	열차충돌	선로전환기 고장정보 확인
	Other	비정상적인 동작	선로전환기 오방향 전환	선로전환기가 잘못된 방향으로 전환되어 안전하지 않은 진로로 진입	열차충돌	선로전환기 고장/방향정보 확인
Limit	More	한계 초과	열차 안전속도 초과	열차 과속으로 인한 안전제동 실패	열차충돌	열차 속도 초과 시, 열차 운행속도 제어
Data	No	Data 없음	열차 이동권한 설정 실패	안전하지 못한 열차이동권한 설정으로 열차간 접근	열차충돌	CRD 시스템 이중계 설계
	Other	비정상적인 Data	열차 진로설정 오류	열차의 잘못된 진로설정으로 인해 타 열차와 접근	열차충돌	CRD 시스템 이중계 설계
			선로전환기 전환 명령 오류	선로전환기의 비정상적인 전환으로 인해 안전하지 못한 진로로 열차 진입	열차충돌	CRD 시스템 이중계 설계

표 3.1.14 HAZARD-2의 HAZOP-KR 분석 결과

Hazard-2	열차의 안전속도를 초과하는 열차					
Parameter	Guide word	Deviation	Causes	Description	Consequences	Mitigation
Interface	No	Interface 불가	열차 속도정보 확인 실패	열차와의 인터페이스 불가로 열차의 고장유무를 확인할 수 없음	열차충돌 및 탈선	열차와의 인터페이스 불가 시, 열차 비상정지
			열차 고장정보 확인 실패	열차의 고장정보 확인 불가로 열차의 고장유무를 확인할 수 없음	열차충돌	열차와의 인터페이스 불가 시, 열차 비상정지
Data	Other	비정상적인 Data	열차임시속도 설정 오류	CRD 시스템의 열차임시속도 설정 오류로 열차 과속	열차충돌 및 탈선	CRD 시스템 이중계 설계

첫 번째 위험원에 대한 HAZOP-KR의 적용결과는 표 3.1.13와 같다. CRD 시스템의 주요 기능 중 하나인 열차간격제어 실패로 선·후행 열차의 간격이 좁아져 충돌이 발생할 수 있는 상황에 대한 원인과 대책이 수립되었다. 위험원에 적용할 수 있는 매개변수는 총 4가지, 안내어는 3 가지가 적용되었으며, 열차와의 인터페이스가 두절된 경우, 선로전환기의 방향전환 불가로 비정상적인 진로로 진입한 경우, 열차의 과속으로 인한 접근, 선로전환기 방향 전환 명령 오류가 발생한 경우로 분석되었다. 또한 분석된 각 위험요인에 대한 대책(Mitigation)이 분석되어졌으며, 이러한 분석결과는 시스템의 설계에 반영되어 해당 위험요인을 허용수준 이하로 제어되도록 하게 된다.

표 3.1.15 HAZARD-3의 HAZOP-KR 분석 결과

Hazard-3	정의된 진로가 아닌 진로/방향으로 운행하는 열차					
Parameter	Guide word	Deviation	Causes	Description	Consequences	Mitigation
Interface	No	Interface 불가	열차의 위치 확인 실패	열차의 위치확인 불가로 열차간 접근을 확인할 수 없음	열차충돌	열차와의 인터페이스 불가 시, 열차 비상정지
			열차진로설정 명령 수신 실패	ATS로부터 진로설정명령을 수신할 수 없음	열차정지	CRD시스템 이중계 설계
			열차 이동권한 전송 실패	열차이동권한 차상으로 전달하지 못함	열차충돌	열차와의 인터페이스 불가 시, 열차 비상정지
Action	No	동작하지 않음	선로전환기 전환 실패	선로전환기가 작동하지 않아 안전하지 못한 방향으로 열차진입	열차충돌	선로전환기 고장정보 확인
	Other	비정상적인 동작	선로전환기 오방향 전환	선로전환기가 잘못된 방향으로 전환되어 안전하지 않은 진로로 진입	열차충돌	선로전환기 고장/방향정보 확인
Data	No	Data 없음	열차이동방향 정보 실패	CRD시스템의 열차이동방향정보 누락	열차충돌	CRD 시스템 이중계 설계
			열차이동권한 설정 오류	열차진로설정과 다른 열차 이동권한 설정	열차충돌	CRD 시스템 이중계 설계
	Other	비정상적인 Data	열차 진로설정 오류	열차의 잘못된 진로설정으로 인해 타 열차와 접근	열차충돌	CRD 시스템 이중계 설계
			선로전환기 전환 명령 오류	선로전환기의 비정상적인 전환으로 인해 안전하지 못한 진로로 열차진입	열차충돌	CRD 시스템 이중계 설계

두 번째 위험원에 대한 HAZOP-KR 분석 결과는 표 3.1.14과 같다. CRD 시스템에서 출력되는 열차허용속도 제어명령과 입력되는 열차속도정보의 처리가 정상적으로 이루어지지 않을 경우 위험원이 발생할 수 있다. 위험원에 적용할 수 있는 매개변수와 안내어는 각각 2 가지가 적용되었으며, CRD와 열차 간 인터페이스가 두절되어 열차의 속도정보 및 고장정보를 확인할 수 없는 경우, CRD에서 열차허용속도 설정에 오류가 발생한 경우로 분석되었다.

세 번째 위험원인 정의된 진로가 아닌 진로·방향으로 운행하는 열차의 HAZOP 결과는 표 3.1.15와 같다. CRD 시스템의 주요 기능 중 하나인 열차진로제어 실패로 열차의 오진로 진입 및 잘못된 방향으로 열차의 이동이 발생할 수 있는 상황에 대한 원인과 대책이 수립되었다. 위험원에 적용할 수 있는 매개변수는 총 3가지, 안내어는 2가지가 적용되었으며, CRD와 열차 간 인터페이스가 두절되어 열차의 위치정보를 확인할 수 없거나 이동권한을 전송할 수 없는 경우, 선로전환기의 비정상적인 동작 그리고 비정상적인 제어명령으로 인한 경우로 분석되었다.

HAZOP-KR을 통한 위험원 분석은 CRD 시스템의 최상위 기능의 정의로부터 도

출한 최상위 위험원을 분석대상으로 하였다. 이러한 위험원 분석 후에, 이에 대한 리스크 분석을 통해 위험원별 THR(Tolerable Hazard Rate)을 할당하게 되고, 하부 시스템의 위험원에 대한 이와 동일한 과정의 반복을 통한 하부시스템에 대한 THR 및 SIL을 할당하는 과정을 거치게 된다. 그리고 할당된 SIL 등급 및 THR과 위험원 분석과정에서 제시된 대책기술들이 시스템의 설계에 반영되는 단계를 거치게 된다.

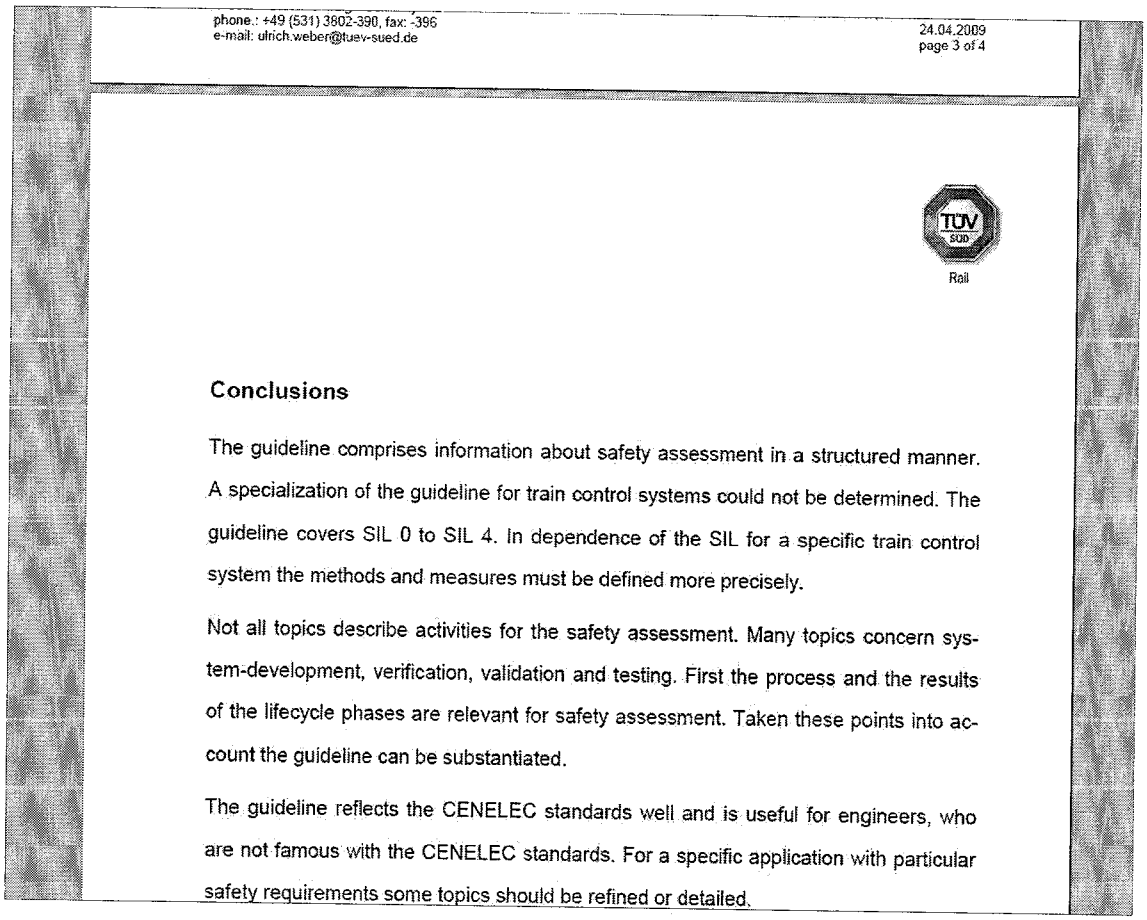
(3) 열차제어시스템 안전성 평가 가이드라인

(가) 안전성 평가 개요

열차제어시스템의 안전성 평가는 궁극적으로 앞 절에서 제시한 안전성 활동의 과정과 그 결과의 분석 및 평가를 통해 이루어지게 된다. 따라서 본 절의 열차제어시스템 안전성 평가 가이드라인은 기본적으로 앞 절에서 제시한 안전성 활동 기술체계를 기반으로 한 안전성 활동 결과의 확인을 중심으로 열차제어시스템 안전성 승인 및 수용을 위한 요구사항을 나타내고 있는 IEC 62425 규격에 적합하도록 작성되었으며, 당해 연도 해외 전문기관(TUV SUD)의 기술자문을 통해 보완하였다. 이러한 평가 가이드라인은 차년도에 평가대상시스템의 Safety Case 분석에 적용 후 최종적으로 작성될 예정이다. 또한 안전성 평가 가이드라인의 체크리스트에 대한 해설서의 필요성에 당해연도 적용성 연구과정에 제기되어, 당해연도에 일부 체크리스트에 대한 해설서를 작성하였지만, 차년도에 대상시스템에 대한 적용성 연구를 통해 전체적인 체크리스트 해설서를 작성할 예정이다. 그리고 이 가이드라인의 체크리스트 EC 4-2-29에 포함되는 소프트웨어 가이드라인의 경우 당해연도에 체크리스트를 보완제시하였으며, 본 보고서 제3장 제2절에 제시하였다.

본 절에서는 앞에서 설명한 안전성 평가조건, 평가업무, 평가자의 단계별 주요 활동 등의 분석과 열차제어시스템 안전성 승인 및 수용을 위한 요구사항을 정의한 IEC 62425, EN 50129 AP, 해외 전문기관의 기술자문, 대상시스템의 제작 및 안전성 활동 수행 등을 바탕으로 열차제어시스템 안전성 평가를 위한 가이드라인을 작성하였다. 이 가이드라인은 전년도에 작성한 안을 바탕으로 보완작성 되었다. 해외 전문기관을 통해 기술자문을 통해 약 30건의 의견을 받았으며, 이러한 의견들이 당해연도의 가이드라인에 반영되었거나 일부는 차년도에 실제 적용성 연구를 통해

보완할 예정이다. 다음 그림은 당해연도에 해외 전문기관으로부터 기술자문을 수행한 결론 부분을 나타낸 것으로, 열차제어시스템에 특화된 가이드라인으로의 보완 등은 현재 수정작업이 진행 중에 있다. 이러한 당해연도의 가이드라인 보완안을 바탕으로 차년도에는 실제 2세부과제에서 작성한 Safety Case를 바탕으로 적용성 연구를 수행하고, 이를 통해 평가가이드라인 최종안을 제시할 예정이다.



phone.: +49 (531) 3802-390, fax: -396
e-mail: ulrich.weber@tuev-sued.de

24.04.2009
page 3 of 4

TÜV SÜD Rail

Conclusions

The guideline comprises information about safety assessment in a structured manner. A specialization of the guideline for train control systems could not be determined. The guideline covers SIL 0 to SIL 4. In dependence of the SIL for a specific train control system the methods and measures must be defined more precisely.

Not all topics describe activities for the safety assessment. Many topics concern system-development, verification, validation and testing. First the process and the results of the lifecycle phases are relevant for safety assessment. Taken these points into account the guideline can be substantiated.

The guideline reflects the CENELEC standards well and is useful for engineers, who are not famous with the CENELEC standards. For a specific application with particular safety requirements some topics should be refined or detailed.

그림 3.1.12 해외 기술자문 결론 부분

다음은 작성한 평가 가이드라인의 목차를 중심으로 결과를 간략하게 정리하여 나타낸 것이다. 각 장의 개요와 가이드라인의 중요한 부분인 평가항목에 대한 도출한 결과를 요약정리 하였다.

■

1. 소개

1.1 개요

이 문서는 열차제어시스템 안전성 평가를 위한 설명서이다. 열차제어시스템의 안전성을 평가하기 위하여 국제 표준인 IEC 62425를 참고하여 작성되었다. 이 문서에서 설명하는 평가방법은 IEC 62425의 요구사항을 기본으로 하였다.

이 문서에서 제안하는 열차제어시스템 소프트웨어 안전성 평가는 IEC 62425 규격의 골격에 따라 크게 문서화, 품질관리 시스템, 안전관리 시스템, 기능 및 기술 안전성 평가 등의 네 가지 분야에서 표준의 각 요구사항을 피평가기관 및 열차제어시스템이 충족하고 있는지를 검증하는 방식으로 이루어진다. 따라서 본 문서에서는 열차제어시스템 안전성 평가를 위하여 다음의 분야에 있어서 표준 적합도를 평가하는 방법을 설명한다.

- *문서화*
- *품질관리 시스템*
- *안전관리 시스템*
- *기능 및 기술안전성 평가*

1.2 관련문서

본 문서는 아래의 IEC 표준과 밀접한 관계를 가지고 있으며, 따라서 이 문서들에 대한 이해가 필수적이다.

- *IEC 62425(EN 50129) : Railway Applications - Safety related electronic systems for signaling*
- *IEC 61508 : Function safety of electrical/electronic/programmable electronic safety-related system*
- *IEC 62278(EN 50126) : The specification and demonstration of RAMS*
- *IEC 62279(EN 50128) : Software for railway control and protection systems*
- *IEC 62280(EN 50159) : Communications, signaling and processing systems*

1.3 관련 이용자

본 문서에서는 열차제어시스템의 안전성 평가를 위한 항목이나 체크리스트들을 설명

하고 있어 평가기관의 평가자들에게는 안전성 평가를 위한 지침서로 이용될 수 있다. 또한 이 문서는 열차제어시스템 안전성 평가를 준비하는 시스템 개발자, 안전 관리자 등이 이해하여 개발하는 열차제어시스템의 안전성을 개선하고, 위험도를 낮추는 목적으로 이용이 가능하다.

1.4 문서의 구성

본 문서의 구성은 다음과 같다. 2장에서는 본 문서에서 제안하고 있는 평가과정 및 방법에 대해 설명하고, 3장에서는 평가를 위해 필요한 문서의 확인에 대해 설명한다. 4장에서는 평가를 위해 필요한 문서의 확인에 대해서 설명한다. 4장에서는 품질관리 시스템의 확인요소에 대해서 설명하고, 5장에서는 안전관리시스템의 확인요소, 6장에서는 기술 및 기능 안전성 평가에 대해 설명한다. 그리고 7장은 피평가 대상인 시스템에 관련된 종합안전대책기술서의 평가에 대해 설명한다.

1.5 문서의 활용 방법

본 문서는 열차제어시스템 안전성 평가를 위한 지침서로서 각 항목별로 관련 국제표준, 표준에 관련된 설명 그리고 체크리스트로 구성되어 있다. 이 중 체크리스트는 안전성 평가를 위한 실제적인 항목을 나타낸다. 실제 적용에 있어서는 본 문서의 체크리스트와 그에 해당하는 본문의 내용을 파악하여 프로젝트 특성에 적합한 새로운 체크리스트를 생성하여 활용하는 것이 필요하다. 즉 본 문서는 열차제어시스템 안전성 평가를 위한 기본 지침서로서, 실제 프로젝트 시스템 평가를 위한 절차 및 체크리스트의 생성을 위한 기본자료로 활용이 가능하다.

2. 평가 방법

2.1 개요

본 장에서는 열차제어시스템 안전성 평가방법과 절차에 대해 설명한다. 열차제어시스템 안전성 평가는 열차제어시스템의 개발을 위한 수명주기 동안의 안전성 활동문서를 바탕으로 목표 안전 요구사항을 충족하였는지 여부를 평가하고, 그 결과에 의거하여 목표의 달성 여부를 판단하는 과정이다. 본 안내서에서는 철도의 열차제어시스템 안전성 승인 및 수용을 위한 표준인 IEC62425를 기준으로 사용하였다.

안전성 평가는 시스템이 의도하는 목표를 만족하는지를 검증 및 평가하는 것으로, 시스템에 관련된 위험원의 리스크가 제거되었거나 허용수준 이하로 낮아졌는지를

확인하는 것이다. 이는 안전성 입증 문서 등 제출된 문서들의 분석을 통해 확인 및 평가가 수행되게 되며, 평가자의 필요에 의해서 성능입증 테스트 등의 추가적인 시험을 통한 확인 및 검증이 요구될 수도 있다.

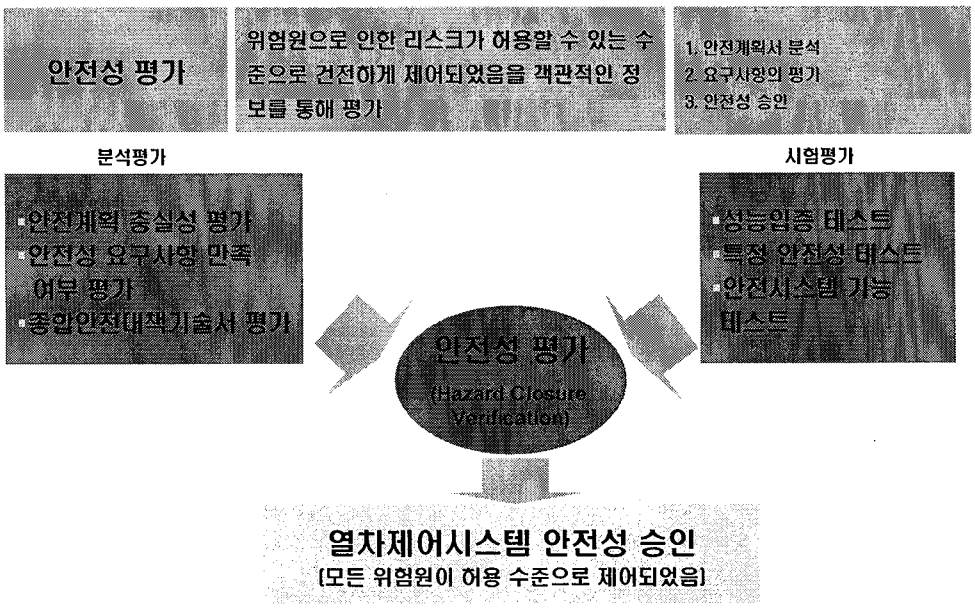


그림 1. 열차제어시스템 안전성 평가 개요

2.2 안전성 활동과 평가와의 관계

그림 2는 본 문서에서 제시하는 시스템 수명주기에 따른 안전성 활동 그리고 이 안전성 활동에 대한 안전성 평가 체계 및 상호간의 관계를 나타낸 것이다. 그림의 왼쪽 부분이 안전성 활동의 단계 및 순서, 그리고 이 안전성 활동에 따른 수명주기 각 단계를 나타낸 것이며, 오른쪽 부분이 이러한 안전성 활동 기술체계에 따른 안전성 평가의 항목 및 구성을 나타낸 것이다. 그림에서처럼 안전성 활동은 크게 리스크 분석 단계와 리스크 제어 단계로 나뉘어 지며, 이러한 안전성 활동에 따른 안전성 평가는 앞에서 설명한 크게 요구사항 단계와 실행단계로 나뉘어 질 수 있다. 요구사항 단계는 그림에서 '데이터 분석' 부분으로 이 과정을 통해 안전성 평가계획이 작성되며, 실행단계는 관련 문서의 평가인 '안전성 분석평가'와 '테스트 평가'로 나뉘어 진다.

[그림 생략 : 안전성 활동과 안전성 평가의 관계]

안전성 분석 평가 단계는 실제적으로 안전성 평가가 수행되는 단계로서 요구사항 단계에서 수립된 안전성 평가계획에 따라 종합안전대책기술서에 포함된 모든 문서들을 통해 앞 절에서 설명한 품질관리 평가, 안전관리 평가, 기술 및 기능 안전성 평가를 수행하는 안전성 평가의 실제적인 단계에 해당한다. 이 단계에서는 위험원별 리스크 저감을 위한 대책기술의 적용 수준 및 결과, 시험평가 등의 수행을 통해 프로젝트 시스템이 도출된 위험원의 리스크가 제거 또는 저감되었는지를 최종적으로 확인(Hazards Closure)하는 단계이다.

테스트 평가 단계는 다시 프로젝트 시스템의 성능확인 테스트, 안전 테스트 그리고 현장테스트로 구분할 수 있다. 이 중 안전 테스트는 시스템의 안전기능을 위해 설계 및 구현된 모듈을 시험하는 것으로 결함주입시험과 같은 형태의 시험이 대표적인 이 테스트에 해당한다.

2.3 안전성 평가보고서의 주요 내용

안전성 평가자가 평가 수행 수 작성하게 될 안전성 평가 보고서에는 본 문서의 체크리스트 확인결과를 포함해서 최소한 다음의 내용들이 포함되어야 한다.

- 평가자 또는 평가 조직의 승인 정보
- 평가 범위
- 역할, 책임, 역량, 독립성(교육훈련, 경험 등의 정보)
- 관련 문서 정보(근거 문서; 종합안전대책기술서, 적용 표준 문서 등)
- 평가절차의 설명
- 안전 요구사항이 적절하게 충족되었다는 근거
- 수용 기준이 충족되었다는 근거
- 방법 및 활동 설명(방법 및 활동의 타당성을 포함하여, 테스트 전략 점검)
- 안전성 관련 응용 조건이 충족되었거나 이의 관리를 작업자나 사용자에게 이전했다는 확증
- 사용 제한 또는 제약 사항과 권고 사항을 포함한 결론

2.4 평가절차

그림 3은 안전성 평가의 흐름을 다이어그램으로 표시한 것으로, 그림에서 왼편은 안전성 평가를 받기 위해 수행하여야 될 안전성 활동들을 간략하게 표시한 것이고,

그림의 오른쪽 부분이 이러한 안전성 활동을 수행한 기관과 독립된 안전성 평가를 수행하는 흐름을 나타낸 것이다. 그림에서와 같이 안전성 평가를 위해서는 품질관리 보고서, 안전관리 보고서, 검증 보고서 및 설계보고서 등의 평가를 통해 수행이 되게 된다. 그림에서와 같이 평가과정은 평가대상인 열차제어시스템의 기능 안전성 및 안전무결성을 평가하고, 국제규격에서 요구하고 있는 문서화 및 안전성 활동이 수행되었는지 그리고 이를 통한 안전 목표가 달성되었는지에 대한 평가를 하는 과정이다. 안전성 평가는 아래의 활동들을 최소한으로 포함해야 한다.

- 평가계획 수립(ISA 계획)
- 자료수집
- 자료의 검증
- 평가 수행
- 평가보고서 작성(ISA 보고서)

[그림 생략 : 열차제어시스템 안전성 평가의 흐름도]

2.5 평가기준

본 문서에서 제안하는 안전성 평가는 IEC 62425에서 요구하는 사항들에 대한 만족도를 평가하여 그 결과에 따라 평가를 수행한다. 상기 국제표준에서 정의하고 있는 요구사항은 크게 문서화, 품질관리 체계, 안전관리 체계, 기술 및 기능 안전에 대한 평가의 네 가지 분야로 구성되어 있다. 따라서 평가는 이들 네 가지 분야의 확인결과를 근거로 이루어진다.

문서화 만족도 평가는 열차제어시스템 개발과정에서 문서들이 체계적으로 작성되고 있으며, 관리되고 있는지 평가한다. 문서들은 열차제어시스템의 기능 안전성과 안전성 무결성 등급 판정을 위하여 요구되는 근거자료들을 체계적이며 명료하게 기술하고 있어야 한다.

품질관리체계와 안전관리체계의 평가는 시스템 개발주기 동안의 관리 활동에 대한 품질 및 안전 측면의 만족도를 평가한다. 열차제어시스템 전주기에 대한 품질관리 및 안전관리 계획을 정의해야 하고 이에 따라 수행되었는지 확인하여야 한다.

기술 및 기능 안전성 평가는 대상 시스템의 목표 안전 무결성 등급에서 요구되는 항

목들의 만족도를 평가한다.

2.6 만족도 평가

평가자는 열차제어시스템 안전성 평가를 위해 다음의 정량적 기준을 이용하여 요구조건들의 만족도를 4단계로 평가한다.

- F Fully achieved 85% 초과 100% 이하 만족
- L Largely achieved 50% 초과 85% 이하 만족
- P Partially achieved 15% 초과 50% 이하 만족
- N Not achieved 0% 이상 15% 이하 만족

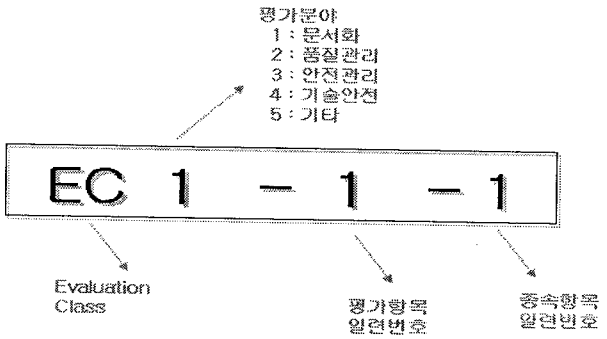
2.7 적용수준

각 평가항목은 반드시 준수해야 하는 의무사항(Mandatory)인지, 권장사항(Recommend)인지를 정의하였다.

- M Mandatory 반드시 준수해야 하는 사항
- R Recommend 준수를 권장하는 사항

2.8 평가항목의 구분

본 문서에서는 문서화, 품질관리시스템, 안전관리시스템, 기술 및 기능 안전성 평가 등의 4개 분야에서 평가를 수행하도록 제안하고 있으며, 각 분야별로 별도의 체크리스트를 제공하여 평가가 이루어지도록 하였다. 각 체크리스트의 평가 ID는 다음과 같이 부여하였다.



3. 문서화

3.1 개요

본 절에서는 IEC 62425에서 정의된 열차제어시스템 안전성 수용 및 승인을 위해 안

전성 평가기관에 제출되어야 할 문서화 요건을 바탕으로 피인증 열차제어시스템의 문서화 정도를 인증하기 위한 만족도 평가항목을 제안한다.

3.2 관련규정

(IEC 62425 5.1) 열차제어시스템의 안전성 입증을 위해 종합안전대책기술서(Safety Case)라는 문서가 준비되었는지 확인한다.

열차제어시스템 안전성 평가를 위해 제출되는 안전성 입증문서인 종합안전대책기술서는 시스템의 설계 및 개발에 따른 안전성 활동에 대한 결과물로서, 피인증 시스템의 안전성을 입증하기 위한 충분한 정보를 포함하는 문서인지를 확인해야 한다. 이를 위해 종합안전대책기술서에는 시스템, 하부시스템 혹은 장치의 요수들에 대하여 문서로 된 안전성 입증자료를 포함하여야 하며, 다음과 같은 구조로 되어있어야 한다.

a) 시스템에 대한 정의

이 부분은 종합안전대책기술서와 관련된 시스템, 하부시스템 혹은 장치를 정확하게 정의하거나 언급되어 있어야 하며, 문서의 수정 및 변경상태를 포함하여야 한다.

b) 품질관리 보고서

피인증 시스템의 품질관리에 대한 근거자료가 포함되어야 한다.

c) 안전관리 보고서

피인증 시스템의 안전관리에 대한 근거자료가 포함되어야 한단.

d) 기술안전 보고서

피인증 시스템의 기능적/기술적 안전에 대한 근거자료를 포함되어야 한다.

e) 관련된 안전대책기술서

피인증 시스템의 안전대책기술서와 관련되어 있는 모든 하부시스템 또는 장치의 안전대책기술서에 대한 참고자료들이 포함되어야 한다. 이는 또한 관련된 하부시스템/장치의 안전대책기술서 각각에 대하여 기술된 안전관련 모든 응용조건들이 피인증 시스템의 안전대책서를 만족하는지, 또는 안전대책기술서의 안전관련 응용조건을 따르는지에 대한 내용이 포함되어야 한다.

f) 결론

종합안전대책기술서의 앞부분에서 설명한 안전성 근거자료가 요약되어 있고, 관련 시스템/하부시스템/장치가 정해진 응용조건에 따라 안전한지에 대한 설

명이 포함되어 있어야 한다.

평가기관에서는 제출된 종합안전대책기술서가

a) 정확하고 간결하게 되었는지 확인해야 한다.

b) 이해하기 쉽게 되었는지 확인해야 한다.

c) 목적에 적합하게 작성되었는지 확인해야 한다.

d) 문서관리가 적절하게 되었는지를 확인해야 한다.

종합안전대책기술서에 포함되는 각 문서들은 문서의 범위를 나타내는 제목이나 명칭이 부여되어 있어야 한다. 또한, 색인 기능을 제공해야 한다. 문서의 구조는 해당 회사의 절차와 업무 관행을 반영할 수 있으므로 평가기관은 문서의 구조를 파악해야 한다.

문서들은 개정 번호를 포함해야 한다. 이는 해당 문서의 다른 버전을 확인할 수 있도록 하는 요소이다. 또한, 문서들은 최신 개정번호에 의해서 관리되고 있는지 확인해야 한다. 모든 관련 문서가 개정, 수정, 검토, 승인을 받아야 하며, 적절한 문서 통제 체계에 의해 관리되고 있는지 확인해야 한다.

열차제어시스템의 안전성 평가를 위해서는 앞에서 설명한 종합안전대책기술서를 기본으로 평가업무를 수행하며, 추가적으로 RAM 활동을 포함한 RAMS 활동에 관련 국제표준인 IEC 62278에서 제시한 시스템 수명주기별 생성되는 문서들도 안전성 평가를 위해 필요하다. 물론 종합안전대책기술서의 일부내용은 수명주기별 생성되는 문서들과 중복된다. 이러한 수명주기 각 단계별 생성되는 문서들은 프로젝트 시스템의 특성에 따라 여러 문서들이 하나의 문서로 통합되어 생성 및 관리되어질 수 있다. 다음 표는 IEC 62425와 IEC 62278에 따른 수명주기 단계별 활동 및 문서 리스트를 간략하게 나타낸 것으로, 표에서와 같이 IEC 62278은 시스템의 RAM 활동을 포함하고 있다. 따라서 열차제어시스템 안전성 평가에서는 안전성관련 국제표준인 IEC 62425의 요구문서들이 기본적으로 준비되어야 하며, 협의에 의해 IEC 62278에서 요구되는 문서들도 추가적인 확인이 가능하다. 따라서 이러한 수명주기별 필요한 문서 리스트는 안전성 평가 시작단계에서 조정 및 확정되어야 한다. 이들의 문서들은 여러 문서가 하나의 문서로 통합되어 작성될 수 도 있으며, 이 경우 통합 문서의 개요에 어떠한 문서를 의미하는지에 대한 설명이 반드시 포함되어야 한다.

[표 생략 IEC 62278과 IEC 62425에 따른 수명주기 단계별 활동 및 문서 리스트]

3.3 체크리스트

평가 ID	평가 항목	만족도 (N~F)	측정결과	비고
EC1-1	시스템 개발단계마다 작성한 문서 리스트가 있는가?			
EC1-2-1	작성된 문서 리스트에 표 3.1의 "IEC 62425"에 언급된 문서들이 포함되어 있는가?			
EC1-2-2	EC1-2-1 문서 외에 "IEC 62280"에 언급된 문서들이 작성되어 있는가?			
. . .	. . .			
EC1-3-6	문서의 작성과 수정이 정해진 절차에 따라 관리되었는가?			

3.4 체크리스트 해설

평가 ID	평가 항목	평가항목 해설
EC1-1	시스템 개발단계마다 작성한 문서 리스트가 있는가?	프로젝트 시스템의 개발 단계별(표 3.1의 수명주기 각 단계) 안전성 입증을 위해 준비한 문서의 리스트가 있는지 여부를 확인하는 것으로, 아래 두 평가항목의 점검에 활용될 수 있음. 또한 문서리스트의 확인으로 안전성 평가에 반드시 필요한 문서들이 누락되었는지 점검함.
EC1-2-1	작성된 문서 리스트에 표 3.1의 "IEC 62425"에 언급된 문서들이 포함되어 있는가?	표3.1에 언급한 문서들이 준비되어 있어야 하며, 표에서 언급한 여러 문서가 하나의 문서로 통합되어 작성된 경우에도 반드시 확인하여 누락된 문서가 없는지 확인한다.

	. . .	. . .

4. 품질관리 보고서

안전성 평가를 위한 첫 번째 조건은 시스템, 하위 시스템 혹은 기기의 품질을 충족하고, 지속적으로 유지하며, 전 수명 주기 동안 효율적인 품질 관리 시스템을 통해 관리하는 것이다. 이러한 품질관리에 대한 증거 및 보조자료들이 품질관리 보고서에 제시되어야 한다. 품질관리 시스템의 목적은 수명 주기의 각 단계에서 인간의 오류를 최소화함으로써 시스템, 하위 시스템 혹은 기기 시스템의 결함 위험을 줄이는 것이다. 프로젝트 시스템의 품질관리 프로세스에 적용되는 방법은 품질계획서에 기술하며, 품질관리 시스템은 IEC 62425에 설명한 대로 시스템 수명주기 내내 적용된다.

4.1 관련규정

안전성 평가 시 참조되는 관련규정은 다음과 같다.

(IEC62425 5.2) 시스템/하부시스템/장치의 품질이 수명주기 동안 효과적인 품질관리 시스템에 의해 통제되어 왔는지 확인한다.
(IEC62425 5.2) 안전 무결성 등급 1~4 모두에 대해서 품질관리를 위한 요구사항에 만족하는지 확인한다.

4.2 품질관리 시스템

일반적으로 품질관리 시스템과 관련하여 다음의 사항들이 기술되어야 한다.

- 회사가 일반적으로 적용하는 품질관리 시스템과 조직의 품질관리 매뉴얼 사이의 관계
- 개발, 생산, 공급, 고객지원 활동에 관련된 프로세스 및 모든 작업자에게 적용되는 품질지표 모니터 결과가 포함된 품질관리 시스템
- 해당사항이 있다면, 철도당국에 의해 승인된 품질관리 시스템 승인사항
- 회사 내부의 품질보증 부서에 의한 내부 품질 점검 주기

4.3 품질관리 계획서

품질관리 계획서에는 프로젝트 개발 조직이 수행할 기획업무, 생산관리, 시스템의 설치에 관한 사항을 기술하며, 또한 조직관련 부분, 구체적인 품질관리 업무절차, 필요한 자원, 품질관리 스케줄과 관련된 사항들이 자세하게 언급되어야 한다. 즉, 프로젝트의 품질관리 계획서는 앞의 품질관리 시스템과 다음에 설명할 품질관리 조직에 관한 사항, 내·외부 품질관리 감사 관련 정보들을 포함한다.

4.4 품질관리 조직

프로젝트 수행에 관련된 조직의 구조를 설명하여야 하며, 일반적으로 프로젝트팀의 조직구조는 그림으로 나타내는 것이 좋다. 프로젝트 수행 조직은 주요 사안들에 대한 효율적인 커뮤니케이션과 협조를 얻어낼 수 있는 조직구조로 운영되어야 한다.

- *상위레벨 관리자로부터 프로젝트 품질관리 관리자와 엔지니어에 이르는 조직 주고를 보여주는 계통도 및 설명*
- *품질관리에 관련 모든 책임자, 관리자 및 엔지니어의 수행 역할*

4.5 품질관리의 증거

품질관리의 증거는 다음 표와 같은 문서들에 의해 확인되어진다. 따라서 IEC 62425 표준에서 제시한 각 단계별 품질관리 증거들이 다음의 표에서 설명하는 문서들에서 확인되어야 한다.

표 4.1 품질관리의 증거 문서

품질관리 확인이 필요한 부분	***기술된 문서***
조직 구조	*- 조직의 품질관리 매뉴얼* *- 품질관리 계획서*
품질관리 계획 및 절차	*- 품질관리 계획서* *- 품질관리 매뉴얼* *- 품질 기록서*
요구사양	*- 시스템 요구사양* *- 하부시스템 요구사양* *- RAMS 및 안전성 요구사항*

설계 관리 :설계관리란 제조업자 혹은 공급자가 설계관리에 따른 제품을 개발할 때 설명된 설계 요구사항이 충족되었음을 입증하기 위한 적합한 문서를 작성하고 보관하는 것으로, 어떤 식으로 설계문서를 관리하고 있는지에 대해 설명해야 한다.	- 설계 계획서
설계 확인 및 검토 :설계확인 및 검토는 시스템의 설계에 관련된 일체의 문서들을 검토 및 검증하는 조직, 검토자의 자격, 검증 및 검토 절차, 검증 및 검토 수행 결과들 대한 자료들을 확인하는 것을 의미한다. 프로젝트의 요구사항과 회사 절차서에서 규정하는 요구사항에 맞춰, 검토자들은 설계나 분석 부분을 점검할 수 있다.	- 설계 계획서 - 공식적인 기술 감사 보고서(절차 및 결과 보고서)
. . .	. . .

4.6 내부 품질 감사

품질관리 관련 프로세스와 활동에 대하여 동일 회사의 독립적인 부서가 내부적으로 실시하는 감사 및 실사 활동을 설명한다. 평가 결과를 예를 들어 도표 형식으로 제시해야 하며, 다음 사항을 포함한다. 단, 프로젝트 초기 단계에 ISA나 철도당국 등 외부 기관이 감사를 실시한다면, 내부 품질 감사를 실시하지 않을 수도 있다.

- 항목 참조 번호
- 감사 대상 프로세스/활동 참조 정보
- 감사 일자
- 감사자
- 감사 결과에 대한 설명이나 의견
- 상태(중요도 표시)
- 권고 사항 및 사후 조치
- 문제 사안의 대책 평가

4.7 하청업체 품질 감사

외부 공급업체와 관련하여 실시한 감사 및 실사 활동을 설명한다. 평가 결과를 예를 들어 도표 형식으로 제시해야 하며, 다음 사항을 포함한다.

- 항목 참조 번호
- 감사 대상 프로세스/활동 참조 정보
- 감사 일자
- 감사자
- 감사 결과에 대한 설명이나 의견
- 상태(중요도 표시)
- 권고 사항 및 사후 조치
- 문제 사안의 대책 평가

4.8 외부 품질 감사

프로젝트의 일환으로 운영 절차의 실태와 관련하여 고객업체와 제 3자(ISA)가 실사를 실시할 수 있다. 다만 그런 사항이 계약 문서와 참조 표준에 규정되어 있을 필요가 있다. 평가 결과를 예를 들어 도표 형식으로 제시해야 하며, 다음 사항을 포함한다.

- 항목 참조 번호
- 감사 대상 프로세스/활동 참조 정보
- 감사 일자
- 감사자
- 감사 결과에 대한 설명이나 의견
- 상태(중요도 표시)
- 권고 사항 및 사후 조치
- 미결 사안의 대책 평가

4.9 평가항목(Check List)

평가 ID	평가 항목	만족도 (N~F)	측정 결과	비고
EC 2-1-1	품질관리보고서 등 프로젝트의 품질관리시스템을 증명할 문서가 있는가?			
EC 2-1-1	품질관리보고서 등 프로젝트의 품질관리 시스템을 증명할 문서가 있는가?			
EC 2-1-2	품질관리보고서 이외의 품질관리를 증명할 다른 공인된 자료가 있는가? (있으면 아래의 평가항목은 생략가능)			
EC 2-2-1	품질관리 계획서에는 품질관리 조직, 업무절차, 필요			

	한 자원, 스케줄이 명기되어 있는가?			
EC 2-2-2	시스템 수명주기 동안 품질을 점검하기 위해 선택한 방법이 제시되어 있는가?			
EC 2-2-3	품질점검을 실시하는 시기가 설명되어 있는가?			
EC 2-2-4	품질점검을 실시하는 사람의 자격수준과 사람이 지정되어 있는가?			
EC 2-2-5	제시된 품질관리 계획이 적절한가?			
. . .	. . .			
EC 2-17-3	내외부 품질관리 감사 결과가 프로젝트 시스템 품질관리 시스템에 반영되어 수행되었음이 확인되는가?			

5. 안전관리 보고서

안전관리의 목적은 전체 프로젝트 수명주기에 걸쳐서 안전관련 인적오류의 발생을 더욱 줄이기 위한 것이고, 이렇게 하여 안전과 관련된 구조적 결함의 리스크를 최소화하는데 있다. 수명주기를 통한 안전관리 과정에 따라 수행되었음을 증명하기 위한 내용을 안전관리 보고서에 설명되어져 있어야 하며, 안전성 평가과정에서 이에 대해 확인하여야 한다.

5.1 관련규정

안전성 평가 시 참조되는 관련규정은 다음과 같다.

(IEC62425 5.3.1) IEC62278의 철도 RAMS 요구사항을 따르는 효과적인 안전성 관리과정에 의해 관리되고 유지되어 왔는지 확인한다.

(IEC62425 5.3.1) 수명주기를 통한 안전관리 과정의 모든 요소들에 순응하는 것을 증명하기 위한 증거문서는 종합안전대책기술서 내의 '안전관리 보고서'에 제공되어야 한다.

(IEC62425 5.3.1) 안전성 관리가 안전무결성 등급 1~4 모두에 대해서 필수적으로 시행되어 왔는지 확인한다.

(IEC62425 5.3.1) 제시된 근거자료의 심도와 보조문서의 범위는 시스템/하부시스템/장치의 안전 무결성 등급에 엄격히 적합한지 확인한다.

(IEC62425 5.3.1) 안전무결성등급의 확인을 위해 IEC62278에 정의된 위험원 분석 및 리스크 평가 과정이 수행되었는지 확인한다.

5.2 안전성 수명주기(Safety Life Cycle)

안전관련 절차는 일련의 여러 단계와 활동으로 구성되며, 이런 단계화 활동이 안전성 수명주기를 구성한다. IEC62278에 설명된 시스템 수명주기에 맞춰서 프로젝트 시스템에 적용한 안전성 수명주기가 설명되어 있고, 이에 근거하여 실행하였는지 확인한다. 안전성 수명주기는 V형 사이클로 하향 방향으로는 요구사항의 설정, 설계 및 개발단계가 있고, 상향방향으로는 통합 및 검증단계가 있다. 표 5.1은 시스템 수명주기 단계와 이에 따른 안전성 활동을 나타낸 것이다. 이 표에서 처럼 안전성 수명주기에 있어서 다음의 내용들이 최소한으로 포함되어 있어야 할 것이다.

- *위험원의 도출 및 분석*
- *위험도 평가*
- *안전요구사항 할당(SIL 요구등급 결정 포함)*
- *안전대책기술 설계*
- *안전 요구사항 충족 여부 입증*

[그림 생략 : 안전성 수명주기 예]

5.3 안전조직

IEC62425에서는 열차제어시스템의 경우 SIL 등급별 안전관련 조직을 다르게 운영할 것을 요구하고 있으며, 또한 구성원의 자격 및 교육훈련도 SIL 등급별 차별화시킬 것을 요구한다. 인증기관에서는 안전조직의 구조, 안전조직의 독립성 운용현황, 구성원의 자격 등이 상세히 설명되어 있는지 확인하여야 한다. 즉, 상위레벨 관리자부터 안전성 V&V 및 프로젝트 관리자와 엔지니어에 이르기까지 안전조직을 보여주는 계통도, 특히 서로 다른 역할을 수행하는 사람들 사이의 계층적/기능적 연계가 명확히 제시되어 있는지 확인하여야 한다. 또한 모든 안전성 및 프로젝트 책임자, 관리자, 엔지니어의 과업에 대한 설명이 문서화되어 있는지 확인되어야 한다.

[표 생략 : SIL 등급별 안전조직 구성 예]

5.4 안전계획 활동(Safety Plan Activities)

안전관리 보고서의 이 부분에서는 안전계획서에 따라 모든 활동이 수행되었다는 증거가 제시된다. 이는 도표형태로 정리될 수 있으며, 안전계획서를 포함한 안전성 활동과 관련된 문서들을 포함한다.

안전계획서는 수명주기를 통해 안전관리 구조, 안전관련 업무 및 일정을 나타내는 문서이다. 안전계획서는 안전성 활동 각 단계별 계속적으로 검토되어야 하며, 안전성 활동 과정에서 변경 또는 추가사항이 발생하면 이를 반영하여 변경이력 및 내역이 관리되어야 한다. 어떻게 안전 목표를 충족시킬 것인지와 안전성 검증 및 확인을 수행할 방법 및 절차에 관한 내용이 필수적으로 포함되어야 한다. 안전관리 보고서의 본 절에는 안전 계획서의 예정활동이 수행되었다는 증거들을 제시하여야 하며, 도표형식으로 정리할 수 있다. 안전성 활동 수행 도중 안전계획서를 검토 및 보완하여야 하며, 안전계획서에는 다음의 내용을 포함할 수 있다.

- *안전계획서의 목표, 목적, 범위 및 구조*
- *개념설계에서 전체에 이르기까지 안전성 활동을 수행하고 관리하기 위한 방법 및 절차*
- *프로젝트로 어떻게 안전성 목표를 충족시킬 것인지에 대한 내용*
- *안전성 검증 및 확인을 어떻게 수행할 것인지에 대한 내용*

5.5 위험원 목록(Hazard Log)

[중략]

5.6 안전 요구사양

5.7 시스템의 설계

5.8 안전성 검토(Reviews)

5.9 안전성 증명 및 검증

5.10 안전성 입증

5.11 시스템 이양

5.12 운영 및 유지보수

5.13 폐기처분

5.14 평가항목(Check List)

평가 ID	평가 항목	만족도 (N~F)	측정 결과	비고
EC 3-1-1	프로젝트에 적용한 안전성 활동 수명주기가 설명되어져 있는가?			
EC 3-1-2	안전성 활동단계에서는 위험원 도출 및 분석, 위험도 평가, 안전요구사항 할당, 안전대책기술 설계, 안전요구사항 충족여부 입증의 단계가 포함되어 있는가?			
EC 3-1-3	적용한 안전성 활동 수명주기가 안전관리를 위해 적절한가?			
EC 3-1-4	적용한 안전성 활동 수명주기를 통한 안전관리가 되었음을 입증할 자료들이 정리되어 있는가?			
EC 3-2-1	SIL 등급별 안전조직의 운영규정이 있고, 이 규정에 따라 조직이 구성되어 안전관리가 이루어졌다는 증거자료가 있는가?			
. . .	. . .			
EC 3-12-1	프로젝트 시스템의 동작수명이 끝날 경우, 그 폐기처분 계획 및 절차가 안전계획서에 설명되어져 있는가?			

6. 기능 및 기술 안전 보고서

이 장에서는 시스템의 기술적 안전성의 특징에 대해 설명한다. 즉, 안전성 확보

를 위해 적용한 안전성 표준 및 설계 방법을 설명하여야 하며, 또한 이의 입증을 위해 시험 및 분석 결과, 검증 및 확인 보고서, 인증서 등의 해당되는 증거를 본 장에서 설명하여야 한다. 이 기능 및 기술 안전 보고서를 기술안전보고서라고도 하며, 다음과 같이 구성할 수 있다.



그림 6.1 기술안전보고서의 구성

6.1 관련규정

(IEC62425 5.4) 안전성이 공인되지 전에 설계의 안전에 대한 기술적인 입증을 위해 기술안전보고서가 문서화 되어야 한다.

(IEC62425 5.4) 기술안전보고서는 시스템/하부시스템/장치들의 설계 안전에 대한 기술적인 근거들을 포함하여야 한다.

(IEC62425 5.4) 기술안전보고서는 안전무결성 등급 1~4 모두에 대해서 필수적으로 시행되어 왔는지 확인한다.

(IEC62425 5.4) 제시된 근거자료의 심도와 보조문서의 범위는 시스템/하부시스템/장치의 안전 무결성 등급에 엄격히 적합한지 확인한다.

(IEC62425 5.4) 기술안전보고서에는 설계 안전성을 보증하는 근거들(예를 들어서 설계원리와 설계결과, 시험사양과 결과, 안전성 분석 등)을 포함하여 설계의 안전을 입증할 기술원리들을 설명해야 한다.

6.2 서론

시스템/하부시스템/장치들의 설계에 대한 요약설명을 포함하며, 또한 시스템 개발 시 적용한 안전성 관련 표준이나 규격 리스트들이 포함되어야 한다.

6.3 정확한 기능적인 동작의 보증

규정된 운용과 안전요구사항들에 따르는 정상적인(Fault-free) 상황에서의 시스템의 정확한 동작을 증명하는데 필요한 모든 근거들이 포함되어야 한다. 다음과 같은 구체적인 사항들이 포함되어야 하며, 블록다이어그램과 같은 형태로 명확하게 설명하는 것이 필요하다.

- *필요하다면 이전 버전 시스템의 개선에 따른 시스템에 대한 설명*
- *안전성 관련 기능이나 새로운 기능에 대한 설명과 분석*
- *관련 설계 문서에 규정된 바에 따른 기능 저하 모드(Degraded Mode) 운용의 정의 및 관리*
- *프로젝트 시스템의 구조*
- *프로젝트 시스템에 적용한 안전성 원칙(가능하면 기존 버전의 시스템과 기능별 일대일로 대비하여 설명)*
- *재사용 기능과 그의 안전성에 대한 설명*

- 적용한 규격 및 기준에 따라 확보한 안전성 수준

- 안전성 레벨을 보장하는 사용 조건과 운영 조건

6.3.1 시스템 구조

시스템/하부시스템/장치 설계에 사용된 기술 및 원리들을 이해하는데 충분할 정도의 심도 있는 설명이 있는지 확인하고 제시된 SIL 등급별 시스템의 구조를 따르는지 확인한다. 제시된 표의 2~7의 방법은 모두 적용되어야 한다는 의미가 아니라, 이들 중 최소한 하나이상이 구조가 적용 되어야 함을 의미한다.

[표 생략 : SIL 등급별 시스템 구조]

6.3.2 인터페이스의 정의

이 절에서는 설계 및 제작한 시스템의 Man-Machine 인터페이스와 시스템 인터페이스에 대한 상세한 설명을 하여야 한다.

[중략]

6.3.3 시스템 요구사항의 충족

6.3.4 안전요구사항의 충족

6.4 위험원 분석 및 리스크 평가

시스템의 안전성 활동은 프로젝트 시스템의 위험원을 도출 및 분석하여야 하며, 도출된 위험원을 제거하거나 허용수준 이하로 줄이기 위한 대책기술을 설계 및 구현하는 일련의 활동으로서, 5.3절의 시스템 안전요구사항의 입증을 위해 필수적인 활동이다. 따라서 5.3절에서는 프로젝트 시스템에서 안전요구사항이 충족되었는지를 확인하고, 본 절에서는 이러한 안전요구사항을 충족하기 위한 안전성 활동의 과정 자체를 평가한다.

안전성 활동 중 위험원 분석 및 리스크 평가 단계에서는 먼저 예비 위험원 분석(PHA), 위험원 도출 및 분석, 리스크 평가 과정을 통해 리스크의 수준을 결정하고 시스템/하부시스템/장치로 안전요구사항을 할당되어야 한다. 그리고 허용수준

이하로 리스크를 줄이고 안전요구사항을 충족시키기 위한 대책기술 설계 등 안전성 활동이 수행되게 된다.

시스템의 위험원 분석방법에는 SIL 등급별 다음 표와 같은 방법들이 복수로 사용되어질 수 있다. 이러한 위험원 분석 및 리스크 평가를 위한 각 방법들은 안전계획서에 제시된 방법에 따라 안전성 활동이 수행되어야 하며, 이의 입증자료가 제시되어야 한다.

표 6.2 시스템의 위험원 분석 방법

기법/수단	SIL 1	SIL 2	SIL 3	SIL 4
PHA	HR	HR	HR	HR
FTA	R	R	HR	HR
FMECA	R	R	HR	HR
HAZOP	R	R	HR	HR
원인-결과 도	R	R	HR	HR
ETA	R	R	R	R
인터페이스 위험원 분석	R	R	HR	HR

6.4.1 관련규정

(IEC62425 5.3) 위험원 목록은 안전수명주기를 통하여 생성 및 관리되었는지 확인하며, 도출 위험원 리스트, 각 위험원별 리스크 분석 및 리스크 제어 정보들이 포함되어야 한다.

(IEC62425 5.3) 안전기능 및 안전무결성이 포함된 안전 요구사항이 도출되어 문서화되어야 한다.

(IEC62425 5.3) 안전요구사항은 위험원 확인 및 분석, 리스크 평가, SIL 등급 할당을 통해 도출되었는지 확인한다.

6.4.2 예비위험원 분석

예비위험원 분석은 프로젝트 시스템의 설계가 시작되기 전인 프로젝트 시작시

점에 수행되어야 하며, 이를 통해 프로젝트 시스템의 위험원 도출 및 리스크의 크기를 예측하기 위함이다. 예비위험원 분석 단계에서는 시스템 정의 및 사양과 기능 요구사항, 운영시나리오, 인터페이스 요구사항 등의 분석, 그리고 프로젝트 시스템과 유사한 시스템의 위험원 분석 등을 바탕으로 프로젝트 시스템의 위험원 리스트 도출하게 된다. 도출된 위험원에 대한 심각도와 발생빈도의 초기평가를 수행하여야 하며 이를 통해 위험원으로 인한 리스크의 크기를 감소시키거나 제거할 위험원을 분류하여야 한다. 다음 표와 같은 예비위험원분석 양식을 사용할 수 있으며, 이와 다른 양식을 사용하더라도 최소한 작업기간 및 날짜, 위험원 리스크, 위험원별 리스크 분석, 대책안 및 대책안 적용 후 리스크 예측의 내용이 포함되어야 한다.

[표 생략 : 예비위험원분석 양식]

6.4.3 위험원 도출 및 분석

예비위험원 분석이 수행된 후 상세한 위험원 도출 및 분석(HIA : Hazard Identification & Analysis)이 수행되어야 하며, 그 결과가 정리되어야 한다. HIA를 위한 기법에는 위의 표에서 제시한 것처럼 FTA, FMEA, ETA, HAZOP 등 다양한 방법들이 적용될 수 있다. 이러한 적용 가능한 여러 기법들 중 프로젝트 시스템의 안전계획서에 제시한 방법과 절차에 의해 위험원 도출 및 분석 과정이 이루어져야 하며, 이러한 과정을 통해 프로젝트 시스템에 영향을 미치는 위험원이 보다 명확하게 규명 및 분석되어지게 된다.

예비 위험원 분석과 HIA 과정을 통해 프로젝트 시스템에 대해 도출된 모든 위험원이 위험원 목록의 형태로 생성 및 관리되어야 한다. 이 위험원 목록은 HIA 단계의 수행을 통해 구체화되고 안전성 활동 전체를 통해 지속적으로 유지되어야 한다. 작성되는 위험원 목록에는 최소한 위험원 이름, 위험원 설명, 하위 위험원, 리스크 평가, 사고시나리오, 위험원 상태가 포함된 양식을 사용하여야 한다.

6.4.4 리스크 평가

HIA 과정에서 도출된 위험원들의 리스크 평가에는 정량적인 방법과 정성적인 방법이 있으며, 일반적으로 정성적인 방법의 하나인 리스크 매트릭스 방법이 많이 적용되고 있다. 그 외에 리스크 매트릭스 방법보다 좀 더 구체화된 방법인 리스크 그래프나 BP-Risk 방법 등이 적용될 수 있다. 프로젝트 시스템의 리스크 평가를

위해 적용하는 방법은 다른 안전성 활동을 위한 방법들과 마찬가지로 안전계획서에 명시한 방법과 절차에 따라 수행되어야 하며, 그 내용이 정리되어야 한다. 이 리스크 평가방법은 HIA 단계에서 사용되어지며, 프로젝트 시스템의 설계·제작된 후 최종적으로 리스크가 허용수준 이하로 제어되었는지를 입증하는 단계에서도 적용되어진다.

[그림 생략 : 리스크 평가를 위한 방법 분류]

6.4.5 안전성 요구사항 할당

[중략]

6.5 시스템 결함에 대한 대책기술 기술 설계

IEC62425 5.2, 5.3에 정의된 품질관리 및 안전관리 시스템에도 불구하고 비정기적인 하드웨어 결함은 여전히 존재할 수 있으므로, 이러한 하드웨어 결함에 대해서도 정량화된 THR 목표를 포함한 요구되는 안전요구사항이 계속 만족한다는 것이 입증되어야 한다. 즉, 비정기적인 하드웨어 결함의 발생에 따라 수반되는 리스크가 허용수준 이하로 줄이거나 제거하기 위해 적절한 대책이 반영되고 입증되어야 한다.

이러한 안전대책들 중 임의의 시스템 내에 결함이 발생하여도 위험한 상황이 발생하지 않고 시스템이 안전 상태를 유지하기 위해서 설계 시 고려되어야할 사항 및 대처방법은 다음 표와 같다.

[표 생략 : 결함에 대한 시스템 설계 시 고려사항]

이 표에서 요구하는 바와 같이 시스템적 결함에 따른 대책으로 단일 결함의 영향, 아이템의 독립성, 단일 결함의 검지 및 검지에 따른 안전상태 유지 기술, 다중 결함의 영향 및 대책들이 설계에 반영되고 입증되어져야 한다. 이러한 결함에 대한 대책기술은 시스템 레벨, 하부 시스템 레벨, 장치 및 부품 레벨로 분류하여 입증되어져야 한다.

시스템 레벨에서는 기본적인 열차제어시스템 안전성 원칙을 기술하고, 그와 관련된 규격과 방법(체계적인 접근 방법 등)을 제시하고, 그의 검증에 관한 증거들을

제시하여야 한다. 하부시스템 레벨에서는 시스템 레벨에서 요구되는 안전한 열차제어 원칙에 의하여 하부시스템 레벨에서도 설계 당시에 채택한 안전성 원칙을 설명하고 그 타당성을 제시하여야 한다.

하부시스템 레벨에서 요구되는 설계원칙에 근거하여 장치 및 부품 레벨에서도 설계 및 제작 시 채택한 안전성 원칙을 설명하고 그 타당성을 제시하여야 한다.

6.5.1 관련규정

(IEC62425 5.4) 임의 하드웨어 결함 상태에서도 규정된 안전요구사양을 계속해서 만족된다는 것이 입증되어야 한다.

(IEC62425 5.4) 계통적 결함으로 인한 리스크를 수용 가능한 수준으로 줄이기 위해 적용된 기술적 방법들을 설명하고 입증되어야 한다.

(IEC62425 5.4 B3.2) 동시에 오동작하면 위험원이 되는 요소를 하나 이상 가지는 시스템에서 요소들 간의 독립성은 기본 전제조건이다.

(IEC62425 5.4 B3.3) 단일결함이거나 혹은 두 번째 결함과 결부된다면 위험할 수 있는 첫 번째 결함은 검지되고 두 번째 결함으로부터 안전하도록 하기 위해 정해진 정량화된 목표 이내의 충분히 짧은 시간 내에 안전한 상태로 가야하며, 정량적인 분석을 통해 입증되어야 한다.

(IEC62425 5.4 B3.3) 허용된 시간 이내에 결함 검지 및 회피를 위해 사용되는 기법들을 입증하기 위한 계산이 제시되어야 하며, 계산에 사용된 고장률 등 기본 데이터의 출처와 분석방법이 명백하게 설명되어야 한다.

(IEC62425 5.4 B3.4) 첫 번째 결함 후 안전상태로 들어가거나 유지되어야 하며, 후속 결함이 안전 상태를 해지시켜서는 안된다.

(IEC62425 5.4 B3.5) 직접적으로 혹은 후속결함과 조합하여 위험할 수 있는 다중결함은 검지되어야 하며 정해진 목표 이내의 충분히 짧은 시간 내에 안전한 상태로 가야하며, 정량적인 분석을 통해 입증되어야 한다.

6.5.2 안전상태의 유지

시스템/하부시스템/장치는 단일결함이 발생한 상황에서 목표 THR을 충족해야 된다. 특히 SIL 3·4등급에 해당되는 시스템은 발생 가능한 것으로 알려진 모든 종류의 단일결함에 대해서도 안전한 상태를 유지할 수 있어야 하며, 이러한 개

념을 안전측 동작(Fail-safe)이라 한다. 시스템/하부시스템/장치가 안전측 동작을 달성하기 위해서는 다음의 사항들이 수행되어야 한다.

- 하드웨어 구성요소 고장모드의 확인
- 확인된 고장모드에 대해서 안전한 상태를 유지하기 위해 안전측 동작 기법을 적용하여 설계
- 확인된 구성요소의 고장모드를 구조적 분석방법 등을 통해 치명적인 단일하드웨어 결함이 없음을 FTA나 FMEA 같은 고장분석 방법을 통해 입증

하나의 시스템 하부 모듈별 각 방법들 중 같은 구조 또는 각기 다른 구조를 사용할 수도 있고 때에 따라서는 복합적으로 적용할 수도 있다. 각 방법들을 적용한 정당한 이유와 실제 모듈에 적용한 구조, 동작메커니즘에 대해 상세히 설명하여야 한다. 이러한 안전측 동작을 이루기 위해서는 다음과 같은 방법들이 적용되어질 수 있다.

[중략]

6.5.3 결함의 영향 최소화

6.5.4 결함의 검지 및 회피

6.7 안전관련 응용조건

시스템/하부시스템/장치가 어떤 응용에 적용될 때 준수되어야하는 규칙, 조건, 제한 등에 대한 설명 등이 포함될 수 있으며, 종합안전대책기술서의 다른 부분에 반영된 것을 제외한 프로젝트 시스템이 실제 적용되기 위해 필요한 조건들이 이 절에서 제시하여야 한다. 본 절에서는 이러한 운용조건들이 다른 부분에 반영되어 있지 않으면 포함시켜야 한다.

6.7.1 관련규정

(IEC62425 5.4) 시스템의 적용 시에 관측되어야 하는 기능적인 안전에 관한 규정, 조건 및 제약조건을 정의해야 한다.

6.7.2 일반적인 응용조건

시스템/하부시스템/장치가 특정 환경에 응용되거나 운영, 유지보수 되어질 때 각 SIL 등급별 조치해야할 방법들은 다음과 같다.

[표생략 : SIL 등급별 응용, 운용 및 유지보수]

시스템/하부시스템/장치가 운용될 때 준수되는 규칙, 조건, 제한 등을 다음과 같이 일반적인 항목과 몇몇 특정한 항목들로 나누어져 있는 내용들은 안전관련 응용조건에서 고려되어야한다. 안전관련 응용조건에서 고려되어야 하는 일반적인 항목은 다음과 같다.

- *특정 운용에 적합하도록 장치의 환경변수 설정*
- *제작, 설치, 시운전에 있어서의 주의 사항*
- *결함 검지와 유지보수를 위한 규정 및 방법*
- *시스템 운용을 위한 지침*
- *안전 경고 및 주의사항*
- *전자파 적합성(EMC) 주의사항*
- *시스템 수정 및 폐기에 대한 정보*
- *설치, 운용, 유지보수 등을 지원하는 검사장비, 설정도구 등과 같은 보조 장비에 대한 안전성 입증문서*

6.7.3 하부시스템/장치 설정 및 구축

가) 장치의 설정

하부시스템/장치가 적용되는 환경에 맞도록 설정되어져야 한다면, 어떤 설정도구 또는 절차가 정의되어져야 한다. 다음과 같은 내용들이 포함되어야 한다.

- *설정 절차*
- *버전 관리*
- *응용되는 장치의 하드웨어 요구조건*
- *응용되는 장치의 소프트웨어 내역*
- *소프트웨어 유지보수*

[중략]

5.7.4 운영 및 유지보수

6.7.5 운영 시 안전감시

6.7.6 폐기처분

6.8 안전품질 시험

기능적 안전 요구사항이 충족된다는 것을 입증하기 위해 실시하는 테스트 또는 평가 활동 이외에, 다음과 같은 목적으로 안전품질 시험을 수행하고 그 결과가 종합안전대책기술서에 반영되어야 한다.

- *프로젝트 시스템이 정해진 운용상의 요구사항을 충족한다는 것에 대한 안전성 평가자에 대한 신뢰성 향상*
- *요구되는 신뢰도 및 안전성 목표를 충족한다는 것에 대한 안전 평가자에 대한 신뢰성 향상*
- *최종 안전성 승인 전에 예방책 및 감시를 제공함으로써 시스템이 상업운영 될 수 있도록 하기 위함*

6.8.1 관련규정

(IEC62425 5.4) 동작조건 하에서 안전품질시험이 성공적으로 수행되었음을 증명하는 자료들이 포함되었는지 확인한다.

이 안전품질시험은 이미 실시한 테스트의 수준이나 운용환경 시험 결과 등을 감안하여 프로젝트 시스템 공급업자와 철도운용자간의 협의에 의해 적절한 시험항목 및 방법, 수준 등을 결정하거나 다른 인증시험으로 대체할 수 있다. 이 시험기간 동안에는 시스템의 안전성은 완전한 것이 아니므로 적절한 예방책, 절차, 감시등이 제공되어야하고, 안전품질시험의 수행 및 결과를 포함하는 모든 기록은 본 절에 문서화되어야 한다.

실험실에서의 시스템이 실제 선로변이나 차상으로 설치되어 운용될 경우 모든 계절과 스트레스 조건을 대상으로 하는 기간을 스트레스/에이징 테스트로 시뮬레이션할 수 있다. 사실 실제 운용환경 테스트를 할 때는 환경변수와 조건을 모두 통제할 수 없으므로 에이징 조건을 현재의 실험실 수준에서 실시하는 것이 적절하다.

복잡한 시스템인 경우에는 새로운 시스템을 상업운용하기에 앞서 새로운 시스템을 엄격한 감독 하에 일정기간 동안 임시운영하고, 이 기간동안 다양한 테스트를 통해 프로젝트 시스템의 안전성을 확신할 수 있는 근거(기존 시스템을 병행하여 운영, 인원 증가 등)들을 정리 및 제시하여야 한다.

본 절에서는 이러한 안전품질시험이 완료될 때까지 프로젝트 시스템의 사용제한 규정, 안전품질시험 동안 테스트 및 시범 운영에 대한 정보들을 정리 및 제시하여야 한다.

6.8.2 체크리스트

평가 ID	평가 항목	만족도 (N~F)	측정 결과	비고
EC 4-1-1	프로젝트의 종합대책기술서에 기술안전보고서가 포함되어 있는가?			
EC 4-1-2	기술안전보고서는 '서론', '정확한 기능적인 동작의 보장', '결함의 영향', '외부영향에 대한 동작', '안전 관련된 응용조건', '안전성 품질조건'으로 구성되어 있는가?			
EC 4-1-3	안전성이 요구되는 시스템의 범위는 설명되어 있는가?			
EC 4-1-4	안전성이 요구되는 시스템 설계의 개략적인 설명이 포함되어 있는가?			
EC 4-1-5	프로젝트 시스템 설계의 기술적 안전을 위해 적용한 규격이나 표준들이 명시되어 있는가?			
EC 4-2-1	규정된 운용과 안전요구사항들에 따르는 정상적인 상황에서 시스템의 정확한 동작을 입증하기 위한 근거들이 정리되어 있는가?			
. . .	. . .			
EC 4-2-28	프로젝트 소프트웨어 검증 보고서가 IEC62279에서 요구하는 내용에 따라 작성되었는가?			

EC 4-2-29	프로젝트 소프트웨어 기능 보증의 확인 ※철도연에 작성한 '열차제어시스템 소프트웨어 안전성 평가 가이드라인'에 따른 소프트웨어 평가결과를 준용하여 본 "평가항목"을 대체함			
. . .	. . .			
EC 4-8-3	안전품질시험의 수행과정 및 결과는 제시되어 있으며 그 결과가 적절한가?			

7. 관련된 종합안전대책기술서

프로젝트 시스템의 종합안전대책기술서는 그 시스템을 구성하는 구성요소인 하부시스템이나 장치의 종합안전대책기술서에 의존적인 경우가 있다. 이러한 경우에는 프로젝트 시스템의 안전성 승인 이전에 하부시스템이나 장치에 대한 안전성 승인이 이루어져야 한다. 본 절에서는 최종 시스템의 구성요소에 관련된 종합안전대책기술서에 대한 내용을 포함하여야 한다.

7.1 관련규정

(IEC62425 5.5.4) 하부시스템/장치에 대한 참조 종합안전대책기술서가 포함되어 있는지 확인한다. (IEC62425 5.5.4) 관련된 하위 레벨의 하부시스템/장치의 응용조건이 상위레벨의 응용조건에 부합하는지 확인한다.

종합안전대책기술서는 일반제품, 일반응용, 특정응용 3 가지의 종류로 나눌 수 있다. 일반제품 종합안전대책기술서는 그림에서와 같이 전체 시스템 구조에서 하위 레벨의 제품화된 장치에 대한 안전성 입증문서이고 일반응용 종합안전대책기술서는 시스템에서 일반적인 기능으로 이루어진 하부시스템에 대한 안전성 입증문서이다. 특정응용 종합안전대책기술서는 특정한 응용에만 적용되어서 사용되는 시스템에 대한 문서이다.

[그림 생략 : 종합안전대책기술서-안전성 승인 사이의 위존 관계]

일반제품과 일반응용 종합안전대책기술서는 안전성 승인이 달성되었다면 특정 응용의 안전성 승인에 대한 참조 종합안전대책기술서로 사용될 수 있다. 이 경우 각 하위 레벨의 종합안전대책기술서에 대한 안전성 승인은 반복할 필요가 없다. 이러한 의존관계에서 반드시 지켜야하는 것은 각 하위 레벨의 종합안전대책기술서의 응용조건은 상위레벨의 종합안전대책기술서의 응용조건을 충족하여야 한다. 그렇지 못하다면 상위 레벨의 안전관련 응용조건들이 각 하위 레벨의 종합안전대책기술서에서 수행되어야 한다. 이미 다른 응용에 사용을 통해 검증된 하부시스템/제품을 재사용하는 경우 다음 사항들이 제시되어야 한다.

- 기존 안전성 및 검증 문서
- 기존의 현장 경험과 관련 정보

7.2 체크리스트

평가 ID	평가 항목	만족도 (N~F)	측정 결과	비고
EC 5-1-1	프로젝트 시스템의 하부시스템/장치에 대한 모든 종합안전대책기술서가 포함되어 있는가?			
EC 5-1-2	관련된 하위 레벨의 시스템/장치의 응용조건이 상위 레벨의 응용조건에 부합하는가?			
EC 5-1-3	상위 레벨의 응용조건에 부합하지 못한 하위 레벨의 종합안전대책기술서는 상위 레벨의 응용조건에 맞춰서 다시 수행되었는가?			

■

제2절 열차제어시스템 S/W 안전성 평가기술 개발

	검증계획서 **(Verification Plan)**	ID No : TC - SR03 - SSR01 - 2010 작성일 : 2010. 05. 14 수정일 :

3. 프로젝트는 열차제어시스템 소프트웨어 안전성 평가기술을 개발하여야 한다.

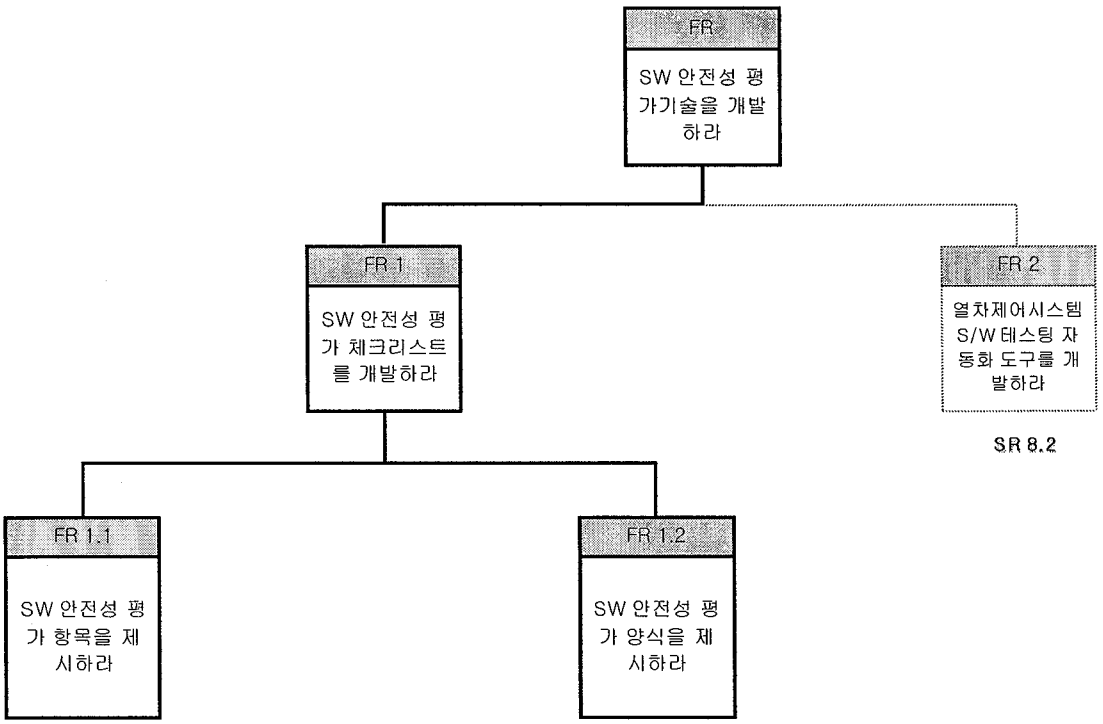
3.1 프로젝트는 열차제어시스템 소프트웨어 안전성 평가기술을 개발하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 안전핵심 S/W 안전성 평가 체크리스트 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 3.1 국제규격 부합 - 3.3 전문가 검토	- SE 검증	- 수정 VRTM - 검증결과표

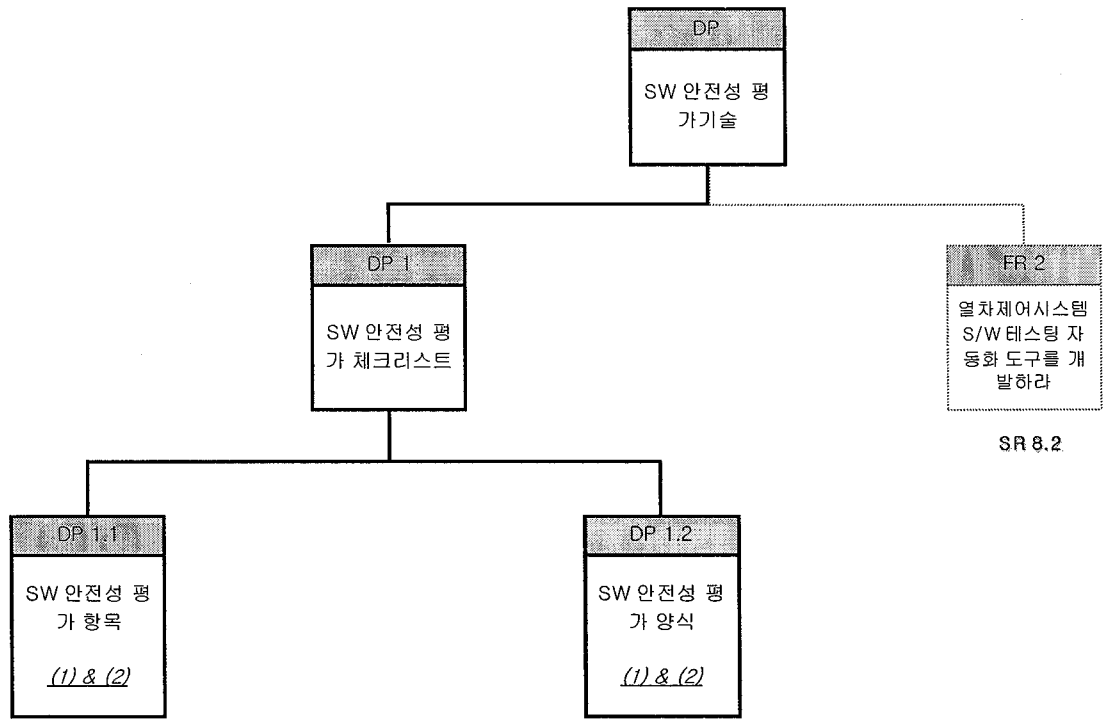
Verification Specification (검증기준) :

1. 안전성 평가 체크리스트의 작성 근거가 적합한가?
2. 국제규격의 요구사항을 반영하고 있는가?
3. 전문가 자문을 수행하였는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

열차제어시스템 소프트웨어의 안전성 평가 체크리스크의 작성은 『SR 3. 프로젝트는 열차제어시스템 안전성 평가기술을 개발해야 한다.』 중 **『SSR. 3.1. 프로젝트는 열차제어시스템 소프트웨어 안전성 평가기술을 개발하여야 한다.』**에 해당하는 내용이다. 당해연도 과제에서는 전년도에 작성한 열차제어시스템 소프트웨어의 안전성을 평가하기 위한 세부 절차 및 기준을 제시한 평가 가이드라인을 보완하여 작성하였다. 특히 평가항목을 제시하는 체크리스트를 중점으로 보완하였다.

나. 설계기준

○ 다음과 같은 소프트웨어 안전성 평가와 관련된 국제규격을 참고하였다.

- IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety - related systems", 2004.
- IEC 62279, "Railway Applications : Communications, Signalling and Processing Systems - Software for Railway Control Protection Systems", 2004.
- MOD 0055, "Requirements for Safety Related Software in Defence Equipment"
- DO 178B, "Software Considerations in Airborne Systems and Equipment Certification"

다. 검증 방법에 따른 증거 자료

전년도 연구개발을 통하여 제시된 열차제어시스템 소프트웨어의 안전성 평가 체크리스트는 소프트웨어 안전성 관련 국제표준인 IEC 61508을 기본으로 하여 작성하였으며, 구체적인 평가항목들은 열차제어 소프트웨어 안전성 관련 규격인 IEC 62279를 적용하여 작성된 초안이다. 당해연도는 전년도 연구결과를 바탕으로 일반 소프트웨어 안전성 국제 표준인 IEC 61508과 열차제어 분야의 국제표준인 IEC62279, 영국 국방기술 분야의 MOD0055, 항공SW 인증체제인 DO-178B를 참고

하여 작성되었다. 이 문서에서 설명하는 평가방법은 IEC61508의 요구사항과 더불어 MOD0055, DO-178B의 평가요건의 일부분을 바탕으로, IEC62279의 열차제어 소프트웨어 분야에 특화시켜 평가하는 방식을 채택하였다. 당해연도 연구에서는 국내의 소프트웨어 테스팅 전문 기관으로부터의 기술자문을 통해 이 부분을 중점적으로 수정하는 보완 과정을 거쳐 최종 열차제어시스템 소프트웨어 안전성 평가 체크리스트를 작성하였다.

라. 성과물의 내용 및 결과

(1) 국내외 SW 안전성 평가관련 개발현황

최근 철도 열차제어시스템에서 사용되는 장치들에 소프트웨어 활용이 증가됨에 따라 열차제어시스템에서의 소프트웨어 안전성이 핵심 이슈로 부각되고 있다. 소프트웨어는 하드웨어와는 다르게 소모, 마멸되지 않기 때문에 있기 때문에 소프트웨어의 안전성을 확보하기 위해서는 개발 단계에서 엄격히 지켜야 하는 절차, 기법 등을 적용하도록 권고하고 있다. 본 연구는 열차제어시스템에 포함되는 소프트웨어 안전성을 평가하기 위한 체크리스트를 개발하기 위한 것이다. 이 체크리스트는 다양한 국제 표준 및 사실 표준 등에서 제안하는 프랙티스를 종합하여 정리한 것이다. 개발 단계, 운영 및 유지보수 단계 등 소프트웨어의 생명주기 내에서 적용해야 하는 프랙티스, 절차, 기법 등을 정리하고 있다. 그리고, 각 기법에 대한 설명, 메트릭 등 평가에 필요한 관련 정보도 포함하고 있다. 그리고 해당 체크리스트는 실제 평가에서 활용할 수 있도록 워크시트로 개발되었다.

(가) 국내의 경우

국내 소프트웨어 안전성 평가 기술은 하드웨어의 안전성 평가 기술에 비해 그 발전 속도가 늦다. 소프트웨어의 경우 시스템 상의 하드웨어의 한 부속품으로 간주되어 그 중요성이 많이 상대적으로 축소되었다. 또한 국내에서 사용되는 대부분의 안전성이 보장되어야 하는 소프트웨어들은 외산 소프트웨어가 그대로 도입되어 사용되는 경우가 많아 실질적으로 안전성을 평가하는 기술이 적용될 수 있는 기회가 적었다고 할 수 있다. 다음 표는 국내외 관련 기술 동향을 간략히 요약한 것이다.

표 3.2.1 SW 안전성 평가기술 국내외 동향

분야	표준	국내외 동향
원자력 안전 소프트웨어	IEC 60880 IEEE 7-4.3.2	(국외) - 엄격한 기준에 의해 인정받은 원전용 산업용 PLC만 사용하도록 함(예: ABB사:AC160, 지멘스: Teleperm-XS, Mitsubish:PWR 등) (국내) - 신고리 3&4 호기 안전계통 설계하여 계통설계기술 자립함 - 원자력법령을 기반으로 원자력안전규제 기술기준을 제정하여 엄격하게 운영중
철도용 안전 소프트웨어	EN 50126 IEC 62279	(국외) - 철도 RAMS(reliability, availability, maintainability, safety) 기준을 충족하는 것을 요구함 - 독일,프랑스,일본 등의 선진국이 주도함 (국내) - 대부분 검증된 선진국 제품을 도입하여 사용함 - 철도안전법을 기반으로 SIL에 따른 "철도소프트웨어안전기준"을 제정함
항공시스템용 안전 소프트웨어	DO-178B	(국외) - 미국 RTCA에서 개발하고 FAA에서 승인 받은 것 - 5가지의 Safety 수준을 정의하고 각 수준 별 준수해야 하는 요구사항을 정의함 - 인증통과 실시간 OS: VxWorks, LynxOS-178, Integrity-178B, uC/OS-II, Nucleus 제품 등 (국내) - KAI 주관의 국책연구사업에서 수행중인 소프트웨어 개발에서 DO-178B 기준을 통과함
자동차시스템용 소프트웨어	ISO 26262	(국외) - IEC 61508을 자동차 분야에 맞게 조정중(현재 Draft 상태) - Part 6가 차량용 전장 소프트웨어 관련 표준임 - SIL과 유사한 ASIL(Automotive Safety Integrity Level)을 A에서 D까지 정의함 (국내) - 해외 OEM 업체들의 요구로 ISO 26262에 대해 대응 중
기타	IEC 61511 IEC 62061 IEC 60601	- 공정(process) 분야, 기계 분야, 의료장비 분야에 대한 안전관련 시스템 또는 소프트웨어 규격이 있음

본 연구는 전년도 연구결과인 열차제어 소프트웨어의 안전성 평가 체크리스트를 수정, 보완한 것으로 열차제어시스템 전문가들과 소프트웨어 테스팅관련 전문기관의 기술자문을 통해 평가항목을 중점적으로 수정 보완하였다. 본 연구에서 활용한 시스템 및 소프트웨어 안전성 관련 국제규격인 IEC 61508과 철도시스템 분야의 규격인 IEC 62279 등에서 요구하고 있는 평가 항목들 중, 소프트웨어 테스팅 자동화 도구로 구현이 가능한 것들은 자동화 도구 개발 모듈에 반영하였다. 따라서 본 평가 가이드라인 중 본 연구과제를 통해 개발하고 있는 소프트웨어 테스팅 자동화 도구에서의 정량적인 분석 결과가 가능한 부분은 개발하고 있는 자동화 도구의 결과를 활용하도록 하였다.

(나) 국외의 경우

국외의 경우 SW 안전성의 중요성을 조기에 파악하여 SW 안전성을 정량화하는 방법으로 SIL(Safety Integrity Level)을 정의하여 사용하여 왔다. SIL은 안전성, 보안성, 소프트웨어 복잡성, 성능, 신뢰도 또는 다른 소프트웨어 특성들을 포함할 수 있다. 국제 표준에서 정의하고 있는 SIL은 0~4 수준까지 있으며, SIL이 높을수록 더욱 안전한 시스템을 나타낸다. 특히 안전성에 관한 대표적 표준인 IEC 61508을 제정하였고, 그 중 Part 3은 소프트웨어 안전성에 관한 내용을 포함하고 있다.

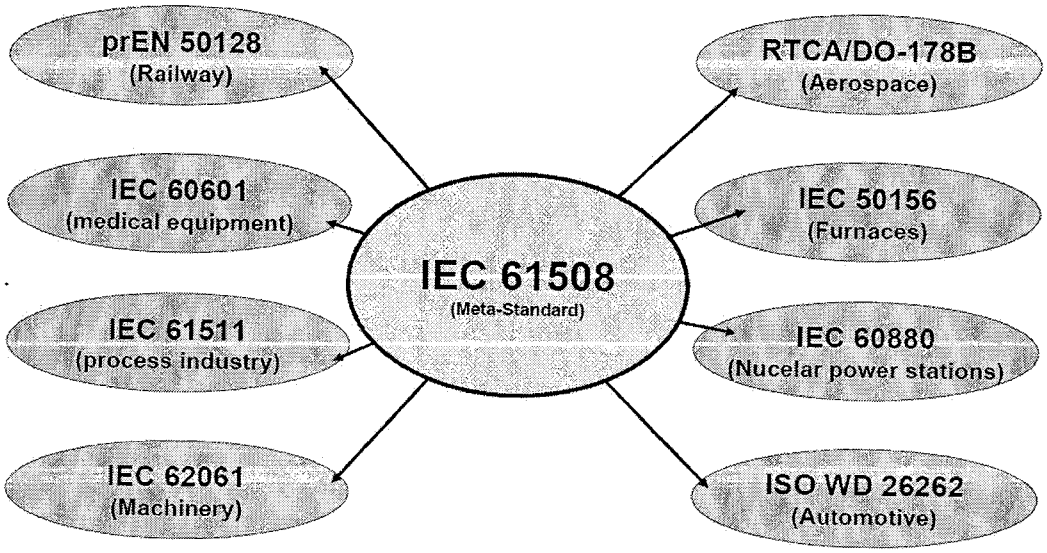


그림 3.2.1 IEC 61508에 기반한 각 분야별 활용 규격

이 표준은 안전성을 확보하기 위해 관리체계, 개발 체계, 지원 체계 등을 갖출 것을 권고하고 있으며, SIL 수준에 따라 소프트웨어 개발 단계에서 적용하여야 하는 기법을 권고하고 있다. 해외에서는 IEC 61508을 기준으로 다양한 표준들이 개발되어 활용되고 있으며, 특히 SW의 경우 별도의 표준을 제정하여 활용하고 있다. 다음은 IEC 61508 표준이 여러 다양한 분야에 적용되어 사용되는 예를 보여주고 있다. 안전성이 강조되면서 기존의 프로세스 평가 모델에도 안전성을 강조하여 확장한 모델을 개발하고 있으며, 다음과 같이 CMMI 및 ISO/IEC 15504를 확장하고 있다.

- +SAFE - A Safety Extension to CMMI, 2004
- ISO/IEC 15504 Part 10 - safety extension(신규개발항목)

SIL 과 유사한 개념으로 RTCA/DO-178B 기준에서는 Class 개념을 도입하고 있으며, 자동차 분야에서는 ASIL 을 별도로 정의하고 있다. 영국에서는 ISO 9000 과 같은 신뢰성 인증 체계(framework)를 운영하고 있다. UKAS(United Kingdom Accreditation Body)에서는 ISO 9001을 인증하는 기관을 인정해 주는 것과 마찬가지로 SIRA 및 BASEEFA 2001 두 개의 기관으로 하여금 IEC 61508에 기반하여 인증 서비스를 제공할 수 있도록 인정하였다. 적용기준으로 CASS Ltd(Conformity Assessment Safety-related Systems)를 제정하였다.

독일의 경우 TUV(Technischer Uberwachungs Verein) 시험소에서는 자체 명성에 기반하여 IEC 61508 표준을 기반으로 인증을 부여하고 있다. 미국의 경우 Factory Mutual에서 IEC 61508을 포함한 다양한 표준에 의해 인증을 부여하고 있다. UL(Underwriters Laboratory) 마크는 다양한 제품에 대한 안전성을 보장해 주는 역할을 한다. 그 외 덴마크 Delta 사에서는 자체적으로 화재경보기(Fire Alarm System)과 같은 안전과 관련된 분야에서 자체 인증 마크를 부여하고 있다.

(2) 열차제어시스템 SW 안전성 평가 체크리스트

(가) 평가방법

① 개요

본 장에서는 열차제어 소프트웨어 안전성 평가방법과 절차에 대해 설명한다. 소프트웨어 안전성 인증은 소프트웨어가 설계과정에서 도출된 목표 안전도 등급을 어느 정도 달성하였는가를 평가하고, 그 결과에 의거하여 목표의 달성 여부를 판단하는 과정이다. 본 평가안내서에서는 일반적인 전기전자관련 안전성 표준인 IEC61508과 열차분야의 안전성 표준인 IEC62279를 평가의 기준으로 사용하였다. 소프트웨어의 기능 안전성을(Functional Safety) 평가하고, 소프트웨어 개발과 관련한 개발수명주기에서의 전반적인 안전성 활동의 수준을 평가하여, 피인증 소프트웨어의 기능 안전성(Functional Safety)과 안전무결성 등급(Safety Integrity Level)을 검증하고, 그 결과가 목표로 한 소프트웨어 안전성에 얼마나 부합했는지(Conformance)에 따라 인증여부를 결정한다.

② 평가기준

본 문서에서 제안하는 소프트웨어 안전성 평가는 IEC61508 및 IEC62279에서 요구하는 사항들에 대한 만족도를 평가한다. 상기 국제표준에서 정의하고 있는 요구사항은 크게 문서화, 소프트웨어 품질관리 체계, 소프트웨어 안전수명주기 요구조건, 기능안전성 평가의 네 가지 분야로 구성되어 있다.

문서화 만족도 평가는 소프트웨어 개발과정에서 문서들이 체계적으로 작성되고 있으며, 관리되고 있는지를 평가한다. 문서들은 소프트웨어의 기능 안전성과 안전무결성 등급 판정을 위하여 요구되는 근거자료들을 체계적이며 명료하게 기술하고 있어야 한다.

소프트웨어 품질관리체계 평가는 소프트웨어 개발주기 동안의 관리 및 기술적 활동에 대한 만족도를 평가한다. 소프트웨어 개발 전주기에 대한 안전성활동 계획을 정의해야 하고, 소프트웨어 형상관리의 적절성 여부도 주요 평가대상이다.

소프트웨어 안전수명주기 요구조건평가는 안전성 생명주기의 각 프로세스마다 피인증 소프트웨어의 개발이 표준에서 요구하는 절차를 어느 정도 충족하고 있는지를 평가한다.

기능안전성 평가는 안전성 생명주기의 각 프로세스마다 평가하는 소프트웨어의 목표 안전무결성 등급(SIL Level)에서 요구되는 항목들의 만족도를 평가한다.

③ 평가절차

소프트웨어 안전성 평가 과정은 특정 기관이 개발한 소프트웨어의 기능 안전성 및 안전무결성과, 소프트웨어가 표준에서 요구하고 있는 문서화 및 품질보증절차를 따라 개발되었는지를 평가한다.

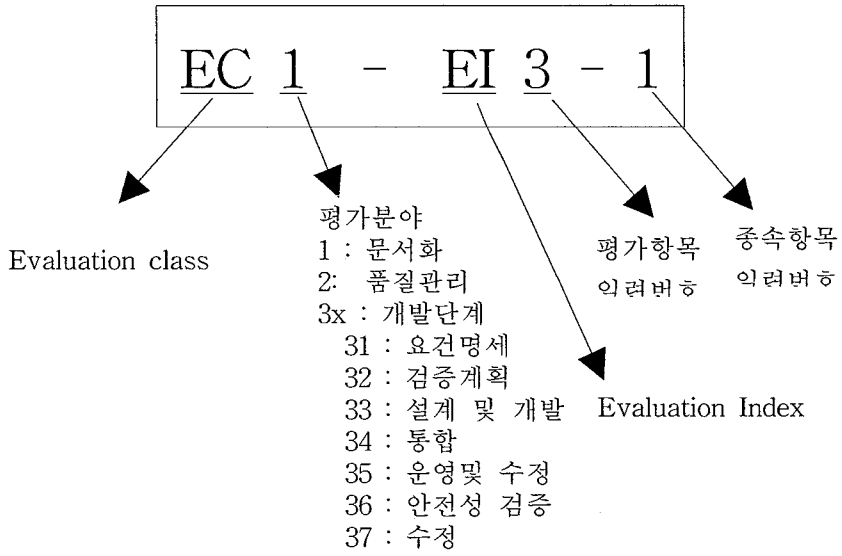
④ 만족도 평가

평가자는 소프트웨어 안전성 평가를 위해 다음의 정량적 기준을 이용하여 요구조건들의 만족도를 4단계로 평가한다.

a) F	*Fully achieved*	*85% 초과 100% 이하 만족*
b) L	*Largely achieved*	*50% 초과 85% 이하 만족*
c) P	*Partially achieved*	*15% 초과 50% 이하 만족*
d) N	*Not achieved*	*0% 이상 15% 이하 만족*

⑤ 평가항목의 구분

본 문서에서는 문서화, 기능안전성관리, 개발단계별 안전성평가, 기능안전성평가 등의 4개 분야에서 평가를 수행하도록 제안하고 있으며, 각 분야별로 별도의 체크리스트를 제공하여 평가가 이루어지도록 하였다. 각 체크리스트의 평가ID는 다음과 같이 부여하였다.



⑥ 체크리스트 구성요소 및 구성방법

본 문서에서 제공하는 체크리스트는 주요 4개 분야인 문서화, 기능안전성관리, 개발단계별 안전성평가, 기능안전성평가와 더불어 평가 기준과 산출물 특성, 기법 설명, 용어정의 등으로 구성되어 있다. 주요 4개 분야는 프로세스별로 공통 평가항목과 SIL 평가항목 등 3개 부분으로 분류되어 평가가 수행되도록 구성되어있다. 각 평가항목은 요건, 산출물, 증거, 평가에 대한 상세내용을 확인 및 평가하도록 구성되었다. 체크리스트의 구성은 아래와 같다.

분류	요건					산출물		증거	평가		
	평가 ID	평가항목	고려사항	평가ID (평가안내서)	관련 표준	산출물명	관련 표준		세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1			EC32-E11							
	2										
	3										
SIL	SIL1										
	SIL2										
	SIL3										
	SIL4										

(나) 평가방법

■ *가. 열차제어시스템 SW 안전성 평가 문서화*

본 절에서는 IEC61508와 IEC62279, MOD 0055에서 정의된 소프트웨어 개발의 문서화 요건을 바탕으로 피인증 소프트웨어의 문서화 정도를 평가하기 위한 만족도 평가항목을 제안한다. 본 절에서 문서로 인정되는 매체는 스크린이나 디스플레이로 표현될 수 있는 컴퓨터 파일, 종이, 필름 등이다.

(관련규정 및 평가 항목)

(IEC61508-1 5.2.1) (IEC61508-1 5.2.2) (IEC61508-1 5.2.3) (IEC61508-1 5.2.6)

(IEC61508-1 5.2.7) (IEC61508-1 5.2.8) (IEC61508-1 5.2.9) (IEC61508-1 5.2.10)

(IEC61508-1 5.2.11) (IEC62279 표 A.1)

(MOD0055 32.1) (MOD0055 32.2) (MOD0055 32.3)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출 물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	문서 내용	소프트웨어 개발단계마다 필요한 문서들이 작성 되었는가 ?	EC32-E11	Part 1 5.2.1	개발 문서				
			기능안전성 관련내용을 포함하고 있는가 ?	EC1-EI2	Part 1 5.2.6	상동				
			⋮			상동				
SIL	SIL 1	기법	"SW 계획서"를 사용하는가?		표A.1(62279) 0055/32.1	SW 계획서	62279/표A.1 0055/32.1			
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	< SIL 3 기법과 동일>		표A.1(62279)					

이와 같이 Check List 작성 방법을 순서대로 설명하면 다음과 같다. 먼저 평가 항목을 앞서 언급한 방법을 적용하여 평가 ID별로 분류한 후, 관련 표준에 근거한 평가항목을 추출해 낸다. 그 후, 적용 수준 및 측정 결과와 만족도를 평가하여 결과를 작성하는 것이다. 같은 방법을 적용하여 앞으로의 각 장에 정리되어 있는 Check List도 작성하면 되는 것이다.

나. 열차제어시스템 SW 기능안전성관리

본 절에서는 소프트웨어의 기능안전성을 보장하기 위하여 IEC61508에서 정의된 소프트웨어 품질 관리 시스템을 기반으로 피인증 소프트웨어의 기능안전성관리에 대한 만

족도 평가항목을 제안한다.

(IEC61508-1 6.2.1) (IEC61508-1 6.2.2) (IEC61508-3 6.2.3) (IEC61508-3 6.2.4)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	안전 관리 및 기술 활동 명시	1.1 안전 방침 및 전략을 명시하고 있는가?	EC2-EI1	Part 1/6.2.1(a)	☞ 안전관리 계획서				
			⋮							
	2	검토	2.1 상기 요건들이 관련조직에 의해 공식적으로 검토되고 합의되는가?	EC2-EI2	Part 1/6.2.2	☞ 안전관리 계획서				
	3	수행	3.1 상기 활동들이 실행되고 진도를 감시하는가?	EC2-EI3-1 EC2-EI3-2 EC2-EI3-3	Part 1/6.2.3	☞ 안전관리 계획서				
	4	공급자	4.1 공급자는 조직이 명시한 제품 및 서비스를 전달하고 적절한 품질경영시스템을 갖추고 있는가?	-	Part 1/6.2.4	☞ 안전관리 계획서				
SIL	SIL1	기법	별도 사항이 없음							
	SIL2	기법	별도 사항이 없음							
	SIL3	기법	별도 사항이 없음							
	SIL4	기법	별도 사항이 없음							

다. 열차제어시스템 SW 개발 단계별 안전성 평가

(1) 소프트웨어 안전 요건 명세(specification)

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 안전 요건 명세에 대한 소프트웨어 개발과정의 만족도 평가항목을 제안한다.

(IEC61508-3 7.2.2.2) (IEC61508-3 7.2.2.3) (IEC61508-3 7.2.2.4) (IEC61508-3 7.2.2.5)

(IEC61508-3 7.2.2.6) (IEC61508-3 7.2.2.7) (IEC61508-3 7.2.2.8) (IEC61508-3 7.2.2.9)

(IEC61508-3 7.2.2.10) (IEC61508-3 7.2.2.11)

(IEC62279 8.4.2) (IEC62279 8.4.13) (IEC62279 표A.2) (IEC62279 표A.15)

(DO178B 11.9)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	SW 안전 요건 명세 도출	1.1 SW 안전 요건명세가 시스템에서 규정한 안전 요건에서 도출되었는가?	-	Part3/7.2.2.2	소프트웨어 안전 요건 유도근거				
			⋮							
	⋮	⋮	⋮							
	5	SW안전 요건 시험 명세	5.1 SW 안전요건명세로부터 SW요건시험명세가 개발되었는가?	-	62279/8.4.13	☞ SW안전요건명세 SW요건시험명세	Part3 /표1			
SIL	SIL 1	기법	"구조적 방법론(Structure Methodology)"을 사용하는가?		62279/표A.2					
	⋮	⋮	⋮							
	SIL 4	기법	정형기법(Formal methods)을 사용하는가?		Part3/표A.1 62279/표A.2					

(2) 소프트웨어 안전성 검증(Validation) 계획 수립

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 안전성 검증 계획단계에 대한 소프트웨어 개발과정의 만족도 평가항목을 제안한다.

(IEC61508-3 7.3.2.1) (IEC61508-3 7.3.2.2) (IEC61508-3 7.3.2.3) (IEC61508-3 7.3.2.4)
(IEC61508-3 7.3.2.5)
(MOD 0055/34.3.6) (MOD 0055/34.3.8)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물 명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	SW 안전 검증 수립 여부	1.1 SW 안전요건 충족 사실을 검증하기 위한 계획이 수립되었는가?	-	Part3/7.3.2.1	☞ SW 안전 검증 계획서				
	2	SW 안전 검증 계획 포함 내용	2.1 검증 시기가 명시되었는가?	EC32-EI1	EC32-EI2	☞ SW 안전 검증 계획서	Part3 /표1			
			:							
	3	SW 안전 검증 계획 검토	3.1 검증 절차의 일부로서 SW 안전 검증 계획의 범위 및 내용이 검토되었는가?	EC31-EI5	Part3/7.3.2.4	☞ SW 안전 요건 명세	Part3 /표1			
SIL	SIL 1	기법	별도사항이 없음							
	SIL 2	기법	별도사항이 없음							
	SIL 3	기법	별도사항이 없음							
	SIL 4	기법	별도사항이 없음							

(3) 소프트웨어 설계 및 개발

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 설계와 개발 단계에 대한 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 소프트웨어 설계와 개발 단계의 평가항목은 공통적으로 적용되는 일반 평가항목과 IEC61508에서 정의된 내용을 따라서

- *소프트웨어 구조의 평가항목(5.3.4)*
- *지원도구(tools)와 프로그래밍 언어를 위한 평가항목(5.3.5)*
- *상세한 설계와 개발을 위한 평가항목(5.3.6)*
- *코드 실행(implementation) 평가항목(5.3.7)*
- *소프트웨어 모듈 테스팅 평가항목(5.3.8)*
- *소프트웨어 통합 테스팅 평가항목(5.3.9)*

로 나뉘어서 제안된다.

(관련규정)

(IEC61508-3 7.4.2.2) (IEC61508-3 7.4.2.3) (IEC61508-3 7.4.2.4) (IEC61508-3 7.4.2.5)
(IEC61508-3 7.4.2.6) (IEC61508-3 7.4.2.7) (IEC61508-3 7.4.2.8) (IEC61508-3 7.4.2.9)
(IEC61508-3 7.4.2.10)
(DO178B/ 11.7) (DO178B/ 11.10)
(MOD 0055/30.4) (MOD 0055/30.5) (MOD 0055/30.2)

(평가항목(Check List))

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	설계 방법 내용	1.1 설계 방법은 복잡도를 관리할 수 있도록 추상화, 모듈화 및 기타 방법을 포함하고 있는가?	EC33-EI1, EC33-EI2	Part3/7.4.2.2 (a) Part3/7.4.2.2 (b) DO178/11.7, 11.10	설계 지침				
			. . .							
	. . .	. . .	. . .							
	3	설계 원칙	3.1 설계 시 안전성 변경에 따른 시험가능성 및 용량이 고려되는가?	EC33-EI3	Part3/7.4.2.3	설계 지침				
			. . .							
SIL	SIL 1	기법	별도사항이 없음							
	SIL 2	기법	별도사항이 없음							
	SIL	기법	별도사항이 없음							

	3									
	SIL 4	기법	별도사항이 없음							

(소프트웨어 구조 관련규정 및 평가항목)

(IEC61508-3 7.4.3.2) (IEC61508-3 7.4.3.3) (IEC61508-3 표A.2)

(IEC62279 9.4.3) (IEC62279 9.4.6) (IEC62279 9.4.10) (IEC62279 표A.3)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	아키텍처 설계 포함 내용	1.1 SW아키텍처 설계시 기법들을 선정하고 그 타당성을 제시하고 있는가?		Part3/7.4.3.2 (a)	☞ SW아키텍처설계서				
			:							
	2	변경 관리	2.1 SW아키텍처 설계가 적용된 후 발생한 변경사항은 문서화되고 승인을 받았는가?	EC33-EI6, EC33-EI7, EC33-EI8, EC33-EI9, EC33-EI10, EC33-EI11	Part3/7.4.3.3 62279/9.4.6	☞ SW아키텍처설계서				
SIL	SIL 1	기법	구조적 방법 (Structured methods (JSD,MASCOT, SADT, Yourdon)) 을 사용하는가?		Part3/표A.2					
	SIL 2	기법	<SIL 1 기법과 동일.>		Part3/표A.2					
	SIL 3	기법	결함탐지 및 진단 ("Fault detection and diagnosis")를 사용하는가?		Part3/표A.2					
			:							
	SIL 4	기법	"Error detecting and correcting codes" 를 사용하는가?		Part3/표A.2					
			:							

(지원도구(tools)와 프로그래밍 언어 관련규정 및 평가항목)

(IEC61508-3 7.4.4.2) (IEC61508-3 7.4.4.3) (IEC61508-3 7.4.4.4) (IEC61508-3 7.4.4.5)

(IEC61508-3 7.4.4.6) (IEC61508-3 표A.3)

(MOD 0055/ 28.1) (MOD 0055/ 28.5) (MOD 0055/ 28.6) (MOD 0055/ 29.1)

(MOD 0055/ 30.4) (MOD 0055/30.5) (MOD 0055/30.2)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물 명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	도구 선정	1.1 안전무결성 등급에 따라 통합 도구들이 선정되었는가?	EC33-EI15	Part3/7.4.4.2 0055/29.5	도구선정 기준	Part3/ 표1			
			:							
	2	프로그래밍 언어	2.1 언어는 번역기/컴파일러를 가지고 있는가?	EC33-EI16, EC33-EI16-1,	Part3/7.4.4.3 (a)	언어 선정 기준	Part3/ 표1			
			:							
	3	코딩 표준	3.1 코팅 표준은 심사원에 의해 목적 적합성이 검토되었는가?	EC33-EI18	Part3/7.4.4.5 (a)	개발도구 및 코딩 표준	Part3/ 표1			
			:							
SIL	SIL 1	기법	적절한 프로그래밍 언어를 사용하는가?				Part3/ 표A.3			
			:							
	SIL 2	기법	인증된 도구 ("Certificated tools")를 사용하는가?				Part3/ 표A.3			
			:							
	SIL 3	기법	언어 부분집합 ("Language subset")을 사용하는가?				Part3/ 표A.3			
	SIL 4	기법	<SIL 4 기법과 동일>				Part3/ 표A.3			

(상세 설계 및 개발 단계 관련규정 및 평가항목)

(IEC61508-3 7.4.5.2) (IEC61508-3 7.4.5.3) (IEC61508-3 7.4.5.4) (IEC61508-3 7.4.5.5)

(IEC61508-3 7.4.6.1) (IEC61508 표A.4) (IEC61508 표B.9)

(IEC62279 10.4.17) (IEC62279 표A.4) (IEC62279 표A.12) (IEC62279 표A.14)
(IEC62279 표A.15) (IEC62279 표A.17) (IEC62279 표A.18) (IEC62279 표A.20)
(DO178B/5.3) (DO178B/11.8) (DO178B/11.11) (MOD 0055/36.1.1)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	사전 준비	1.1 상세 설계 전에 SW 안전 요건 명세가 가용한가?		Part3/ 7.4.5.2	☞ SW안전요건명세서				
			⋮							
	2	설계	2.1 SW는 모듈성, 시험 가능성, 변경용이성을 갖도록 설계되었는가?	EC33-EI22, EC33-EI23	Part3/ 7.4.5.3	☞ SW아키텍처설계서 ☞ SW모듈설계서				
			⋮							
SIL	SIL 1	기법	구조화된 방법 ("Structured methods")을 사용하는가?		Part3/ 표A.4					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	"Semi-formal methods"를 사용하는가?		Part3/ 표A.4, 표B.7 62279/ 표A.18					
			⋮							

(코드 구현(implementation) 관련규정 및 평가항목)

(IEC61508-3 7.4.6.1) (IEC61508-3 7.4.6.2)
(MOD 0055/36.1.1) (MOD 0055/36.3)
(DO 178B/5.3) (DO 178B/11.8) (DO 178B/11.11)

분	요건	산출물	평가

류	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	코딩	1.1 소스 코드는 가독성 있고, 이해가능하고, 시험가능한가?	EC33-EI31	7.4.6.1(a)	☞ 소스코드 목록				
			:							
SIL	SIL 1	기법								
	SIL 2	기법								
	SIL 3	기법								
	SIL 4	기법								

(소프트웨어 모듈 테스팅 관련규정 및 평가항목)

(IEC61508-3 7.4.7.1) (IEC61508-3 7.4.7.2) (IEC61508-3 7.4.7.3) (IEC61508-3 7.4.7.4)

(IEC61508-3 표A.5) (IEC61508-3 표B.2) (IEC61508-3 표B.3)

(MOD 0055/37.3.2) (DO178B/6.4.3c)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	모듈 시험	1.1 각 SW 모듈은 SW설계 중 명시된 대로 시험되었는가?	EC33-EI39	7.4.7.1	☞ SW모듈설계명세서 ☞ SW모듈시험명세서				
			:							
SIL	SIL 1	기법	데이터 기록 및 분석("Data recording and analysis")을 사용하는가?		표A.5					
			:							
	SIL 2	기법	동적 분석 및 시험("Dynamic analysis and testing") 을 사용하는가?		표A.5, 표B.2					
			:							
	SIL	기법	기능 및 블랙박스 시험							

	3		("Functional and black box testing")을 사용하는가?							
			⋮							
	SIL 4	기법	확률적 시험 ("Probabilistic testing")을 사용하는가?		표A.5					
			⋮							

(소프트웨어 통합 테스팅 관련규정 및 평가항목)

(IEC61508-3 7.4.8.1) (IEC61508-3 7.4.8.2) (IEC61508-3 7.4.8.3) (IEC61508-3 7.4.8.4)

(IEC61508-3 7.4.8.5) (IEC61508-3 표A.5) (IEC61508-3 표B.6)

(IEC62279-3 11.4.10) (IEC62279-3 11.4.15)

(MOD 0055/37.3.3)

(DO178B/6.4.3b)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	준비 사항	1.1 각 SW 모듈은 SW설계 중 명시된 대로 시험되었는가?		7.4.8.1	☞ SW통합 시험명세서				
	⋮	⋮	⋮							
	4	변경	4.1 SW통합 시 SW에 대한 변경이 발생하면 영향 분석을 통해 모든 영향 받는 SW모듈을 결정하고, 필요한 재확인 및 재설계 활동을 결정하는가?	-	7.4.8.5	☞ SW통합 시험결과				
SIL	SIL 1	기법	데이터 기록 및 분석 ("Data recording and analysis")을 사용하는가?		표A.5					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	확률적 시험 ("Probabilistic testing")을 사용하는가?		표A.5					
			⋮							

(4) 하드웨어와 소프트웨어의 통합

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 하드웨어와 소프트웨어의 통합 단계에 대한 피인증 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 여기에서는 하드웨어와 소프트웨어의 호환성과 할당된 안전무결성 등급 요건의 만족도를 확인한다.

(관련규정 및 평가항목)

(IEC61508-3 7.5.2.1) (IEC61508-3 7.5.2.2) (IEC61508-3 7.5.2.3) (IEC61508-3 7.5.2.4)
(IEC61508-3 7.5.2.5) (IEC61508-3 7.5.2.6) (IEC61508-3 7.5.2.7) (IEC61508-3 7.5.2.7)
(IEC61508 표A.6) (IEC61508 표A.14) (IEC61508 표B.3)
(IEC62279 표A.6) (IEC62279 표A.14)
(MOD 0055/37.3.4) (MOD 0055/37.3.5) (MOD 0055/37.3.6)
(DO 178B/6.4.3a)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출 물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	준비 사항	1.1 시스템에서 HW와 SW의 호환성을 보장하기 위한 통합 시험이 설계 및 개발 단계에서 명시되어 있는가?		7.5.2.1 12.4.1 (62279)					
	⋮	⋮	⋮							
	4	변경	4.1 통합 시 통합시스템에 대한 변경이 발생하면 영향 분석을 통해 모든 영향 받는 SW모듈을 결정하고, 필요한 재확인 활동을 결정하는가?	EC34-EI5	7.5.2.6					
SIL	SIL 1	기법	기능 및 블랙박스 시험("Functional and black box testing")을 사용하는가?		표A.6,표B.3 표A.6 (62279) 표A.14 (62279)					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	성능 시험("Performance testing")을 사용하는가?		표A.6,표B.6 표A.17 (62279)					

(5) 소프트웨어 운영과 수정 절차

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 운영과 수정 절차 단계에 대한 피인증 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 평가항목은 운영 및 수정 중에 소프트웨어의 기능 안전성에 영향을 끼치는 요건들로 구성된다.

(관련규정 및 평가항목)

(IEC 61508-3 7.6.2.1) (IEC 61508-3 7.6.2.2) (IEC 61508-3 7.6.2.3) (IEC 61508-3 7.6.2.4)
(IEC 61508-3 7.6.2.5) (IEC 62279 표A.11)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안에서)	관련 표준	산출물명	관련 표준	세부 항목 평가	평가 결과 증학	평가 결과 설명
공통	1	운영 및유 지보 수 절차 내용	1.1 운영 및 유지보수 절차에 "설계된 대로" 기능 안전성을 유지하기 위해 수행되는 일상적인 활동이 명시되어 있는가?		Part 2/7.6.2.1(a)	☞ SW 운영 및변 경절 차				
	:	:	:							
	4	운영 및 유지 보수 시행	4.1 운영 및 유지보수 시 시스템에 미치는 영향을 평가하고 있는가?		Part 2/7.6.2.4					
			:							
SIL	SIL 1		영향 분석("Impact Analysis")을 사용하는가?		62279/표A. 11					
			:							
	:	:	:							
	SIL 4		SIL 3와 동일							

(6) 소프트웨어 안전성 검증(Validation)

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 안전 검증 단계에 대한 피인증 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 평가항목은 소프트웨어에 할당된 안전무결성 등급에서 요구하는 요건을 바탕으로 생성된다.

(관련규정 및 평가항목)

(IEC61508-3 7.7.2.2) (IEC61508-3 7.7.2.3) (IEC61508-3 7.7.2.4) (IEC61508-3 7.5.2.6)
(IEC61508-3 7.5.2.7) (IEC61508-3 7.5.2.8) (IEC61508 표A.7) (IEC61508 표B.3)
(IEC61508 표B.5) (IEC62279 13.4.5) (IEC62279 13.4.7) (IEC62279 13.4.8)
(IEC62279 13.4.11) (IEC62279 13.4.12) (IEC62279 표A.7) (IEC62279 표A.14) (IEC62279 표A.17)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출 물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	검증 계획	1.1 검증 활동은 SW안전성 검증 계획에 따라 수행되었는가?	EC36-EI3, EC36-EI4, EC36-EI5, EC36-EI6	Part3/7.7.2.2 62279/13.4.5	☞ SW검증계획				
	⋮	⋮	⋮							
	4	검증 결과	5.1 SW검증 결과에서 시험은 SW안전성에 대한 모든 명시된 요건이 정확하게 수행되고 SW시스템이 의도되지 않은 기능을 수행하지 않음을 보여주는가?	EC36-EI10	Part3/7.7.2.8(a)	☞ SW안전성검증결과				
			⋮							
SIL	SIL 1	기법	기능 및 블랙박스 시험("Functional and black box testing")을 사용하는가?		Part3/표A.7, 표B.3 62279/표A.14					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	기능 및 블랙박스 시험("Functional and black box testing")을 사용하는가?		Part3/표A.7, 표B.3 62279/표A.14					
			⋮							

(7) 소프트웨어 수정(변경)

본 절에서는 IEC61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 수정 단계에 대한 피인증 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 평가항목은 소프트웨어에 할당된 안전무결성 등급의 요건을 바탕으로 생성된다.

(관련규정 및 평가항목)

(IEC61508-3 7.8.2.1) (IEC61508-3 7.8.2.2) (IEC61508-3 7.8.2.3) (IEC61508-3 7.8.2.4)
(IEC61508-3 7.8.2.5)(IEC61508-3 7.8.2.6) (IEC61508-3 7.8.2.7) (IEC61508-3 7.8.2.8)
(IEC61508-3 7.8.2.9) (IEC61508-3 7.8.2.10) (IEC61508 표A.8)
(IEC62279 16.4.9)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출 물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공	1	변경	1.1 SW변경을 수행하기 전		Part3/7.8.2.1	SW				

통		절차	에 SW변경절차가 가용한가?			변경절차				
	⋮	⋮	⋮							
	4	변경수행	4.1 안전계획에 따라 변경이 이루어지는가?		Part3/7.8.2.7 62279/16.4.9					
			⋮							
SIL	SIL 1	기법	영향분석(impact analysis)를 사용하는가?		Part3/표A.8					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	<SIL 3 기법과 동일>		Part3/표A.8					

(8) 소프트웨어 검증(verification)(입증)

본 절에서는 IEC 61508에서 정의된 소프트웨어 개발단계 중 소프트웨어 검증 단계에 대한 피인증 소프트웨어 개발과정의 만족도 평가항목을 제안한다. 평가항목은 소프트웨어에 할당된 안전무결성 등급의 요건을 바탕으로 생성된다.

(관련규정 및 평가항목)

(IEC61508-3 7.9.2.1) (IEC61508-3 7.9.2.2) (IEC61508-3 7.9.2.3) (IEC61508-3 7.9.2.4)

(IEC61508-3 7.9.2.5) (IEC61508-3 7.9.2.6) (IEC61508-3 7.9.2.7) (IEC61508-3 7.9.2.8)

(IEC61508-3 7.9.2.9) (IEC61508-3 7.9.2.10) (IEC61508-3 7.9.2.11) (IEC61508-3 7.9.2.12)

(IEC61508-3 7.9.2.13) (IEC61508b표A.9) (IEC61508 표B.8)

(IEC62279 11.4.4) (IEC62279 표A.5) (IEC62279 표A.13) (IEC62279 표A.19)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출물명	관련 표준	세부항목 평가	평가결과 종합	평가결과 설명
공통	1	SW 입증계획	1.1 SW입증 계획이 수립되고 문서화되어 있는가?		Part3/7.9.2.1 62279/11.4.4	☞ SW입증계획				
			⋮							
	2	입증수행	2.1 계획에 따라 SW입증이 수행되는가?		Part3/7.9.2.3 Part3/7.9.2.7	☞ SW입증계획				

			⋮							
SIL	SIL 1	기법	정적 분석("Static analysis")을 사용하는가?		Part3/표A.9,표 B.8 62279/표A.5 62279/표A.19					
			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	정적 분석("Static analysis")을 사용하는가?		Part3/표A.9,표 B.8 62279/표A.5 62279/표A.19					

(8) 열차제어시스템 SW 기능 안전성 평가

본 절에서는 IEC61508에서 정의된 기능 안전성 평가에 대한 피인증 소프트웨어의 만족도 평가항목을 제안한다. 소프트웨어 기능안전성 평가의 목적은 피인증 소프트웨어가 표준에서 요구하는 기능안전성 요건을 만족하였는가를 평가하기 위함이다. 기능안전성 평가는 개발이 완료된 최종 소프트웨어를 대상으로 하며, 피 인증기관은 테스트 또는 이에 준하는 테스트 결과를 근거자료로 제시하여야 한다. 인증기관은 제출된 테스트 결과 문서들을 분석하여 표준에서 요구하는 기능안전성 평가가 이루어 졌는지 검증한다.

(관련규정 및 평가항목)

(IEC61508-1 8.2.1) (IEC61508-1 8.2.2) (IEC61508-1 8.2.3) (IEC61508-1 8.2.4)
(IEC61508-1 8.2.5) (IEC61508-1 8.2.6) (IEC61508-1 8.2.7) (IEC61508-1 8.2.8)
(IEC61508-1 8.2.9) (IEC61508-1 8.2.10) (IEC61508-1 8.2.11) (IEC61508-1 8.2.12)
(IEC61508-1 8.2.13) (IEC61508-1 8.2.14) (IEC61508 표A.9) (IEC61508 표A.10)
(IEC61508 표B.4) (IEC62279 표A.9)

분류	요건					산출물		평가		
	평가 ID	평가 요건	평가항목	평가ID (평가안내서)	관련 표준	산출 물명	관련 표준	세부 항목 평가	평가 결과 종합	평가 결과 설명
공통	1	심사원	1.1 SW입증 계획이 수립되고 문서화되어 있는가?		Part 1/8.2.1	☞ SW기능안전성심사계획서				
			⋮							
	⋮	⋮	⋮							
	3	입증 수행	3.1 심사원은 필요한 사람 및 정보, 장비(SW 및 HW)에 접근할 수 있는가?		Part 1/8.2.2	☞ SW기능안전성심사보고서				
			⋮							
SIL	SIL 1	기법	체 크 리 스 트 ("Checklists")를 사용하는가?		62279/표A.9					

			⋮							
	⋮	⋮	⋮							
	SIL 4	기법	SIL 3와 동일		Part3/표A.10					

(9) 작업산출물 특성

본 절에서는 IEC61508과 IEC62279, MOD0055, DO178B에서 정의된 평가 4개 분야의 평가항목 산출물을 각 프로세스별로 특성들을 정리하여 평가 시 중요 근거자료로 활용될 수 있도록 하였다. 작업산출물 특성의 일부는 아래와 같으며 상세내용은 본 보고서의 부록(철도SW안정성 평가기준_작업산출물 특성)에서 확인할 수 있다.

구분	작업 산출물 ID	작업산출물 이름	작업산출물 특성	관련 표준	비고
문서화	DOC	-			
기능 안정성 관리	MGT	-			
안전 요건 명세	SRS-01	SW안전 요건명세	-소프트웨어가안전한상태를유지하기위한필요한모든요구사항을기술한다. - 사용된 표준을 식별함 - 소프트웨어구조고려사항/제약사항을 식별함 - 필요한 소프트웨어 구성요소를 식별함 - 소프트웨어 요소간의 관계를 식별함 - 다음을 고려함: - - 필요한 소프트웨어 성능특성 - - 필요한 소프트웨어 인터페이스 - - 필요한 보안특성 - - 데이터베이스설계요구사항 - - 필요한 오류처리 및 복구속성 '-다음과 같은 요소들도 기술되어야 한다. o 입력변수 o 처리기능 o 안전한 상태 혹은 출력변수의 값(Safety state or value of output variable)	ISO/IEC 15504-5 (17-11) 'SR-D-01	
		⋮	⋮	⋮	

(10) 메트릭 측정

본 절에서는 철도연구원에서 개발하고 있는 14개 모듈을 기반한 메트릭을 제공하며 필요시 일부 추가할 수 있도록 한다. 메트릭 측정표의 일부는 아래와 같으며 상세내용은 본 보고서의 부록(철도SW안정성 평가기준_메트릭 측정)에서 확인할 수 있다.

단계	번호	메트릭명	메트릭설명	측정식	측정값	비고	SIL 별 관단 기준			
							SIL 1	SIL 2	SIL 3	SIL 4
상세 설계 및 개발	1	설계 및 코딩 표준 준수율	자동차(예. MISRA-C, 118개 규칙), 철도(예. IEC 61508, 7개 규칙, IEC 62279, 10개 규칙) 분야의 SW 관련 표준 및 규칙을 준수하는 비율							
	2	Boundary value analysis 결과	블랙박스 테스팅 중 Boundard value analysis 결과가 목적을 충족시키는 비율							
	3	equivalence Class testing 값	블랙박스 테스팅 중 equivalence Class testing 결과가 목적을 충족시키는 비율							
	4	Performance testing 값	Latency, Throughput, resource, 기타 성능지표							
:	:	:	:							
기능 안전성 심사	1	체크리스트	체크리스트 충족도							
	2	control flow analysis 값	statement coverage, branch coverage, decision coverage, LCSAJ 커버리지							
	3	data flow analysis 값	데이터별 Definition-Uses 분석							
	4	control flow analysis 값	statement coverage, branch coverage, decision coverage, LCSAJ 커버리지							
	5	data flow analysis 값	데이터별 Definition-Uses 분석							

SIL 별로 특정 메트릭 값의 기준을 정하는 것은 어플리케이션의 context를 고려해야 한다. 따라서 모든 상황에 적합한 기준을 정의할 수 없다. 어플리케이션의 context로는 어플리케이션의 규모(size), 적용 분야, 목적, 적용한 개발 방법론, 조직 규모 등이 있다.

위의 메트릭 정의에는 포함되어 있지 않지만 소프트웨어의 정적 구조를 평가하는 대표적인 것으로 복잡도 메트릭(Cyclomatic Complexity: CC)이 있다. CC 값은 코드 내 모든 경로를 실행하는데 필요한 테스트의 최소수를 나타낸다.

이 메트릭은 소프트웨어 모듈 내 control flow의 수를 측정하는 것으로, 모듈 내 경로가 많아질수록, 복잡도가 높아지고 테스트하기 어려우며, 향후 유지보수 에도 어려움이 있다는

것을 의미한다.

미국 NASA의 기준에서는 CC값 20을 threshold로 간주한다. 소프트웨어 모듈에 대한 CC 값에 따른 위험을 분류하여 정의하면 다음과 같다.

[표] 복잡도에 따른 위험 분류

CC	모듈 유형	위험
1~4	간단한 모듈	낮음
5~10	잘 구조화되고 안정된 모듈	낮음
11~20	좀 복잡한 모듈	적절함
21~50	복잡한 모듈, 우려됨	높음
> 50	에러 발생가능성이 높고, 극단적으로 문제가 많음.	매우 높음

(출처: Avisto web site http://www.aivosto.com/proejct/help/pm-complexity.html
SEI web site http://www.sei.cmu.edu/activities/str/descriptions/mitmpm.html)

SIL 수준과 위험의 관련성이 있기 때문에 복잡도 메트릭에 따른 적절한 기준을 설정할 수 있다. 높은 SIL 수준이 될수록 허용 가능한 CC 값이 작아질 것이다.

SIL 수준별로 메트릭 값을 결정하는 것은 장기간에 걸친 경험 데이터가 축적되어야 하고 통계적으로 접근하는 것이 타당하지만 여전히 현실적인 어려움이 있다. 소프트웨어의 경우 운영 프로파일(operational profile)을 작성하여 분석하는 것도 모든 상황을 고려하는 것이 어려우며, 소스 코드 내의 현상을 파악하는 것도 어려울 수 있다.

(11) 기법설명

본 절에서는 각 프로세스에 적용된 기법에 대한 상세내용을 정리하였다. 기법목록은 IEC61508-3 Annex A&B에 근거한 것이며 각 기법에 대한 설명은 IEC 61508에 따른 것이다. 적용기법을 정리한 표의 일부는 아래와 같으며, 상세내용은 본 보고서의 부록(철도 SW안정성 평가기준_기법설명)에서 확인할 수 있다.

구분	번호	기법 이름	기법 설명	관련 표준	비고
SW 안전 명세	1	Computer-aided specification tools	목적:모호성및완정성을자동으로탐지하는것을지원하는명세기법의사용 설명: -명세를DB형태로생성하여일관성및완전성을자동으로검사할수있도록하는기법 -명세도구는사용자에게시스템의다양한측면을역동적으로제시함 -이기법은명세생성뿐아니라설계및기타단계도지원함	B.2.4	
	2a	Semi-formal methods	목적:명세의일부분을모호하지않고일관되게표현하여,실수및누락을탐지할수있도록함 설명:	B.2.3	

			-명세,설계및코딩과같은개발단계에서시스템기술서를개발하는수단을 제공함 - 기술서는 기계에 의해 해석되거나 시스템 행위의 다양한 측면을 동적으로 보여줌 -예. . Logic/function block diagrams . Sequence diagrams . Data flow diagrams . Finite state machines/state transition diagrams . Time Petri nets . Decision/truth tables		
기능적 안전 점검	1	Checklists	목적: 정확한 요건을 상세히 점검하기보다 포괄적으로 시스템의 중요한 측면에 대해 평가를 하기위함 설명: -대상시스템에 적합한 질문이 준비되어 있어야함 -체크리스트활용은 경험 및 판단에 많이 의존함 -관련내용에 대해 타당성 근거를 문서화하여야함	B.2.5	

■

제3절 열차제어시스템 바이탈 소프트웨어 테스팅 자동화 도구의 개발

	검증계획서 (Verification Plan)	**ID No :** TC - SR08 - SSR02 - 2010 작성일 : 2010. 05. 14 수정일 :

8. 프로젝트는 안전성 평가를 위한 열차제어시스템 소프트웨어 시험장치를 개발해야 한다.

8.2 프로젝트는 열차제어시스템 소프트웨어 안전성 평가를 위한 시험기를 제작하여야 한다.

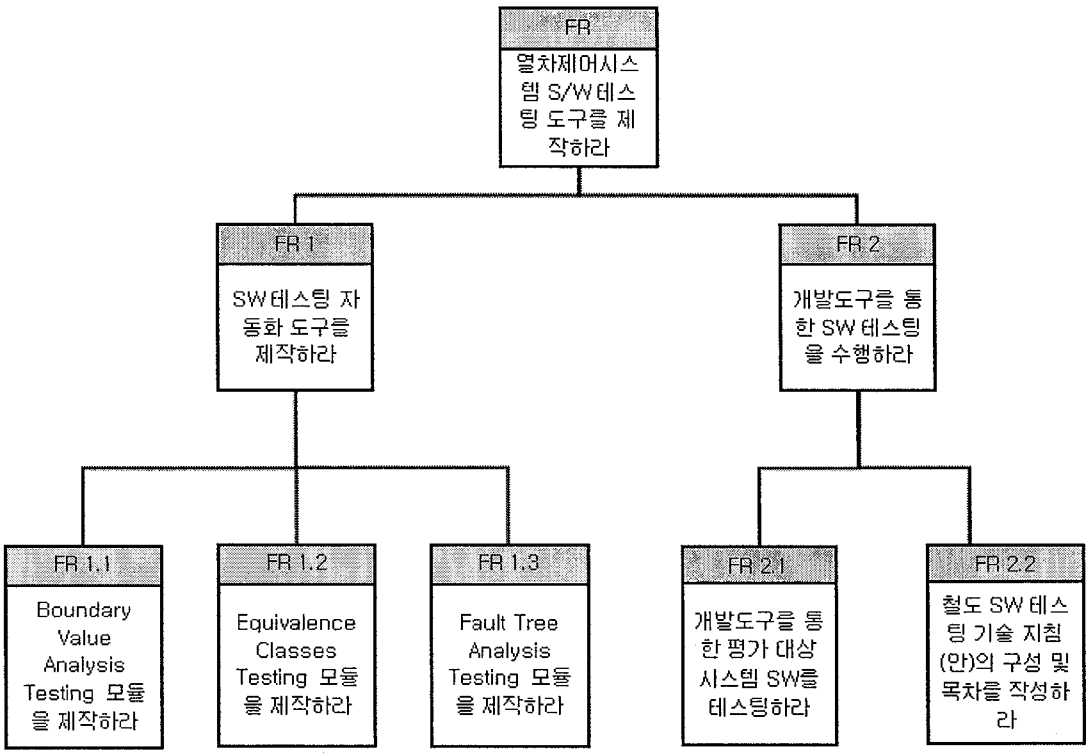
8.3 프로젝트는 평가 대상시스템 소프트웨어를 테스팅 하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : SW 테스팅 자동화 도구 시제품 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 3.1 국제규격의 부합 - 3.3 시제품	- SE 검증	- 수정 VRTM - 검증결과표

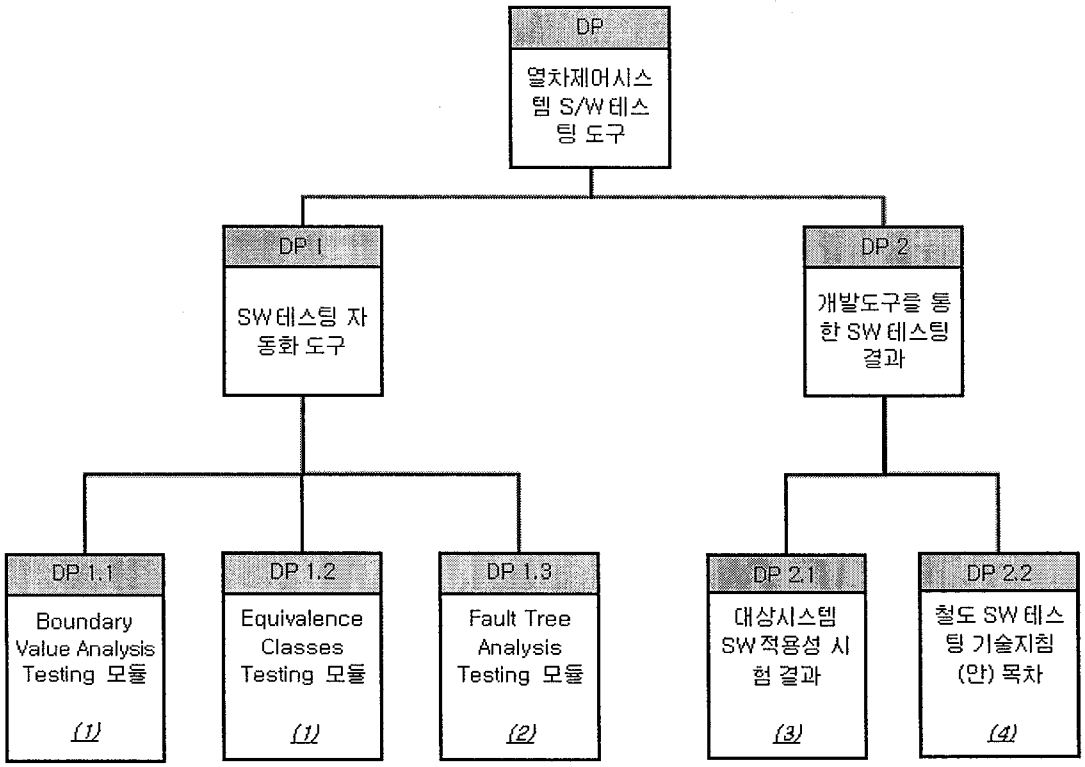
Verification Specification (검증기준) :

1. 열차제어시스템 소프트웨어 테스팅 모듈(Boundary Value Analysis 모듈, Equivalence Classes Testing 모듈, Fault Tree Analysis 모듈)의 설계 및 제작이 이루어 졌는가?
2. 기 개발한 모듈을 적용하여 평가 대상시스템에 대한 소프트웨어 테스팅이 이루어 졌는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

열차제어시스템 소프트웨어 안전성 테스트 도구 개발사양은 『SR 8. 프로젝트는 안전성 평가를 위한 열차제어시스템 소프트웨어 시험장치를 개발해야한다.』 중 **『SSR 8.2 프로젝트는 열차제어시스템 소프트웨어 안전성 평가를 위한 시험기를 제작하여야 한다.』 『SSR 8.3 프로젝트는 평가대상시스템 소프트웨어를 테스팅 하여야 한다.』**에 해당하는 내용이다. 전체 자동화 테스팅 항목 14개에 대해 연차별로 설계 및 개발을 추진하고 있다. 전년도 까지 9개의 하부 모듈에 대한 개발을 완료하였으며, 당해연도에는 다음에 해당하는 세 개 모듈에 대한 설계 및 제작이 수행되었다. 또한 지난년도까지 개발한 하부 모듈들을 통해 다른 세부과제에서 제작하고 있는 평가대상시스템의 소프트웨어를 대상으로 한 적용성 시험이 수행되었다.

- Boundary Value Analysis 모듈
- Equivalence Classes Testing 모듈
- Fault Tree Analysis 모듈

나. 설계기준

○ 열차제어시스템 소프트웨어 테스팅 자동화 도구의 설계 및 제작은 다음과 같은 열차제어시스템 소프트웨어 안전성 평가와 관련된 국내 문서 및 국제규격을 참고하였다.

- IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety - related systems", 2004.
- IEC 62279, "Railway Applications : Communications, Signalling and Processing Systems - Software for Railway Control Protection Systems", 2004.

다. 검증 방법에 따른 증거 자료

본 절에서는 열차제어시스템 소프트웨어 테스팅 자동화 도구의 설계 및 시제품

제작 내용을 설명하고 있다. 당해년도에는 테스팅 도구 개발사양에 대한 분석을 통해 3개의 하부모듈에 대한 설계 및 제작을 수행하였다. 즉, 철도시스템 소프트웨어 관련 국제규격 등의 분석을 통해 도출된 열차제어시스템 안전성 평가를 위한 테스트 항목 및 관련 상용화된 테스팅 도구들의 조사분석 결과를 바탕으로 개발하고자 하는 테스팅 자동화 도구의 개발사양을 도출하였으며, 3차년에 걸친 순차적인 설계 및 제작을 추진하고 있다. 이에 따라 당해연도에는 3개의 하부모듈(Boundary Value Analysis 모듈, Equivalence Classes Testing 모듈, Fault Tree Analysis 모듈)에 대한 설계 및 시제품 제작이 수행되었다.

라. 성과물의 내용 및 결과

(1) 개요

목표로 하는 열차제어시스템 소프트웨어 테스팅 자동화 도구는 표 3.3.1과 같은 14가지 항목에 대한 테스팅이 가능한 자동화된 도구이다.

표 3.3.1 목표시스템의 하부모듈 구성

하부 모듈	세부 모듈
소스코드 분석 자동화 도구 개발	- Design & Coding Standard 검사 모듈 - Fagan Inspection 모듈 - Checklist 검사 모듈 - Metric 지원 모듈 - Impact Analysis 모듈
화이트박스 테스팅 자동화 도구 개발	- Control Flow Testing 모듈 - Data Flow Testing 모듈 - Performance Testing 모듈 - Symbolic Execution 모듈
블랙박스 테스팅 자동화 도구 개발	- **BoundaryValueAnalysis 테스팅 모듈** - **EquivalenceClasses 테스팅 모듈** - Decision Table 테스팅 모듈 - **FaultTreeAnalysis 테스팅 모듈** - Probabilistic Analysis 테스팅 모듈

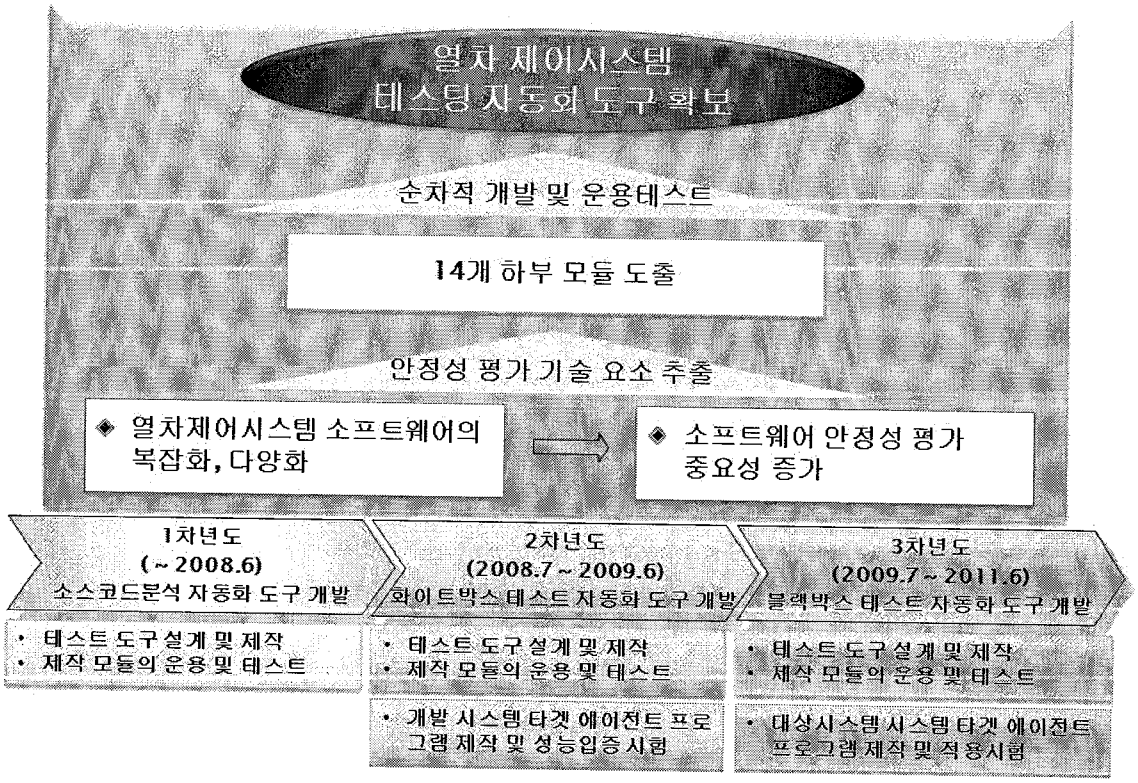


그림 3.3.1 목표 시스템 개발계획 개요

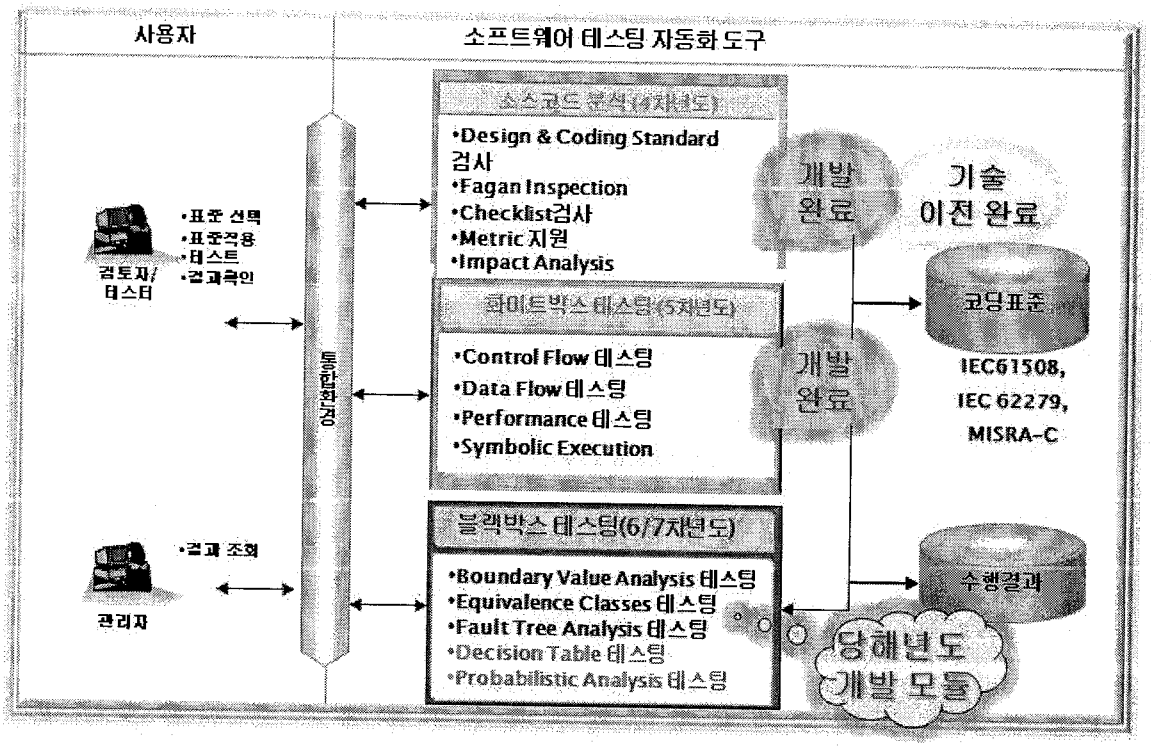


그림 3.3.2 전체 시스템 구조

개발하고자 하는 도구는 그림 3.3.1과 같이 3년에 걸쳐 순차적으로 개발할 계획이며, 본 과제를 통해 제작하고 있는 안전성 평가대상 열차제어시스템의 소프트웨어 테스팅에 적용하여 운용테스트를 수행할 계획이다. 당해 연도에는 3개의 하부모듈(Boundary Value Analysis 모듈, Equivalence Classes Testing 모듈, Fault Tree Analysis 모듈)에 대한 설계 및 시제품 제작이 수행되었다.

또한 당해연도에는 개발 시제품의 적용성 연구를 위해 본 핵심과제의 세부과제 2에서 제작하고 있는 평가대상 시스템 소프트웨어의 테스팅을 수행하였다. 대상시스템 소프트웨어를 대상으로 한 테스팅에는 기 제작한 'Design & Coding Standard 검사 모듈', 'Control Flow 테스팅 모듈', 'Data Flow Testing 모듈'이 활용되었다.

그리고 본 연구를 통해 제작한 시제품의 실용화를 위해 당해연도에는 철도운영기관 및 국내 열차제어시스템 제작사의 의견을 수렴하였으며, 특히, 기 제작한 일부 모듈에 대한 기술이전이 수행되는 등 본 연구과제를 통해 개발한 시제품의 실용화를 위한 노력이 진행되었다. 개발하고 있는 소프트웨어 테스팅 자동화 도구의 실용화를 위해서 철도 운용기관 및 열차제어시스템 제작사의 의견 수렴 결과 열차제어시스템 소프트웨어 테스팅 기술지침의 필요성이 제기 되었다. 따라서 본 연구를 통해 개발하고 있는 소프트웨어 테스팅 자동화 도구 시제품의 실용화 측면에서 '열차제어시스템 소프트웨어 테스팅 기술지침(안)'을 작성하고자 당해연도에는 기술지침(안)의 구성과 기본방향을 설정하였으며, 차년도에 소프트웨어 테스팅 전문가, 철도운영기관과 제작사의 의견 수렴 과정을 통해 '열차제어시스템 소프트웨어 테스팅 기술지침(안)'을 작성할 예정이다.

(2) Boundary Value Analysis / Equivalence Classes Testing 모듈

본 절에서는 블랙박스 테스팅 자동화 도구의 Boundary Value Analysis Testing 모듈과 Equivalence Classes Testing 모듈의 설계 내용을 기술한다.

Boundary Value Analysis Testing 모듈은 입력 조건의 경계값을 분석하고 그 값을 시험 대상 체계에 입력해 봄으로써 예상결과가 올바르게 출력되었는지를 확인한다. 또한 Equivalence Classes Testing 모듈은 입력 조건의 동치영역을 분석하고 각 영역의 대표값을 선정하고 그 값을 시험 대상 체계에 입력해 봄으로써 예상

결과가 올바르게 출력되었는지를 확인한다. Boundary Value Analysis Testing 모듈의 수행 기능과 Equivalence Classes Testing 모듈의 수행 기능은 일부 동일한 부분이 있고 상호 기능을 참조하는 경우가 존재하기 때문에 두 모듈을 통합하여 하나의 모듈로 구현한다.

(가) 시스템 구조

Boundary Value Analysis / Equivalence Classes Testing 모듈의 목표는 사용자의 조작을 최소한으로 줄이고 테스트 준비에서부터 수행, 결과 분석까지의 과정을 자동으로 수행하는 것이다.

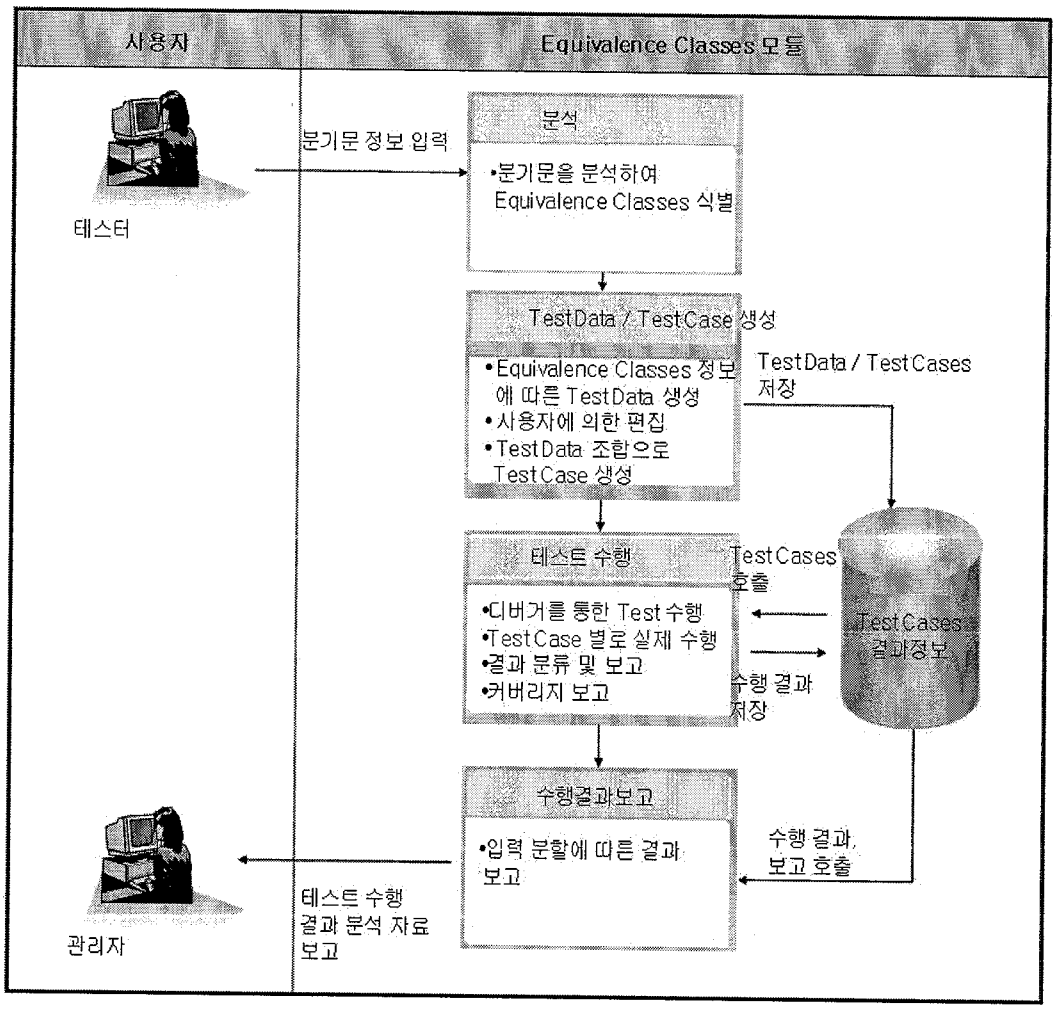


그림 3.3.3 Equivalence Classes Testing 기능구성도

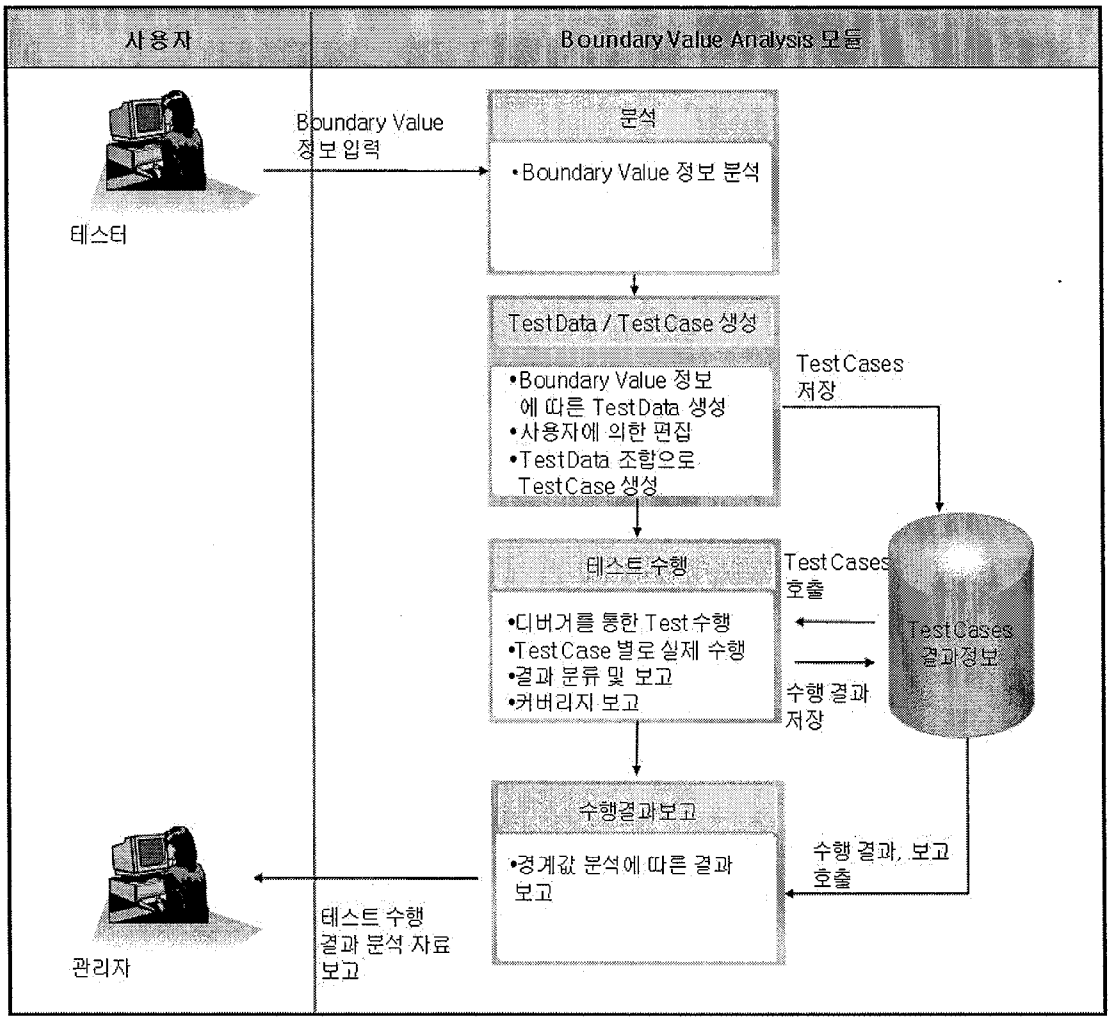


그림 3.3.4 Boundary Value Analysis Testing 기능구성도

Boundary Value Analysis / Equivalence Classes Testing 모듈은 테스터가 입력한 시나리오의 분기 조건을 분석하여 동치영역을 자동으로 분할하고, 영역의 대표값 또는 경계값을 입력값으로 하는 테스트케이스를 생성 및 수행하며, 그 출력값을 분석하여 오류를 검출하고 이를 바탕으로 보고서를 생성하는 작업을 수행한다. 다음 표는 주요 기능에 대한 설명이다.

표에서와 같은 각 기능을 구현하기 위해서 Boundary Value Analysis / Equivalence Classes Testing 모듈은 다음과 같은 세부 모듈들로 구성된다.

- Equivalence Classes Analyzer : 시나리오 정보를 바탕으로 동치영역 분석 및 동치영역 내 임의의 값을 대표값으로 선정

표 3.3.2 Boundary Value Analysis/Equivalence Classes Testing 모듈 기능 리스트

기 능	설 명
동치영역 자동 생성	- 테스터로부터 입력 받은 시나리오의 분기 조건을 분석하여 동치 영역을 자동으로 생성 한다. - 정의된 동치 영역의 대표값을 선정하고 이를 저장소에 저장한다.
경계값 자동 생성	- 분기조건의 경계값 목록을 생성한다. - 테스터는 이를 편집할 수 있으며 최종 정의된 경계값을 저장소에 저장한다.
테스트케이스 생성	- 생성 및 수정 완료된 동치영역의 대표값 또는 경계값을 기준으로 테스트케이스를 자동으로 생성한다. - 생성된 테스트케이스의 기대 결과값을 테스터로부터 입력 받고 이를 저장소에 저장한다.
테스트 수행	- 디버거를 활용하여 대상체계에 테스트케이스 정보를 입력하여 테스트를 수행한다. - 테스트 수행후 출력값을 저장소에 저장한다.
테스트 수행 결과 판단	- 테스트 출력값과 사용자가 기 입력한 기대 결과값을 비교하여 프로그램이 올바르게 수행되었는지를 검증한다. - 검증 결과를 저장소에 저장한다.
테스트 수행 결과 보고	- 테스트 수행 결과 판단 내용을 바탕으로 보고서를 생성한다.

- Boundary Value Analyzer : 시나리오 정보를 바탕으로 경계값 분석
- Testcase Generator : 기 정의된 대표값 혹은 경계값을 조합하여 테스트케이스 생성
- Execution Engine : 시험 대상 체계(SUT)를 조작하여 테스트케이스를 수행및

출력값 획득

- Test Report Generator : 테스트 수행 결과 분석 및 출력 및 저장할 수 있는 형태의 도식화된 보고서 작성

(나) 동작 시나리오

Boundary Value Analysis / Equivalence Classes Testing 모듈의 동작 시나리오는 프로젝트 정보 입력, 시나리오 정보 입력, 동치영역 분할 및 대표값 선정, 동치영역 및 대표값 수정, 경계값 분석, 경계값 수정, 테스트케이스 생성, 테스트케이스 예상 수행결과 입력, 테스트 수행, 테스트 보고서 생성 순으로 진행된다.

테스터는 동치영역 분할 후 선택에 의해 영역의 대표값을 이용하여 테스트케이스를 생성할 수도 있고, 추가적으로 경계값 분석 단계를 거쳐 선정된 경계값을 이용해 테스트케이스를 생성할 수도 있다.

Boundary Value Analysis / Equivalence Classes Testing 모듈은 시나리오 정보 입력과 테스트 기대 결과값 입력을 제외한 모든 과정을 자동으로 수행하되, 자동 선정된 동치영역 및 대표값과 경계값에 대해서 테스터가 별도로 수정할 수 있는 것이 주요 동작 시나리오의 내용이다.

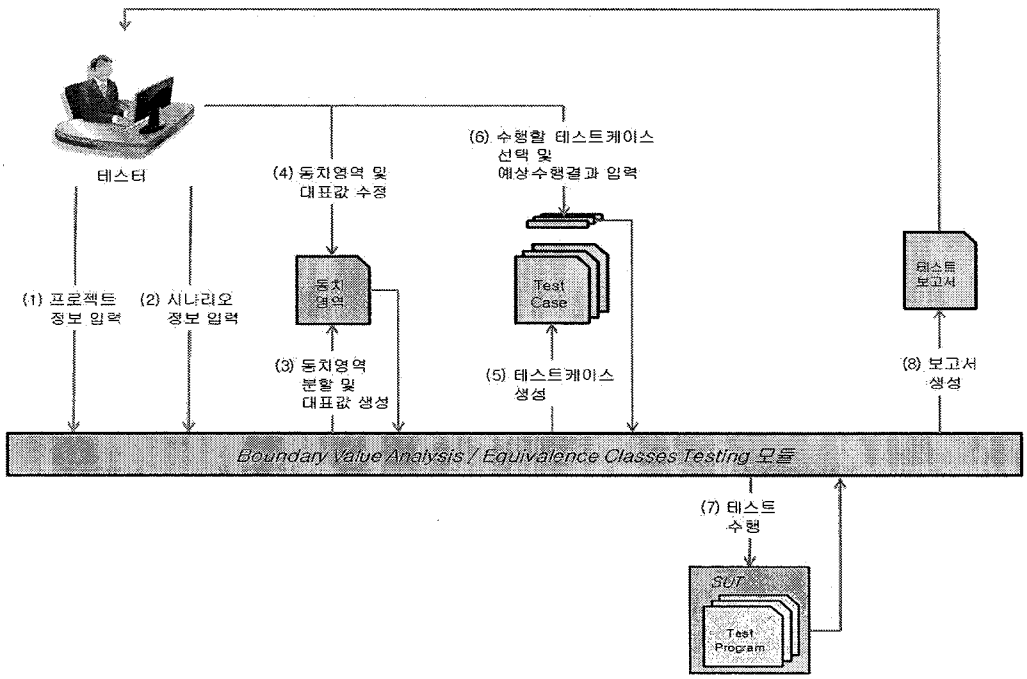


그림 3.3.5 동치영역 대표값을 이용한 테스트 수행 시나리오

그림 3.3.5와 3.3.6은 테스트케이스 입력값 생성 방법 별로 수행하는 동작 시나리오에 대한 그림과 순서에 대한 설명이다.

○ 동치영역 대표값을 이용한 테스트 수행

- 프로젝트 정보 입력 : 테스터는 수행할 테스트 프로젝트의 정보를 입력한다.
- 시나리오 정보 입력 : 테스터는 테스트할 시나리오 정보를 입력한다.
- 동치영역 분할 및 대표값 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시나리오 정보를 바탕으로 동치영역을 자동 분할하고, 각 동치영역내 임의의 값을 대표값으로 선정한다.
- 동치영역 수정 : 테스터는 자동 분할된 동치영역과 대표값의 내용을 확인하고 수정한다.
- 테스트케이스 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시나리오와 동치영역의 대표값을 이용하여 테스트케이스를 자동 생성한다.
- 수행할 테스트케이스 선택 및 예상수행결과 입력 : 테스터는 수행할 테스트케이스를 선택하고 예상되는 수행 결과값을 입력한다.
- 테스트케이스 수행 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시험대상체계를 제어하여 테스트를 수행한다.
- 테스트보고서 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 테스트 수행 결과와 테스터가 입력한 예상 수행결과값 비교 등의 분석과정을 거쳐 보고서를 생성한다.

○ 경계값을 이용한 테스트 수행

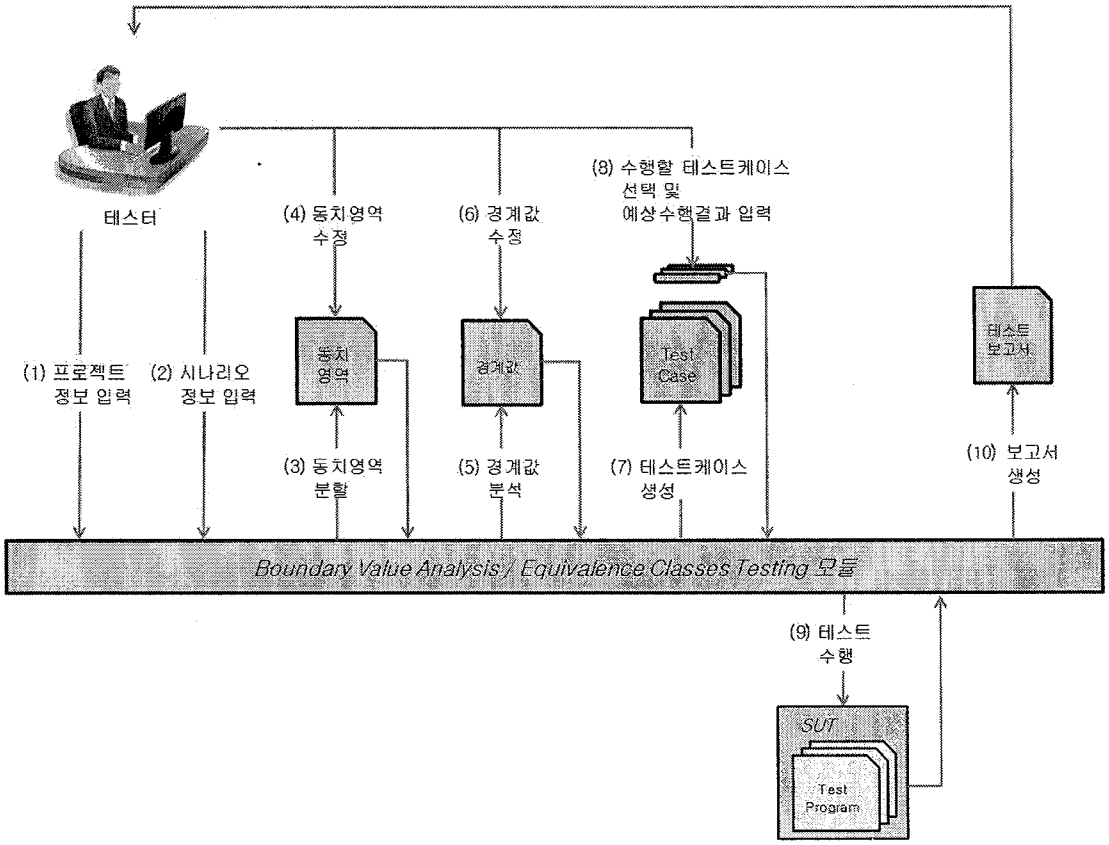


그림 3.3.6 경계값을 이용한 테스트 수행 시나리오

- 프로젝트 정보 입력 : 테스터는 수행할 테스트 프로젝트의 정보를 입력한다.
- 시나리오 정보 입력 : 테스터는 테스트할 시나리오 정보를 입력한다.
- 동치영역 분할 및 대표값 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시나리오 정보를 바탕으로 동치영역을 자동 분할하고, 각 동치영역내 임의의 값을 대표값으로 선정한다.
- 동치영역 수정 : 테스터는 자동 분할된 동치영역의 내용을 확인하고 수정한다.
- 경계값 분석 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 동치영역을 분석하여 경계값을 생성한다.
- 경계값 수정 : 테스터는 자동 생성된 경계값의 내용을 확인하고 수정한다.
- 테스트케이스 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시나리오와 경계값 정보를 이용하여 테스트케이스를 자동 생성한다.

- 수행할 테스트케이스 선택 및 예상수행결과 입력 : 테스터는 수행할 테스트케이스를 선택하고 예상되는 수행 결과값을 입력한다.
- 테스트케이스 수행 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 시험대상체계를 제어하여 테스트를 수행한다.
- 테스트보고서 생성 : Boundary Value Analysis / Equivalence Classes Testing 모듈은 테스트 수행 결과와 테스터가 입력한 예상수행결과값 비교 등의 분석과정을 거쳐 보고서를 생성한다.

(다) 화면 설계

① 화면 구성

○ 프로젝트 설정 입력 화면

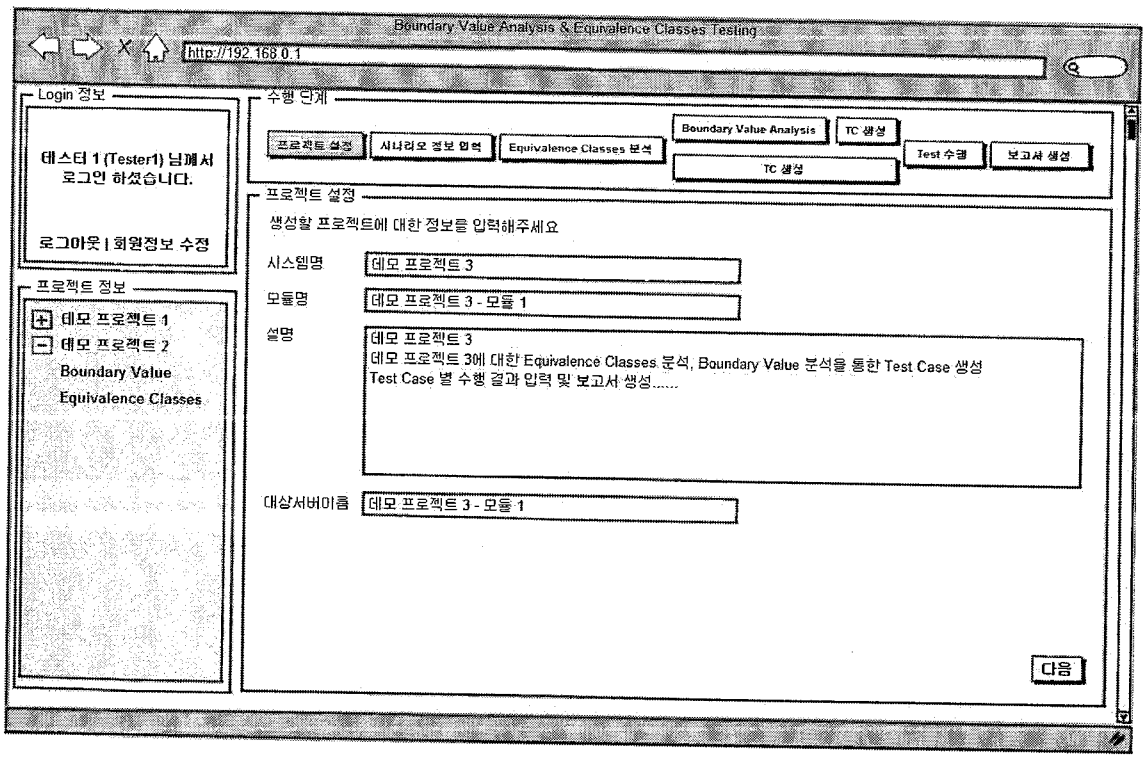


그림 3.3.7 프로젝트 설정 입력 화면

프로젝트 설정 입력 화면은 테스터가 새로운 테스트 프로젝트를 생성할 때 표시된다. 테스터는 시험할 시스템과 모듈의 이름, 테스트의 설명 및 시험을 수행할 대상 서버 이름을 입력 한다.

○ 시나리오 정보 입력 화면

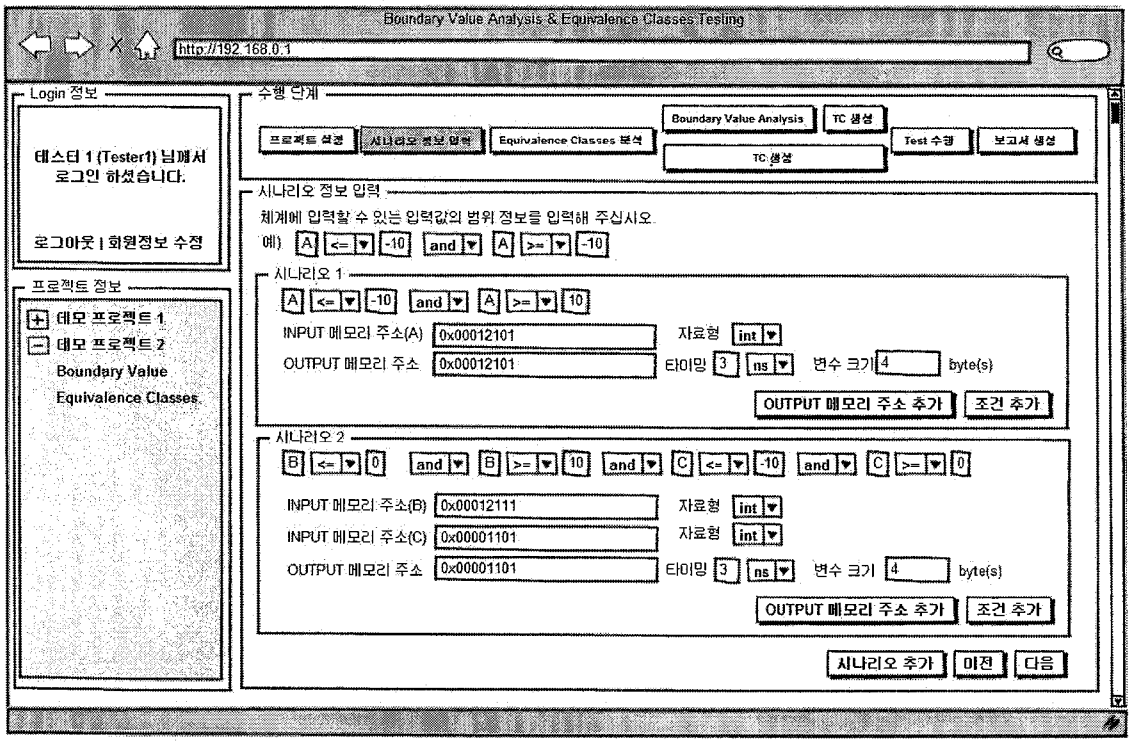


그림 3.3.8 시나리오 정보 입력 화면

시나리오 정보 입력 화면에서는 시나리오별로 분기 조건, 입/출력 메모리 정보등을 입력할 수 있는 환경을 제공한다. 다수의 시나리오를 입력할 경우 '시나리오 추가' 버튼을 클릭하면 새로운 시나리오를 입력할 수 있는 폼이 표시된다. 하나의 시나리오에는 다수의 조건과 출력 메모리 주소가 존재하며, 입력된 조건의 변수마다 입력 메모리 주소를 입력할 수 있는 폼이 생성된다. 시나리오의 조건을 추가하거나 다수의 출력 메모리를 검사할 필요가 있을 경우에는 각각 '조건 추가', 'OUTPUT 메모리 주소 추가' 버튼을 통해 해당 사항을 입력할 수 있는 환경을 추가할 수 있다.

○ 동치영역 자동 분할 및 수정 화면

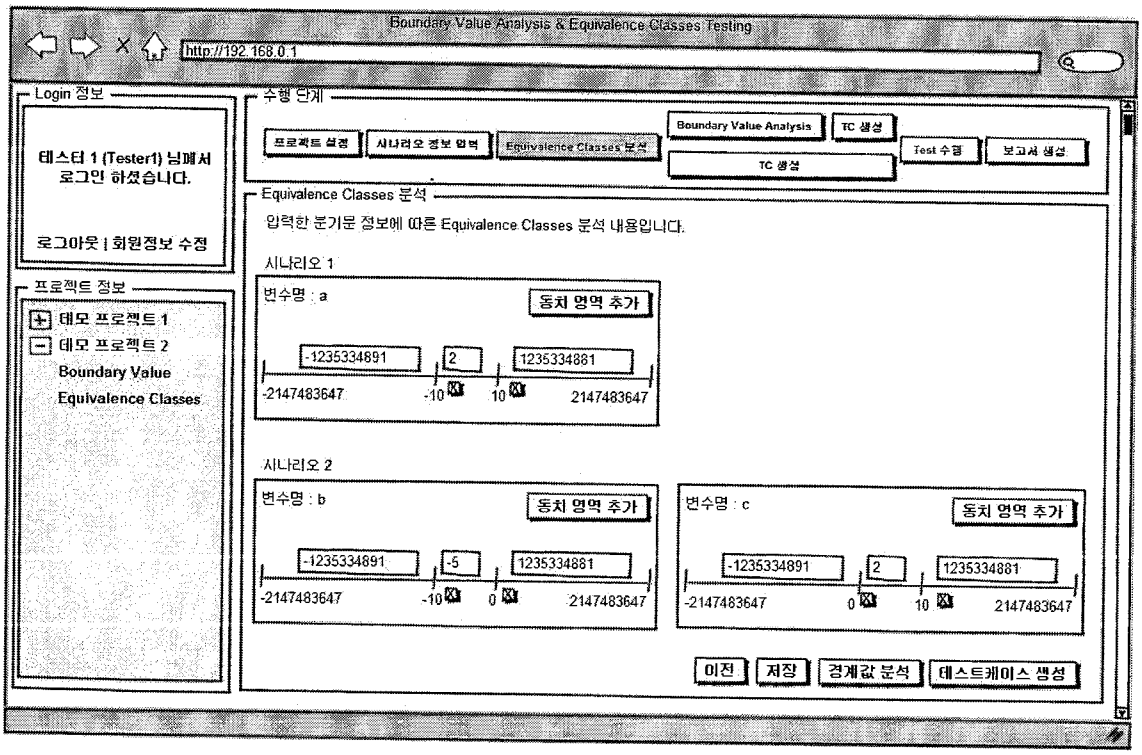


그림 3.3.9 동치영역 자동 분할 및 수정 화면

기 입력된 시나리오 정보를 바탕으로 자동 생성한 동치영역을 그래프로 표시한다. 단, 한 시나리오 내 다수의 입력 변수가 존재할 경우 각 변수별로 별도의 동치영역 표시란을 출력한다. 테스터가 동치영역을 추가하기를 원한다면 '동치영역 추가' 버튼을 클릭하여 새롭게 표시된 창에서 동치영역 경계값을 입력하여 추가할 수 있으며, 임의로 선정된 대표값을 수정하기를 원한다면 현재 대표값이 출력된 입력창의 값을 수정하고 '저장' 버튼을 클릭하면 된다.

○ 경계값 자동 분석 및 수정 화면

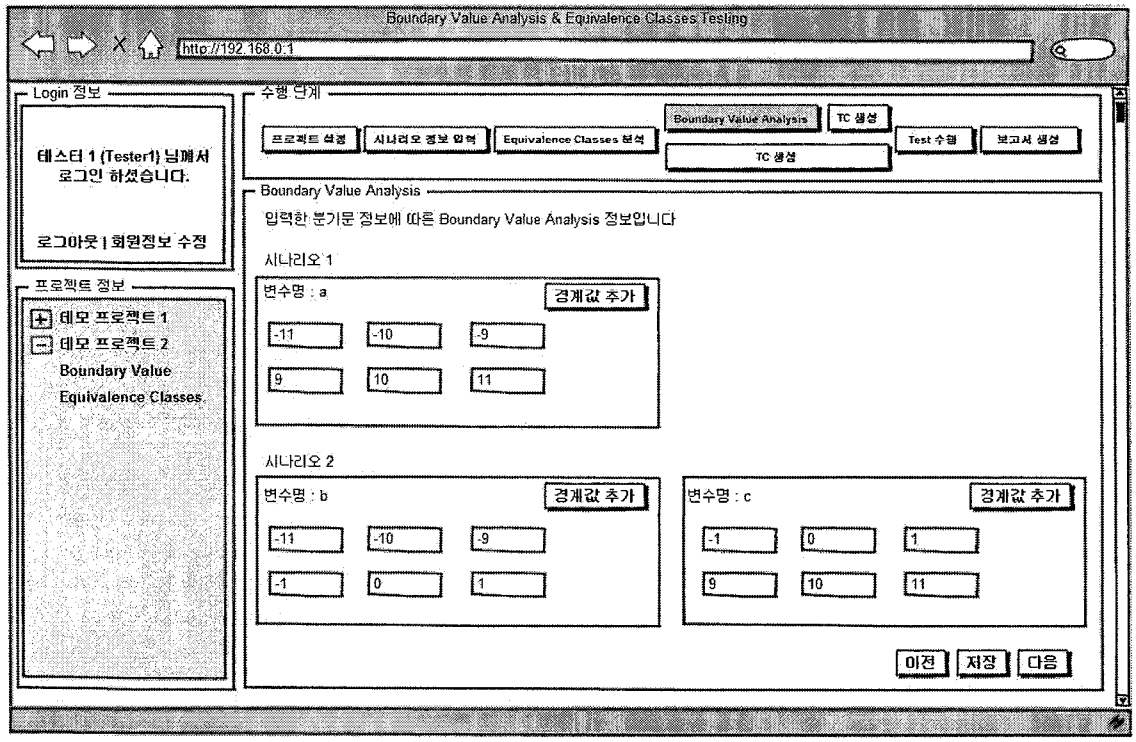


그림 3.3.10 경계값 자동 분석 및 수정 화면

기 입력된 시나리오 정보를 바탕으로 자동 생성된 경계값을 출력한다. 단, 한 분기 내 다수의 입력 변수가 존재할 경우 각 변수별로 별도의 경계값 표시란을 출력한다. 테스터가 새로운 값을 추가하기를 원한다면 '경계값 추가' 버튼을 클릭하여 새롭게 표시된 창에서 값을 입력하여 추가할 수 있으며, 자동 분석된 경계값을 수정하기를 원한다면 현재 경계값이 출력된 입력창의 값을 수정하고 '저장' 버튼을 클릭하면 된다.

○ 동치영역 대표값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면

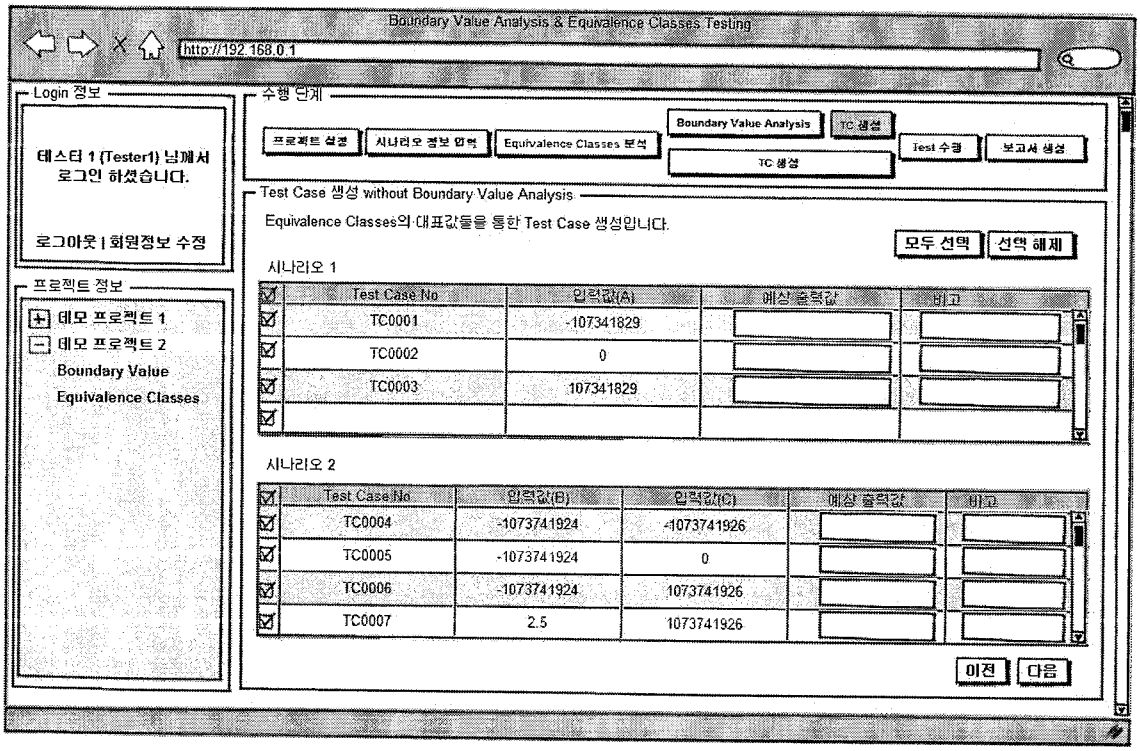


그림 3.3.11 동치영역 대표값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면

기 정의된 동치영역 대표값 정보를 바탕으로 생성된 테스트케이스 목록을 출력한다. 테스터는 테스트케이스 수행후 기대되는 예상 출력값과 비고 사항을 각 테스트케이스의 '예상 출력값', '비고' 입력란에 입력할 수 있으며, 특정 테스트케이스만 수행하고 싶을 경우 원하는 테스트케이스의 체크박스를 지정하여 선택할 수 있다.

○ 경계값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면

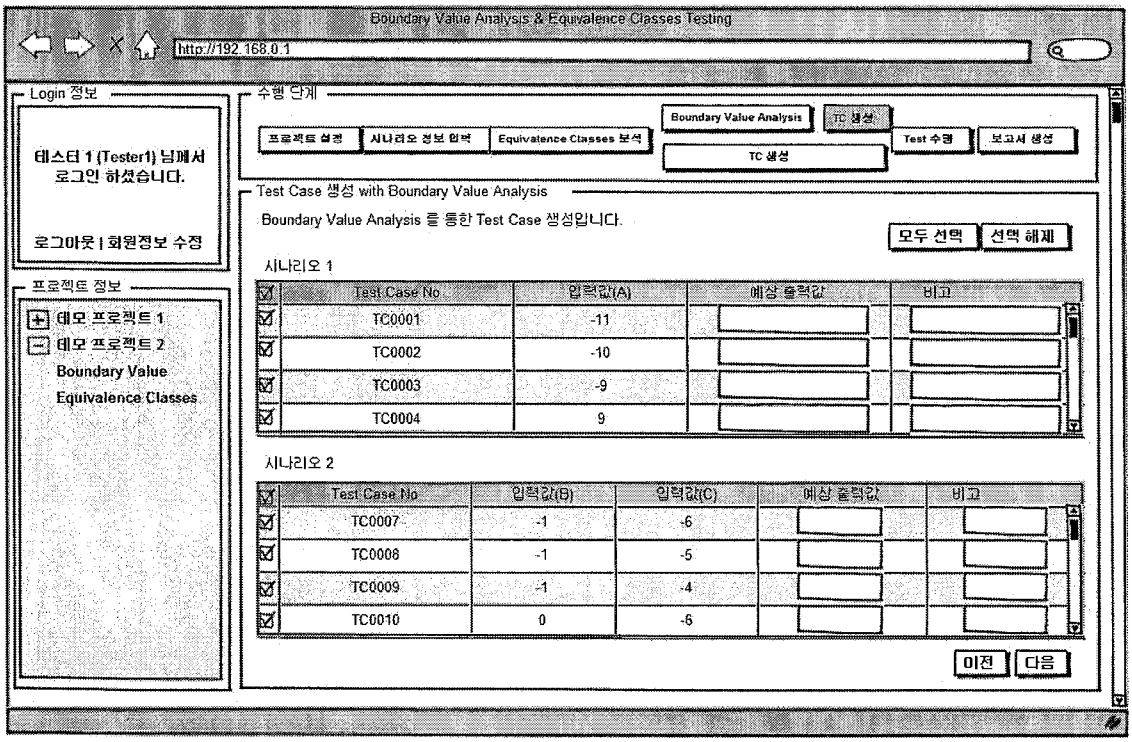


그림 3.3.12 경계값을 이용한 테스트케이스 생성 및 예상 출력값 입력 화면

기 정의된 경계값 정보를 바탕으로 생성된 테스트케이스 목록을 출력한다. 테스터는 테스트케이스 수행후 기대되는 예상 출력값과 비고 사항을 각 테스트케이스의 '예상 출력값', '비고' 입력란에 입력할 수 있으며, 특정 테스트케이스만 수행하고 싶을 경우 원하는 테스트케이스의 체크박스를 지정하여 선택할 수 있다.

○ 테스트 수행 화면

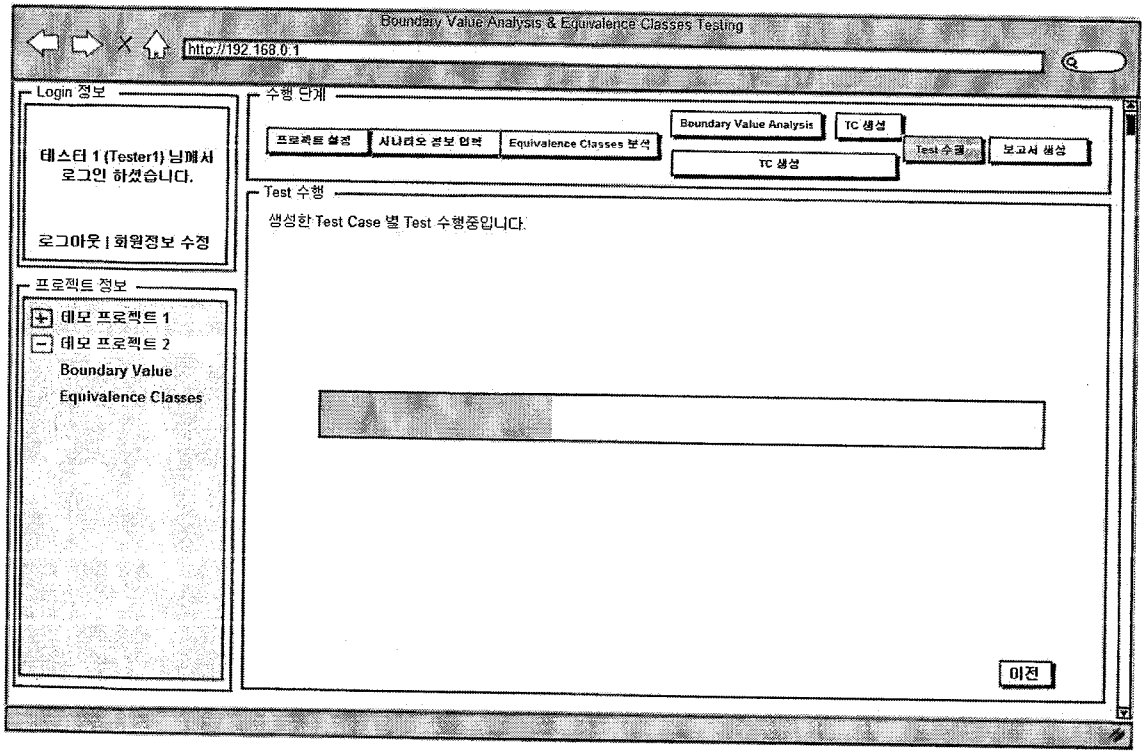


그림 3.3.13 테스트 수행 화면

수행엔진이 테스트 수행을 마무리 할 때 까지 해당 화면을 출력한다.

○ 보고서 생성 화면

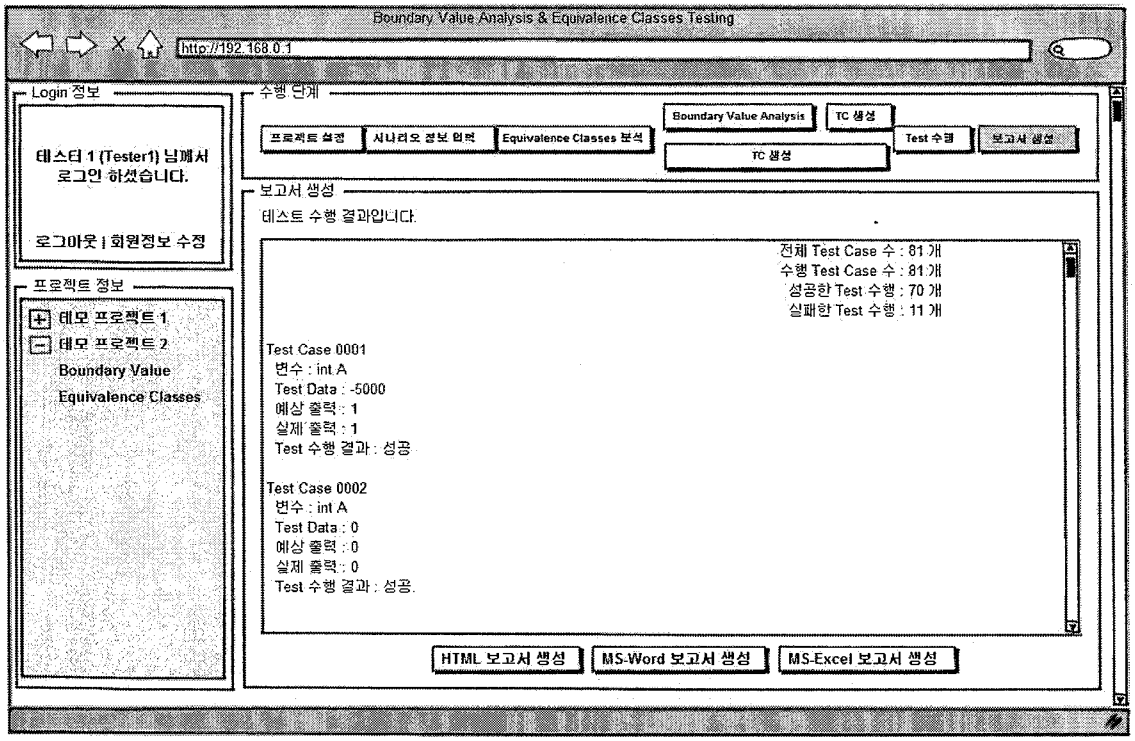


그림 3.3.14 보고서 생성 화면

수행된 테스트의 요약 결과와 각 테스트케이스별 결과를 출력한다. 테스터는 하단의 'HTML 보고서 생성', 'MS-Word 보고서 생성', 'MS-Excel 보고서 생성' 버튼을 클릭하여 각 형식별로 보고서를 생성할 수 있다.

② 화면 구현 방식

Boundary Value Analysis / Equivalence Classes Testing 모듈의 사용자 인터페이스는 ASP 기반의 웹페이지 형태로 구현한다. 테스터는 웹 브라우저를 통해 도구에 접근하여 대화식으로 테스트를 준비하고 진행한다.

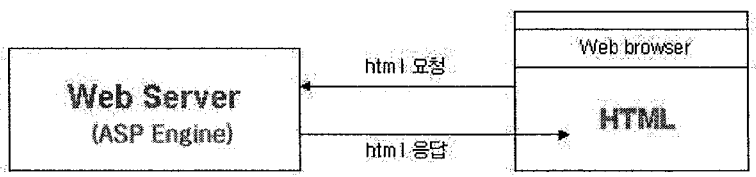


그림 3.3.15 ASP 수행 개념

(라) 기능 설계

Boundary Value Analysis / Equivalence Classes Testing 모듈의 기능은 다음과 같은 세부 모듈로 구성이 되며, 각 세부모듈은 아래 그림과 같은 관계로 구성된다.

표 3.3.3 기능별 세부 모듈

기 능 명	구현 모듈
동치영역 자동 분할 기능	Equivalence Classes Analyzer
동치영역 대표값 자동 생성 기능	Equivalence Classes Analyzer
경계값 자동 생성 기능	Boundary Value Analyzer
테스트케이스 생성 기능	Testcase Generator
테스트케이스 분석 기능	Execution Engine
테스트 수행 기능	Execution Engine
테스트 결과 판정 기능	Test Report Generator
테스트 결과 출력 기능	Test Report Generator
테스트 보고서 자동 생성 기능(HTML)	Test Report Generator
테스트 보고서 자동 생성 기능(MS-Word)	Test Report Generator
테스트 보고서 자동 생성 기능(MS-Excel)	Test Report Generator

① 각 모듈과의 관계도

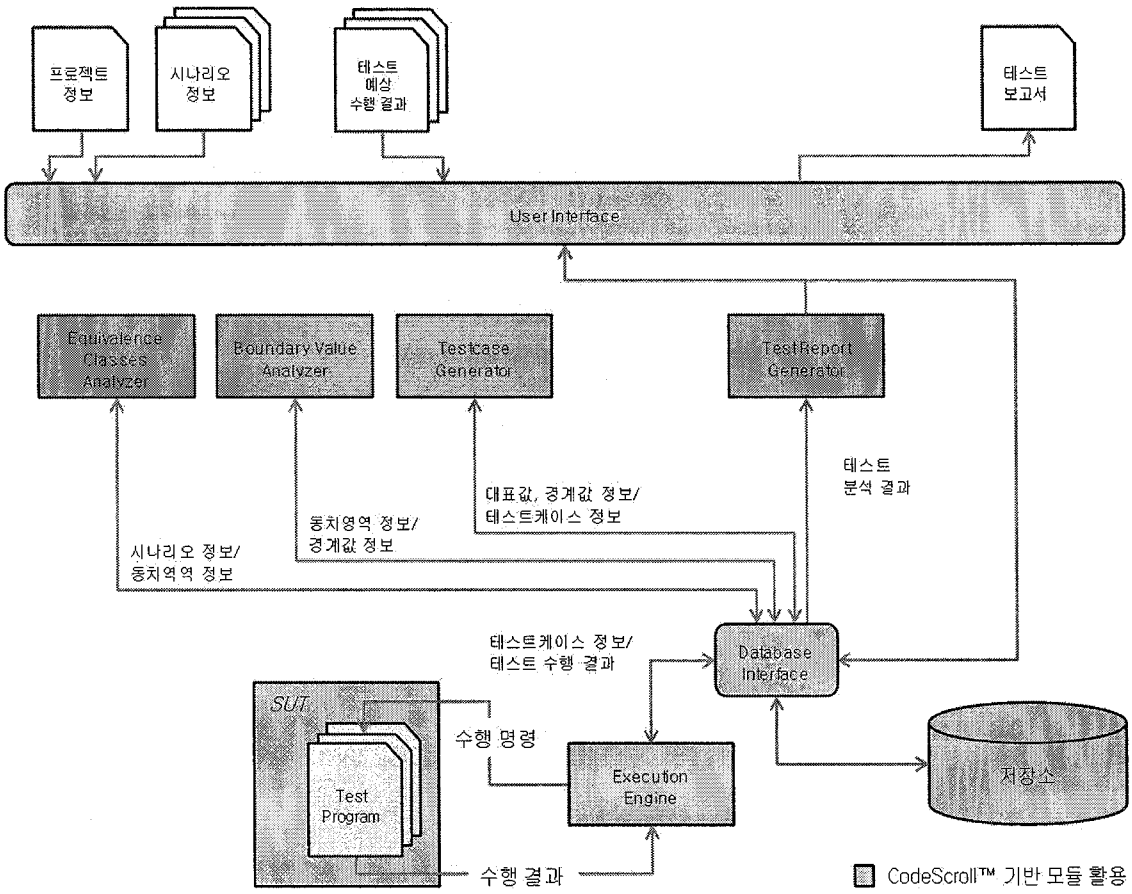


그림 3.3.16 각 모듈과의 관계도

Boundary Value Analysis Testing 모듈은 위 그림과 같이 Equivalence Classes Analyzer, Boundary Value Analyzer, Testcase Generator, Execution Engine, Test Report Generator의 5개 세부모듈과 User Interface, Database Interface로 구성된다. Equivalence Classes Analyzer는 사용자가 입력한 시나리오 정보를 분석하여 동치영역을 자동을 분할하고 각 동치영역 내의 임의의 값을 선정하여 대표값으로 정의한다. Boundary Value Analyzer는 Equivalence Classes Analyzer가 분할한 동치영역 정보를 분석하여 각 영역의 경계값을 정의한다.

Testcase Generator는 테스터의 선택에 따라 Equivalence Classes Analyzer가 정의한 대표값 또는 Boundary Value Analyzer가 정의한 경계값을 바탕으로 테스트케이스를 생성한다.

Execution Engine은 Testcase Generator가 생성한 테스트케이스 정보를 분석하고 이를 바탕으로 시험대상체계를 조작하여 테스트를 수행하며, 각 입력값에 대한 시험대상체계의 출력값을 얻어온다.

Test Report Generator는 Execution Engine이 모든 테스트케이스에 대한 테스트 수행을 마치면 사용자가 입력한 예상 출력값과 실제 출력값을 비교하여 프로그램 오류 여부를 판별하며, 이를 바탕으로 테스트 보고서를 자동 생성한다. 또한 테스터의 요청에 따라 HTML, MS-Word, MS-Excel 형식으로 테스트 보고서를 생성한다.

User Interface는 웹페이지의 보이는 형태로 존재하며, 사용자의 입력값과 각 모듈의 수행 결과를 Database Interface를 통해 주고 받는다.

Database Interface는 각 모듈과 User Interface에서 생성되는 모든 데이터를 저장소에 저장하며, 요청 시 이를 제공한다.

표 3.3.4 Equivalence Classes/Boundary Value Analysis Testing 모듈 기능 리스트

구현 모듈	설명
Equivalence Classes Analyzer	- 시나리오 정보 분석 - 동치영역 자동 분할 - 대표값 자동 생성
Boundary Value Analyzer	- 동치영역 분할 결과 분석 - 경계값 자동 생성
Testcase Generator	- 동치영역 대표값 선정 결과 분석 - 경계값 생성 결과 분석 - 테스트케이스 생성
Execution Engine	- 테스트케이스 분석 - 시험대상체계 접근 설정 - 테스트 수행
Test Report Generator	- 테스트 결과 판정 - 테스트 결과 출력 - 테스트 보고서 자동 생성(HTML) - 테스트 보고서 자동 생성(MS-Word) - 테스트 보고서 자동 생성(MS-Excel)

② 기능별 모듈의 상세설계

○ Equivalence Classes Analyzer

- 알고리즘

소프트웨어나 시스템의 입력값은 입력의 결과로 나타날 결과값이 동일한 경우 하나의 그룹(클래스)으로 간주될 수 있다. 그리고 이러한 그룹 내의 입력값은 내부적으로 같은 방식으로 처리됨을 가정한다. 동치영역 분할 방법은 이러한 원리를 이용하여 입/출력값 영역을 유한개의 상호 독립적인 집합으로 나누어 수학적인 등가 집합을 만든 후, 각 등가 집합의 원소 중 대표값 하나를 선택하여 테스트 케이스를 선정하는 것이다.

동치영역 분할을 자동으로 수행하기 위하여 테스터는 시나리오 정보를 입력해야 하며, 시나리오 정보에는 입력값의 조건이 포함되어야 한다. Equivalence Classes Analyzer는 이 조건을 다음과 같은 분석 알고리즘을 통하여 동치영역 분할을 수행한다.

```
for (조건값을 기준으로 오름차순 정렬된 모든 조건 영역) {
        1. 첫 조건 영역일 경우 이전 값 = -∞
        2. 이번 부호를 "=" 포함으로 변경
        3. if (이전 부호 == 이번 부호) {
                continue
        } else {
                4. if ((이번 부호가 "=<" 또는 "=>") {
                        이전 값과 이번 값 사이의 대표값 생성 및 동치영역 저장
                }
                5. else if (이번 부호가 "==" 이고, 이전 부호가 "<=") 또는,
                (이번 부호가 "!=" 이고, 이전 부호가 ">=") {
                        이번값을 대표값으로 갖는 동치영역 저장
                }
        }
}
```

1. for 루프의 첫 번째 수행일 경우 연산에 사용해야 하는 "이전 값"을 -∞로 정의한다.
2. 동치영역 분석에 조건 영역의 등호 포함 여부는 영향을 미치지 않기 때문에 부호 비교를 용이하기 위하여 등호 포함으로 통일한다.
3. 이전 조건영역과 이번 조건영역의 부호가 동일하면 같은 동치 영역 내에 존재하기 때문에 연산을 수행하지 않고 다음 조건 영역으로 넘어간다. 이 때 다음 조건 영역 연산시 사용할 이전 값과 이전 부호는 갱신하지 않고, 현재 루프 진입시 정의되어 있던 값을 사용한다.
4. 이번 부호가 "<=" 또는 ">="일 경우 이전 값과 이번값을 새로운 동치영역으로 저장한다. 이 때 이전값과 이번값 사이의 임의의 값을 대표값으로 선정한다.
5. 이번 부호가 "==" 이고 이전 부호가 "<="이거나, 이번 부호가 "!=" 이고 이전 부호가 ">="일 경우 이번 값을 대표값으로 갖는 새로운 동치영역을 저장한다.

- 자료구조

표 3.3.5 Equivalence Classes Analyzer의 자료구조

자료구조	필드명	자료형	의미
CONDITION	condID	int	조건 ID
	andOr	bool	AND, OR 식별자
	varName	String	조건의 해당 변수명
	boundaryType	int	부등호 코드 0 : <= 1 : < 2 : >= 3 : > 4 : == 5 : !=
	scnID	int	소속 시나리오 ID

자료구조	필드명	자료형	의미
EC	ecID	int	동치영역 ID
	rightValue	int	동치영역의 최대값
	representativeValue	int	.동치영역의 대표값
	varName	String	동치영역의 해당 변수명
	scnID	int	소속 시나리오 ID

○ Boundary Value Analyzer

- 알고리즘

프로그램의 입력 범위는 입력 클래스 수로 나누어지므로 클래스의 모든 경계와 극단을 대상으로 시험해야 하며, 프로그램에서 동시에 발생하는 정의된 입력범위의 경계 값에 대하여 체크를 해야 한다. 경계값 분석은 파라미터의 한계 또는 경계에서 발생하는 소프트웨어 오류를 제거하기 위한 시험기법이다.

경계값 분석을 자동으로 수행하기 위하여 테스터는 시나리오 정보를 입력해야 하며, 시나리오 정보에는 입력값의 조건이 포함되어야 한다. Boundary Value Analyzer는 테스터가 입력한 시나리오 정보의 조건을 이용하여 경계값을 분석할 수 있지만 Equivalence Classes Analyzer가 분석한 동치영역을 정보를 바탕으로 분석을 진행하면 생성되는 테스트케이스의 수를 줄일 수 있다. 다음은 동치영역 정보를 바탕으로 경계값을 분석하는 알고리즘이다.

```
for (최소값을 기준으로 오름차순 정렬된 모든 동치영역) {
        1. if (최대값 == +∞) {
                break;
        }

        2. if (경계값 목록에 최대값 - 1이 없다) {
```

```
                경계값1 = 최대값 - 1
        }
        3. if (경계값 목록에 최대값이 없다) {
                경계값1 = 최대값
        }
        4. if (경계값 목록에 최대값 + 1이 없다) {
                경계값1 = 최대값 + 1
        }
}
```

1. 경계값의 정의는 동치영역의 최대값을 기준으로 수행하기 때문에 해당 동치영역의 최대값이 +∞일 경우 루프를 종료한다.
2. 현재까지 정의한 경계값 목록에 최대값 - 1이 존재하지 않으면 이를 추가한다.
3. 현재까지 정의한 경계값 목록에 최대값이 존재하지 않으면 이를 추가한다.
4. 현재까지 정의한 경계값 목록에 최대값 + 1이 존재하지 않으면 이를 추가한다.

- 자료구조

표 3.3.6 Boudary Value Analyzer의 자료구조

자료구조	필드명	자료형	의미
EC	ecID	int	동치영역 ID
	rightValue	int	동치영역의 최대값
	representativeValue	int	동치영역의 대표값
	varName	String	동치영역의 해당 변수명
	scnID	int	소속 시나리오 ID
BV	bvID	int	경계값 ID
	boundar	int	경계값

자료구조	필드명	자료형	의미
	yValue		
	varNam e	String	경계값의 해당 변수명
	scnID	int	소속 시나리오 ID

○ Testcase Generator

- 알고리즘

테스트 수행을 위한 테스트케이스의 생성은 각 시나리오 단위로 생성되며, 테스트케이스 입력값의 수는 각 시나리오 입력 변수의 수와 일치한다. 각 입력값은 각 변수별 동치영역 분석시 정의한 대표값 혹은 경계값의 완전 조합으로 정의되며, 테스트케이스의 수는 각 변수별 대표값 혹은 경계값 수의 곱과 동일하다.

- 자료구조

표 3.3.7 Testcase Generator의 자료구조

자료구조	필드명	자료형	의미
TestCase	testcase ID	int	테스트 DB의 테스트 케이스ID
	inputs	list<TestCaseInpu t>	테스트 케이스의 입력값 정보 리스트
	outputs	list<TestCaseOutp ut>	테스트 케이스의 출력값 정보 리스트
TestCase Output	value	int64_t	출력 된 실제 값 (float제공시 변경 예정)
	valueSiz e	unsigned int	출력 값의 Byte 사이즈
	waitTim e	unsigned int64_t	출력 값을 가지고 오기 위한 대기 시간 (ms)
	varAddr ess	addr_t	출력 변수의 SUT 메모리 주소

○ Execution Engine

- 알고리즘

Execution Engine은 테스트케이스 정보와 시험 대상 체계에 접속하기 위한 타겟 서버 이름을 전달받아 수행 된다. 수행이 이루어지면 테스트 수행 정보가 담긴 데이터베이스로부터 테스트 케이스들의 목록을 얻어온 후, SUT에 접속하여 테스트 케이스마다 SUT에 지정된 메모리에 입력값을 쓰고 지정된 시간만큼 대기한 뒤, SUT내에 지정된 출력 메모리로부터 출력 값을 읽어와 이를 다시 테스트 정보 데이터베이스에 업데이트 하는 동작을 반복한다. 다음은 Execution Engine의 수행 구조도이다.

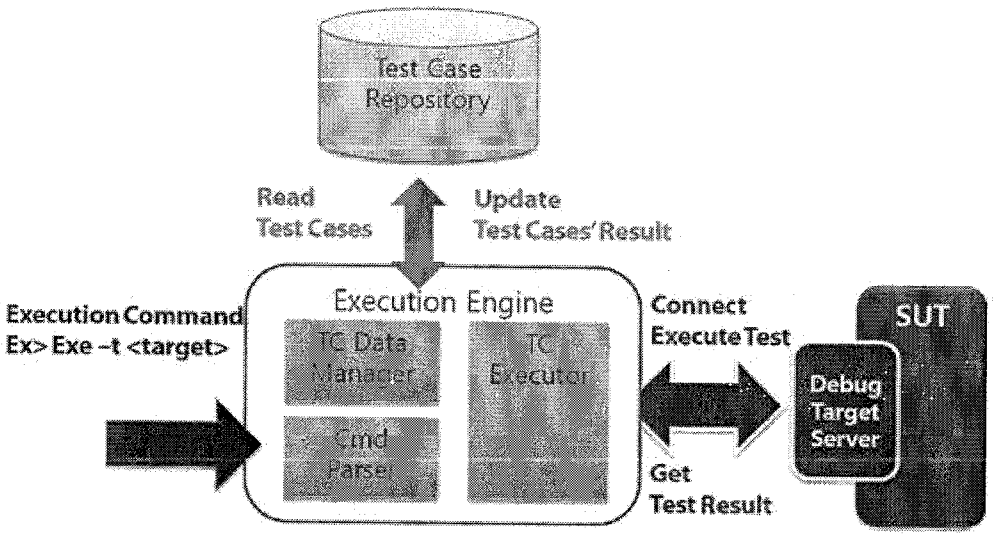


그림 3.3.17 Execution Engine 수행 구조도

- 자료구조

표 3.3.8 Execution Engine의 자료구조

자료구조	필드명	자료형	의미
TestCase	testcase ID	int	테스트 DB의 테스트 케이스ID
	inputs	list<TestCaseInput>	테스트 케이스의 입력값 정보 리스트
	outputs	list<TestCaseOutput>	테스트 케이스의 출력값 정보 리스트

자료구조	필드명	자료형	의미
TestCase Input	value	int64_t	입력 값 (float제공시 변경 예정)
	valueSize	unsigned int	입력 값의 Byte 사이즈
	varName	string	입력 변수의 접근 이름
	varAddress	addr_t	입력 변수의 SUT 메모리 주소
TestCase Output	value	int64_t	출력 된 실제 값 (float제공시 변경 예정)
	valueSize	unsigned int	출력 값의 Byte 사이즈
	waitTime	unsigned int64_t	출력 값을 가지고 오기 위한 대기 시간 (ms)
	varAddress	addr_t	출력 변수의 SUT 메모리 주소

○ Test Report Generator

- 알고리즘

Test Report Generator는 수행한 모든 테스트케이스에 대하여 수행 결과와 대조 작업을 수행하여 프로그램 오류 여부를 확인하고 이를 보고서 형태로 출력한다.

- 자료구조

표 3.3.9 Test Report Generator의 자료구조

자료구조	필드명	자료형	의미
TestCase	testcaseID	int	테스트 DB의 테스트 케이스ID
	inputs	list<TestCaseInput>	테스트 케이스의 입력값 정보 리스트
	outputs	list<TestCaseOutput>	테스트 케이스의 출력값 정보 리스트
TestCase Output	value	int64_t	출력 된 실제 값 (float제공시 변경 예정)

자료구조	필드명	자료형	의미
	valueSize	unsigned int	출력 값의 Byte 사이즈
	waitTime	unsigned int64_t	출력 값을 가지고 오기 위한 대기 시간 (ms)
	varAddress	addr_t	출력 변수의 SUT 메모리 주소

(마) 개발 결과

① 프로그램 초기 화면

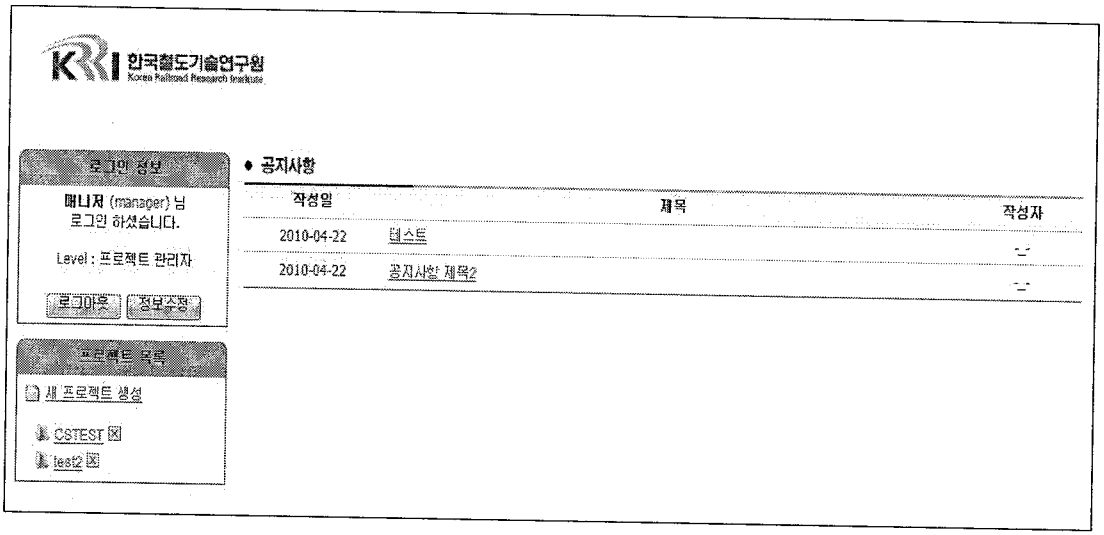


그림 3.3.18 프로그램 초기 화면

테스터 ID와 비밀번호를 입력하고 로그인 하면 초기 화면이 출력된다. 초기화면의 좌측에는 로그인 정보와 테스터가 진행중인 테스트 프로젝트의 정보가 출력되고 메인화면에는 공지사항이 출력된다.

② 프로젝트 설정 입력

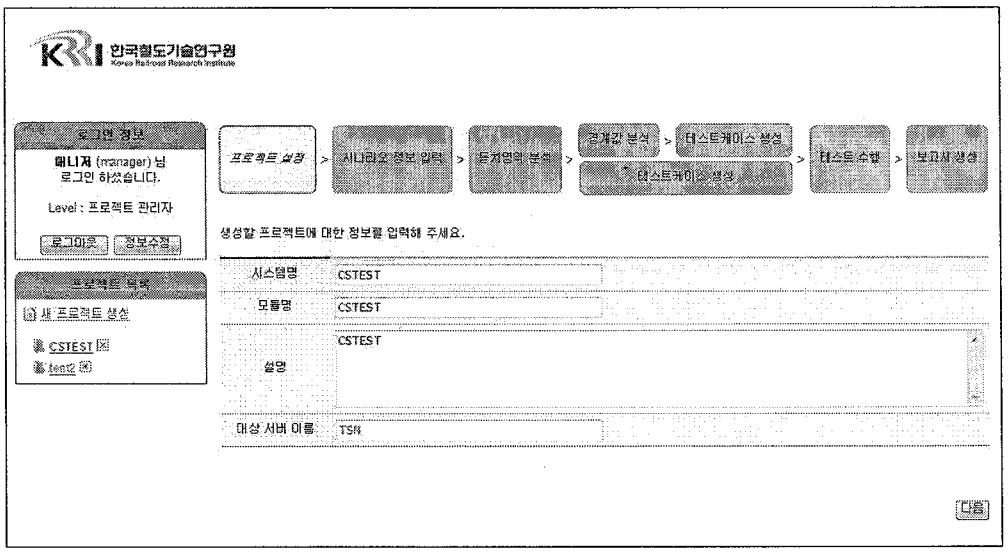


그림 3.3.19 프로젝트 설정 입력

시스템명, 모듈명, 프로젝트 설명, 대상서버 이름 등 테스트 프로젝트의 기본정보를 입력한다.

③ 시나리오 정보 입력

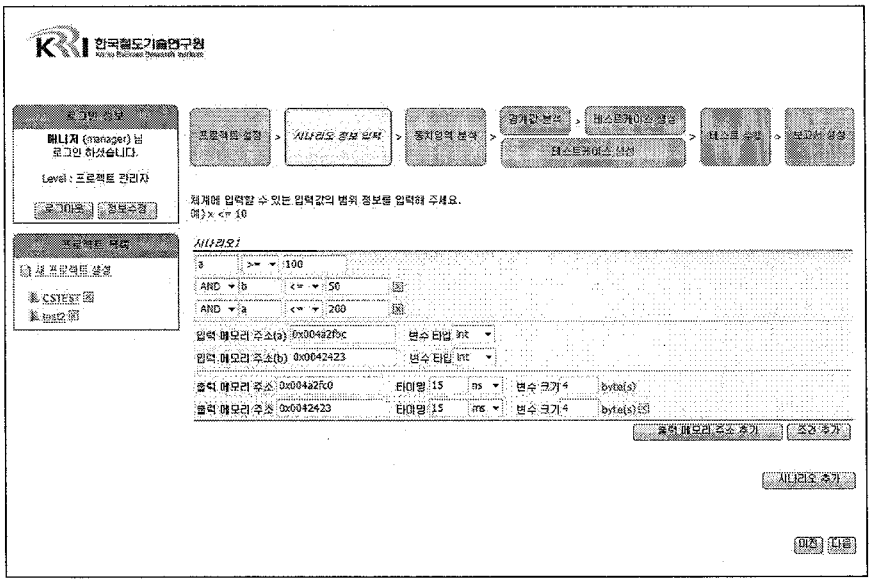


그림 3.3.20 시나리오 정보 입력

변수명, 부등호, 경계값 등의 분기 조건, 입력 변수의 메모리 주소와 변수 타입, 출력 메모리 주소와 획득 시간 및 단위, 크기 등의 시나리오 정보를 입력한다.

④ 동치영역 자동 분할 및 수정

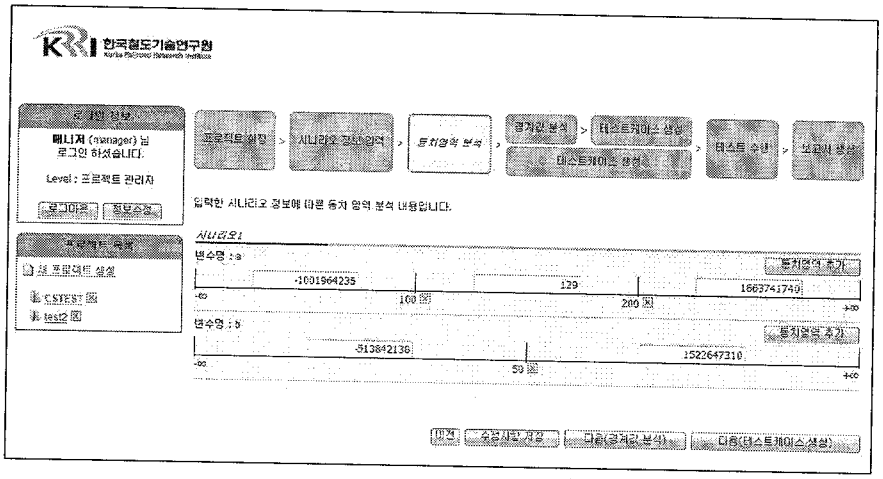


그림 3.3.21 동치영역 자동 분할 및 수정

자동 분석한 동치영역을 그래프 형태로 출력한다. 동치영역의 대표값을 수정할 필요가 있을 경우 해당 대표값을 수정하고, 새로운 동치영역을 추가할 필요가 있을 경우 "동치영역 추가" 버튼을 클릭하고 새로운 동치영역의 경계값을 입력한다.

⑤ 경계값 자동 분석 및 수정

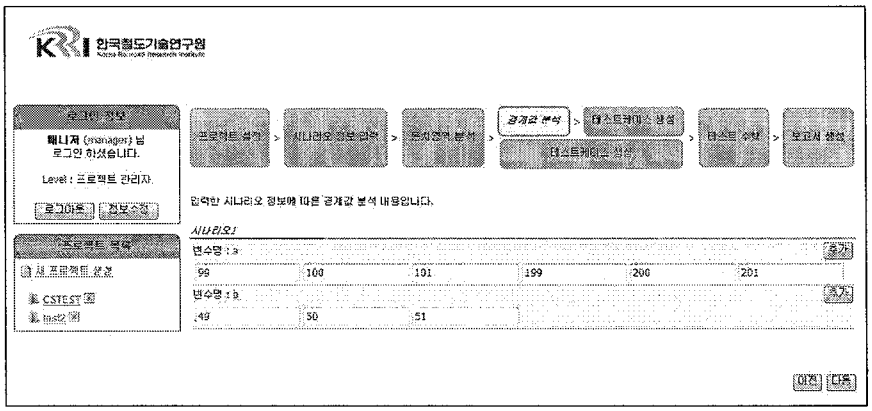


그림 3.3.22 경계값 자동 분석 및 수정

자동 분석한 경계값을 출력한다. 경계값을 수정할 필요가 있을 경우 해당 경계값을 수정하고, 새로운 경계값을 추가할 필요가 있을 경우 "추가" 버튼을 클릭하고 새로운 경계값을 입력한다.

⑥ 동치영역 대표값 테스트케이스 생성 및 예상 출력값 입력

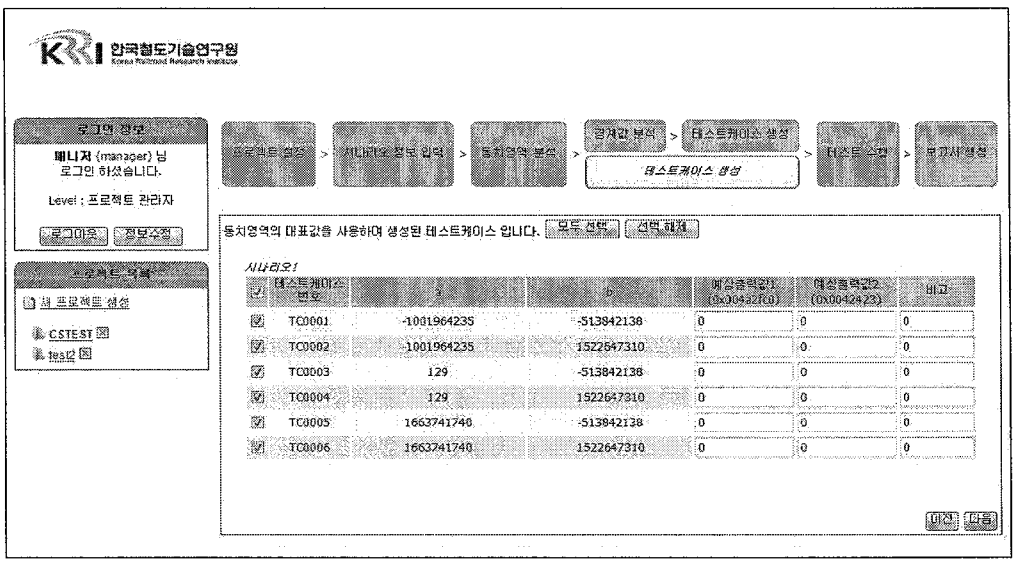


그림 3.3.23 동치영역 대표값 테스트케이스 생성 및 예상 출력값 입력

동치영역의 대표값을 바탕으로 생성된 테스트케이스의 목록을 확인하고, 각 테스트케이스의 예상 출력값을 입력한다. 또한 특정 테스트케이스만 수행하기를 원한다면 해당 테스트케이스의 좌측에 존재하는 체크박스를 선택한다.

⑦ 경계값 테스트케이스 생성 및 예상 출력값 입력

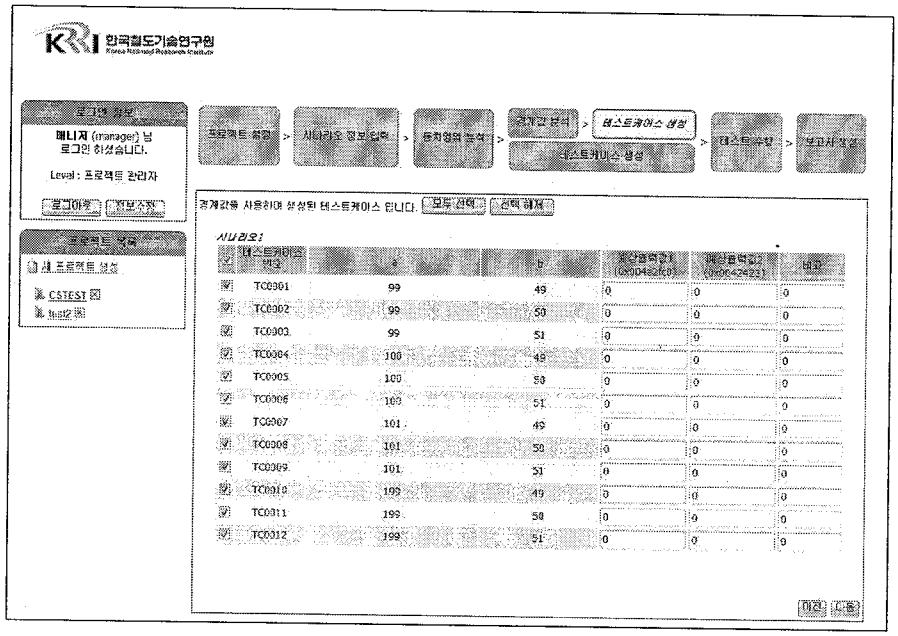


그림 3.3.24 경계값 테스트케이스 생성 및 예상 출력값 입력

경계값을 바탕으로 생성된 테스트케이스의 목록을 확인하고, 각 테스트케이스의 예상 출력값을 입력한다. 또한 특정 테스트케이스만 수행하기를 원한다면 해당 테스트케이스의 좌측에 존재하는 체크박스를 선택한다.

⑧ 테스트 수행

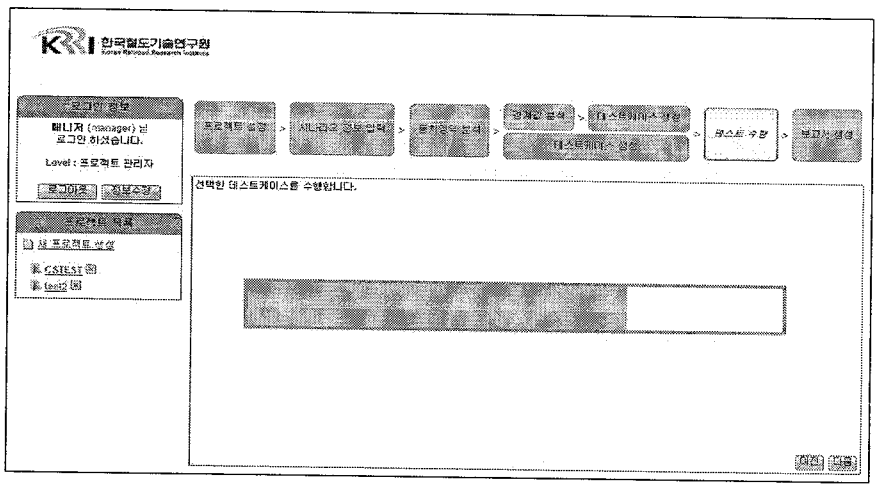


그림 3.3.25 테스트 수행

수행엔진이 각 테스트케이스를 바탕으로 테스트를 수행한다.

⑨ 보고서 생성

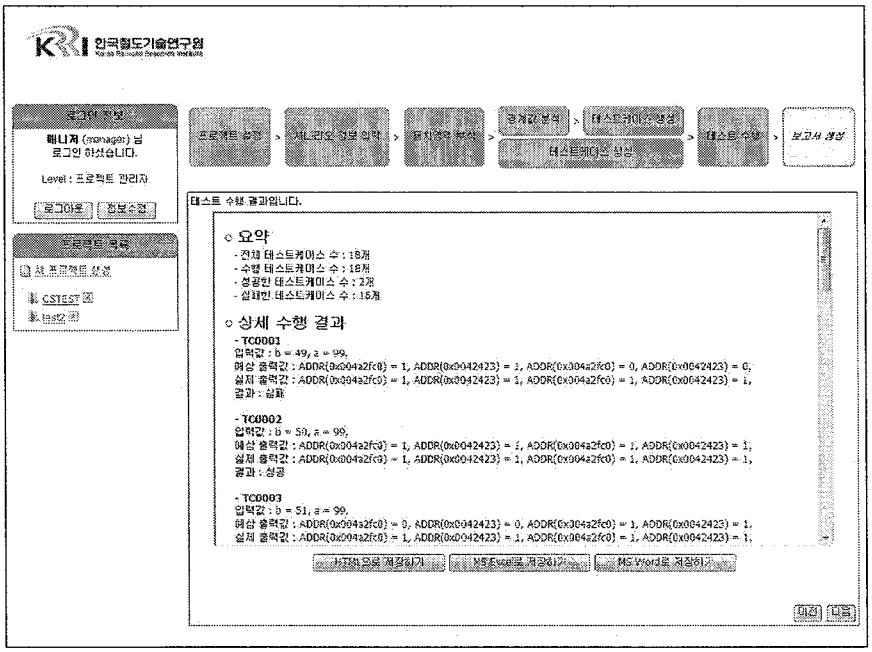


그림 3.3.26 보고서 생성

테스트 수행 결과를 바탕으로 보고서를 생성, 출력한다. 보고서의 상단에는 전체 테스트케이스, 수행 테스트케이스 수, 성공 / 실패 테스트케이스의 수를 출력해주고, 하단에는 각 테스트케이스의 입력값과 사용자가 입력한 기대 출력값, 테스트 수행 후의 실제 출력값을 출력해준다.

(3) Fault Tree Analysis모듈

본 절에서는 Java 언어로 작성된 코드에 대하여 Fault Tree Analysis를 수행하는 Fault Tree Analyzer(FTA) 모듈을 구현하기 위한 설계 및 구현 결과의 내용을 기술한다.

(가) 시스템 구조

FTA는 신뢰성 및 안전성 분석을 위한 기법 중 하나로, 1962년 Bell 연구소에서 미 공군 연구를 위해 처음 개발되었다. Fault Tree는 시스템의 오류 상황에 대해 구분 가능한 하위 사건들을 나열하고, 이들 간의 관계를 분석하여 최종 원인 관계를 분석하는 방법이다. FTA를 수행하는 일반적인 절차는 다음 그림에서 명시한 단계를 따른다.

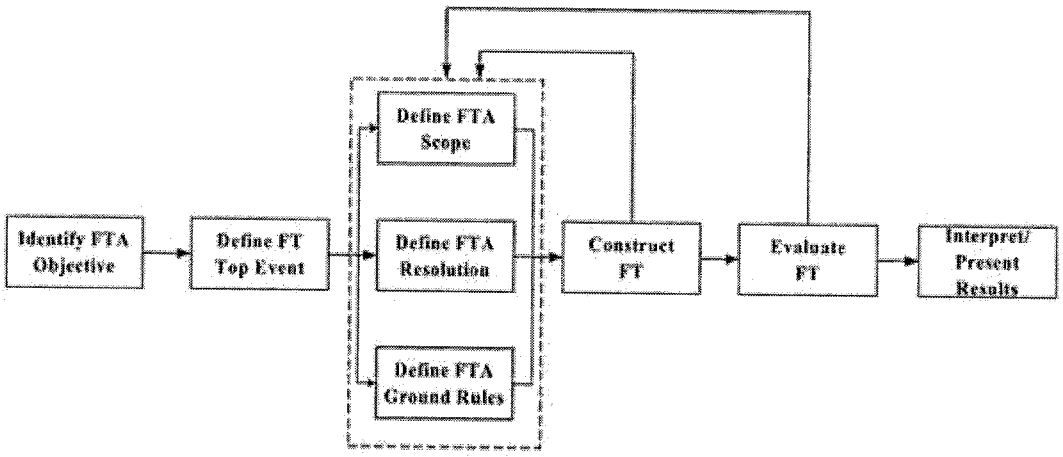


그림 3.3.27 Fault Tree Analysis Steps

상위 5단계는 FTA를 위한 문제의 정의를 위해 필요한 단계이고, 나머지 3단계는 직접적으로 FT를 생성하고, 평가하고, FT 결과를 해석하는 단계로 구분 할 수 있다. 그림에서 보여지 듯 대부분의 단계는 순차적으로 수행되나, 3-5의 단계는 병렬적으로 수행된다. 6단계와 7단계로부터의 피드백이 명시되어 있다.

① Fault Tree Analysis의 목적 구분

FTA를 수행하기 이전 가장 먼저 FTA의 목적을 정의해야 한다. 성공적인 Fault

Tree 분석 결과에도 불구하고, 결정권자나 관리자의 목적을 만족시키지 못하는 경우가 발생하는 것을 사전에 방지하기 위해 분명한 목적을 정의하도록 한다. 목적은 분석 대상의 시스템의 실패를 고려하도록 정의한다.

② Fault Tree의 최상위 사건 정의

Fault Tree의 최상위 사건은 Failure들로 인해 발생하는 최종 사건으로 해결 대상이며, 위험도가 계산되어야 할 사건이다. 결국 FTA가 분석하려는 시스템의 failure mode를 정의한다.

③ Fault Tree Analysis의 범위 정의

FTA은 특정 시점의 시스템의 단면적인 행위에서 보여지는 오류에 대해 분석하는 방법이다. 따라서 시스템 전체 중 분석 대상만으로 한정하고, 해당 대상 중에서도 오류와 관계된 사건들의 조합만으로 한정해야 한다. 마지막으로 특정 시점에 나타나는 단면적인 행위에 대해 분석하기 위해 재차 한정하여 최종 범위를 지정한다. 예를 들어 비행기의 비행 조종 시스템의 실패를 대상으로 가정하는 경우, 1) 분석될 시스템의 버전을 명시하여 구분하고, 2) 수행될 기능의 모드를 정의하고, 3) 시스템 기능과 관련된 하위 시스템 및 연계 중 분석 대상 및 제외 대상을 구분하여 나열할 수 있다.

④ Fault Tree Analysis의 Resolution 정의

FTA에서 Resolution을 정의하는 작업은 Fault Tree에서 최상위 사건으로부터 어느 수준의 하위 사건들의 조합으로 나타낼지를 정하는 것을 의미한다. 일반적으로 시스템의 형태나 최상위 사건의 형태에 따라 다양한 resolution 수준을 정의할 수 있다. 의도하지 않은 종료나 운영 실패 등의 시스템의 기능적 실패 사건을 최상위 사건으로 정의하는 경우, 최상위 사건은 시스템을 구성하는 서브시스템들로 분리될 수 있다. 재앙수준의 엔진 시스템 폭발과 같은 현상적인 실패를 최상위 사건으로 정의하는 경우, 시스템의 구성보다는 폭발의 원인들로 Fault Tree의 사건들을 설계할 수 있다. 따라서 분석가는 주어진 시스템 및 정의하고자 하는 최상위 사건에 대한 적합한 Resolution을 정의해서, 분석을 수행해야 한다.

⑤ Fault Tree Analysis의 기본 원칙(ground rule) 정의

FTA를 위한 기본 원칙을 정하는 단계는 Fault Tree를 작성하는 절차나, Fault Tree의 각 노드들을 생성하고, 명명하는 것까지의 세세한 방법까지를 기술하는 것을 의미한다. 다수의 분석가로부터 생성된 다양한 Fault Tree에 대해 일관성을 부여 할 수 있으며, Fault Tree 간의 이해, 분석, 조합을 위해 제공되어야 하는 기본 정보에 해당한다. 설계 기본 원칙은 특정 컴포넌트 실패, 인간 오류, 공통 실패를 설계하는 방법을 포함하기도 한다.

⑥ Fault Tree의 작성

정의된 Fault Tree의 형식에 따라 Diagram을 작성한다. 작성에 대한 사항은 다음 절에서 추가 설명된다.

⑦ Fault Tree의 평가

Fault Tree는 정성적, 정량적 평가를 의미한다. 정성적 평가는 최상위 사건에 대한 minimal cut set을 생성하여 평가할 수 있다. 분석된 Cut Set들은 최상위 사건을 야기할 수 있는 기본 사건들의 조합 정보를 제공하기 위해 Cut Set에 포함된 기본 사건의 개수에 따라 정렬되어 제공된다.

정량적 평가는 Fault Tree를 구성하는 기본 사건, 기본 사건들의 조합, 그리고 최상위 사건의 발생 확률을 계산하는 것이다. 효율적인 확률 계산을 위해서 발생 확률에 따라 Cut Set을 정렬하고, 낮은 확률의 Cut Set은 분석 대상에서 제외되기도 한다.

⑧ 결과 해석 및 보고

다수의 FTA 기법들은 보고 절차에서 단순한 보고를 작성함으로 FTA의 결과를 충분히 제공하지 못하고 있으나, 직관적인 보고를 통해 분석 목적에 잠재적으로 영향을 미칠 수 있는 소지를 분명하게 제공한다.

모듈의 주요한 기능은 다음 표와 같다.

표 3.3.10 Fault Tree Analyzer 주요 기능 리스트

주요기능	설명
Fault Tree 명세 작성	사용자가 GUI를 이용하여 Fault Tree를 입력할 수 있는 WISWIG 편집 기능을 제공한다.
Fault Tree 확률 입력	확률 기반의 해석을 위한 확률 입력 기능을 제공한다.
Fault Tree 확률 해석	확률 모델로부터 사건 확률을 자동 계산하는 기능을 제공한다.
시험결과로 위험도 계산	시험 도구에 의해 수행된 시험 결과로 계측된 오류 발생 빈도와 시험 도구에서 고려하는 Fault Tree를 입력받아, 시스템의 Fault 위험도를 계산해주는 기능을 제공한다.

① Fault Tree 명세 작성

일반 Diagram 편집 수준의 Fault Tree 편집 기능을 제공한다. 생성된 Diagram은 파일로 저장 및 로드 기능을 제공한다. 안전성 분석자의 편의성을 최대한 고려한 Diagram 편집 도구 기능을 제공한다.

② Fault Tree 확률 입력

작성된 Fault Tree에 대해 확률 해석을 수행하기 위한 확률 값 입력 기능을 제공한다. 확률 모델은 사전 정의된 모델에 대해서만 제공되며, 해당 모델을 통해 해석에 필요한 확률 값을 손쉽게 입력 받을 수 있는 GUI를 제공한다. 입력 완료된 확률 모델은 Fault Tree와 연계되어 관리되며, Save / Load 기능을 고려한다.

③ Fault Tree 확률 해석

Fault Tree 와 확률 모델을 기반으로 확률 계산을 수행하여 위험도를 계산한다. 자동으로 계산된 위험 분석 결과는 보고서로 생성되며 사용자에게 전달된다. 수행 완료된 결과는 저장, 관리되어, 분석 완료된 이후에도 중복하여 확률 분석하지 않고, 접근 가능케 한다.

④ 시험 결과로 위험도 계산

외부 시험 도구로부터 시험을 위해 오류 상황을 분석한 Fault Tree 와 실제 시험을 진행하며 전체 수행된 횟수에 비한 오류 발생 횟수의 비율을 사건의 확률로 입력 받아 일반적인 Fault Tree의 위험도 계산을 수행한다. 외부 도구에서 정의한 Fault Tree에 따라 위험도 계산이 달라질 수 있으며, Fault Tree의 각 사건의 발생 확률은 해당 외부 시험 도구가 계산한다. 계산된 위험도 결과는 도구로 전달되고 종료된다. 외부 시험 도구는 수행된 위험도 결과에 신규 시험 결과를 반영하여 위험도 계산을 요청할 수 있다. 기존 위험도 계산이 완료된 입력물에 대해 변경 확률이 전달되는 경우, 위험도를 갱신해서 재 전달한다.

(나) 동작 시나리오

FTA는 독립적으로 수행되는 응용 프로그램으로 Fault Tree 명세에 대한 위험도 분석이 주요 목적이다. 사용자는 위험 분석을 수행할 사건에 대해 Fault Tree를 작성하게 되고, Fault Tree를 구성하는 다양한 사건에 대한 발생 확률을 입력하게 된다. 입력 완료된 Fault Tree는 FTA에 의해 Fault Tree 내의 모든 사건에 대해 자동 계산되며, 특정 대상 사건에 대한 발생 확률로 계산된다. 일련의 과정을 통해 생성된 사건들의 발생 확률은 위험도 수준을 반영하는 위험 분석 보고서로 생성되고, 최종 사용자에게 전달된다.

또한 FTA는 외부 시험 도구와의 연계를 제공하여, 시험 수행에 따른 위험도 계산 기능을 제공할 수 있다. 외부의 시험 도구는 FTA에서 정의한 형식에 따라 Fault Tree를 설계하고, 시험 수행에 따른 오류 발생 빈도를 Fault Tree의 사건의 발생 확률로 대체하여 입력할 수 있다. FTA는 시험 도구로부터 입력되는 Fault Tree와 각 사건에 따른 발생 확률을 기반으로 오류 Fault Tree의 위험도를 계산하고, 도구로 보고 해 주는 기능을 제공한다.

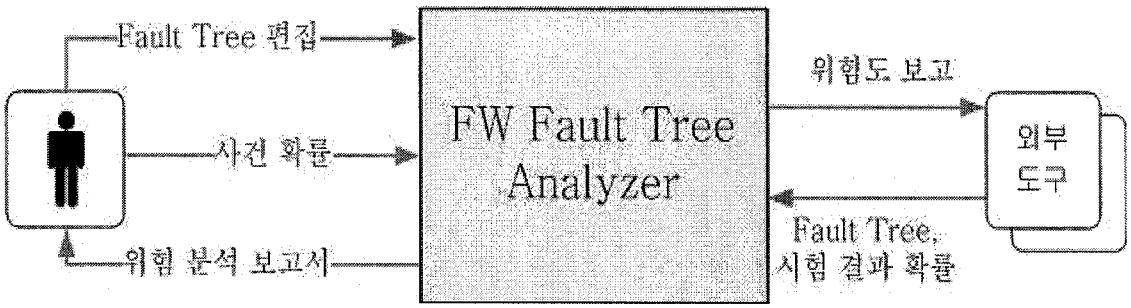


그림 3.3.28 Fault Tree Analyzer system interface

본 모듈의 동작 시나리오는 다음과 같다.

① FTA 프로젝트 생성

Fault Tree Analysis Project를 생성한다. Project는 여러 개의 page를 가질 수 있으며 Project를 생성하면 열리는 page에서 Fault Tree 명세를 작성하고 위험도 계산을 수행할 수 있다.

② Fault Tree Symbol 생성 및 편집

Fault Tree Editor의 Palette에서 사전에 정의한 Symbol을 선택할 수 있다. 필요한 Symbol을 선택하여 Diagram에 추가하고 Connection을 연결한다. Diagram에 추가된 Symbol은 Label과 Probability를 보여준다. Property View에서 선택한 Symbol의 정보를 확인할 수 있으며 값을 수정할 수 있고 변경된 값은 Diagram과 Probability Viewer에 바로 반영되어 확인할 수 있다. 확률 값 입력은 가장 하위 노드에 존재하는 Event에만 입력할 수 있으며 나머지 Symbol은 계산된 확률 값을 보여주기만 한다.

③ 확률 계산

Editor의 Context Menu에서 항목을 선택하여 각 Symbol에서 편집한 Probability 값으로 확률을 계산한다. 최하위 사건에 주어진 확률을 이용해서 중간 단계의 Gate의 발생 확률을 계산한다. 반복적으로 하위 사건 노드들의 확률을 계산하며, 최상위 사건의 확률까지 계산하여 위험도를 계산할 수 있다.

④ XML 저장 및 파싱

확률 계산 수행 후 변경된 정보와 Diagram의 내용을 XML 문서로 저장할 수 있다. Eclipse Application을 시작하면 저장된 XML 문서를 읽어 들여 저장된 시점부터 편집이 가능하다.

⑤ 보고서 생성

Fault Tree Analysis Project를 생성하고 확률을 계산하는 과정을 통해 나온 결과를 html 형식의 보고서로 생성한다.

(다) 화면 설계

① 화면 구성

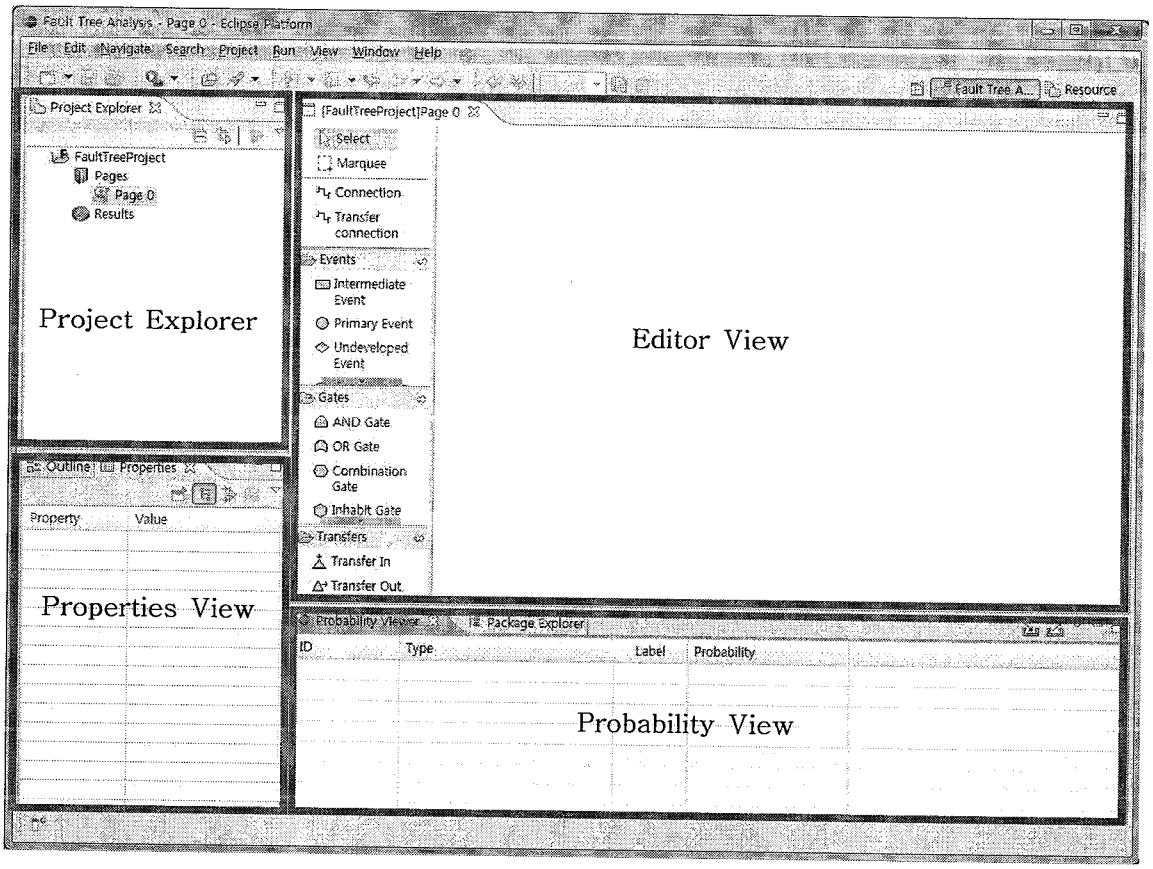


그림 3.3.29 FTA 화면 구성

Fault Tree Analyzer 모듈은 크게 Project Explorer, Properties View, Editor 4개의 View로 구성된 Perspective를 가진다. 각각의 View에서의 역할은 다음과 같다.

- Project Explorer : 본 모듈에서 작업 중인 프로젝트 정보를 보여주는 화면
- Properties View : Editor에서 작업 중인 항목의 자세한 properties를 제공하고 편집하기 위한 화면
- Probability Viewer : Editor에서 작업 중인 모든 항목을 보여주는 화면
- Editor View : 작업 내용을 Fault Tree Symbol을 이용해 Tree 형태의 그래프로 보여주는 화면

② 화면 구성 방식

Fault Tree Editor 모듈은 Java 언어로 작성된다. Eclipse RCP (RichClient Platform) 응용 프로그램으로 작성되며 Eclipse에서 사용하는 GEF(그래픽 라이브러리)를 사용하여 UI가 구성된다. 생성된 응용 프로그램은 OS에 종속적이지 않도록 설계하며, 기본으로 Microsoft Windows OS에 대해 결과를 확인한다.

③ 화면 설계

화면 구성에서 설명한 4개의 View에서 보여지는 각각의 화면에 대해 설계한다.

○ Project Explorer 화면 설계

본 모듈에서 정의한 프로젝트에 대한 개요를 보여주는 화면으로 트리 기반의 화면을 제공한다. Project를 최상위 노드로 하여 Pages와 Results라는 자식 노드를 갖는다. Pages 노드는 프로젝트에서 작업 중인 page들을 자식 노드로 갖는다. Pages 노드 아래 page를 생성하여 자식 노드를 추가할 수 있다. page들은 생성될 때 부여되는 번호를 이름으로 갖는다. page의 이름은 Rename dialog에서 변경할 수 있다.

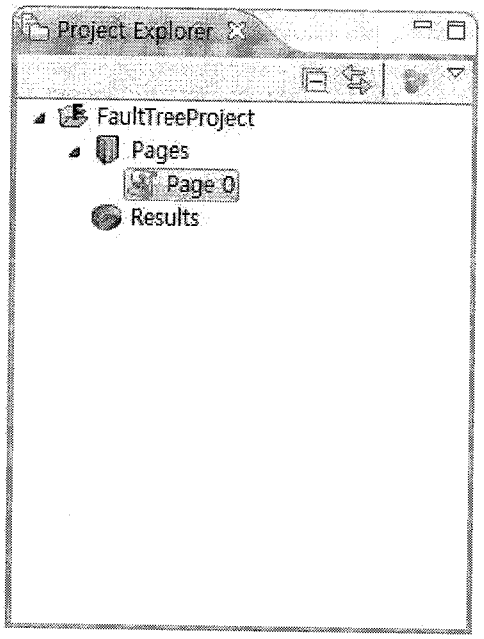


그림 3.3.30 Project Explorer 화면

○ Properties View 화면 설계

Properties View는 Eclipse에서 제공하는 UI component로 선택된 항목에 대해 정의된 property를 보여준다. Editor에서 작업 중인 Symbol을 선택할 경우 선택한 Symbol의 ID, Label, Probability, Location, Description을 보여주며 Label, Probability, Description의 편집이 가능하다.

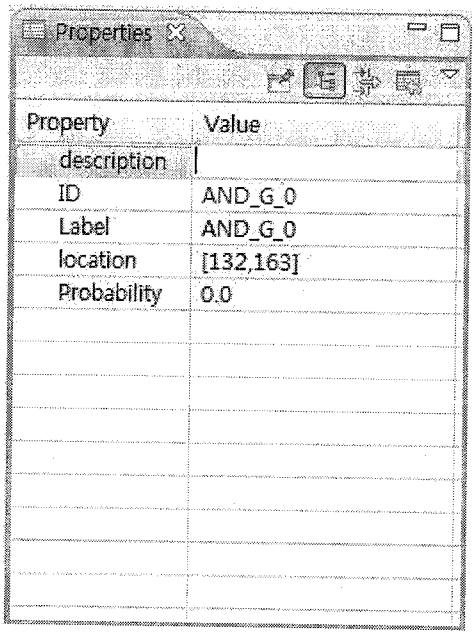


그림 3.3.31 Properties View 화면

○ Probability Viewer 화면 설계

Editor에서 작업 중인 모든 Symbol의 목록을 보여준다. Diagram에 Symbol을 추가할 때마다 Probability Viewer에도 등록되며 각 Symbol의 ID, Type, Label, Probability를 볼 수 있다.

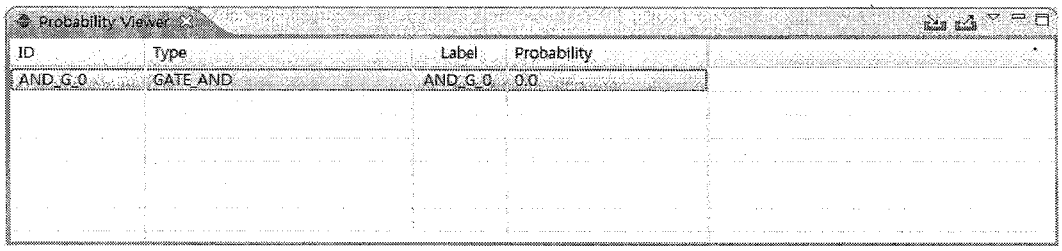


그림 3.3.32 Probability Viewer 화면

○ Editor View 화면 설계

작업 중인 page들을 보여주며 작업을 하는 공간이다. Editor View는 Palette와 Diagram 두 개로 구성된다.

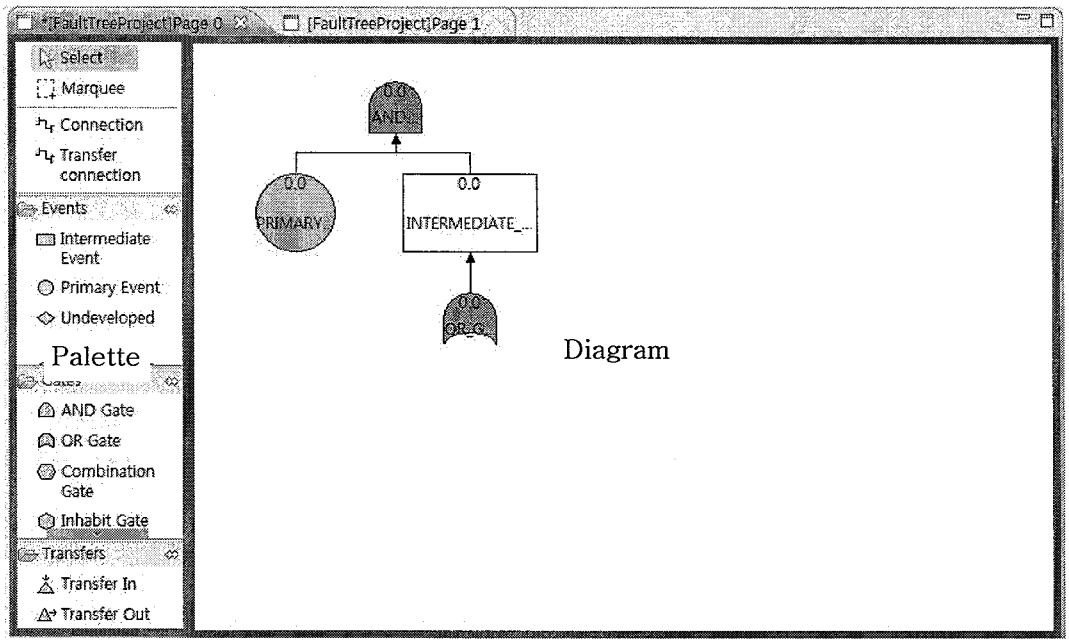


그림 3.3.33 Editor View

- Palette : Fault Tree 작성에 필요한 도구를 제공한다. Diagram에 그릴 Symbol을 추가하거나 Connection을 추가할 수 있다.
- Diagram : Fault Tree 작성에 필요한 Symbol을 그리고 작업 내용을 볼 수 있다. Fault Tree Diagram을 작성하기 위한 캔버스이다.

(라) 기능 설계

Fault Tree Analyzer는 Fault Tree 명세를 작성하여 분석을 위한 입력을 제공하는 FTEditor 와 확률 기반의 분석을 수행하는 FTEngine로 구성된다. FTEditor는 작성된 Fault Tree 명세의 저장, 로드 등의 관리적인 기능을 제공하며, 작성된 명세는 FTStructure로 변환되어 저장되거나 확률 계산을 위해 FTEngine으로 전달된다.

FTEngine은 Editor로부터 전달받은 확률 값을 통해 분석 결과를 도출한다. 분석에 따른 결과는 Report Generator를 통해 보고서 형태로 작성되며, 사용자에게 전달된다. 각각에 대한 상세 설계 사항은 다음과 같다.

① FTEditor

FTEditor는 Fault Tree 명세를 작성하여 분석을 위한 입력 기능을 제공한다.

○ FTA package

본 package는 Fault Tee Diagram을 XML 문서로 저장/로딩하는 기능을 수행한다.

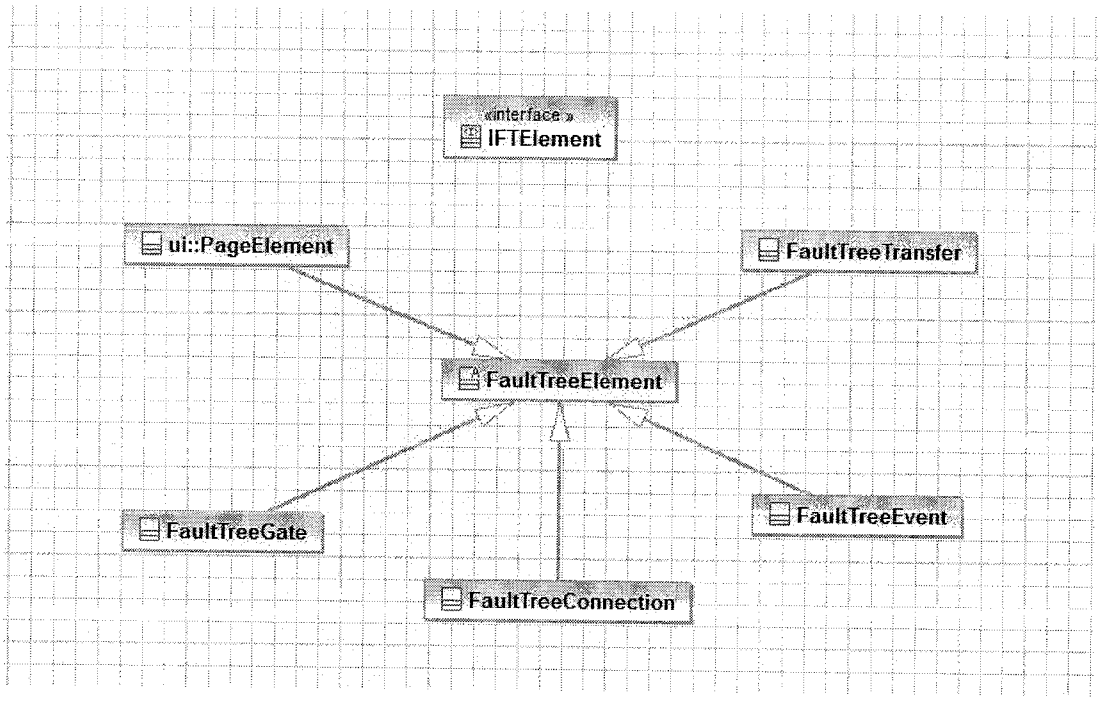


그림 3.3.34 FTA package class diagram

- FaultTreeElement class

표 3.3.11 FaultTreeElement Class 설계 사항

Identification	M1.1.1
Type	FT XML Class
Purpose	Fault Tree Diagram을 XML로 기록하고 파싱하기 위한 클래스
Function	Diagram에 추가된 Shape들의 정보를 XML 형태로 기록하고 XML 문서에서 노드를 읽어 FaultTreeElement 객체로 반환한다.
Subordinates	FautlTreeConnection,
Dependencies	FautlTreeConnection, FaultTreeEvent, FaultTreeGate, PageElement
Resources	N/A
Data	N/A

- FaultTreeEvent class

표 3.3.12 FaultTreeEvent Class 설계 사항

Identification	M1.1.2
Type	FT XML Class
Purpose	Event Symbol 객체를 XML로 기록하고 파싱하기 위한 클래스
Function	Event를 XML형태로 기록하기 위해 Event Shape 객체를 생성할 때 FaultTreeEvent 객체를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FaultTreeGate class

표 3.3.13 FaultTreeGate Class 설계 사항

Identification	M1.1.3
Type	FT XML Class
Purpose	Gate Symbol 객체를 XML로 기록하고 파싱하기 위한 클래스
Function	Gate를 XML형태로 기록하기 위해 Gate Shape 객체를 생성할 때 FaultTreeGate 객체를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FaultTreeTransfer class

표 3.3.14 FaultTreeTransfer Class 설계 사항

Identification	M1.1.4
Type	FT XML Class
Purpose	Transfer Symbol 객체를 XML로 기록하고 파싱하기 위한 클래스
Function	Transfer를 XML형태로 기록하기 위해 Transfer Shape 객체를 생성할 때 FaultTreeTransfer 객체를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FaultTreeConnection class

표 3.3.15 FaultTreeConnection Class 설계 사항

Identification	M1.1.5
Type	FT XML Class
Purpose	Symbol에 연결된 하위 Symbol 객체를 XML로 기록하고 파싱하기 위한 클래스
Function	Symbol의 Source Connection에 연결된 Symbol을 XML 형태로 기록하고 XML 문서에서 Connection 노드를 읽어 FaultTreeConnection 객체를 반환한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui package

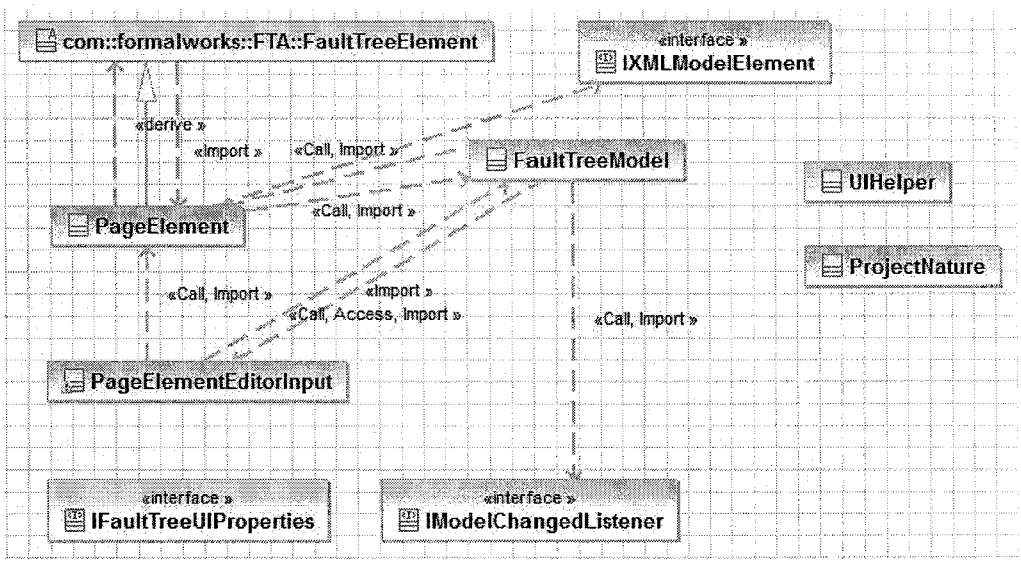


그림 3.3.35 UI package class diagram

- FaultTreeModel class

표 3.3.16 FaultTreeModel Class 설계 사항

Identification	M1.2.1
Type	FT UI Class
Purpose	Fault Tree Project와 관련한 파일을 관리하는 클래스
Function	파일 저장 및 로딩 기능을 수행하며 그에 맞는 적절한 model과 page를 반환한다.
Subordinates	PageElement
Dependencies	N/A
Resources	N/A
Data	N/A

- PageElement class

표 3.3.17 PageElement Class 설계 사항

Identification	M1.2.2
Type	FT UI Class
Purpose	page를 XML로 기록하기 위한 클래스
Function	XML 문서에서 page를 읽어들이고 page를 XML로 기록한다.
Subordinates	FaultTreeModel, ITFElement
Dependencies	N/A
Resources	N/A
Data	N/A

- PageElementEditorInput class

표 3.3.18 PageElementEditorInput Class 설계 사항

Identification	M1.2.3
Type	FT UI Class
Purpose	Fault Tree Project의 page를 관리하는 클래스
Function	page의 number와 label을 설정하고 반환한다.
Subordinates	FaultTreeModel, PageElement
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.actions package

본 Package는 모듈에서 필요한 Action을 정의하고 수행한다.

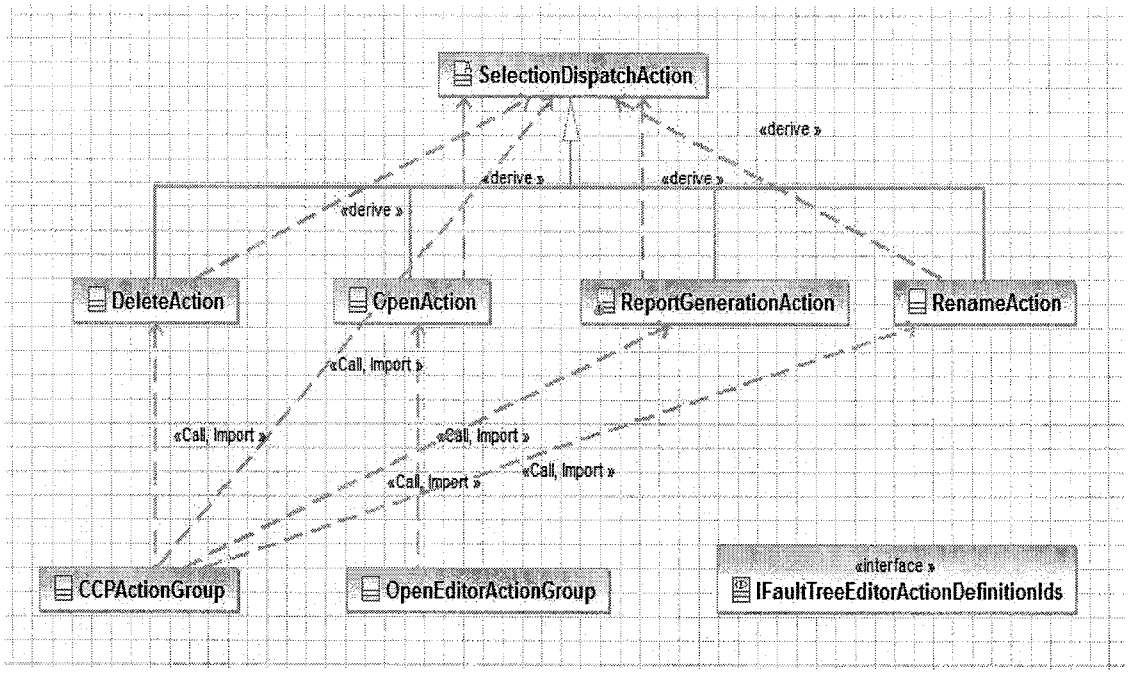


그림 3.3.36 action package class diagram

- CCPActionGroup class

표 3.3.19 CCPActionGroup Class 설계 사항

Identification	M1.3.1
Type	Action Class
Purpose	action을 정의한 클래스
Function	Editor에서 사용할 action들을 context menu에 추가한다.
Subordinates	SelectionDispatchAction
Dependencies	N/A
Resources	N/A
Data	N/A

- SelectionDispatchAction class

표 3.3.20 SelectionDispatchAction Class 설계 사항

Identification	M1.3.2
Type	Action Class
Purpose	action을 생성하는 클래스
Function	action을 생성한다.
Subordinates	N/A
Dependencies	DeleteAction, OpenAction, RenameAction, ReportGenerationAction
Resources	N/A
Data	N/A

- DeleteAction class

표 3.3.21 DeleteAction Class 설계 사항

Identification	M1.3.3
Type	Action Class
Purpose	삭제 기능을 정의한 클래스
Function	page 또는 project를 삭제하는 기능을 정의한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- OpenAction class

표 3.3.22 OpenAction Class 설계 사항

Identification	M1.3.4
Type	Action Class
Purpose	page를 여는 기능을 수행하는 클래스
Function	Fault Tree Editor를 open한다.
Subordinates	FaultTreeUIEditor
Dependencies	N/A
Resources	N/A
Data	N/A

- OpenEditorActionGroup class

표 3.3.23 OpenEditorActionGroup Class 설계 사항

Identification	M1.3.5
Type	Action Class
Purpose	open action을 정의한 클래스
Function	Editor를 open하는 action을 context menu에 추가한다.
Subordinates	OpenAction
Dependencies	N/A
Resources	N/A
Data	N/A

- RenameAction class

표 3.3.24 RenameAction Class 설계 사항

Identification	M1.3.6
Type	Action Class
Purpose	rename 기능을 정의한 클래스
Function	page의 이름을 변경하기 위한 dialog를 열고 변경된 값을 설정한다.
Subordinates	PageElement
Dependencies	N/A
Resources	N/A
Data	N/A

- ReportGenerationAction class

표 3.3.25 ReportGenerationAction Class 설계 사항

Identification	M1.3.7
Type	Action Class
Purpose	오류 보고서 생성을 위한 action을 정의한 클래스
Function	오류 보고서 생성을 위한 dialog를 열고 오류 보고서 작성을 위한 diagram 이미지를 반환한다.
Subordinates	PageElement
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.dialog package

본 Package는 모듈에서 사용하는 Dialog를 생성하는 기능을 수행한다.

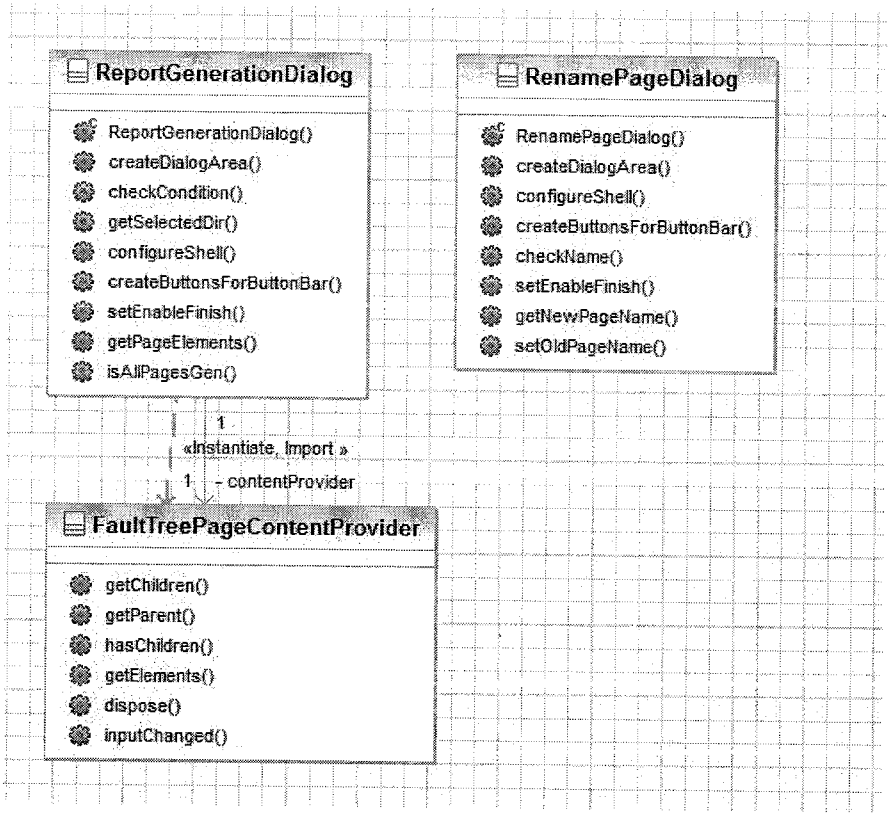


그림 3.3.37 dialog package class diagram

- FaultTreePageContentProvider class

표 3.3.26 FaultTreePageContentProvider Class 설계 사항

Identification	M1.4.1
Type	Dialog Class
Purpose	page 관련 dialog 클래스
Function	page를 생성하기 위한 dialog를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- RenamePageDialog class

표 3.3.27 RenamePageDialog Class 설계 사항

Identification	M1.4.2
Type	Dialog Class
Purpose	page 관련 dialog 클래스
Function	page이름을 변경하기 위한 dialog를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- ReportGenerationDialog class

표 3.3.28 ReortGeneration Class 설계 사항

Identification	M1.4.3
Type	Dialog Class
Purpose	report 생성 dialog 클래스
Function	오류 분석 보고서를 생성하기 위한 dialog를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.editor package

본 Package는 FTA Editor를 생성하고 필요한 기능을 정의한다.

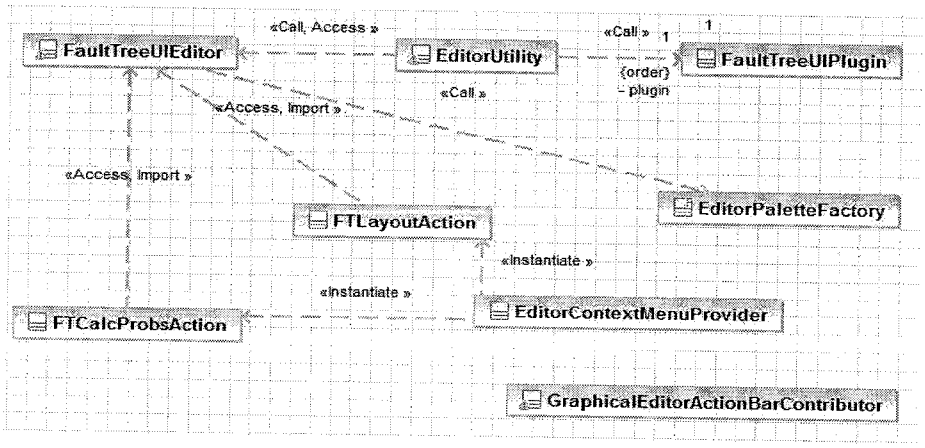


그림 3.3.38 editor package class diagram

- EditorContextMenuProvider class

표 3.3.29 EditorContextMenuProvider Class 설계 사항

Identification	M1.5.1
Type	Editor Class
Purpose	context menu를 관리하는 클래스
Function	Fault Tree Editor의 context menu를 정의하고 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- EditorPaletteFactory class

표 3.3.30 EditorPaletteFactory Class 설계 사항

Identification	M1.5.2
Type	Editor Class
Purpose	Palette menu를 관리하는 클래스
Function	Fault Tree Editor의 Palette를 생성하고 구성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- EditorUtility class

표 3.3.31 EditorUtility Class 설계 사항

Identification	M1.5.3
Type	Editor Class
Purpose	Fault Tree Utility 클래스
Function	Editor를 open한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FaultTreeUIEditor class

표 3.3.32 FaultTreeUIEditor Class 설계 사항

Identification	M1.5.4
Type	Editor Class
Purpose	Fault Tree UI를 관리하는 클래스
Function	UI를 구성하고 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FultTreeUIPlugin class

표 3.3.33 FaultTreeUIPlugin Class 설계 사항

Identification	M1.5.5
Type	Editor Class
Purpose	Plug-in을 관리하는 클래스
Function	plug-in을 시작하고 종료한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FTCalcProbsAction

표 3.3.34 FTCalcProbsAction Class 설계 사항

Identification	M1.5.6
Type	Editor Class
Purpose	Calc Probability action을 실행하는 클래스
Function	Editor의 context menu에서 Calc Probability를 선택했을 때 action을 수행한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- FTLayoutAction

표 3.3.35 FTLayoutAction Class 설계 사항

Identification	M1.5.7
Type	Editor Class
Purpose	layout action을 실행하는 클래스
Function	Editor의 context menu에서 Layout을 선택했을 때 action을 수행한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- GraphicalEditorActionBarContributor class

표 3.3.36 GraphicalEditorActionBarcontributor Class 설계 사항

Identification	M1.5.8
Type	Editor Class
Purpose	toolbar를 관리하는 클래스
Function	toolbar에 action을 추가한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.editor.model package

본 package는 Fault Tree Diagram을 작성하고 관리하는 기능을 수행한다.

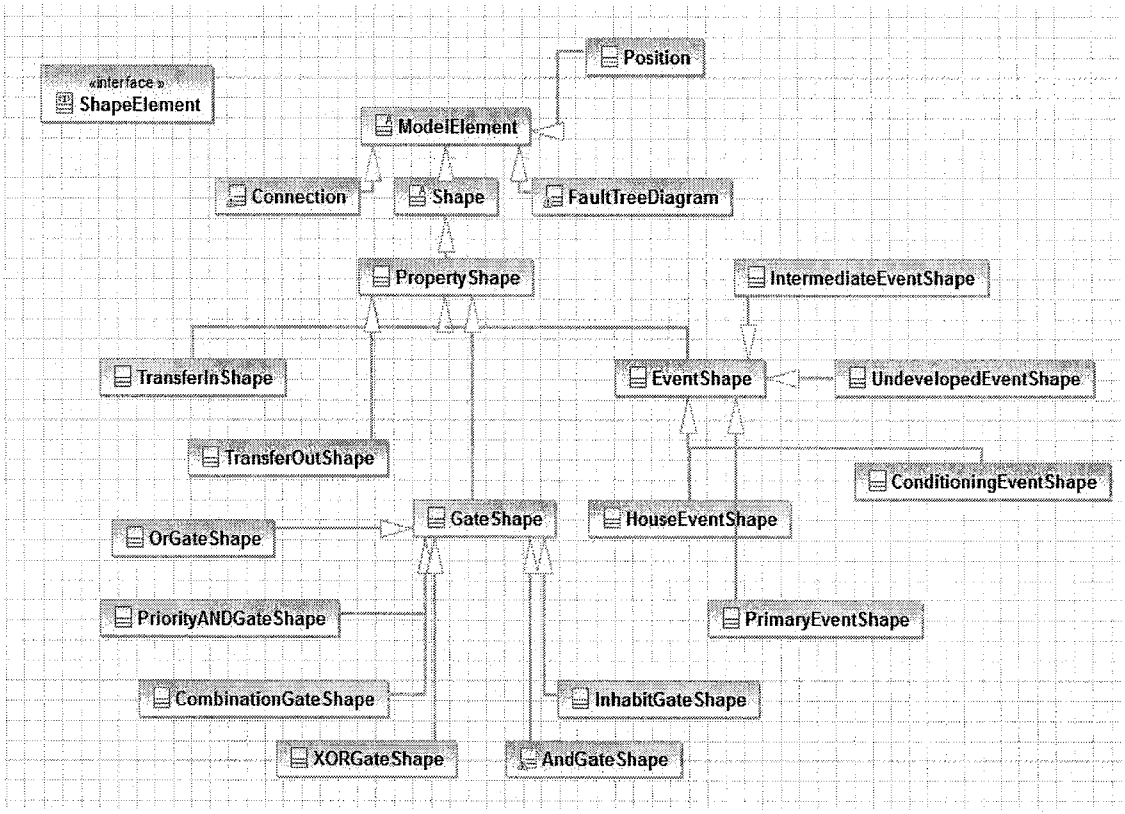


그림 3.3.39 model package class diagram

- ModelElement class

표 3.3.37 ModelElement class 설계 사항

Identification	M1.6.1
Type	Model class
Purpose	Fault Tree Diagram을 작성하기 위한 모든 Model의 최상위 클래스. Model이 변경될 때마다 변경 사항을 갱신하기 위한 리스너를 관리한다.
Function	리스너를 등록하여 변경 사항을 해당 리스너에게 알리고 프로그램이 종료될 때 리스너를 제거한다.
Subordinates	N/A
Dependencies	Shape, Connection, FaultTreeDiagram, Position
Resources	N/A
Data	N/A

- Shape class

표 3.3.38 Shape class 설계 사항

Identification	M1.6.2
Type	Model class
Purpose	Fault Tree diagram에 그려지는 Symbol을 관리하기 위한 클래스.
Function	Symbol에 값을 설정하고 반환한다.
Subordinates	N/A
Dependencies	PropertyShape
Resources	N/A
Data	Symbol의 위치, 크기, ID, Label, Description, Connection, Probability

- Connection class

표 3.3.39 connection class 설계 사항

Identification	M1.6.3
Type	Model class
Purpose	Symbol을 연결하는 Connection을 관리하는 클래스
Function	Symbol에 값을 설정하고 반환한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	Connection의 style , source/target Shape

- FaultTreeDiagram class

표 3.3.40 FaultTreeDiagram class 설계 사항

Identification	M1.6.4
Type	Model class
Purpose	Fault Tree diagram을 생성하는 클래스
Function	Diagram에 Shape을 추가하고 추가하는 Shape에 ID를 부여한다. 저장된 문서를 읽어 생성된 IFTElement 객체를 Diagram에 그려준다.
Subordinates	Shape, IFTElement
Dependencies	N/A
Resources	N/A
Data	N/A

- Position class

표 3.3.41 Position class 설계 사항

Identification	M1.6.5
Type	Model class
Purpose	Shape의 Position을 관리하는 클래스
Function	Shape의 position을 반환한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

- PropertyShape class

표 3.3.42 PropertyShape class 설계 사항

Identification	M1.6.6
Type	Model class
Purpose	Property View를 관리하는 클래스
Function	선택한 Shape의 정보를 가져와 Property View에 보여주고 편집한 값을 Shape에 설정한다.
Subordinates	Shape
Dependencies	EventShape, GateShape, TransferInShape, TransferOutShape
Resources	N/A
Data	N/A

- EventShape class

표 3.3.43 EventShape class 설계 사항

Identification	M1.6.7
Type	Model class
Purpose	Event Symbol 을 관리하는 클래스
Function	Event Symbol의 IFTElment Type을 반환한다.
Subordinates	IFTElement
Dependencies	IntermediateEvnetShape, PrimaryEventShape, HouseEventShape, ConditioningEventShape, UndevelopsedEvnetShape
Resources	N/A
Data	N/A

- GateShape class

표 3.3.44 GateShape class 설계 사항

Identification	M1.6.8
Type	Model class
Purpose	Gate Symbol을 관리하는 클래스
Function	Gate 확률 계산을 위한 AND 연산과 OR 연산을 정의하여 결과를 반환한다.
Subordinates	IFTElement
Dependencies	AndGateShape, OrGateShape, XORGateShape, InhabitGateShape, PriorityAndGateShape, CombinationGateShape
Resources	N/A
Data	N/A

- AndGatShape class

표 3.3.45 AndGateShape class 설계 사항

Identification	M1.6.9
Type	Model class
Purpose	AND Gate 를 생성하기 위한 클래스
Function	AND Gate 객체를 만들고 값을 설정한다.
Subordinates	FaultTreeGate, Shape
Dependencies	N/A
Resources	N/A
Data	N/A

나머지 GateShape을 상속 받는 클래스는 AndGateShape 클래스와 동일하므로 생략한다.

- PrimaryEvent class

표 3.3.46 PrimaryEvent class 설계 사항

Identification	M1.6.10
Type	Model class
Purpose	Primary Event를 생성하기 위한 클래스
Function	Primary Event 객체를 만들고 값을 설정한다.
Subordinates	FaultTreeEvent
Dependencies	N/A
Resources	N/A
Data	N/A

나머지 EventShape을 상속 받는 클래스는 PrimaryEvnetShape 클래스와 동일하므로 생략한다.

- TransferInShape class

표 3.3.47 TransferInshape class 설계 사항

Identification	M1.6.11
Type	Model class
Purpose	Transfer In Symbol을 관리하기 위한 클래스
Function	Transfer In Symbol객체를 생성하고 값을 설정한다.
Subordinates	FaultTreeTransfer, IFTElement
Dependencies	N/A
Resources	N/A
Data	N/A

Transfer OUT 객체를 생성하는 클래스는 TransferInShape 클래스와 동일하므로 생략한다.

○ FTA.ui.editor.editpart package

본 Package는 Figure 및 Model을 관리하는 기능을 수행한다.

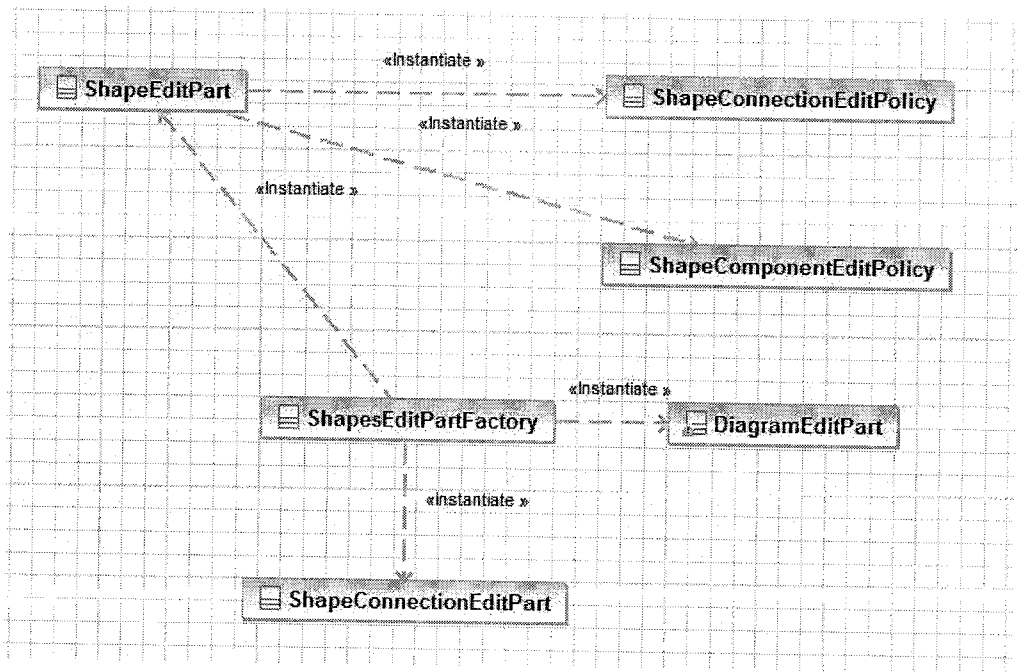


그림 3.3.40 editpart package class diagram

- ShapeEditPart class

표 3.3.48 ShapeEditPart class 설계 사항

Identification	M1.7.1
Type	Control class
Purpose	Shape과 Connection을 diagram에 그려주기 위한 클래스
Function	Palette에서 선택한 model에 해당하는 figure를 반환하고 Connection이 연결되는 anchor의 위치를 반환한다.
Subordinates	Shape, FaultTreeFigure
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeEditParFactory class

표 3.3.49 ShapeEditPartFactory class 설계 사항

Identification	M1.7.2
Type	Control class
Purpose	EditPart를 생성한다.
Function	model에 해당하는 EditPart를 생성하여 반환한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- DiagramEditPart class

표 3.3.50 DiagramEditPart class 설계 사항

Identification	M1.7.3
Type	Control class
Purpose	Fault Tree Diagram의 상태를 관리한다.
Function	Diagram에 Symbol이 추가되거나 삭제되었을 때 상태를 갱신하기 위한 리스너를 등록하거나 삭제한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeComponentEditPolicy class

표 3.3.51 ShapeComponentEditPolicy class 설계 사항

Identification	M1.7.4
Type	Control class
Purpose	Fault Tree Diagram에서 Shpae의 상태를 관리한다.
Function	Diagram에서 Symbol이 삭제되었을 때 삭제를 알린다.
Subordinates	ShpaeDeleteCommand
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeConnectionEditPart class

표 3.3.52 ShapeConnectionEditPart class 설계 사항

Identification	M1.7.5
Type	Control class
Purpose	Fault Tree Diagram에서 Connection의 상태를 관리한다.
Function	Diagram에 Connection이 추가되거나 삭제될 때 상태를 갱신하기 위한 리스너를 관리하고 Connection의 모양을 정의한다.
Subordinates	Connection
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeConnectionEditPolicy class

표 3.3.53 ShapeConnectionEditPolicy class 설계 사항

Identification	M1.7.6
Type	Control class
Purpose	Fault Tree Diagram에서 Connection의 제약 사항을 정의한다.
Function	Connection을 연결 할 때 연결될 수 있는지 여부를 반환한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.editor.command package

본 package는 EditPart에서 전달 받은 Diagram의 상태 변경 정보를 model에 설정하는 기능을 수행한다.

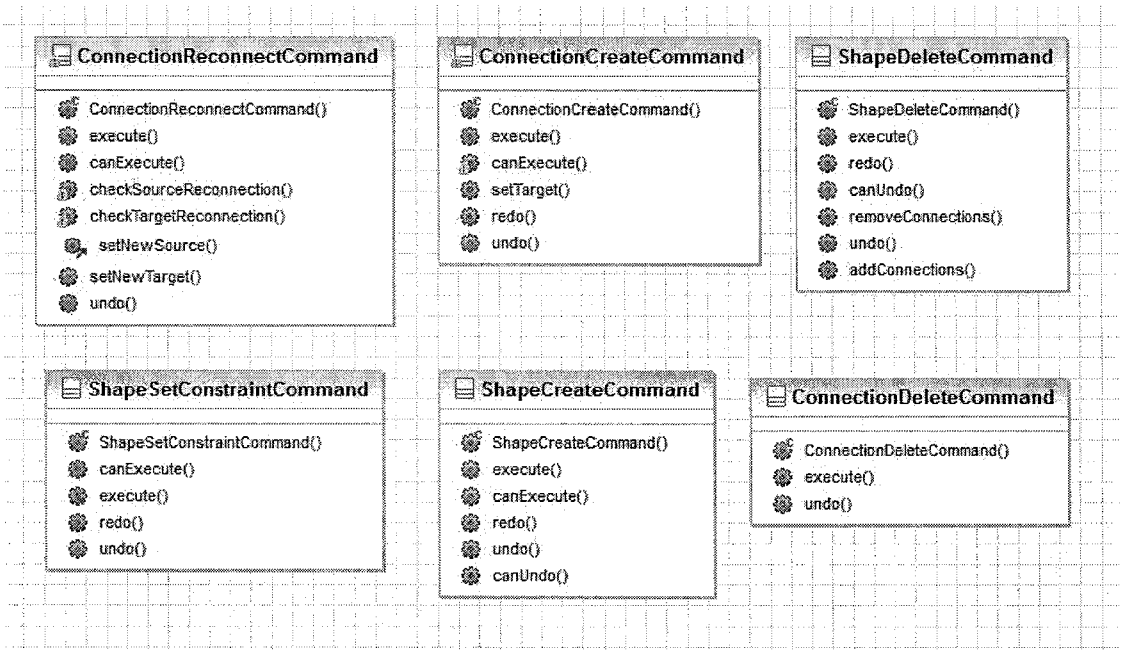


그림 3.3.41 command package class diagram

- ShapeCreatCommand class

표 3.3.54 ShapeCreateCommand class 설계 사항

Identification	M1.8.1
Type	Command class
Purpose	Diagram에 추가되는 Shape의 상태를 설정한다.
Function	Diagram에 추가되는 Shape의 위치, 크기를 설정한다.
Subordinates	Shape, FaultTreeDiagram
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeDeletecommand class

표 3.3.55 ShapeDeleteCommand class 설계 사항

Identification	M1.8.2
Type	Command class
Purpose	Diagram에서 삭제되는 Shape의 상태를 설정한다.
Function	Shape을 삭제할 때 Diagram에서 제거하고 연결된 Connection을 제거한다.
Subordinates	Shape, FaultTreeDiagram
Dependencies	N/A
Resources	N/A
Data	N/A

- ShapeSetConstraintCommand class

표 3.3.56 ShapeSetConstraintCommand class 설계 사항

Identification	M1.8.3
Type	Command class
Purpose	Diagram에서 변경되는 Shape의 상태를 설정한다.
Function	Shape의 위치가 변경될 때 새롭게 변경된 값을 설정한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

- ConnectionCreateCommand class

표 3.3.57 ConnectionCreateCommand class 설계 사항

Identification	M1.8.4
Type	Command class
Purpose	Connection이 연결될 때 Connection의 상태를 설정한다.
Function	Connection이 연결되는 Shape을 저장한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

- ConnectionDeleteCommand class

표 3.3.58 ConnectionDeleteCommand class 설계 사항

Identification	M1.8.5
Type	Command class
Purpose	Connection이 삭제될 때 Connection의 상태를 설정한다.
Function	삭제되는 Connection에 연결되어 있던 Shape을 삭제한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

- ConnectionReconnectCommand class

표 3.3.59 ConnectionReconnectCommand class 설계 사항

Identification	M1.8.6
Type	Command class
Purpose	Connection이 재연결될 때 Connection의 상태를 설정한다.
Function	Connection을 재연결하면서 변경되는 Shape의 정보를 설정한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.editor.figure package

본 Package는 Model을 Diagram에 그리기 위한 기능을 수행한다.

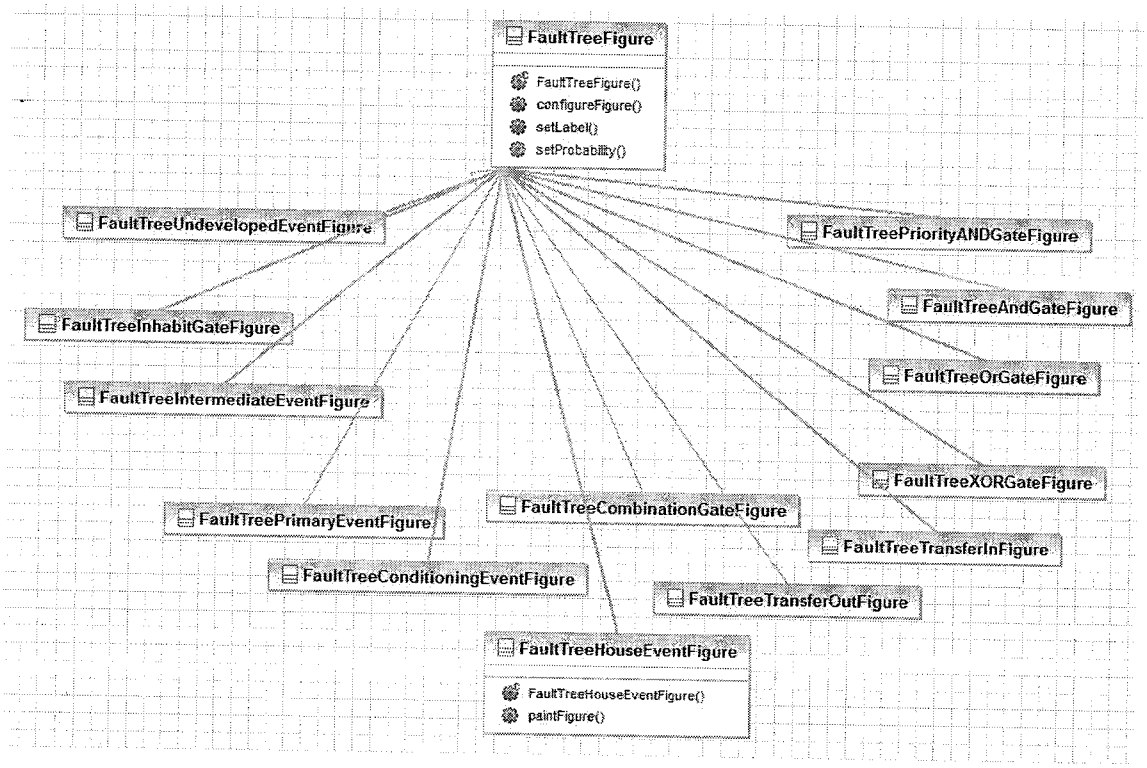


그림 3.3.42 figure package class diagram

- FaultTreeFigure class

표 3.3.60 FaultTreeFigure class 설계 사항

Identification	M1.9.1
Type	Figure class
Purpose	Diagram에 그리기 위한 figure를 관리한다.
Function	Diagram에 그려질 figure에 보여줄 label와 probability를 설정하여 FaultTreeFigure 객체를 생성한다.
Subordinates	N/A
Dependencies	FaultTreeAndGateFigure 외 동일 package의 12 개 클래스
Resources	N/A
Data	N/A

- FaultTreeAndGateFigure class

표 3.3.61 FaultTreeAndGateFigure class 설계 사항

Identification	M1.9.2
Type	Figure class
Purpose	AND Gate Symbol의 모양을 정의한다.
Function	AND Gate Symbol을 그린다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

나머지 FaultTreeFigure를 상속 받아 Symbol을 그리는 Figure class는 위와 동일하므로 생략한다.

○ FTA.ui.perspective package

본 Package는 FTA의 Perspective를 생성하는 기능을 수행한다.

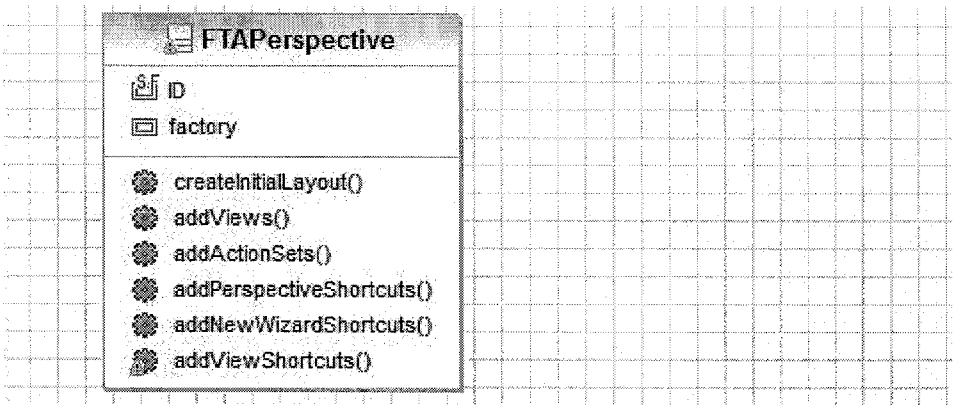


그림 3.3.43 perspective package class diagram

- FTAPerspective class

표 3.3.62 FTAPerspective class 설계 사항

Identification	M1.10.1
Type	Perspective class
Purpose	perspective를 생성한다.
Function	FTA에 필요한 Project Explorer, Outline View 등의 perspective를 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

○ FTA.ui.views package

본 Package는 Probability Viewer와 관련된 기능을 수행한다.

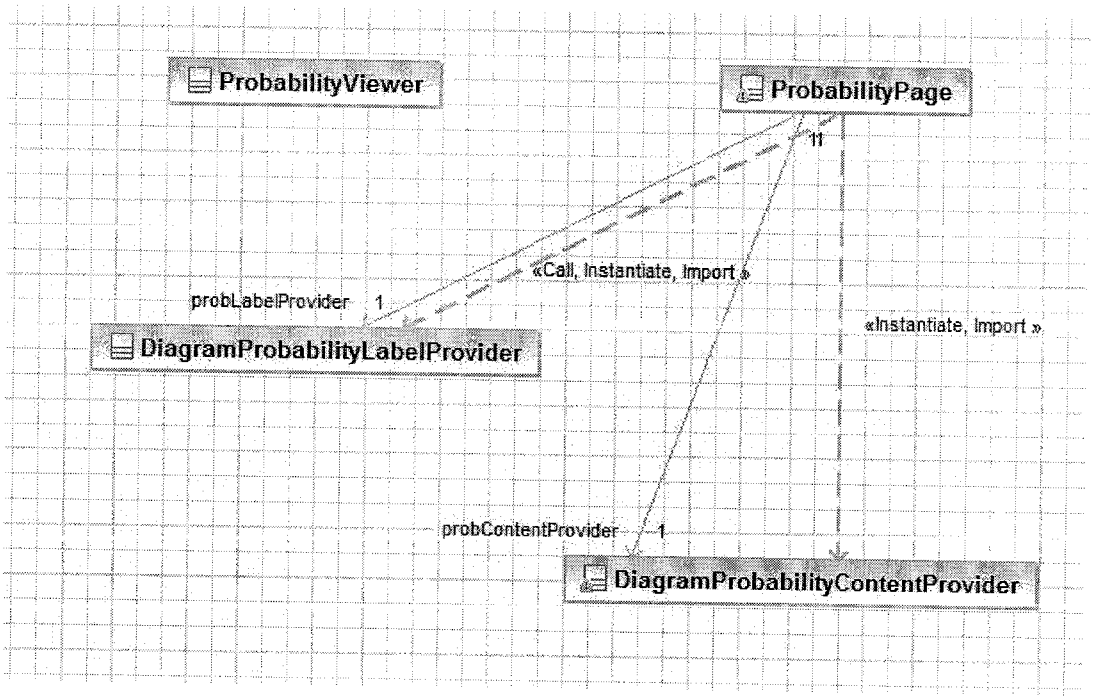


그림 3.3.44 views package class diagram

- DiagramProbabilityContentProvider class

표 3.3.63 DiagramProbabilityContectProvider class 설계 사항

Identification	M1.11.1
Type	Probability View class
Purpose	Diagram이 변경됐을 때 Proabability Viewer를 갱신하기 위한 클래스
Function	Diagram에 추가된 model을 Viewer에 보여준다.
Subordinates	FalutlTreeDiagram
Dependencies	N/A
Resources	N/A
Data	N/A

- DiagramProbabilityLabelProvider class

표 3.3.64 DiagramProbabilityLabelProvider class 설계 사항

Identification	M1.11.2
Type	Probability View class
Purpose	Probability Viewer에 값을 보여준다.
Function	Viewer의 항목에 적절한 값을 설정한다.
Subordinates	Shape
Dependencies	N/A
Resources	N/A
Data	N/A

- ProbabilityPage class

표 3.3.65 ProbabilityPage class 설계 사항

Identification	M1.11.3
Type	Probability View class
Purpose	FaultTreeUIEditor와 1:1 연결된 PageBookView에서 보여주는 UI 클래스
Function	Viewer Table을 생성한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

② FTEngine

FTEngine은 확률 기반의 분석을 수행한다.

○ FTA.utils.html package

본 Package는 HTML 오류 분석 보고서를 생성하는 기능을 수행한다.

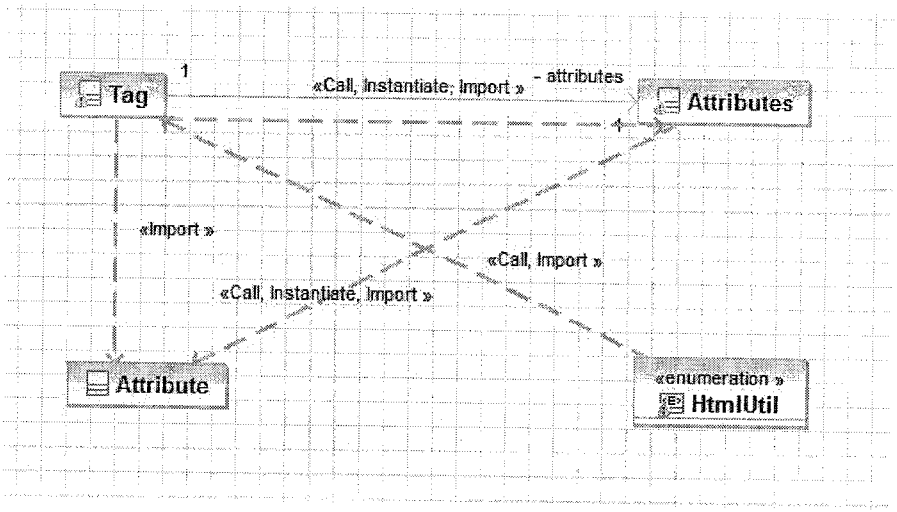


그림 3.3.45 html package class diagram

- Attribute class

표 3.3.66 Attribute class 설계 사항

Identification	M2.1.1
Type	Report Generate class
Purpose	attribute를 관리하기 위한 클래스
Function	보고서 생성에 사용하는 attribute의 값을 설정하거나 반환한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- Attributes class

표 3.3.67 Attributes class 설계 사항

Identification	M2.1.2
Type	Report Generate class
Purpose	html attribute에 값을 설정하기 위한 클래스
Function	보고서를 작성하기 위해 html tag의 attribute에 알맞은 값을 설정한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- HtmlUtil calss

표 3.3.68 HtmlUtil class 설계 사항

Identification	M2.1.3
Type	Report Generate class
Purpose	Fault Tree Project에서 보고서를 생성하는 클래스
Function	보고서를 생성하기 위한 String을 반환한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

- Tag class

표 3.3.69 Tag class 설계 사항

Identification	M2.1.4
Type	Report Generate class
Purpose	html tag를 작성하기 위한 클래스
Function	html 문서를 생성하기 위한 tag를 반환한다.
Subordinates	N/A
Dependencies	N/A
Resources	N/A
Data	N/A

(마) 인터페이스 설계

Fault Tree Analyzer는 Fault Tree 명세를 작성하여 분석 결과를 보고서 형태로 사용자에게 전달한다. 작성된 명세는 FTStructure로 변환되어 저장된다.

① FTStructure

FTStructure는 XML 형식으로 생성되며 XML은 다음과 같은 형식으로 제공된다.

○ Project Element

하나의 Project를 관리하며 Diagram Page를 생성 및 관리한다.

표 3.3.70 Project Element

목적	프로젝트의 기본 설명을 저장한다.
속성	이름(name). 설명(description), 프로젝트 생성 날짜(createDate), 작성자(author)
자식노드	1개 이상의 Page

○ Page Element

Diagram을 출력하는 하나의 Page를 나타낸다. 각 Page에는 사건(Event)들과 이들의 연관 관계를 나타내는 Gate들이 이미지 형태로 표현된다.

표 3.3.71 Page Element

목적	출력 화면의 기본 단위인 Page의 정보를 저장한다.
속성	ID(ID). 페이지 이름(LABEL)
자식노드	Gate/Event/Transfer 노드

○ Gate Element

사건(Event)들을 연결 시켜 확률을 계산하는 기능을 가진 Gate를 나타낸다. Gate는 AND Gate, Priority AND Gate, OR Gate, XOR Gate, Combination Gate, Inhabit Gate의 6종류가 있다.

표 3.3.72 Gate Element

목적	출력 화면의 기본 단위인 Page의 정보를 저장한다.
속성	ID(ID). Gate 종류(TYPE), Gate 이름(LABEL), 확률 값 (PROBABILITY), X좌표(X), Y좌표(Y), Gate 설명(DESCRIPTION), 번호(NUMBER)
자식노드	Connection 노드

○ Event Element

하나의 사건(Event)을 나타내며 각각은 사건에 대한 확률 값을 가진다. 사건은 Intermediate Event, Primary Event, Undeveloped Event, Conditioning Event, House Event 로 5종류가 있다.

표 3.3.73 Event Element

목적	Gate의 정보를 저장한다.
속성	ID(ID). Event 종류(TYPE), Event 이름(LABEL), 확률 값 (PROBABILITY), X좌표(X), Y좌표(Y), Event 설명 (DESCRIPTION),
자식노드	Connection 노드

○ Transfer Element

현재 Page에 있는 Event나 Gate를 다른 Page에서 링크로 사용할 수 있도록 해준다. 링크로 연결된 Event나 Gate의 ID를 가진다. Transfer는 Transfer IN과 Transfer OUT 두 종류가 있다.

표 3.3.74 Transfer Element

목적	Event의 정보를 저장한다.
속성	ID(ID). Transfer 종류(TYPE), Transfer 이름(LABEL), 확률 값 (PROBABILITY), X좌표(X), Y좌표(Y), Transfer 설명 (DESCRIPTION),
자식노드	Connection 노드

○ Connection Element

Gate, Event, Transfer Element의 하위에 연결된 Symbol을 나타낸다. 일반적으로 Connection으로 연결되는 하위 Symbol은 OUT이라는 type을 갖지만 Inhabit Gate에 연결되는 Conditioning Event는 CONDITION이라는 type으로 구분한다.

표 3.3.75 Connection Element

목적	Transfer의 정보를 저장한다.
속성	Connection 종류(TYPE), X좌표(X), Y좌표(Y), 상위 Symbol ID(TARGETID), 상위 Symbol의 종류(TARGETTYPE)
자식노드	없음

○ FTStructure 입력 예제

다음 표와 같이 Fault Tree Diagram이 구성되어 있을 때 FTStructure Code는 다음과 같다.

표 3.3.76 Fault Tree Diagram 구성 예

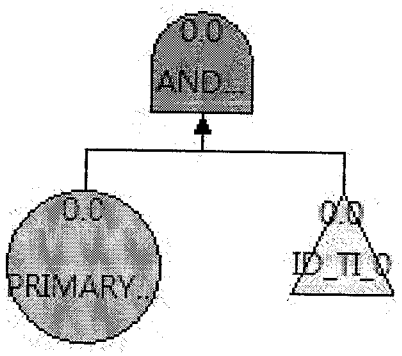
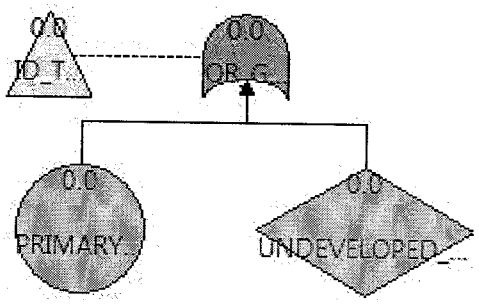
page 0	page 1
	

표 3.3.77 FTStructure Code

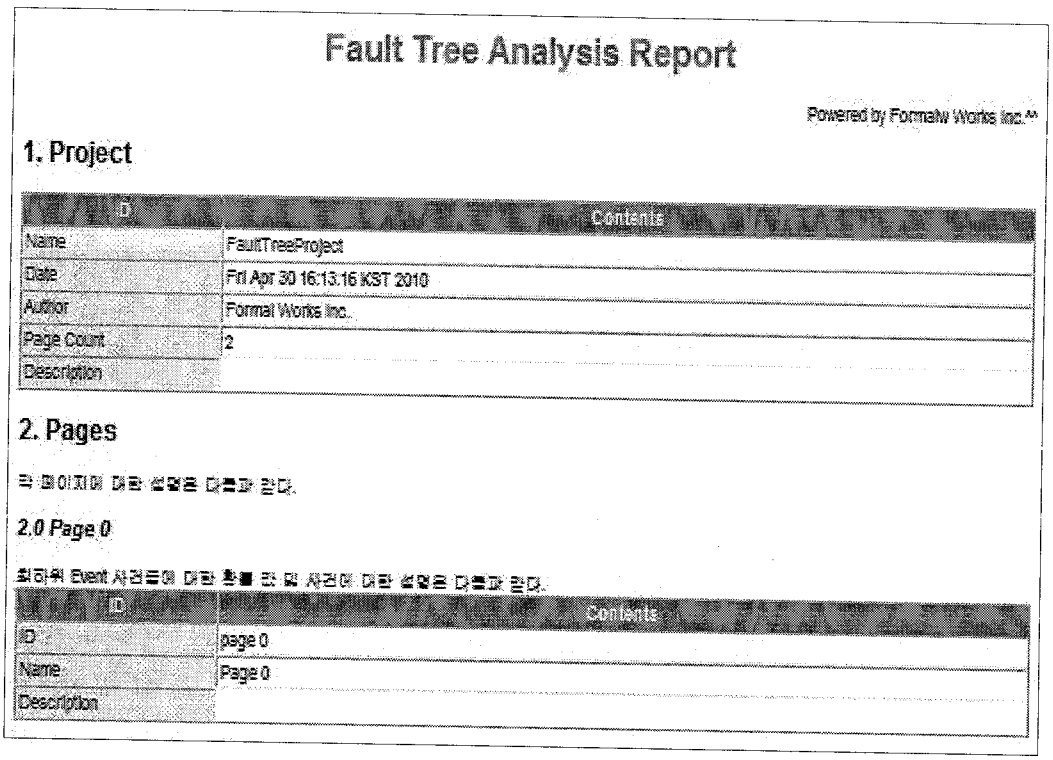
```
<?xml version="1.0" encoding="UTF-8" ?>
 <PROJECT name="FTtest" description="FTStructure" createDate="2010년 5월 4일 (화)" author="Formal Works">
 <PAGE ID="0" LABEL="Page 0">
 <EVENT ID="0" TYPE="PRIMARY" LABEL="PRIMARY_E_0" PROBABILITY="0.0" X="82" Y="148" DESCRIPTOIN="">
   <CONNECTION TYPE="OUT" X="121" Y="65" TARGETID="0" TARGETTYPE="AND" />
</EVENT>
 <TRANSFER ID="0" TYPE="IN" LABEL="ID_TI_0" PROBABILITY="0.0" X="186" Y="145" DESCRIPTOIN="">
    <CONNECTION TYPE="OUT" X="121" Y="65"TARGETID="0" TARGETTYPE="AND" />
</TRANSFER>
<GATE ID="0" TYPE="AND" LABEL="AND_G_0" PROBABILITY="0.0" X="121" Y="65" DESCRIPTOIN="" NUMBER="0" />
</PAGE>
 <PAGE ID="1" LABEL="Page 1">
 <GATE ID="0" TYPE="OR" LABEL="OR_G_0" PROBABILITY="0.0" X="134" Y="81" DESCRIPTOIN="" NUMBER="0" />
<TRANSFER ID="0" TYPE="OUT" LABEL="ID_TO_0" PROBABILITY="0.0"X="43" Y="108" DESCRIPTOIN="">
   <CONNECTION TYPE="OUT" X="134" Y="81" TARGETID="0" TARGETTYPE="OR" />
</TRANSFER>
 <EVENT ID="0" TYPE="PRIMARY" LABEL="PRIMARY_E_0" PROBABILITY="0.0" X="79" Y="194" DESCRIPTOIN="">
   <CONNECTION TYPE="OUT" X="134" Y="81" TARGETID="0" TARGETTYPE="OR" />
</EVENT>
  <EVENT ID="0" TYPE="UNDEVELOPED" LABELL="UNDEVELOPED_E_0" PROBABILITY="0.0" X="163" Y="206" DESCRIPTOIN="" />
</PAGE>
</PROJECT>
```

② 보고서 생성

Fault Tree 명세를 작성하고 위험도를 분석한 결과를 보고서로 생성한다. 보고서는 html 문서로 생성된다. 오류 분석 보고서의 내용은 다음 표와 같다.

표 3.3.78 오류 분석 보고서

항목	설명
프로젝트 설명	작성한 Fault Tree Analysis Project에 대한 설명을 기술한다.
다이어그램	작성한 Fault Tree Diagram의 이미지를 보여준다.
사건 명세	하위 Event 사건들에 대한 설명과 확률을 기술한다.
사건 명세 간 연결과 계산 확률	사건들 간의 연결을 이용하는 Gate 들에 대한 설명을 기술하고 하위 사건으로부터 계산한 결과를 기술한다.
최종 결과	각 페이지의 Fault Tree 의 최상위 Gate 의 계산 결과를 기술하고 모든 페이지에 대해 계산한 최종 결과를 기술한다.



Fault Tree Analysis Report

Powered by FormalW Works Inc.^^

1. Project

ID	Contents
Name	FaultTreeProject
Date	Fri Apr 30 16:13:16 KST 2010
Author	Formal Works Inc.
Page Count	2
Description	

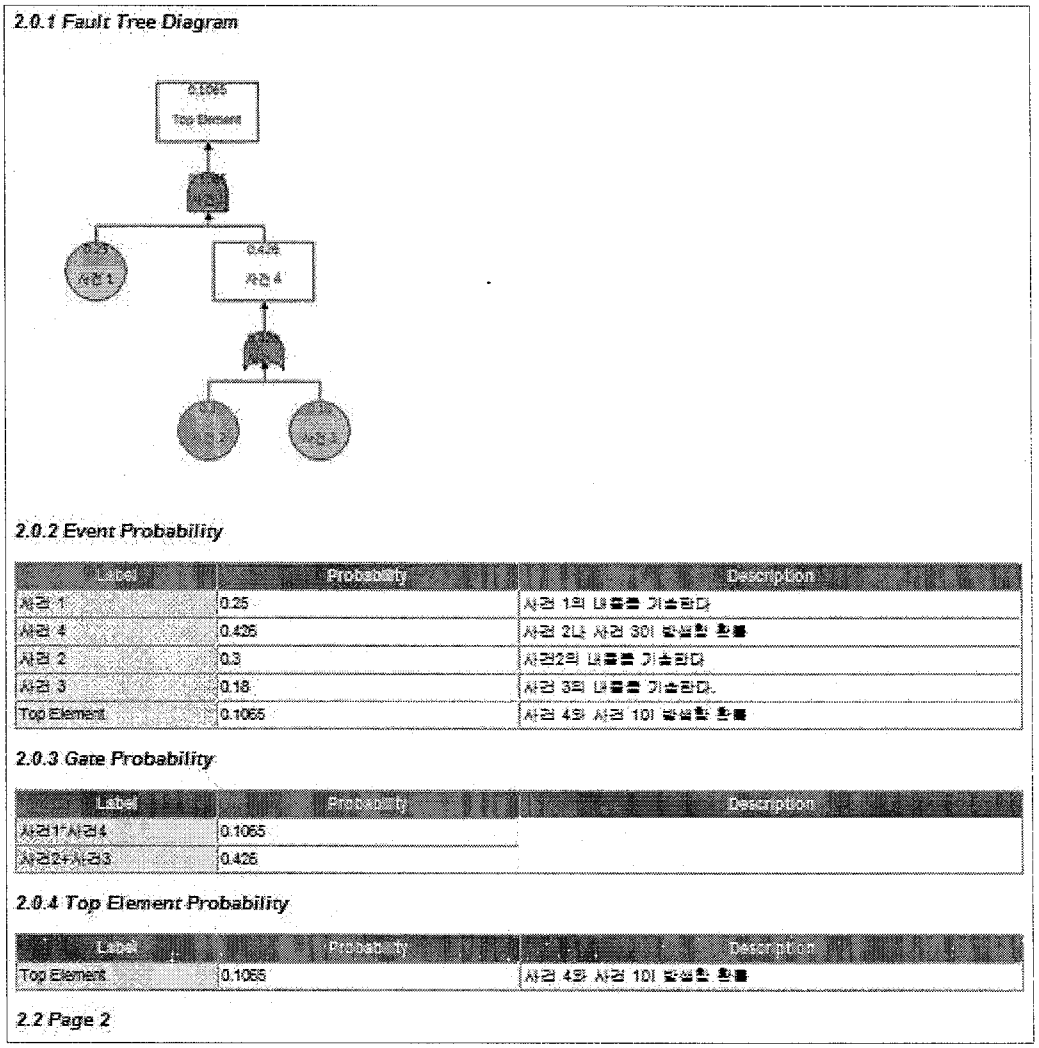
2. Pages

각 페이지에 대한 설명은 다음과 같다.

2.0 Page 0

최하위 Event 사건들에 대한 확률 값 및 사건에 대한 설명은 다음과 같다.

ID	Contents
ID	page 0
Name	Page 0
Description	



2.0.1 Fault Tree Diagram

2.0.2 Event Probability

Label	Probability	Description
사건 1	0.25	사건 1의 내용을 기술한다.
사건 4	0.426	사건 2나 사건 3이 발생할 확률
사건 2	0.3	사건2의 내용을 기술한다.
사건 3	0.18	사건 3의 내용을 기술한다.
Top Element	0.1065	사건 4와 사건 1이 발생할 확률

2.0.3 Gate Probability

Label	Probability	Description
사건1*사건4	0.1065	
사건2+사건3	0.426	

2.0.4 Top Element Probability

Label	Probability	Description
Top Element	0.1065	사건 4와 사건 1이 발생할 확률

2.2 Page 2

그림 3.3.46 오류분석 보고서

(바) 개발 결과

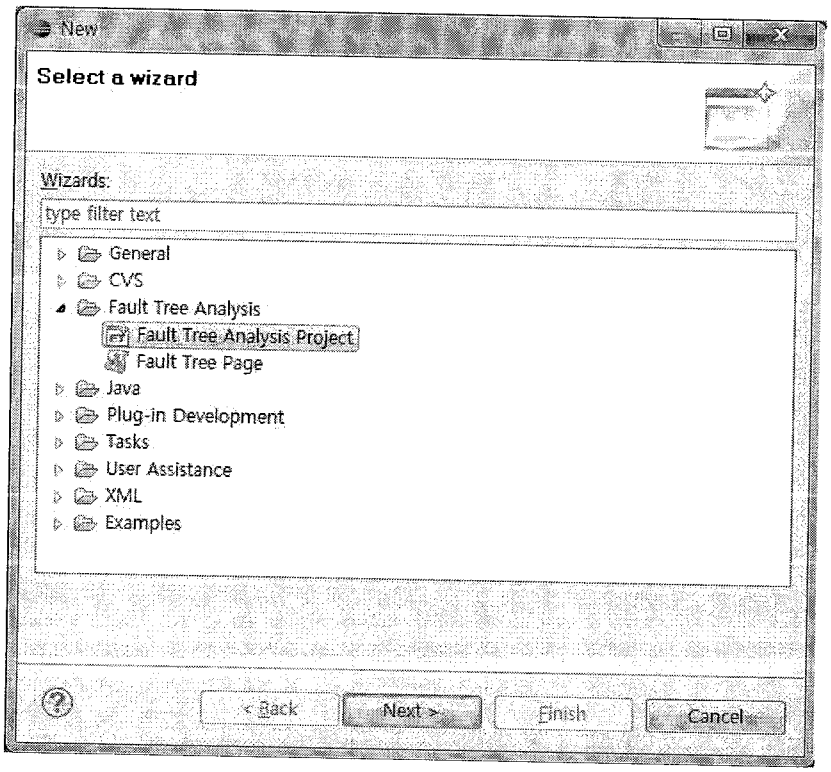
Fault Tree Analysis 모듈은 Eclipse Plug-in 형태로 개발되며, 운영체제 비 종속적인 Eclipse RCP Application으로 구동되어 동작한다.

① 제약 사항

Fault Tree는 부울 대수식으로 사건들이 연결되며, 각 사건 간의 관계(독립, 상호배반, 의존관계 등) 에 따라 확률 계산 방법이 달라질 수 있다. 상호 배반 및 의존관계에 대한 자연어 기술 방법의 제약에 따라 본 모듈은 Fault Tree의 조합하는 사건들을 서로 독립 사건으로 간주하고, 사건의 조합에 대해 확률을 계산한다.

② 수행 절차

○ 본 모듈을 구동하고 다음과 같이 새 프로젝트를 생성한다. Project Name은 "FaultTreeProject"로 한다.



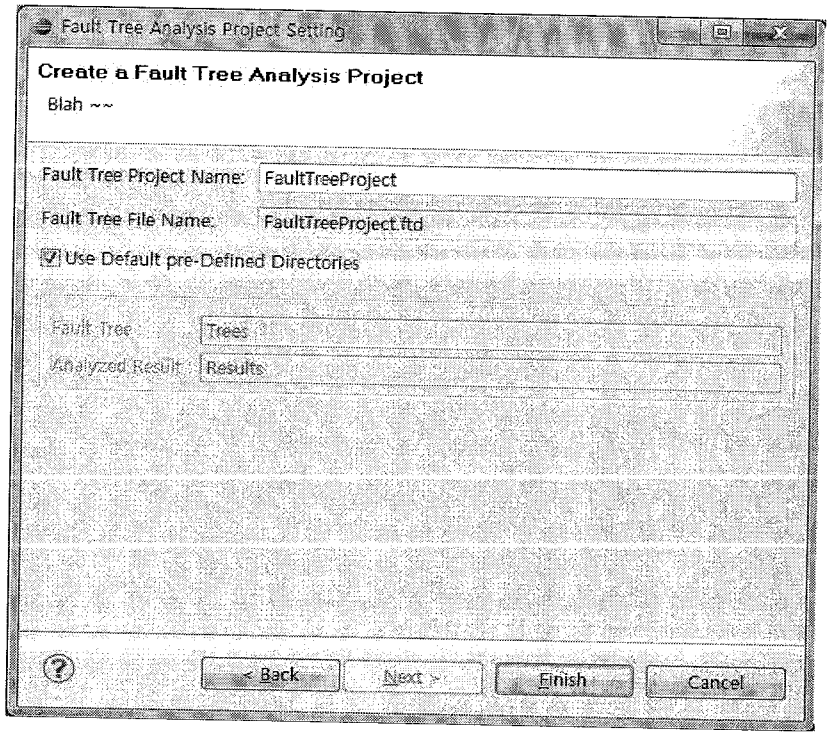


그림 3.3.47 Fault Tree Analysis Project 생성

○ 프로젝트를 생성하면 다음 그림과 같이 기본적으로 한 개의 page가 함께 생성된다. page를 열면 빈 diagram을 볼 수 있다.

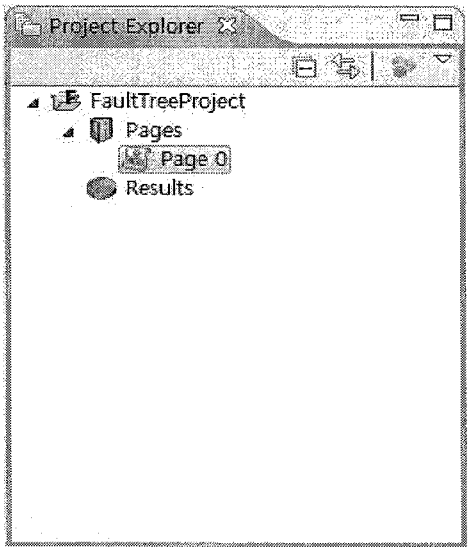


그림 3.3.48 Projec Explorer 화면

○ Pages 아래 새로운 page를 추가할 수 있다. 다음 그림 화면에서처럼 Project Explorer의 Pages에서 오른쪽을 클릭하여 New > Fault Tree Page 항목을 선택하면 dialog가 나타난다. dialog에서 page를 생성할 Project를 선택하고 이름을 정하여 Finish를 누르면 page가 추가된다.

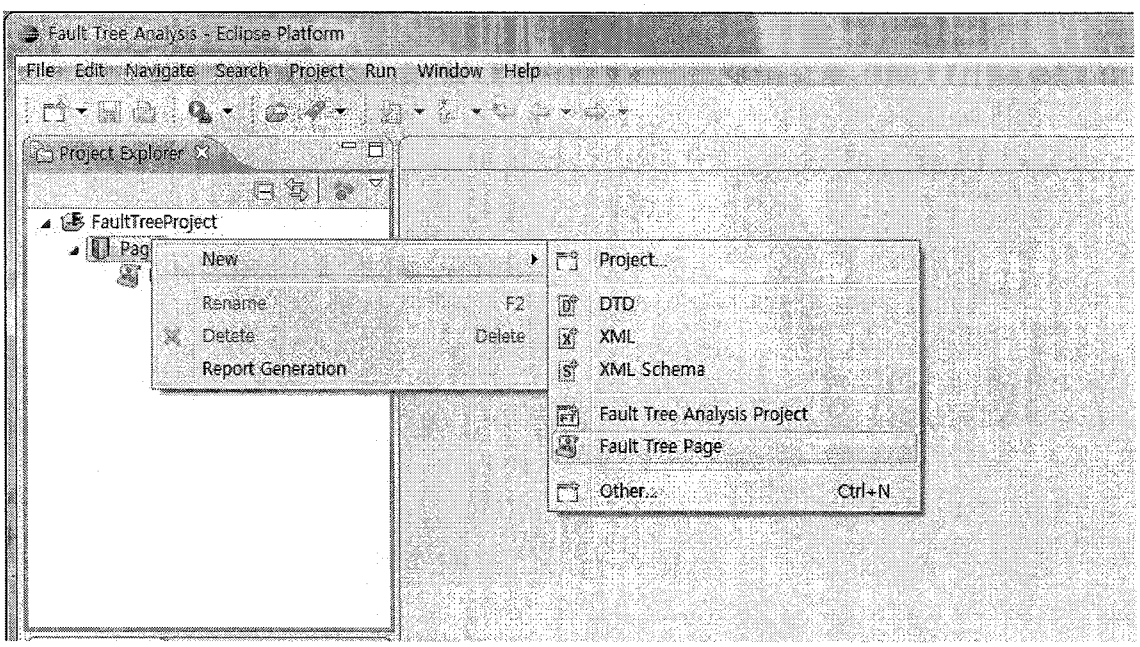


그림 3.3.49 Fault Tree Page 추가

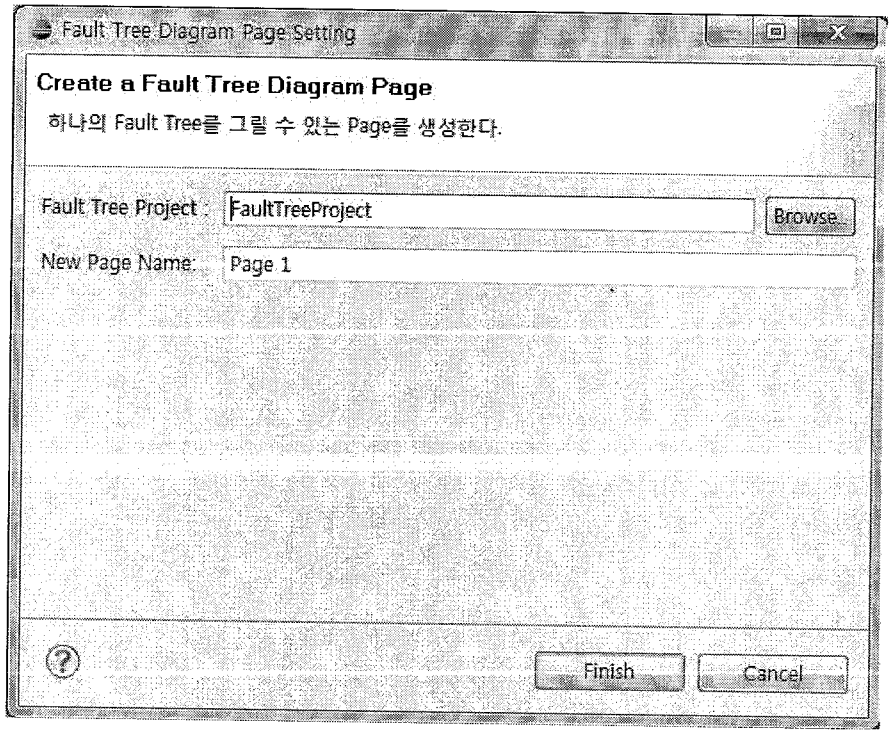


그림 3.3.50 Create Fault Tree Page Dialog

○ 확률 계산을 위한 간단한 예제를 만든다. Editor View에 보이는 Diagram page에서 다음의 그림처럼 Symbol을 선택하여 추가하고 Connection을 연결한다.

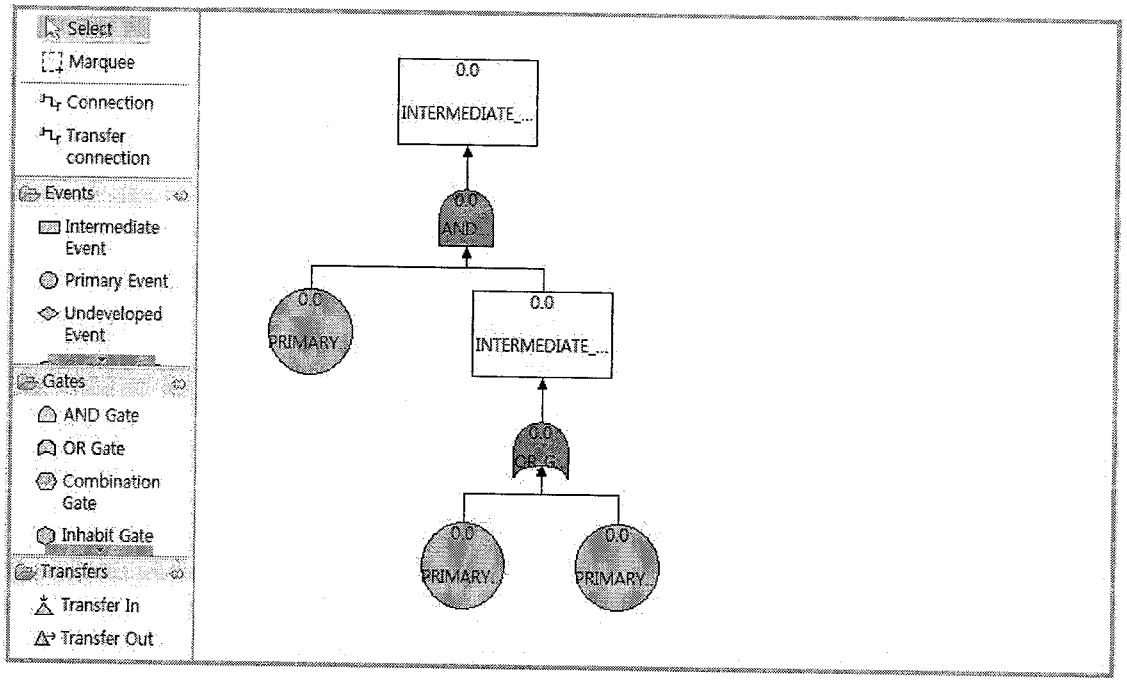


그림 3.3.51 Fault Tree Diagram 예제

- 왼쪽의 palette에서 AND Gate, OR Gate 한 개와 Primary Event 세 개, Intermediate Event 두 개를 diagram에 추가한다. Event는 하위 Symbol을 갖지 못하며 Gate 위에는 Intermediate Event를 항상 연결해야한다. 가상 상위에는 Intermediate Event가 있어야한다.
- Connection을 선택하여 각 Symbol을 연결한다. Connection은 Gate와 Event를 연결하며 Transfer connection은 Gate나 Event에 Transfer Out을 연결하기 위한 점선이다. Transfer connection은 본 예제에서는 사용하지 않는다.
- Diagram에 추가 된 Primary Event Symbol에 확률을 입력한다. 각 Symbol을 선택하여 Property View에서 PRIMARY_E_0에는 0.25, PRIMARY_E_1에는 0.3, PRIMARY_E_2에는 0.18을 입력한다.
- Symbol의 Label과 Description도 마찬가지로 Property View에서 변경할 수 있다.

다음 그림에서처럼 diagram에서 오른쪽을 클릭하여 Layout을 선택하면 그림 3.3.52처럼 정렬할 수 있다.

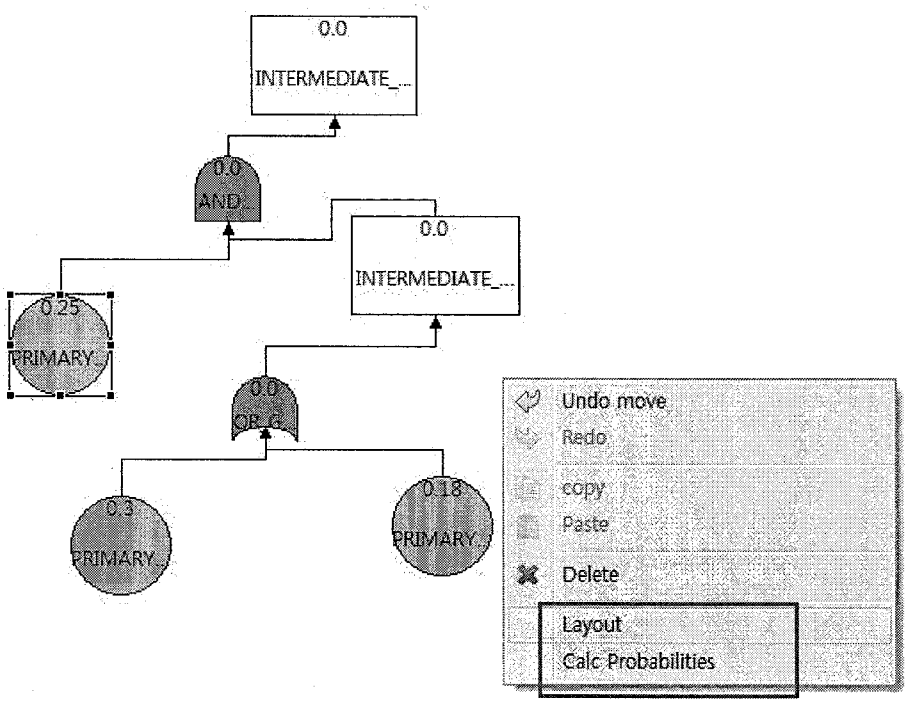


그림 3.3.52 Layout

○ Event에 입력한 확률 값으로 확률 계산을 한다. 위 그림에서 Context Menu의

맨 아래 Calc Probabilities를 선택하면 아래 그림과 같이 모든 Symbol에 계산된 결과를 보여준다.

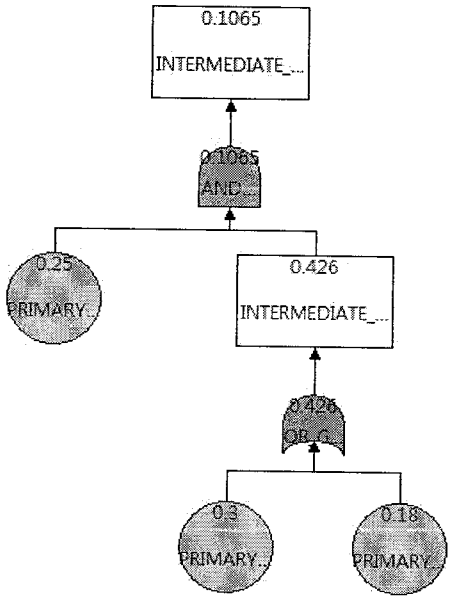


그림 3.3.53 Probability 계산 결과

- 지금가지 예제를 저장한다. File > Save 를 선택하거나 Ctrl+s를 눌러 Project를 저장한다. 오류 보고서를 생성하기 전에 저장해야 한다.
- 오류 분석 보고서를 생성한다. Project Explorer의 Pages를 선택하고 오른쪽을 클릭해서 Report Generation 을 선택하면 그림 3.3.55와 같은 Dialog가 나타난다. Report를 생성할 Directory 위치를 지정하고 OK 버튼을 클릭한다.

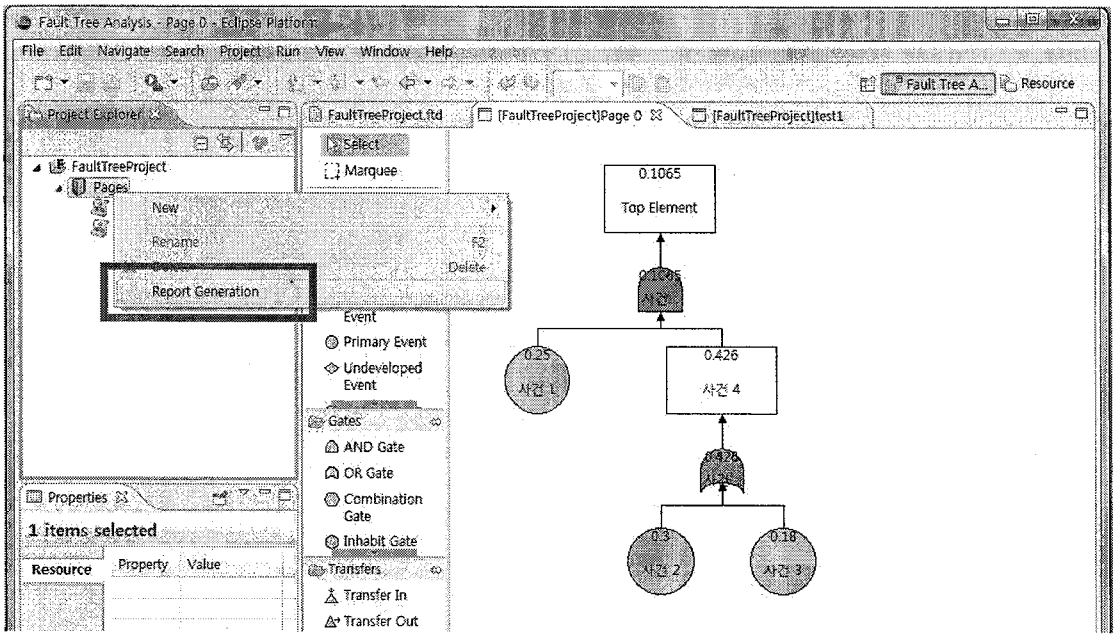


그림 3.3.54 Report Generation

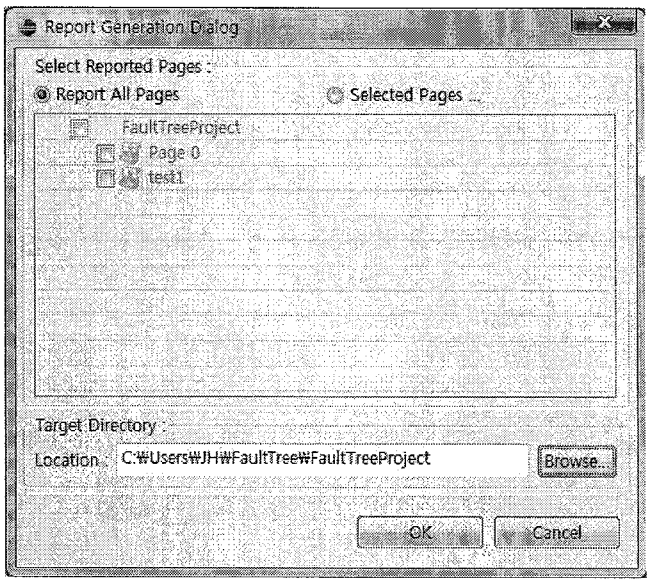


그림 3.3.55 Report Generation Dialog

○ Report를 생성한 폴더를 보면 다음 4 개의 파일이 생성된 것을 확인할 수 있다. page 수만큼의 Diagram 이미지가 생성되며 html 문서 한 개와 스타일 시트 문서가 생성된다. index.html을 열면 생성된 보고서를 확인할 수 있다.

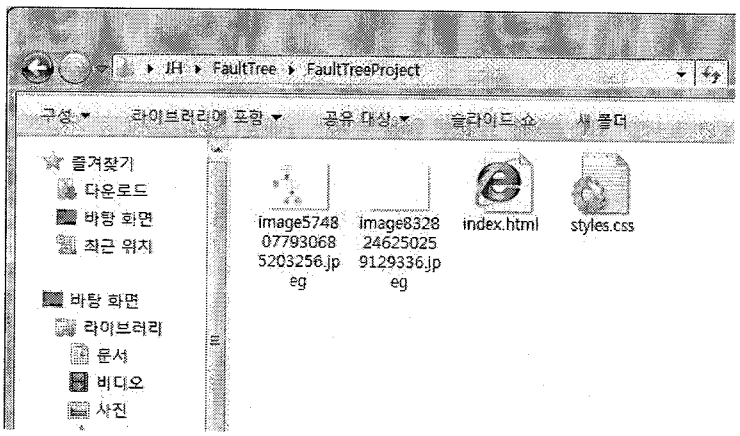


그림 3.3.56 오류 보고서 파일 생성

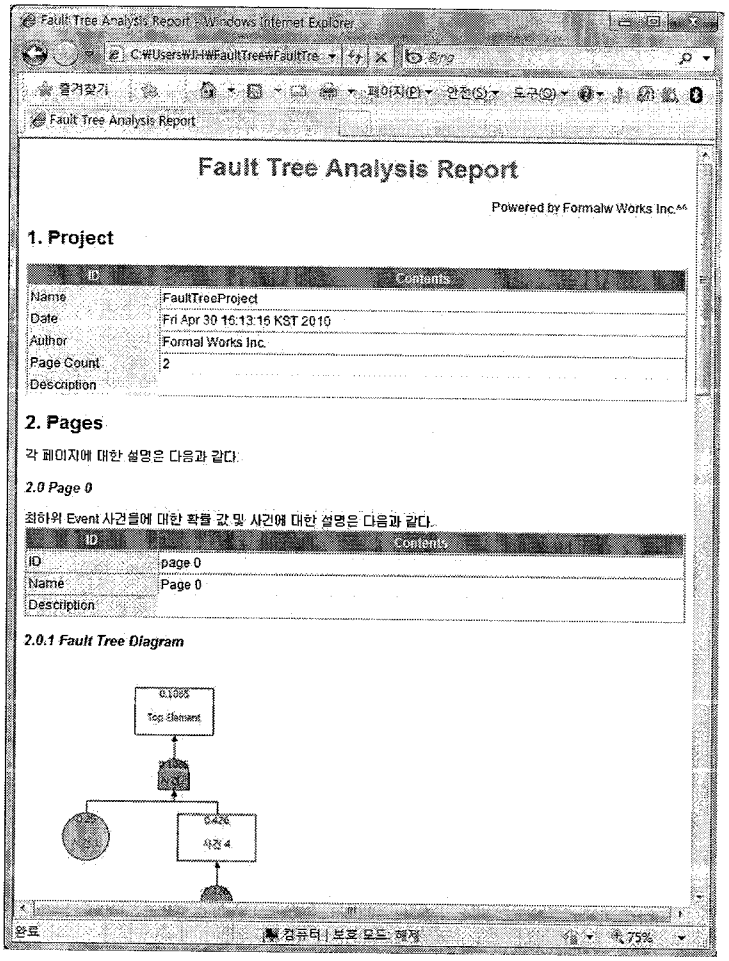


그림 3.3.57 Fault Tree Analysis Report

③ 수행 요약

수행 절차에서 간단한 Fault Tree Diagram을 만들고 오류 분석 보고서를 생성함으로써 확률 계산을 통한 위험도 분석을 수행했다. 예제를 통해 Diagram 형태로 Fault Tree 명세를 작성하면서 Symbol을 편집할 때의 제약 사항과 Connection을 연결 할 때의 제약 사항도 함께 확인 할 수 있다. 확률 계산은 각각의 사건을 독립 사건이라고 가정하였으며 각 Gate Symbol에 따른 확률 계산 방법을 적용하여 적합한 결과 값을 보여준다.

(4) 평가 대상시스템 소프트웨어에 적용 결과

본 절에서는 안전성 평가 대상시스템 소프트웨어를 대상으로 기 제작한 'Design & Coding Standard 검사 모듈', 'Control Flow 테스팅 모듈', 'Data Flow Testing 모듈'을 활용한 테스팅 수행 결과에 대해 제시하였다. 먼저 각각의 모듈에 대한 간략한 개요 소개 및 테스팅 방법에 대해 살펴보면 다음과 같다.

Design & Coding Standard 검사 모듈은 크게 두 가지 방식으로 구성될 수 있다. 첫 번째는 클라이언트/서버 구조로서 품질 관리팀에서 설정한 규칙을 개발자들이 적용하는 방식이다. 이 구조에서는 개발자들이 자신의 규칙을 임의로 설정할 수 없으므로 개발 산출물의 품질을 일관되게 보장할 수 있는 장점이 있다. 두 번째는 별도의 서버를 두지 않고, 개발자가 규칙을 설정할 수 있는 지역(Local) 구조를 지원한다. 이 구조는 개발자가 개발을 진행하면서 개발 진행과 동시에 품질을 확인해 볼 수 있는 장점이 있다.

Control Flow Testing에서는 소스 코드의 영역 및 분기, 조건문 등의 실행 여부에 따라 커버리지를 측정하여 보고한다. 커버리지는 S/W 테스트의 품질을 나타내는 대표적인 척도로써 사용된다. S/W 테스트 분야에서는 여러 커버리지를 제시하고 있다. Control Flow Testing 모듈은 그 중에 블록 커버리지, 분기 커버리지, MCDC를 제공한다.

Data Flow Testing 모듈은 소스 코드에서 자료의 정의/사용 정보를 분석하여 자료의 흐름을 추출한다. 추출한 자료는 Control Flow Testing 모듈에서 제공하는 제어 흐름 그래프에 표현되는 블록 단위이며, 복잡한 자료 흐름을 제어 흐름 그래프 상에 표현해주므로 시각적인 이해가 가능하다. 분석 모듈에 의해 추출된 정보를 이용해 테스트를 수행하면 자동으로 생성된 테스트 데이터와 사용자가 입력한 테스

트 데이터가 자료 흐름 커버리지(Data Flow Coverage)를 얼마나 만족시켰는지 평가한다. Data Flow Test 모듈은 데이터 프로그램 코드 내에 특정 변수의 정의와 사용에 근거하여 테스트 수행 품질을 평가한다.

Data Flow Testing 모듈은 크게 위에 설명한 것처럼 All-Def 적합성 기준과 All-Uses 적합성 기준 그리고 All-DU Paths 적합성 기준에 대한 커버리지 정보를 제공한다. **All-Def** 적합성 기준이란, 특정 함수 내에서 사용된 변수들의 정의 i = 0; 이나 i = a + b;와 같은 문장이 함수 내 곳곳에 있을 수 있다. 이 곳곳에 있는 정의문들을 모두 실행했는지 여부를 평가하는 기준이 All-Def가 된다. 예를 들어 어떤 변수가 프로그램 코드 내에서 3번 정의가 되었는데, 실제 프로그램 실행에서 3개 중에 2개의 문장만이 실행되었다면 All-Def를 100% 만족하지 못하고, 66%만 만족했다고 판단한다. **All-Uses**의 경우도 마찬가지이다. 프로그램 코드 내에 특정 변수에 대해 사용이 일어나는 부분이 여러 곳일 수 있다. 이러한 사용이 실제 프로그램 실행 중에 모두 실행되었는지 여부를 판단한다. 예를 들어 어떤 변수가 코드 내에서 5번 사용되었는데, 실제 수행해 보니 3곳만 사용되었다면 All-Uses를 60%만 만족한 것이다. **All-DefUse Paths**는 프로그램 내에 특정 변수가 정의되고 사용되는 모든 경로를 추적하여, 모두 실행되었는지를 판단한다. 예를 들어 변수가 정의되고 사용된 경로가 분석해 보니 총 12개 나왔는데, 실제 실행해 보니 그 중에 6개만 실행되었다면, All-DefUse Paths를 50%만 만족한 것이 된다.

(가) 테스팅 도구를 적용하기 위한 평가 대상시스템 정보

세부과제에서 기 개발한 안전성 평가 대상시스템의 개발 환경 및 Control Flow Testing 모듈, Data Flow Testing 모듈을 적용한 환경은 다음 표 3.3.153와 같으며, 적용한 평가 대상 시스템의 기본 정보는 다음 표 3.3.79과 같다.

표 3.3.79 개발 환경 및 테스트 환경 정보

구분	개발 환경	테스트 환경
OS	VxWorks	Windows XP
Compiler	PPC	embedded parser, 치

표 3.3.80 제어기 시뮬레이터(Mock-up)의 기본 정보

구분	설명
Language	VxWorks
Compiler	PPC
OS	VxWorks
Number of File	4 개
Line of Code	4,906

(나) Design & Coding Standard 검사 / Control Flow / Data Flow Testing 적용 절차

테스트 적용 절차는 다음 그림과 같다.

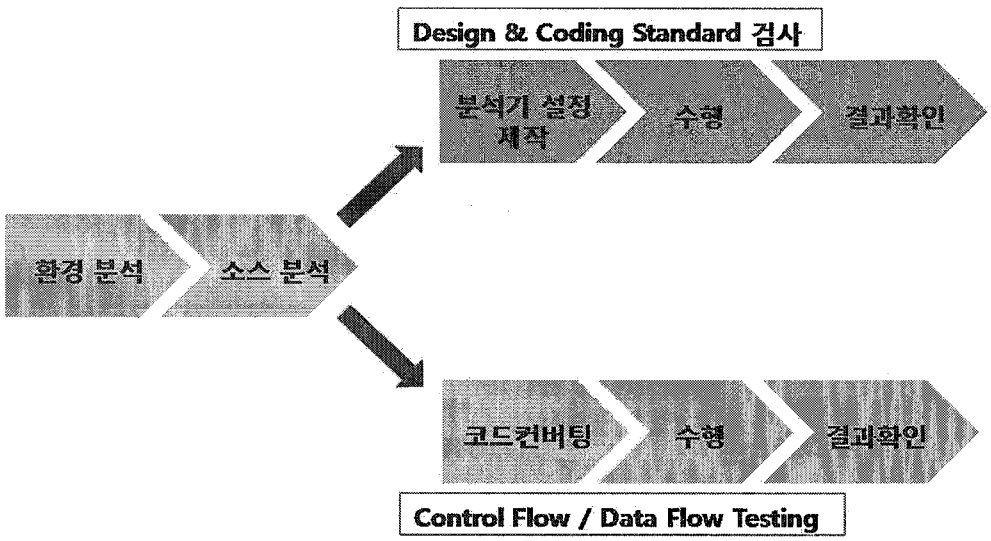


그림 3.3.58 테스트 적용 절차

Design & Coding Standard 검사와 Control Flow / Data Flow Testing 모듈을 수행하는데 있어 그 시작은 모두 시험 대상의 환경을 분석하는 것이다. 환경 분석을 마치면 해당 환경에서 컴파일되고 수행될 수 있는 소스 코드를 분석하게 된다. 소스 코드의 분석 결과를 바탕으로 Design & Coding Standard 검사를 위해 분석기 설정 및 제작을 거쳐 실제 검사를 수행하게 된다. 그리고 역시 소스 코드의 분석 결과를 바탕으로 Control Flow / Data Flow Testing을 위하여 소스 코드를

Testing 모듈이 수행될 수 있는 환경에서 소스 코드가 Testing 될 수 있도록 코드 컨버팅 작업을 거친다. 컨버팅된 소스 코드를 이용 Control Flow / Data Flow Testing 모듈을 수행시킨다.

(다) 테스팅 적용 결과

① Design & Coding Standard 검사

Design & Coding Standard 검사를 위한 검출 규칙 및 심각도는 다음 표와 같다.

표 3.3.81 주요 검출 규칙 및 심각도

구분	규칙 심각도	갯수
61508-3	매우 낮음	47
61508-5	낮음	2
61508-6	낮음	2
61508-7	매우 낮음	18
62279-2	매우 낮음	47
62279-5	매우 낮음	5
62279-6	낮음	2
62279-8	매우 낮음	13
62279-9	낮음	2
SURE_BASIC-02	낮음	2
SURE_BASIC-08	낮음	16
SURE_BASIC-09	매우 높음	1
SURE_BASIC-10	높음	2
SURE_BASIC-11	매우 낮음	1
SURE_BASIC-16	매우 낮음	3
SURE_BASIC-22	높음	20
SURE_BASIC-29	낮음	2
SURE_BASIC-31	매우 낮음	13
SURE_BASIC-40	낮음	1

○ IEC61508-7 검출 사례

선언된 파라미터가 함수 안에서 사용되지 않음 (Testing.c / line 2182)

```
2181  /* ------------------------------------------------------------------------
2182  STATUS StartIcmInfo(int seqno)
2183  {
2184      int i,Len;
2185      unsigned short crc;
2186      BYTE msg[MAX_SIZE_DATA];
2187
2188      msg[0]=AIS;
2189      msg[1]=NONE;
2190      msg[2]=ICM;
2191      msg[3]=NONE;
2192      msg[4]=0x00;
```

그림 3.3.59 IEC61508-7 검출 사례

○ IEC62279-2 검출 사례

포인터가 검사 없이 사용됨 (Testing.c / line 1934)

```
1930  STATUS SwitchLock(BYTE sw_id)
1931  {
1932      SWITCH_ID switch_id;
1933      switch_id = (int)sw_id;
1934      semTake(smSwitch,WAIT_FOREVER);
1935      if(!(switch_data[switch_id].status & S_INTERLOCK))
1936      {
1937        switch_data[switch_id].status |= S_INTERLOCK;
1938      }
1939      semGive(smSwitch);
1940  #ifdef LOG_
```

그림 3.3.60 IEC62279-2 검출 사례

○ IEC62279-5 검출 사례

소스파일의 길이가 320라인을 초과함 (db.h / linkSyms.c / prgParams.h / prjConfig.c / Testing.c)

```
1   /*------------------------------------------------------------------------*/
2   /*BLOCK Device                                                            */
3   /*------------------------------------------------------------------------*/
4   typedef enum {
5       B201 = 201,    /* 201(00C9) */
6       B202,    /* 202(00CA) */
7       B203,    /* 203(00CB) */
8       B204,    /* 204(00CC) */
9       B205,    /* 205(00CD) */
10      B206,    /* 206(00CE) */
11      B207,    /* 207(00CF) */
```

그림 3.3.61 IEC62279-5 검출 사례

○ IEC62279-6 검출 사례

헤더파일에 전역변수가 정의 (Testing.h / line 233)

```
228 typedef struct {
229     REMAIN_RT re_rt[100];
230     int length;
231 }RtList;
232
233 RtList rtList;
234 TRAINLIST tr_list;
235
236 void RtListInit(RtList * rlist);
237 /*-------------------------------------------------------------*/
238 /*function define                                              */
239 /*-------------------------------------------------------------*/
```

그림 3.3.62 IEC62279-6 검출 사례

○ IEC62279-8 검출 사례

함수에 1개 이상의 exit point가 존재 (Testing.c / line 922)

```
918     trlist->count = 0;
919
920 }
921 int SearchTrainId(TRAINLIST * trlist,BYTE trId)
922 {
923     int i;
924     int flag = 0;
925     for(i = 1; i<= trlist->count ; i++)
926     {
927       if(trlist->tr_data[i].trainId == trId)
928       {
929         flag = i;
930         return flag;
931       }
```

그림 3.3.63 IEC62279-8 검출 사례

○ IEC62279-9 검출 사례

함수의 복잡도 값이 10을 초과 (Testing.c / 함수 CONRoute)

```
1588 STATUS CONRoute(void)
1589 {
1590     int i,j,length=0;
1591     REMAIN_RT Re_rt;
1592     ROUTE_ID rt_id;
1593     SUBROUTE_ID sub_id,nsub_id;
1594     SWITCH_ID switch_id;
1595     int count=0;
1596     FOREVER
1597     {
1598       //진로 리스트의 길이를 확인함.
1599       length=rtList.length;
1600       if(length <= 0)
```

그림 3.3.64 IEC62279-9 검출 사례

○ SURE_BASIC-02 검출 사례

매크로 파라미터가 # 혹은 ##로 연결되지 않으면서 괄호로 쌓여있지 않음 (Testing.h / line 111)

```
107
108  /* ------------------------------------------------------------
109  /* 2Bytes의 정수값을 상위 Byte, 하위 Byte로 구분하는 Macro 정의
110  /* ------------------------------------------------------------
111  #define HighByte(x)  (BYTE)(x >> 8)
112  #define LowByte(x)   (BYTE)(x & 0x00FF)
113
114
115  typedef unsigned char BYTE;
```

그림 3.3.65 SURE_BASIC-02 검출 사례

○ SURE_BASIC-08 검출 사례

조건식에서 0에 대한 비교 시 논리연산자 사용 안함 (Testing.c / line 1907)

```
1903  STATUS SwitchLockVerify(BYTE sw_id)
1904  {
1905    SWITCH_ID switch_id;
1906    switch_id = (int)sw_id;
1907    if(switch_data[switch_id].status & S_INTERLOCK)
1908    {
1909      return(OK);  //OK : lock
1910    }
1911    else
1912    {
1913  //    logMsg("NOT OK\n",0,0,0,0,0,0);
1914      return(ERROR);    //ERROR : unlock
1915    }
```

그림 3.3.66 SURE_BASIC-08 검출 사례

○ SURE_BASIC-09 검출 사례

변수 i는 값이 할당되지 않음 (Testing.c / line 1229)

```
1224    tmValue.it_interval.tv_sec = 2;
1225    tmValue.it_interval.tv_nsec =0;
1226
1227    if(timer_create(CLOCK_REALTIME,NULL,&pTmrid) == ERROR)
1228    {
1229      logMsg("timer create error %d \n",i,0,0,0,0,0);
1230    }
1231    if(timer_connect(pTmrid,(VOIDFUNCPTR)TInt,0) == ERROR)
1232    {
1233      logMsg("timer connect Error\n",0,0,0,0,0,0);
1234    }
1235    if(timer_settime(pTmrid,0,&tmValue,NULL) == ERROR)
```

그림 3.3.67 SURE_BASIC-09 검출 사례

○ SURE_BASIC-10 검출 사례

해더파일이 #ifdef, #define, #endif로 중복 금지 되어있지 않음 (Testing.h / db.h)

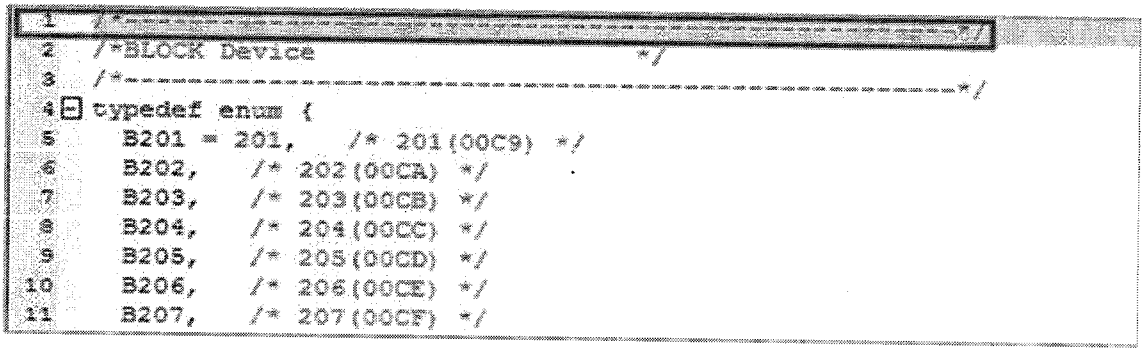


그림 3.3.68 SURE_BASIC-10 검출 사례

○ SURE_BASIC-11 검출 사례

Nested Comment 사용 (Testing.c / line 40)

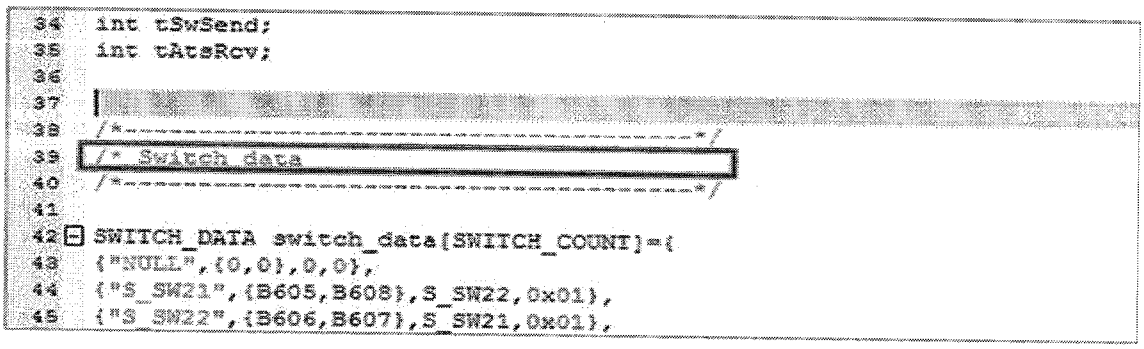


그림 3.3.69 SURE_BASIC-11 검출 사례

○ SURE_BASIC-16 검출 사례

External linkage로 선언된 배열 사이즈의 명시적인 표시 또는 초기화가 되어 있지 않음 (prjConfig.c / line 135)

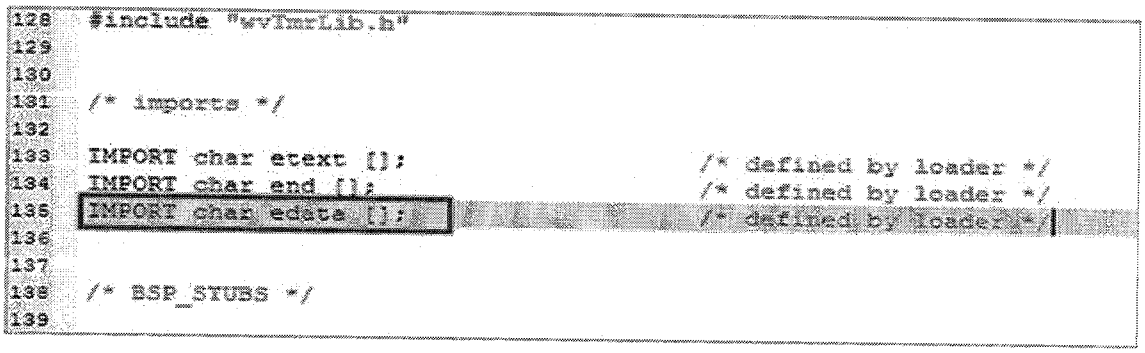


그림 3.3.70 SURE_BASIC-16 검출 사례

○ SURE_BASIC-22 검출 사례

Bitwise 연산자에 signed 타입의 피연산자 사용 (Testing.h / line 2291)

```
2283  unsigned short  CalcCrc (BYTE Buf[], int Len)
2284  {
2285      unsigned short  count;                          /* 계산 하는 ch의 순서   */
2286      unsigned short  index;                          /* crc table 의 entry no */
2287      unsigned short  crc;                            /* 일시적인 crc 값       */
2288
2289      for (count = 0, crc = 0; count < Len; count++)
2290      {
2291          index = (crc ^ Buf[count]) & 0x00FF;        /* CRC Table의 Entry No */
2292          crc = (crc >> 8) ^ CrcTable[index];         /* CRC 갱신             */
2293      }
2294
2295      return(crc);
2296  }
```

그림 3.3.71 SURE_BASIC-22 검출 사례

○ SURE_BASIC-31 검출 사례

연산자 혼용 시 괄호를 사용하지 않음 (Testing.c / line 2208)

```
2200    for(i=0;i<=BLOCK_COUNT;i++)
2201    {
2202      if(i==0)
2203      {
2204        msg[11]=BLOCK_COUNT-1;
2205      }
2206      else
2207      {
2208        msg[i*2+10]=LowByte(block_data[i].rt_id);
2209        msg[i*2+11]=LowByte(block_data[i].tr_id);
2210      }
2211    }
2212    for(i=0;i<=SWITCH_COUNT;i++)
```

그림 3.3.72 SURE_BASIC-31 검출 사례

○ SURE_BASIC-40 검출 사례

Enum 타입 선언 시 각 요소는 =를 통해 모두 할당되거나, 또는 첫 번째 요소만 =를 통해 할당되거나, 모든 요소가 할당되지 않아야 함 (db.h / line 4)

```
4  typedef enum {
5      B201 = 201,   /* 201(00C9) */
6      B202,    /* 202(00CA) */
7      B203,    /* 203(00CB) */
8      B204,    /* 204(00CC) */
9      B205,    /* 205(00CD) */
10     B206,    /* 206(00CE) */
11     B207,    /* 207(00CF) */
12     B208,    /* 208(00D0) */
13     B209,    /* 209(00D1) */
14     B210,    /* 210(00D2) */
15     B211,    /* 211(00D3) */
16     B212,    /* 212(00D4) */
17     B213,    /* 213(00D5) */
18     B214,    /* 214(00D6) */
19     B215,    /* 215(00D7) */
20     B216,    /* 216(00D8) */
21     B217,    /* 217(00D9) */
22     B218,    /* 218(00DA) */
23     B219,    /* 219(00DB) */
24     B220,    /* 220(00DC) */
25     B301 = 301, /* 301(012D) */
26     B302,    /* 302(012E) */
```

그림 3.3.73 SURE_BASIC-40 검출 사례

② Control Flow / Data Flow Testing

○ 주요 검출 사례

배열의 인덱스를 반복문의 증가 인자로 설정하여 파라미터로 전달되는 비교값이 클 경우 배열의 참조 범위를 벗어나 시그날 발생 (함수 RtListAdd / Block 4)

```
1099    semTake(smRoute,WAIT_FOREVER);
1100    for(i=0;i<=rlist->length;i++)
1101    {
1102      //진로를 저장할 시 열차ID와 진로ID가 있는지 확인
1103
1104      if(rlist->re_rt[i].rt_id == rt.rt_id)
1105        if(rlist->re_rt[i].tr_id == rt.tr_id)
1106        {
1107          //똑같은 진로 시 덮어 씀.
1108          rlist->re_rt[i] = rt;
1109          flag = 1;
1110        }
```

그림 3.3.74 Control Flow / Data Flow Testing 주요 검출 사례

(5) 열차제어시스템 소프트웨어 테스팅 기술지침(안) 구성 제안

본 연구를 통해 제작한 소프트웨어 테스팅 자동화 도구의 실용화를 위해서 '열차제어시스템 소프트웨어 테스팅 기술지침(안)'을 작성하고자 당해연도에는 다음과 같이 기술지침(안)의 구성과 기본방향을 설정하였다. 먼저 큰 틀에서의 목차와 간략한 포함내용을 정리하였으며, 추후 차년도에 소프트웨어 테스팅 전문가, 철도운영기관과 제작사의 의견 수렴 과정을 통해 '열차제어시스템 소프트웨어 테스팅 기술지침(안)'을 구체적으로 작성할 예정이다.

■

철도 소프트웨어 테스팅 기술 지침서
Railway Software Testing Guide

1. 개 요

1.1. 지침서의 목적

1.1.1. 본 지침서에서는 철도 소프트웨어의 안전성 향상을 위한 테스팅을 수행하기 위해 적용하고자 하는 테스팅 기법들과 관련 지침을 제공함을 목적으로 한다.

1.1.2. 본 지침서는 철도 소프트웨어의 설계 및 시험을 수행하는 개발자들뿐만 아니라, 기개발된 소프트웨어에 대한 테스팅을 수행하여 그 결과를 검증하려는 평가자들의 활용을 위해 작성되었다.

1.1.3. 본 지침서는 철도 소프트웨어 테스팅의 수행 지침에 대한 지침을 제공하여, 철도 소프트웨어 오류로 인해 발생할 수 있는 인적, 물적 피해의 최소화에 기여하고자 한다.

1.2. 지침서의 범위

1.2.1. 본 지침서의 평가 주요대상은 열차 제어를 위한 소프트웨어로 하며, 기타 철도 관련 분야의 다른 소프트웨어에도 적용이 가능하다.

1.2.2. 본 지침서는 철도 소프트웨어의 설계·개발 단계부터 최종 평가·검증 단계까지 해당 소프트웨어의 테스팅을 하기 위해 적용할 수 있다.

1.2.3. 본 지침서는 철도 소프트웨어 검증에 요구되는 정적분석 테스팅, 동적 테스팅 및 기능 테스팅까지를 주요 범위로 한다.

2. 철도 소프트웨어 테스팅 기법(Railway Software Testing Method)

2.1.1. 본 지침서에 의해 제시된 철도 소프트웨어의 테스팅 기법은 다음과 같다.

(1) 정적 분석 테스팅
① 코딩규칙 검사
② 소프트웨어 메트릭 검사

(2) 동적 테스팅
① 제어/자료 흐름 테스팅
② 성능 테스팅

(3) 기능 테스팅
① 기능 요구사항 테스팅
② 경계값 분석 및 동치 영역 분석 테스팅
③ 소프트웨어의 FTA 및 FMEA 수행을 통한 테스팅

(4) 테스팅 결과의 문서화

3. 정적 분석 테스팅

3.1. 코딩규칙 검사

3.1.1. 코딩규칙 검사를 통해서 해당 소프트웨어의 소스코드가 관련 규격 등에서 요구하

는 코딩 규칙을 준사하는지 여부를 반드시 확인하여야 한다.

3.1.2 본 검사에서 적용하는 코딩 규칙은 다른 산업용 임베디드시스템 소프트웨어에 일반적으로 적용하는 MISRA-C 코딩 규칙 및 철도시스템 소프트웨어 개발관련 규격인 IEC 61508, IEC 62279를 통해 도출한 코딩 규칙을 따른다.

3.2. 메트릭 검사

3.2.1. 메트릭 검사를 통해서 해당 소프트웨어 소스코드의 복잡도, 응집도, 결합도, 크기, 함수간 인터페이스 형태를 분석하여야 한다.

3.2.2. 소스코드의 함수에 대한 복잡도를 측정하기 위하여 Cyclomatic Complexity를 이용한다. (참조 문서 : T.J. McCabe. "A Complexity Measure." IEEE Trans. on Software Engineering, Vol. SE-2, No. 4, Dec. 1976)

<복잡도 값 범위>

복잡도 값 범위	설명
1 ~ 10	단순함 (Simple)
11 ~ 20	약간 복잡함 (Complex)
21 ~ 50	복잡함 (More Complex)
51 이상	매우 복잡함 (Very Complex)

3.2.3. 소프트웨어 소스코드는 높은 응집도를 가져야 하며, 철도 소프트웨어의 응집도를 측정하기 위하여 LCOM (Lack of COhesion in Methods) 메트릭을 기반으로 측정한다. (참조 문서 : Chidamber, S.R.; Kemerer, C.F. "A Metrics Suite for Object Oriented Design." IEEE Transactions on Software Engineering, Vol. 20, Issue 6, Jun. 1994)

3.2.4. 소프트웨어 소스코드는 낮은 결합도를 가져야 하며, 철도 소프트웨어의 결합도를 측정하기 위하여 구조적 방법론에서 말하는 함수 각각의 Fan-In, Fan-Out을 주요 메트릭으로 측정한다. (참조 문서 : I. Sommerville "Software Engineering",

Addison Wesley)

Fan-In : 자신을 호출하는 모듈의 수 (caller)
Fan-Out : 자신이 호출하는 모듈의 수 (callee)

3.2.5. 철도 소프트웨어의 해당 프로그램의 크기를 소스코드의 파일별, 함수별로 각각 분석하여 측정하여야 한다.

3.2.6 철도 소프트웨어의 해당 프로그램 전체 함수간의 호출 관계를 분석하여 함수들 간의 연관 관계를 파악하여야 한다.

4. 동적 테스팅

4.1. 제어/자료 흐름 테스팅

4.1.1. 제어흐름 테스팅을 통해 해당 소프트웨어 소스코드의 영역 및 분기, 조건문 등의 실행여부에 따라 커버리지를 측정하여야 한다. 본 테스팅을 통해 측정하는 커버리지는 MCDC, 블록 커버리지, 분기 커버리지가 해당된다.

4.1.2. 제어흐름 테스팅에서는 MCDC, 블록 커버리지, 분기 커버리지 수치를 기반으로 테스트가 충분한지를 평가한다. 테스트 수행 결과가 목표 수치에 도달하지 않을 경우는 테스트를 더 해야 하며, 목표 수치에 도달하도록 테스트 케이스를 보강해야 한다.

4.1.4 자료흐름 테스팅을 통해 해당 소프트웨어 소스코드에서 자료의 정의/사용 정보를 분석하여 자료의 흐름을 추출해야 하며, 소스코드 내에 특정 변수의 정의와 사용에 근거하여 테스트 수행 품질을 평가해야 한다.

4.1.5. 자료흐름 테스팅에서 All-Def 적합성 기준과 All-Uses 적합성 기준 그리고 All-DefUse Paths 적합성 기준에 대한 커버리지를 측정해야 한다.

4.1.6. All-Def는 소스코드 내의 정의문들을 모두 실행했는지 여부를 평가하는 것이고,

All-Uses는 특정 변수에 대해 사용이 일어나는 부분이 여러 곳일 수 있는데 실제 프로그램 실행 중에 모두 실행되었는지 여부를 판단한다. All-DefUse Paths는 프로그램 내에 특정 변수가 정의되고 사용되는 모든 경로를 추적하여, 모두 실행되었는지를 판단하는 것을 말한다.

4.2. 성능 테스팅

4.2.1. 성능 테스팅을 통해 해당 소프트웨어 시스템이 정의된 성능요구조건을 만족하는지를 확인해야한다.

4.2.2. 해당 소프트웨어에 평균부하 및 과부하를 적용한 후, 타겟에서 소프트웨어의 성능을 측정하도록 한다.

4.2.3. 성능 테스팅을 통해 해당 소프트웨어의 동적 기능시험 항목으로서 과부하·스트레스 시험, 응답시간 및 메모리 제한 시험 등을 수행하여야 한다.

5. 기능 테스팅

5.1. 기능 요구사항 테스팅

5.1.1. 소프트웨어의 기능 요구사항들에 대해 기능을 확인할 수 있는 Test Case를 생성할 수 있어야 하고, 각 Test Case의 수행 결과가 모두 만족하는지 여부를 확인해야 한다.

5.2. 동치 영역 분석 및 경계값 분석 테스팅

5.2.1. 동치 영역 분석 및 경계값 분석 테스팅을 통해 해당 소프트웨어가 초기 요구한 사용자 요구사항을 만족하는지 여부에 대해 확인해야 한다.

5.2.2. 시험대상체계가 처리 가능한 입력데이터의 분기 정보에 대해 동치 영역 분석을 수행하여야 한다. 분석 정보를 바탕으로 Test Data를 생성하고, 생성한 Test

Data를 조합하여 Test Case과 각 Test Case를 수행 시 기대되는 수행 결과값을 정의하여 동치 영역 분석 테스팅을 수행하여야 한다.

5.2.3. 시험대상체계가 처리 가능한 입력데이터의 분기 정보 및 동치 영역 분석 결과에 대해 경계값 분석을 수행하여야 한다. 분석 정보를 바탕으로 Test Data를 생성하고, 생성한 Test Data를 조합하여 Test Case과 각 Test Case를 수행 시 기대되는 수행 결과값을 정의하여 경계값 분석 테스팅을 수행하여야 한다.

5.3. 소프트웨어의 FTA 및 FMEA 수행을 통한 테스팅

5.3.1. 소프트웨어의 FTA 및 FMEA를 수행하여 각 Fault와 Failure Mode를 검증할 수 있는 Test Case를 개발하여야 한다. 또한 각 Test Case의 수행 결과가 모두 만족하는지 여부를 확인해야 한다.

6. 테스팅 결과의 문서화

6.1. 정량적 기준 제시

6.1.1. 메트릭의 복잡도, 응집도, 결합도 등의 정량적 평가기준

<table>
<tr><td>복잡도 측정 결과</td><td>
<table>
<tr><td colspan="5">SWSIL</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>NIL</td><td colspan="2">복잡도 1~50 허용</td><td colspan="2">복잡도 1~20 허용</td></tr>
</table>
Cyclomatic Complexity
참고 문서 : T.J. McCabe. "A Complexity Measure." IEEE Trans. on Software Engineering, Vol. SE-2, No. 4, Dec. 1976)
</td></tr>
<tr><td>응집도 측정 결과</td><td>
<table>
<tr><td colspan="5">SWSIL</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>NIL</td><td colspan="2">응집도 측정 권고</td><td colspan="2">응집도 측정 필수</td></tr>
</table>
LCOM4 (Lack of COhesion in Methods)
참고 문서 : Chidamber, S.R.; Kemerer, C.F. "A Metrics Suite for Object Oriented Design." IEEE Transactions on Software Engineering, Vol. 20, Issue 6, Jun. 1994
</td></tr>
<tr><td>결합도 측정 결과</td><td>
<table>
<tr><td colspan="5">SWSIL</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>NIL</td><td colspan="2">결합도 측정 권고</td><td colspan="2">결합도 측정 필수</td></tr>
</table>
</td></tr>
</table>

	참고 문서 : I. Sommerville "Software Engineering", Addison Wesley

6.1.2. 테스트 커버리지의 정량적 평가기준

블록 커버리지(Block Coverage)	SWSIL 0 | 1 | 2 | 3 | 4 NIL | 블록 커버리지 100% 만족 필수 | 블록 커버리지 100% 만족 권고 참고 문서 : ISO/DIS 26262-6
분기 커버리지(Branch Coverage)	SWSIL 0 | 1 | 2 | 3 | 4 NIL | 분기 커버리지 100% 만족 권고 | 분기 커버리지 100% 만족 필수 참고 문서 : ISO/DIS 26262-6
변경 조건/결정 커버리지 (MC/DC : Modified Condition/Decision Coverage)	SWSIL 0 | 1 | 2 | 3 | 4 NIL | 변경 조건/결정 커버리지 100% 만족 권고 | 변경 조건/결정 커버리지 100% 만족 필수 참고 문서 : ISO/DIS 26262-6
자료 흐름 커버리지 (Data Flow Coverage)	SWSIL 0 | 1 | 2 | 3 | 4 NIL | 자료 흐름 커버리지 측정 권고 | 자료 흐름 커버리지 측정 필수 참고 문서 : Khedker, U. P. Sanyal, A. Karkare, Bageshri. "Data Flow Analysis: Theory and Practice", CRC Press (Taylor and Francis Group)

6.2. 테스팅 결과 보고서 작성

6.2.1. 테스팅 결과 보고서는 철도 소프트웨어 테스팅의 결과를 의뢰자 및 검토자에게 명확히 이해시키는 것을 목적으로 작성된다.

6.2.2. 철도SW의 테스팅 결과 보고서는 소프트웨어 테스트 문서화 표준(Stadard for Software Test Documentation - IEEE 829)를 기반하여 작성되어야 하며, 다음의 장절을 반드시 포함하고 있어야 한다.

- 테스트 계획(Test Plan)

- 테스트 케이스 설계/테스트 설계(Test Case Specification/Test Design Specification)
- 테스트 절차(Test Procedure Specification)
- 테스트 수행 기록(Test Log)
- 테스트 실패 항목 분석서(Test Incident Report)
- 테스트 요약 보고서(Test Summary Report)

■

제4절 안전성 평가기술 적용을 위한 안전성 평가용 대상 열차제어시스템 보완 제작

	검증계획서 **(Verification Plan)**	**ID No :** **TC - SR07 - SSR02 - 2009** 작성일 : 2010. 06. 18 수정일 :

7. 프로젝트는 열차제어시스템 안전성 평가 및 사고방지기술 개발을 위한 평가대상 열차제어시스템을 설계 제작하여야 한다.

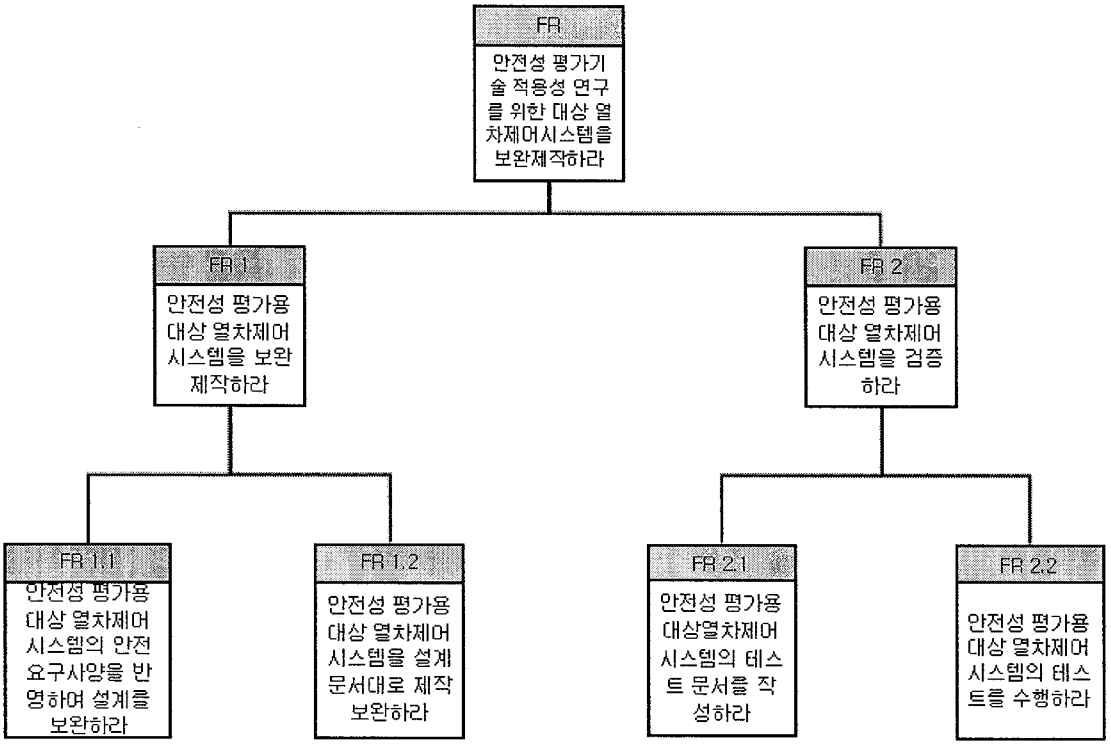
7.2 프로젝트는 안전성 평가기술 적용을 위한 평가대상 열차제어시스템을 설계하고 제작하여야 한다.

입력물 :	**업무 :**	**출력물 :**
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 안전성평가용 대상 열차제어시스템 설계 문서 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 2.1 단순 상황분석 - 5.3 기능시험	- SE 검증	- 수정 VRTM - 검증결과표

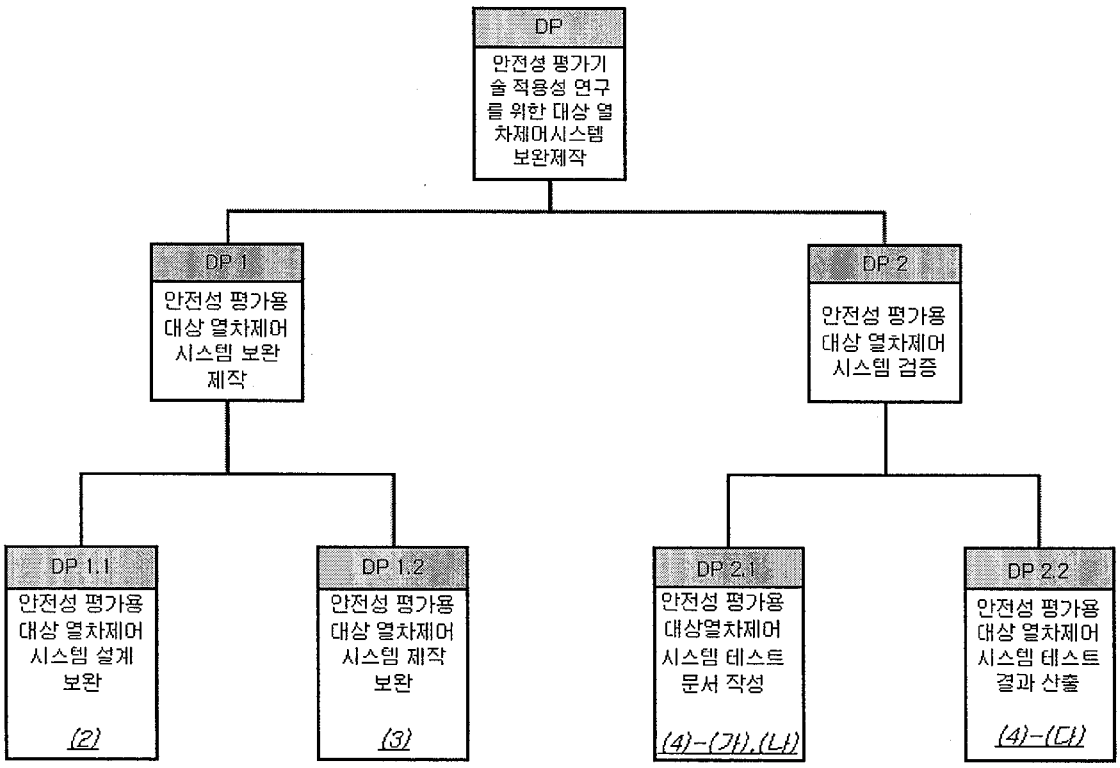
Verification Specification (검증기준) :

1. 안전성평가용 대상 열차제어시스템이 요구사양 및 설계문서대로 보완 제작되었는가?
2. 안전성평가용 대상 열차제어시스템의 검증을 위한 테스트는 수행되었는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

안전성 평가기술 적용을 위한 안전성 평가용 대상 열차제어시스템 보완제작은 『SR 7. 프로젝트는 열차제어시스템 안전성 평가 및 사고방지기술 개발을 위한 모의열차제어시스템을 설계 제작하여야 한다.』 중 **『SSR. 7.2. 프로젝트는 안전성 평가기술 적용을 위한 안전성 평가용 대상 열차제어시스템을 설계하고 제작하여야 한다.』**에 해당하는 내용이다. 당해년도 과제에서는 안전성 평가용 대상 열차제어시스템의 보완제작 내용과 테스트 수행 결과를 제시하였다.

나. 설계기준

- 철도종합안전기술개발사업, '열차제어시스템 안전성능 평가 및 사고방지기술 개발 연구보고서', 2009. 8.
- 해외 통신기반 열차제어시스템 시험사양 참조(Alcatel사)
- 'ERTMS Safety : ERTMS/ETCS-Class 1 SRS'문서 참조(ADTRANZ, ACLATEL, ALSTOM 등)
- 'ERTMS Safety : ERTMS/ETCS-Class 1 ETCS Application Level 1-Safety Analysis' 문서 참조
- 'ERTMS Safety : Safety Requirement for the technical interoperability' 문서 참조
- 'IEEE System 및 Software 개발 관련 규격, IEEE Computer Society' 규격
- '신호제어시스템(Signalling Control System)', 2003년, 김영태
- '진로제어시스템(연동)', 2005년, 유광균

다. 검증 방법에 따른 증거 자료

열차제어시스템 안전성 평가기술 적용을 위해 본 절에서는 당해연도 연구수행 내용인 안전성 평가용 대상 열차제어시스템의 보완제작과 테스트 수행에 대한 내용을 기술하였다. 안전성 평가용 대상 열차제어시스템 보완제작을 위해 요구사양을 반영한 설계문서에 대한 보완이 완료되었으며, 제작에 대한 보완작업 또한 수행하

였다. 이에 따른 안전성 평가용 대상 열차제어시스템의 검증을 위한 테스트 문서 산출과 테스트를 수행하였다.

- 보완된 안전성 평가용 대상 열차제어시스템 설계 문서
- 테스트 관련 문서

라. 성과물의 내용 및 결과

(1) 안전성 평가용 대상 열차제어시스템

(가) 안전성 평가용 대상 열차제어시스템 개요 및 구성

안전성 평가용 대상 열차제어시스템은 진로제어 및 열차간격을 제어하는 시스템인 CRD와 CRD의 기능을 구현하기 위해 필요한 시뮬레이터 장비로서

- 자동열차감시장치인 ATS(Automatic Train Supervision)시뮬레이터
- 실제 모의열차운행을 위해 차상장치 기능을 구현하기 위한 차상시뮬레이터
- 현장의 선로변에 설치되어 선로전환기를 제어하는 모의 현장신호제어 설비인 신호설비제어시뮬레이터 및 신호설비(선로전환기)시뮬레이터로 구성된다.

요구되는 기능들의 특성상, 시스템은 부분적으로 차상과 지상 장치에 설치되어야 한다. 따라서 시스템은 지상 및 차량 시스템으로 구성되며, 지상시스템은 다음과 같은 장비로 구성된다.

- CRD : 열차방호를 위한 열차간격제어 및 진로명령처리와 같은 연동기능을 수행한다.
- ATS시뮬레이터 : 열차운행 및 현장신호설비상태를 감시하고 열차운행조정 명령 및 현장신호설비제어 명령 기능을 수행한다.
- 신호설비시뮬레이터 및 신호설비제어시뮬레이터(현장신호설비 및 제어장치) : 선로전환기 전환제어 및 전환 기능을 수행한다.

차상시스템은 하나의 장비에 다음과 같은 기능을 하는 시스템으로 구성된다.

- 차상ATP시뮬레이터(자동열차보호장치) : 자동열차보호장치는 열차 운행의 안전성을 보장하여야 하며, 열차의 안전과 관련된 vital 기능을 수행하는 장치로 열차의 운행에 대한 감시와 제어기능을 제공한다.

- 차상ATO시뮬레이터(자동열차운행장치) : 자동열차운행 시스템은 완전 자동열차 운전을 수행 하여야 하며, 자동열차보호(ATP)의 감시 하에 속도제어, 정위치 정차 및 출입문 제어와 같은 Non-vital 기능을 수행한다.

다음은 시스템 전체구성에 대한 블록 다이아그램을 나타내었다.

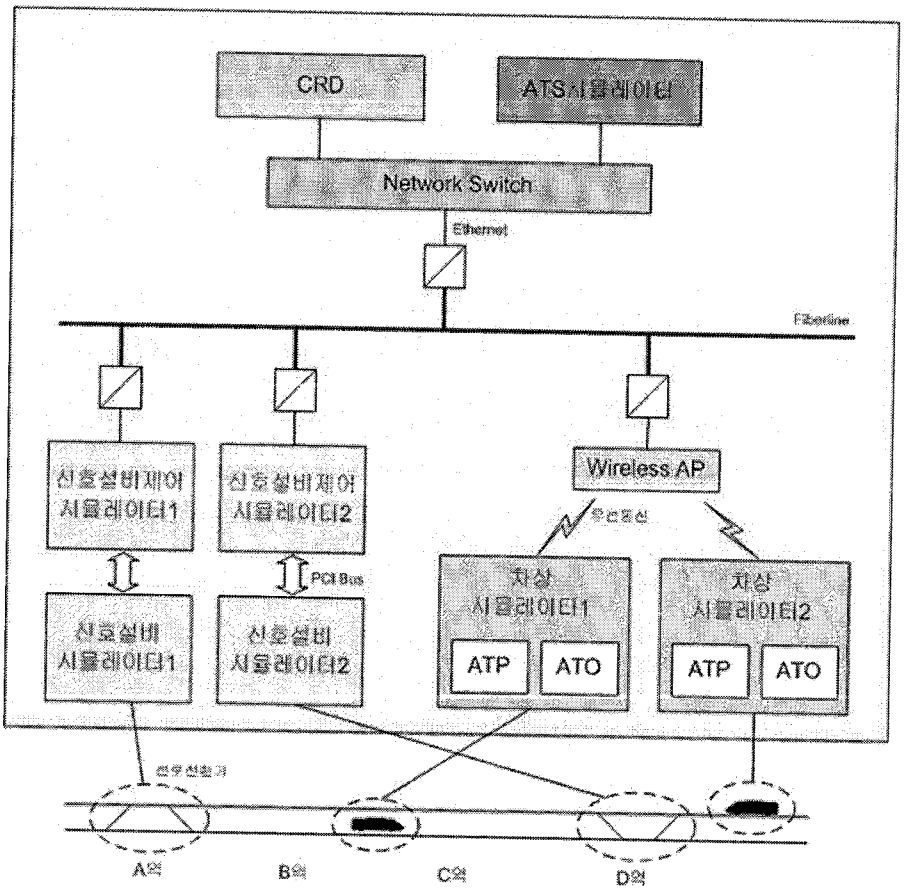


그림 3.4.1 안전성 평가용 열차제어시스템 구성도

(나) 안전성 평가용 대상 열차제어시스템 기능

과제수행을 위한 안전성 평가용 대상 열차제어시스템은 진로제어 및 열차간격을 제어하는 시스템으로 구성하며, 이를 위해 다음과 같은 시스템의 기능이 요구된다.

- 진로제어와 같은 연동기능과 열차간격제어를 위한 지상자동열차보호(CRD)
- 열차운행제어와 감시를 위한 자동열차감시(ATS시뮬레이터)
- 열차보호와 운행을 위한 차상 자동열차보호/자동열차운행(차상시뮬레이터)

- 선로전환기와 같은 현장신호설비시스템(신호설비제어/신호설비 시뮬레이터)

시스템은 정상상태에서 완전자동모드로 동작되도록 설계되며 운전자 없이 열차를 운전하기 위한 완전자동모드에서는 새로운 장비를 추가하지 않고도 운전자에 의한 수동모드와 같은 수준의 안전성을 가지고 완전히 자동으로 운행된다. 이와 같이 안전성평가용 대상 열차제어시스템은 주 시스템인 CRD시스템과 주변 시뮬레이터로 구성되며, CRD의 주요 기능은 다음과 같다.

CRD시스템은 ATS시뮬레이터로부터 수신되는 진로설정 제어명령 처리 등 현장 제어명령 처리 기능, 현장 신호설비상태를 수신하여 처리하는 기능, 차상시뮬레이터(ATP)로부터 열차운행정보를 수신하여 처리하는 기능, 차상시뮬레이터(ATP)의 모의 열차운행을 위한 열차간격제어 처리 등과 같은 열차자동방호 기능 등을 수행한다. CRD 시스템의 핵심 기능을 담당하는 CPU 모듈은 다음 그림과 같이 진로제어와 같은 연동기능을 담당하는 ICM과 열차간격제어와 같은 열차방호기능을 담당하는 DCM으로 구분되며 각각의 기능은 다음과 같다.

표 3.4.1 CRD 주요 기능

ICM	
주요 기능	- 연동기능 열차이동과 충돌, 탈선을 방지하기 위한 연동기능을 수행하며, 이를 위해 ATS시뮬레이터로부터 진로제어/선로전환기전환 명령을 수신하여 정보의 유효성을 판단한 후 유효할 경우 해당 진로제어/선로전환기전환을 위한 처리를 수행한다. - 진로설정/취소명령처리 - 전체진로취소명령처리 - 개별 선로 전환기제어명령처리
검증 기능	- 연동처리 검증 외부로부터 수신한 진로 및 선로전환기 정보와 관련되어 연동처리를 수행해야 하며, 이러한 연동처리를 위해 다음 상태에서의 쇄정상태를 항상 검증한다. · 블록쇄정 · 진로쇄정 · 보류쇄정 · 선로전환기 위치검지쇄정 - 진로 검증

	진로처리를 위해 다음과 같은 형태로 유효성검사를 통한 진로처리검증기능을 수행한다. 진로설정 시에는 · 진로 설정이 유효한 진로 설정인가? · 유효한 열차 ID에 대해 진로가 설정 되었는가? ·· 충돌하는 진로설정이 있는가? · 동일한 열차 ID에 대해 설정된 다른 진로가 있는가? 에 대한 검증기능을 수행한다. 진로취소 시에는 · 진로가 유효한 ID를 가지고 있는가? · 유효한 열차 ID에 진로 설정이 되어 있는가? · 설정되어 있는 진로인가? 에 대한 검증기능을 수행한다. - 선로전환기 전환 검증 선로전환기 전환 처리를 위해 다음과 같은 형태로 유효성검사를 통한 선로전환기 전환 처리검증기능을 수행한다. · 관련 블록이 폐쇄상태이면 선로전환기 전환 불가 · 관련 블록의 점유 상태 검사하여 점유상태이면 선로전환기 전환 불가 · 열차 이동을 위해 예비된 상태이면 선로전환기 전환 불가 · 선로전환기 고장 상태이면 선로전환기 전환 불가 에 대한 검증기능을 수행한다.
DCM	
주요 기능	- 열차간격제어 DCM은 안전한 열차간격을 확보하기 위해 최악의 고장 조건하에서도 열차를 보호할 수 있는 충분한 안전거리를 확보한다. 즉, DCM은 고정된 block 길이에 기초해서 최소한으로 필요한 안전 제동거리를 확보함으로써 열차의 간격을 안전하게 유지한다. 본 시스템에서 열차의 안전한 열차간격유지는 블록에 설정되는 적색, 황색, 녹색 허용이동권한(PMA) 이동모드신호를 이용하여 이루어진다. - 열차위치확인(결정) 열차의 이동은 블록 단위로 이루어 지며, DCM은 차상시뮬레이터에서 전송된 정보 중 열차위치정보를 찾아내어 현재 열차의 위치를 확인하고 결정한다. - 열차이동/방향 감시

	DCM은 수신한 현재열차위치정보와 기존에 DCM이 저장하고 있던 해당 열차의 열차위치정보를 비교 분석하여 해당 열차가 열차진행방향으로 정상적으로 이동하고 있는지를 감시한다. - 블록 개방/폐쇄 DCM은 ATS 시뮬레이터에서 블록폐쇄 명령을 전달받으면 해당 블록을 폐쇄한다. DCM은 열차를 분실한 경우와 같은 비상상황의 경우 열차보호를 위해 관련된 블록을 폐쇄한다. ATS 시뮬레이터가 블록 개방 명령을 DCM 에게 전송하면 DCM 은 해당 블록 상태를 확인하여, 블록개방이 가능한 경우 해당블록을 개방한다.
검증 기능	- 열차위치검증 다음의 열차위치 적합성 검사를 통하여 열차의 위치가 적절한지를 점검하고 열차를 추적하는 기능을 수행한다. · 열차가 최대 속도에서 진행시간의 3초 이내에 점유할 수 있는 모든 가능한 블록에 열차가 위치해 있는지 검사 · 마지막 보고된 열차 위치로부터 3초 안에 현재 열차 위치를 보고 받지 못하면 열차위치 적합성 검사는 실패 · 보고된 열차 이동 방향이 마지막 보고된 열차 위치에서 현재 보고된 열차 위치로 이동하는 이동 방향과 일치 하지 않을 때 열차위치 적합성 검사는 실패 • 블록상태검증 열차에 의해 블록은 점유, 해정, 검지손실의 3가지 상태를 가지며 DCM은 3가지 상태에 대한 검증을 수행한다. · 점유상태 : 블록에 열차가 점유, 열차가 열차위치 적합성 검사를 실패할 경우 · 해정상태 : 열차가 통과한 블록, 열차위치 적합성 검사를 통과할 경우 · 검지손실상태 : 열차와의 통신이 15초 이상 두절될 경우 • 블록개방검증 DCM은 블록 개방을 수행하기 전 반드시 다음 사항을 먼저 확인하여 해당 사항이 존재하지 않음을 검증한 후에 블록 개방이 이루어지도록 한다. · 관련 선로전환기가 존재하는 경우 선로전환기 상태가 정상인 경우에만 블록을 개방 · 인접블록에 열차가 존재하는 경우 블록 개방되지 않음 · 동일블록에 열차가 존재하는 경우 블록 개방되지 않음

	· 열차와의 통신이 15초 이상 두절되어 검지손실로 설정된 블록은 개방되지 않음 · 열차위치 적합성 검사에 실패한 블록은 개방되지 않음

(2) 안전성 평가용 대상 열차제어시스템 설계내용 보완

안전성 평가용 대상 열차제어시스템을 제작하기 위한 설계 문서는 CENELEC 규격에 의해 시스템 정의 문서를 바탕으로 7개 주요 문서와 첨부 문서가 산출되었으며, 당해연도에는 각각의 문서에 대한 전년도 내용을 보완 작성하였다.

- 시스템 요구 사양서
- 시스템 구조 사양서
- 소프트웨어 요구 사양서
- 소프트웨어 구조 사양서
- 소프트웨어 설계 사양서
- 소프트웨어 모듈 설계 사양서
- 소프트웨어 모듈 시험 사양서

(가) 시스템 요구 사양서

시스템 요구 사양서는 향후 설계 내용이 시스템/하위시스템/장비 요구사양서 내에서 어떻게 운영적, 기능적 요구사항이 설계에 만족하게 되었는지를 보여주는 문서로서 그 기준이 된다. 따라서 향후 설계 문서에는 요구사양서에서 언급된 운영적, 기능적 요구사양을 충족시키기 위한 내용이 기술되어야 한다. 시스템 요구사양서에는 다음 두 부분이 고려되어져야 한다.

- 안전과 관련 없는 요구사항 (운영, 기능 요구사항 포함)
- 안전과 관련된 요구사항

안전과 관련된 요구사항은 일반적으로 안전 요구사항이라고 명하며 각각의 사항은 각각의 안전 요구사양서에 포함 될 수 있다. 결국, 시스템 요구 사양서는 안전 요구사항 및 비안전(Non-safety) 요구사항을 다뤄야만 한다. 안전 요구사항의 자세한 내용은 시스템 안전 요구 사양서에 설명되어야 한다. 시스템 요구 사양서의 목적은 프로젝트 개발에 있어 다음의 사항들을 설명하는 것이다.

- 기능적 요구사항 (안전 및 비안전)

- 비기능적(Non-functional) 요구사항
- RAMS
- 인터페이스
- 제한(Constraints)
- 물리적 · 기술적

본 과제에서 산출된 시스템 요구 사양서는 다음의 구조를 갖추어 작성되었다.

- EN 규격과 같은 표준규격과 일치되도록 작성
- 문서 내용이 일관성이 있어야 하며 모순되지 않고 불분명하지 않도록 작성
- 이후 개발 단계에 적합하도록 작성
- 문서에 요구사항, 주석, 설명을 분명히 열거하고 표시되도록 작성
- 비안전(Non safety) 요구사항과 안전 요구사항간에 구분이 되도록 작성
- 시스템 요구사항의 적합성을 검증하기 위해 추적성에 대한 절차가 이루어지도록 작성
- 잘 정의된 인터페이스가 표시되도록 작성
- 시스템의 응용 조건이 상세히 표시되도록 작성

시스템 요구사양서의 구조는 아래의 표를 고려하여 작성한다.

표 3.4.2 시스템 요구 사양서 구조

구조		내용
일반 정보	목적	종합적인 정의는 문서의 내용에 따른 성과를 이루기 위한 목적을 얻는 것에 있다.
	범위	문서를 적용하고 철도수송분야 시스템이 사용될수 있도록 시스템을 명확히 해야 한다.
	관련 문서	관련문서(규격,법률,규정,사양서 등)들을 리스트화한다. 리스트화된 문서들은 참고하기에 유용하며 문서에 포함된 정보를 뒷받침 할 수 있는 것들이어야 한다. 리스트화된 각 문서는 최종버전이나 코드, 발행일에 따른 개정버전의 문서 안의 참조를 가르키는 번호를 포함해야만 한다.
	정의, 약어	문서에서 가장 자주 되풀이 되는 단어와 문서의 이해를 위해 유용하게 사용되는 정의와 약어의 리스트화가 필요하다.

요구사항	입력 요구사항	수명주기 1,2,3단계 (혹은) 모든 문서와 활동의 정확한 개발을 위해 필요한 모든 자료들을 바탕으로 문서들을 명확히 하는 것이 필요하다.
	시스템 정의	목적과 범위를 포함한 시스템을 정의하는 것이 필요하다.
	임무 개요	시스템의 최대 운행 성능 요구사항을 정의하는 것이 필요하다.(예: 연속 서비스, 하루/시간 당 요구/운행 숫자 등)
	기능적 요구사항	한계치와 일반값을 포함하여 시스템이 수행해야만 하는 기능들의 정의가 필요하다.
	RAM 요구사항	시스템에 의해 수행되는 각각의 기능에 대하여 시스템이 갖추고 실행해야하는 (필요시) RAM 수치(혹은 전략이나 구조)의 정의가 필요하다.
	안전 요구사항	시스템에 의해 수행되는 각각의 안전 기능들은 안전무결성등급에 따라 설계되고 개발된 기능에 대한 안전 요구사항의 정의가 필요하다.
	진단 요구사항	시스템의 유지보수성, 가용성의 개선을 위해 사용되는 진단 기능 (예: 시스템 로그와 에러검출)에 대한 요구사항의 정의가 필요하다.
	논리적 뒷받침 문서	시스템개발을 위해 사용되는 (인력,기술, 기계) 자원의 요구사항의 정의가 필요하다.
	인터페이스 요구사항	시스템간의 연결을 위한 다른 시스템들 사이의 인터페이스의 정의가 필요하다. (전압 레벨, 통신 프로토콜 등 포함)
	운행환경	본 주제에 관한 적절한 EN 참조를 통해 시스템이 설치될 운행 환경의 정의가 필요하다.

(나) 시스템 구조 사양서

시스템 구조 사양서에는 어떻게 규정된 안전 기능 요구사양이 설계에서 충족시킬 수 있는 가가 기술되어야 하며 다음 사항에 따라 작성되어야 한다.

- '기능적 안전' 및 '안전 무결성'사항을 시스템 구조 사양서에서 고려
- 시스템의 경계에 대해 시스템 상에서 명확하게 구분
- 시스템 요구 사양서와의 일관성 확보
- 시스템 요구사항에 부합되는지의 확인(Verification)을 위한 추적성 확보
- 별도의 장이나 절에서 시스템 외부 다른 시스템과의 물리적, 논리적 독립성에 대한 요약 설명
- 개발 및 확인에 대해 비 안전 요구사항과 안전 요구사항간의 구별에 대한 명시

(다) 소프트웨어 요구 사양서

소프트웨어 요구사양서는 요구되는 특성을 개발하는 절차가 아닌 개발되는 소프트웨어의 특성을 표현해야 하며 다음 사항을 포함해야 한다.

- 기능성
- 신뢰성 및 유지보수성
- 안전성
- 효율성
- 유용성
- 이식성
- 시스템 요구 사양서 기능과의 일관성
- 기능들에 대한 요구사항을 완전하게 규정
- 향후 데이터 보호 혹은 시스템 무결성에 대한 감시(예를 들면 자기시험)에 대한 기능 등을 필요시 규정
- 시스템 장애와 관련된 소프트웨어 요구사항 명시(기능저하 모드 혹은 안전상태로의 진입 및 유지)
- 시스템에서 소프트웨어 수준 혹은 시스템 요구사양서 기능들에 연결이 되는 요구사항들에 대한 정제(추적성)
- 데이터 준비/시스템 엔지니어링(데이터 및 절차)에 대한 요구사항들에 대한 명시
- 시스템 수명 주기 동안 모두에게 이해 가능하도록 작성
- 모든 현존하거나 계획 중인 인터페이스, 운영자와 함께 내부 혹은 외부의 장비를 포함하여 명시
- 모든 운영 방법과 관련된 것을 포함
- 특정 장애 동작에 대해 모든 동작 방법을 포함
- 모든 하드웨어와 소프트웨어간의 모든 제한을 포함
- 모든 소프트웨어의 자가 점검과 하드웨어 점검을 포함
- 기능의 정기적인 시험을 포함
- 시스템 운영 중 안전 기능의 시험 능력을 포함
- 시스템 안전 무결성과 관련한 모든 기능을 포함
- 비안전 관련 기능들을 포함

- 시스템 수명주기 동안에 요구사항을 추적 가능하도록 작성
- 추적 불가능한 구성요소는 시스템 안전 혹은 무결성과 관련이 없음을 증명

(라) 소프트웨어 구조 사양서

소프트웨어 구조사양서는 모든 하드웨어와 소프트웨어 상호 영향의 중요함에 대해 정의, 평가가 이루어져야 하며 이를 상세히 설명해야 한다. 이런 사항은 요구되는 SIL 등급에 따라서 고려될 수 있다. 소프트웨어 구조 사양서는 다음의 3가지 주된 목적을 가지고 작성된다.

- 시스템 구조에 의한 소프트웨어 요구사항의 검토
- 안전을 위한 하드웨어와 소프트웨어간의 상호작용의 감정과 평가
- 사전 정의 되어있지 않은 디자인 방법의 선택

또한, 소프트웨어 구조사양서는 다음의 요구사항을 참조하여 작성된다.

- 신규 혹은 기존의 가용할 수 있는 소프트웨어의 할당 선언(ex. COTS 소프트웨어의 경우)
- 데이터베이스 구조에 대한 요구사항 명시
- 시스템 요구 사양서 및 소프트웨어 요구 사양서와 일관성
- 모순성의 배제
- 제공자와 개발자에 의해 확립되고 기술
- 요구된 소프트웨어 안전무결성등급에 따라 소프트웨어 요구사양서에 의한 시행 가능성을 고려하여 작성
- 소프트웨어 요구사양 및 SwSIL 만족에 따른 적합성의 정당함 증명
- SwSIL에 따라 소프트웨어 개발 전략을 파악
- SwSIL에 따라 안전 소프트웨어 요구사양의 기술과 측정의 선택이 정당함을 증명
- 모든 하드웨어와 소프트웨어의 구체적인 상호작용을 포함
- 모든 소프트웨어 요소들에 대하여 다음의 사항들을 파악
  · 새로운 것, 이전에 있던 것 혹은 독점적인 것인가?
  · 사전 확인된 것과 확인 환경
- 모든 소프트웨어 요소들에 대하여 SwSIL 감정 수행
- COTS 소프트웨어는 다음 사항들 이후에 사용

· 확인
· 가능한 장애의 분석
· 장애에 대한 탐색 및 보호 전략의 정의
· 보호 전략의 확인
· 에러 로그의 검토
· COTS 소프트웨어의 기본적인 기능만을 사용

- 사전 개발된 소프트웨어의 명확한 감정과 문서 첨부
- 소프트웨어의 안전 관련 부분 최소화
- 장애 회피와 장애 운용 전략 사이의 균형이 정당함을 증명

(마) 소프트웨어 설계 사양서

소프트웨어 설계 사양서는 소프트웨어 모듈 설계 사양서 및 소프트웨어 모듈 시험 사양서를 갖는 각각의 모듈을 기반으로 소프트웨어 설계의 내용이 설명되어야 하며 다음과 같은 목적을 가져야 한다.

- 소프트웨어 요구사양서와 소프트웨어 구조 사양서로부터 정의된 소프트웨어 안전 무결성 등급에 맞도록 설계하고 시행하는 것
- 분석, 시험, 검증, 유지보수가 가능한 소프트웨어를 만드는 것. 개개의 고려사항은 설계와 개발을 하는 동안에 결과 시스템을 확실히 하고 소프트웨어가 최초에 쉽게 시험 가능하도록 하기 위해 검증과 시험시에 제시하는 것
- 확인, 검증, 평가와 유지보수를 돕는 소프트웨어의 전체의 수명주기동안 소프트웨어 안전무결성 등급을 위한 언어와 컴파일러를 포함한 최적의 방법을 찾아내는 것
- 소프트웨어의 완성 수행

소프트웨어 설계사양서는 아래의 요구사항을 참조하여 작성된다.

- 시스템 요구 사양서 및 소프트웨어 요구 사양서 및 소프트웨어 구조 사양서와 일관성
- 모순성의 배제
- 소프트웨어 도구 및 코딩 규격 목록화
- 데이터 베이스 설계 내용

- 소프트웨어의 절차 우선순위 및 주기는 함께 표현되어야 하며 종속관계 혹은 상호 관계 설명
- 개발되는 소프트웨어는 가능한 적고 간단하게 명시
- 소프트웨어 설계사양서는 다음 내용을 포함하여 작성
  · 소프트웨어 요소들의 소프트웨어 구조사양서와 SwSIL과의 부합성
  · 환경과의 인터페이스
  · 요소들 간의 인터페이스
  · 자료 구조
  · 요구사항의 구분
  · 주요 알고리즘과 경로
  · 다이어그램
- 자기모순이 없으며 모듈의 코딩이 가능하도록 작성
- 각 소프트웨어 모듈은 읽기 가능, 이해 가능, 시험 가능하도록 작성
- 총 소프트웨어 수명주기 동안 장비, 방법, 언어와 컴파일러는 SwSIL에 따라 사용
- SwSIL에 따라 선택된 번역기/컴파일러는 다음 사항을 포함
  · 인지된 규격에 대한 확인 인증서
  · 목적의 적합성을 기술한 평가 보고서
  · 번역 에러 탐색에 공급하는 과정을 기본으로 한 여분의 사인 제어
- 언어의 선택
  · 프로그램 에러 판별의 편리함
  · 설계 방법과 일치하는 특징 지원
- 언어의 선택이 적합하지 않을 때, 소프트웨어 구조사양서 혹은 소프트웨어 품질보증 계획서에 대체 언어와 그것의 목적 적합성의 기술에 대한 정당성을 기록
- 소프트웨어 품질보증 계획서 참조 코딩 규격은 모든 소프트웨어의 개발에 사용되도록 작성
- 코딩 규격의 특성
  · 적합한 프로그램 실습
  · 소스 코드 문서화의 절차

· 금지된 비안전 언어의 특징

- 소스코드 내의 각 소프트웨어 모듈은 모든 모듈의 동일한 규격 양식에서 최소한 다음의 것들을 포함하도록 명시

· 저작자

· 구성도 연혁

· 짧은 설명

- SwSIL에 따라 설계 하며 다음 사항에 용이하도록 작성

· 추상성, 모듈방식과 다른 복잡성, 특성제어

· 다음 사항의 명확한 표현

· 기능성

· 정보 흐름

· 순서와 시기

· 협력

· 데이터 구조와 특성

(바) 소프트웨어 모듈 설계 사양서

소프트웨어 모듈 설계 사양서는 그 자체로 충분해야 하며 해당 모듈의 코딩 또한 가능하도록 작성한다. 소프트웨어 모듈설계사양서는 소프트웨어 설계사양서로부터 작성된다. 그러므로 소프트웨어 모듈설계사양서와 소프트웨어 설계사양서의 요구사항은 동일한 목적을 갖는다. 소프트웨어 모듈설계사양서는 소프트웨어 설계사양서 요구사항외 다음 사항을 참조하여 작성된다.

- 소프트웨어 설계 사양서와의 일관성
- 각 소프트웨어 모듈은 해독가능하고 이해가능하며, 시험 가능하도록 작성
- 요구사양의 기능과 소프트웨어 모듈사양서에 설명된 기능들에 대한 연결이 이루어지도록 작성

(사) 소프트웨어 모듈 시험 사양서

각각의 소프트웨어 모듈은 그에 해당되는 소프트웨어 모듈 시험 사양서를 가져야 한다. 이 시험들은 각각의 모듈이 그 의도하는 기능을 수행하는 것을 보여 주어

야 한다. 소프트웨어 모듈 시험 사양서는 요구되는 시험의 범위 정도를 정의해야 한다. 소프트웨어 모듈 시험 사양서는 다음 사항을 참조하여 작성된다.

- 모든 시험에 필요한 입력 데이터 추가
- 오류 보고 및 추적에 대한 적절한 방법 및 절차 정의. 설계 혹은 사양서의 오류의 경우(특히 안전과 관련된 오류) 문서를 포함한 소프트웨어 수명 주기의 어떠한 단계에서든 오류 정정 행위가 필요하며 안전과 관련된 오류에 대해서는 전문가 및 안전 관리자가 오류를 규정하고 이에 대한 분석에 참여하여 작성
- 시험을 선택할 때에 요구되는 시험 범위를 고려하여 작성
- 시험 범위의 필요 등급을 정의

(3) 안전성 평가용 대상 열차제어시스템 보완제작

안전성 평가용 대상 열차제어시스템은 안전성 활동을 수행하기 위해 제작되는 시스템으로서 전년도에 설계문서에 정의된 요구사양 및 기능을 구현해서 제작하였으며 당해연도에 제작 결과를 일부 보완하였다. 제작된 안전성평가용 대상 열차제어시스템은 아래 그림과 같다.

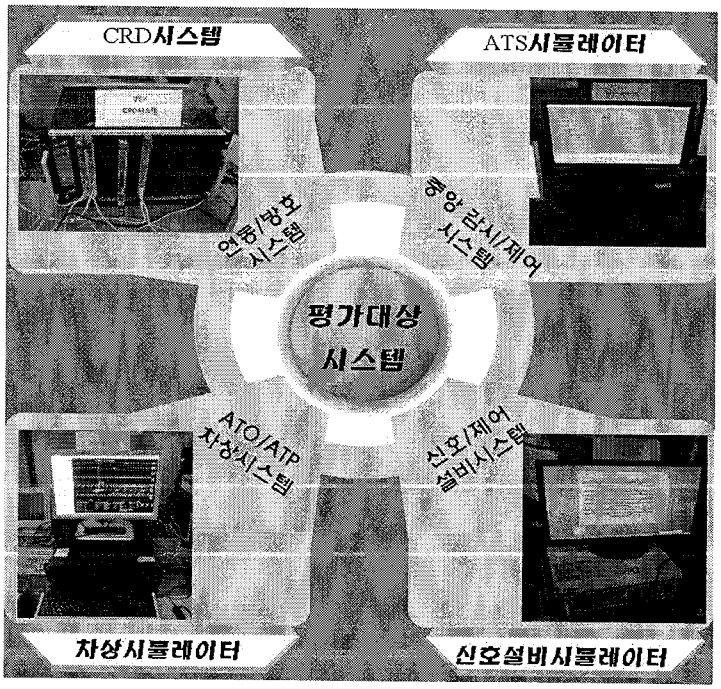


그림 3.4.2 제작된 안전성 평가용 열차제어시스템

안전성 평가용 대상 열차제어시스템은 안전과 관련된 안전요구사항에 대한 내용을 설계문서에 적용하고 적용된 내용에 따라 제작되어야 한다. 안전성 평가용 대상 열차제어시스템에 안전요구사항이 적용되어 제작된 주요 내용은 다음과 같으며, 당해연도에 안전요구사항을 다시 재확인하고 제작 결과를 보완하였다.

- 안전요구사항 1 : CRD시스템의 이중계 구성
  - CRD시스템은 Hot-stand by 이중계 시스템으로 구성하여 입,출력 데이터를 비교하여야 한다.
  - CRD시스템은 Redundant시스템으로 구성되어, 주계 장애 발생시 즉시 절체되어 안전성을 확보해야 한다.
  - 주계의 고장이 검지될 경우 부계에서 모든 처리 및 출력 전담하며, 데이터 비교 없이 단독으로 운영되어야 한다.
  - 제작 적용 내용

    CRD 시스템은 진로제어 및 연동 제어를 담당하는 ICM, 열차 간격 제어를 담당하는 DCM, 외부시스템과의 인터페이스를 담당하는 EIM, 그리고 각 모듈에 전원을 공급하는 전원모듈로 구성된다.

    CRD 시스템은 두 개의 시스템 단위로 구성된 Redundant 시스템으로서, 하나는 ON_LINE으로 동작하고 다른 하나는 STANDBY 시스템으로 동작하게 되며, 만약 ON_LINE 시스템에 장애가 발생할 경우 STANDBY 시스템이 즉시 ON_LINE 시스템으로 절체 되어 안정적으로 연속적인 기능을 수행하여야 한다. 이중계 구현을 위한 실시간 처리를 위해, 계 사이의 통신라인과 별개로 Monitor 라인을 두어 항상 다른 계의 상태를 확인하고, 계의 상태를 알려주도록 한다.ON_LINE 시스템과 STANDBY 시스템은 별개의 VME bus로 구성되어, 별개의 Sub-rack에 장착되며, 직렬 통신 또는 Ethernet을 통해 상호간의 Data를 교환할 수 있도록 구성한다. 이를 통해 양쪽 계의 입·출력 정보를 공유하도록 하여 입·출력 정보를 비교 처리할 수 있도록 구성하며, 비교된 정보가 동일할 경우에만 주계(ON_LINE)에서 정보를 출력하도록 한다.

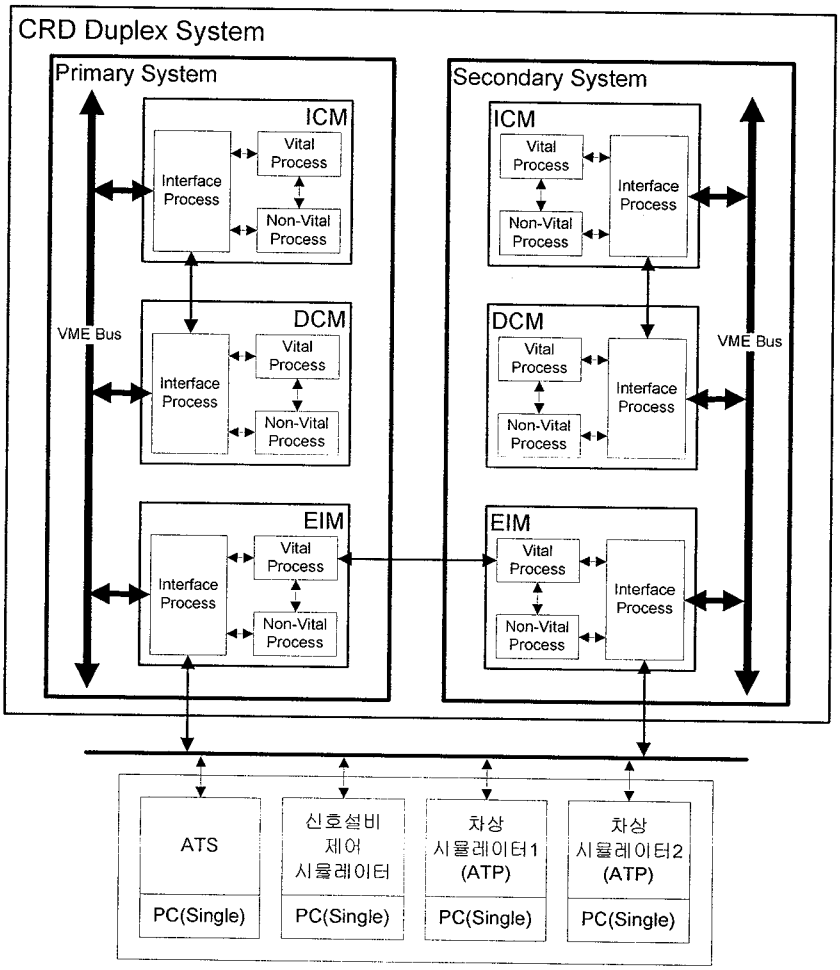

CRD Duplex System
Primary System
Secondary System
ICM
Vital Process
Non-Vital Process
Interface Process
DCM
EIM
VME Bus
ATS
PC(Single)
신호설비 제어 시뮬레이터
차상 시뮬레이터1 (ATP)
차상 시뮬레이터2 (ATP)

그림 3.4.3 이중계 구성

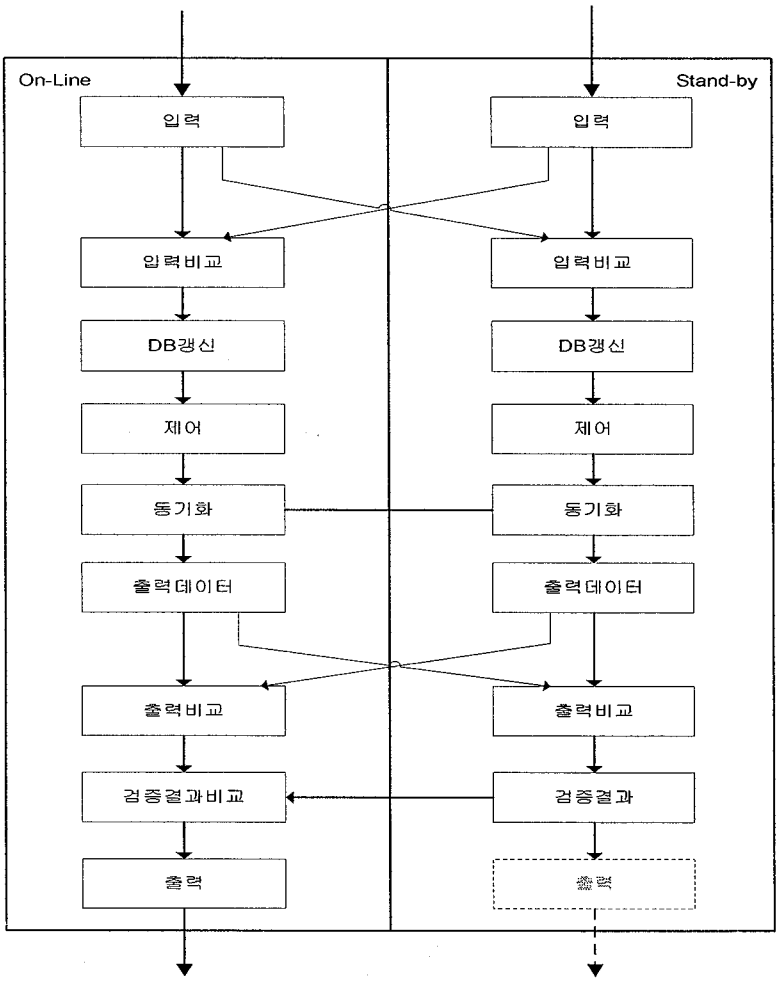


그림 3.4.4 데이터 비교 처리 흐름도

- 안전요구사항 2 : 신뢰성 있는 네트워크 구성
  - CRD와 주변시뮬레이터와의 인터페이스는 신뢰성이 보장되는 고속의 장거리 통신이 보장되어야 한다.
  - 광케이블을 이용하여 외부로부터의 Surger나 Noise같은 위험에 대비한다.
  - 케이블의 절손시에도 장치간 인터페이스가 가능하도록 구성한다.
  - 제작 적용 내용

    본 과제에서는 이런 위험을 방지하기 위하여 다음 그림과 같이 광스위치를 설치한 후 CRD와는 Network Switch를 통하여 연결시키고 주변시뮬레이터와는 광점퍼케이블을 이용하여 연결한다. 즉, 광스위치간 연결은 광점퍼케이블을 이용하여 연결한다. 또한 네트워크망을 Ring형으로 구성하여 광케이블

의 절손되었을 경우에도 장치간 데이터의 송·수신이 이루어지도록 구성한다.

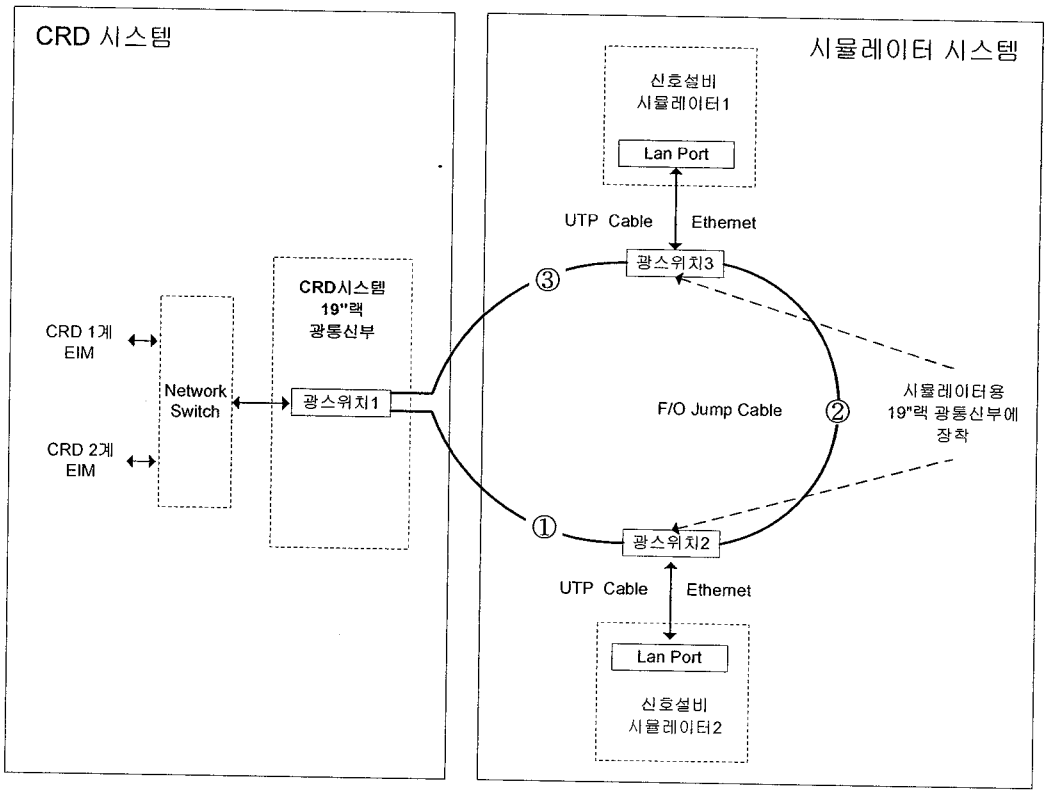


그림 3.4.5 광통신을 이용한 네트워크 구성도

광스위치 모듈간에는 주기적으로 Watchdog Packt을 전송하여 광점퍼케이블의 절손상태를 끊임없이 점검한다. 예를 들어 위 그림에서 광점퍼케이블①이 절손된 경우 데이터 전송은 광점퍼케이블②, ③을 사용하여 다음과 같이 이루어진다.

표 3.4.3 광케이블 절손상태에서 광통신 계통

장치간	기능(구성)
CRD → 신호설비제어시뮬레이터1	CRD → Network Switch → 광스위치1 → ③광점퍼케이블 → 광스위치3 → 신호설비제어시뮬레이터1
신호설비제어시뮬레이터1 → CRD	신호설비제어시뮬레이터1 → 광스위치3 → ③광점퍼케이블 → 광스위치1 → Network Switch → CRD
CRD → 신호설비제어시뮬레이터2	CRD → Network Switch → 광스위치1 → ③광점퍼케이블 → 광스위치3 → ②광점퍼케이블 → 광스위치2 → 신호설비제어시뮬레이터2
신호설비제어시뮬레이터2	신호설비제어시뮬레이터2 → 광스위치2 → ②광점퍼

→ CRD	케이블 → 광스위치3 → ③광점퍼케이블 → 광스위치1 → Network Switch → CRD

- 안전요구사항 3 : 신뢰성있는 전원 공급

  · 정전시 설치된 모듈이 정지되지 않고 정상적으로 동작할 수 있도록 한다.

  · 정전압, 정주파수, 무정전상태인 양질의 교유전원을 무중단 공급해야 한다.

  · 제작 적용 내용

  정전시 보상을 위해 축전지로부터 전원을 공급하는 ON-LINE방식의 충분한 정전보상시간을 갖는 무정전전원장치를 장착한다. 다음은 장착되는 무정전전원장치의 주요사양과 장착된 도면이다.

표 3.4.4 무정전전원장치 사양

No	항목	성능 및 규격
1	입력전압	·110V:80 ~ 138V, 220V:160 ~276V
2	입력주파수	·50 or 60 Hz ±3Hz
3	출력전압	·100/110/115/120/220/230/240V ±2%(정현파 출력)
4	배터리 보호 기능	·자동 Self-Test, 방전보호, 배터리 교환 지시기
5	과부하 탐지	·105% 부하일때 10초, 130% ±10% 부하일때 300ms
6	절체시간	·0ms
7	소음	·45dBA(기기 정면으로부터 1m)
8	LED 상태	·배터리 용량, 부하용량, 정전, bypass, Line 모드 표시
9	알람	·정전 감지후 4초마다 Beep 발생, 배터리 저전압시 1초마다
10	크기	·483 ´ 362 ´ 44mm

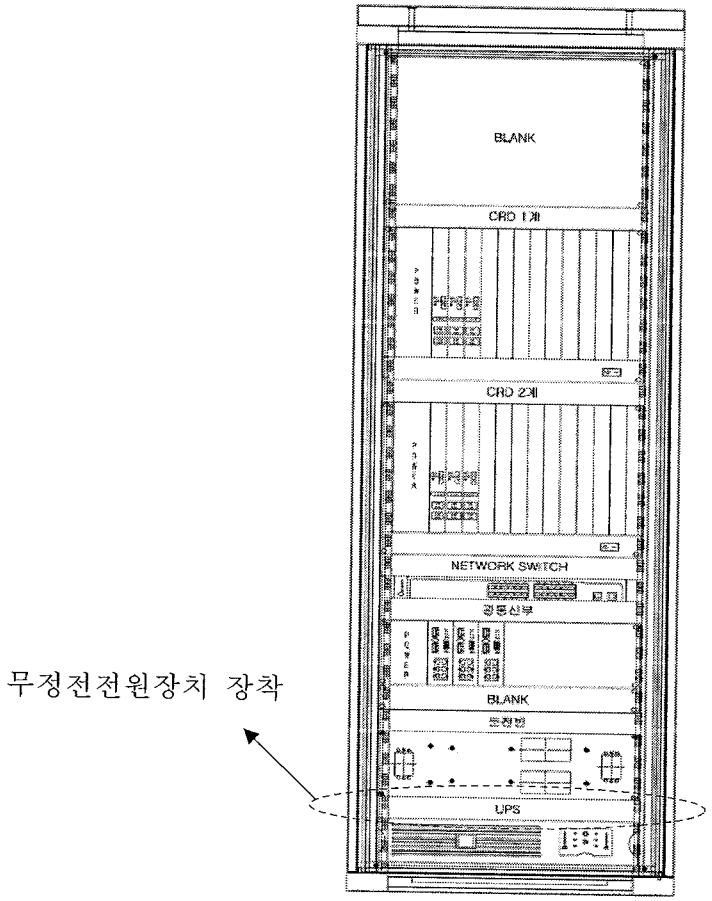


그림 3.4.6 무정전전원장치 장착

(가) 시험 수행을 통한 시스템 보완 제작

CRD시스템과 ATS시뮬레이터, 차상시뮬레이터 테스팅을 위한 시험절차서 및 체크리스트 그리고 시스템간 인터페이스 테스팅을 위한 시험절차서와 체크리스트 그리고 마지막으로 평가대상시스템의 운영을 위한 운영 시나리오 시험절차서 및 체크리스트를 작성하였으며 이를 토대로 평가대상시스템의 테스팅을 수행하였다. 또한, 이러한 테스팅 수행을 통해 여러 가지의 시스템 보완이 수행되었다. 이러한 테스팅과 시스템의 보완은 테스팅의 결과가 모두 close 될 때까지 반복적으로 수행되었다. 다음은 이러한 테스팅 과정에서 도출된 사항에 대한 시스템 보완 제작에 대한 몇 가지 예시 내용이다.

- CRD 이중계 구성 및 데이터입,출력 비교 모듈 수정 보완

  · CRD 1계(마스터)와 CRD 2계(슬레이브)간의 데이터 비교 처리과정 중 기존의 Serial 통신방식을 Reflective Memory(공유 메모리)에 의한 방식으로 수

정하여 처리 함

· Serial 방식을 통한 데이터 전송 오류 및 싱크 문제를 해결함

- ICM 진로 큐잉 작업 시 메모리 접근 에러 문제

· ATS 시뮬레이터에서 수신된 진로 제어 명령을ICM에서 진로 큐에 삽입 과정 중 메모리 접근 에러로 인한 오류 문제를 세마포어 설정으로 메모리 접근 차단

- DCM 블록 해제 시 PMA 설정 오류

· ATS 시뮬레이터에서 하나의 블록 폐쇄 후 블록 해제 시 PMA 설정은 올바르나 좌,우 블록에 연이어 블록 폐쇄 설정 한 후, 블록 하나에 블록해제 명령 시 각 연관 블록의 조건을 확인 후 PMA 설정하도록 함

- EIM 통신 모듈 수정

· 각 시뮬레이터와 통신 방식을 UDP 멀티 캐스트 방식은 동일하나 각 시뮬레이터와 1:1로 통신 하도록 설정함

- 차상 시뮬레이터 속도제한 오류 수정

· 차상 시뮬레이터 속도 제한 블록 점유 시 속도가 급격히 저하 되어지는 것을 서서히 감속하도록 설정함

- 차상 시뮬레이터 비상제동 설정 시 속도 오류

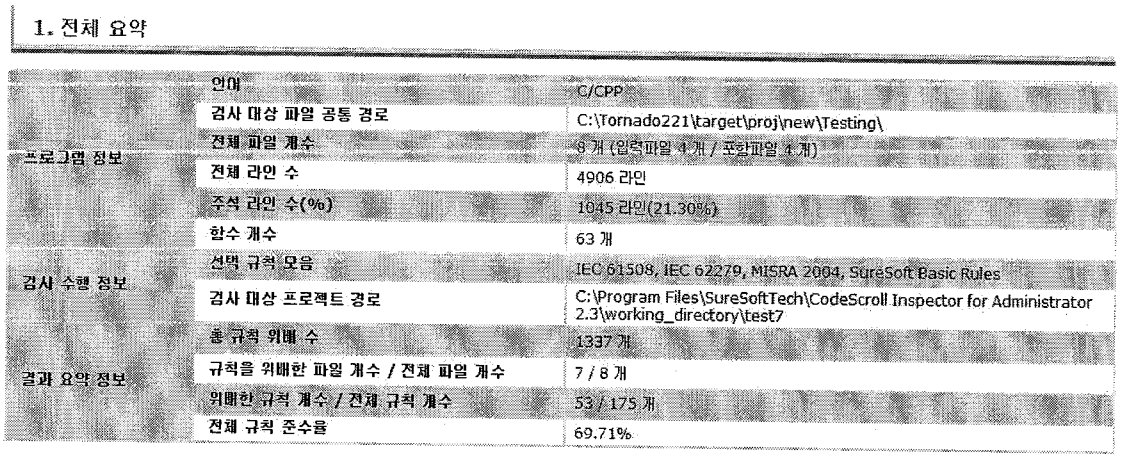
· PMA 또는 블록 폐쇄에 의한 비상 제동 설정 시 차상 시뮬레이터 속도가 급격히 감속 하는 것을 상용제동 보다 빠르게 설정 되도록 수정함

- ATS 블록 개방,폐쇄 선택 오류

· ATS 시뮬레이터에서 블록 개방 및 폐쇄 설정 시 단일 선택에 의한 제어를 여러 블록을 선택하여 설정 가능하도록 변경 함

(나) 소프트웨어 테스팅 자동화도구를 이용한 보완 제작

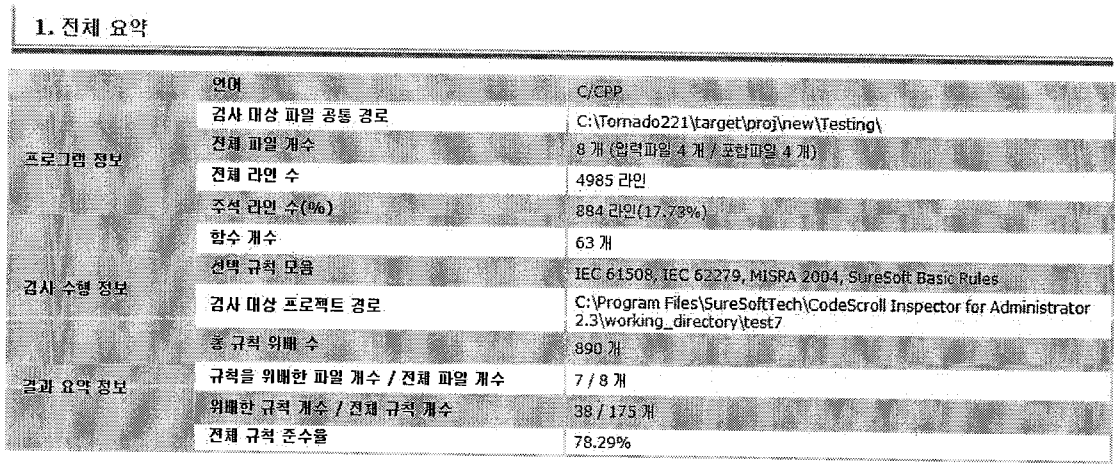
핵심과제에서 연구개발된 소프트웨어 테스팅 자동화도구를 이용하여 평가용 대상 열차제어시스템의 소스코드를 분석하여 분석된 결과를 바탕으로 소스코드를 수정하여 평가용 대상 열차제어시스템의 소프트웨어에 대한 안전성을 보완하였다. 다음은 당해연도에 수행한 최초 소스코드 분석 결과와 소스코드 분석 결과에 따라 1차 소스코드를 수정한 후의 소스코드 분석 결과를 비교한 내용이다. 아래 결과에서처럼 총 규칙 위배 수는 하향 조정되고 전체 규칙 준수율은 상향되어 평가용 대상 열차제어시스템의 소프트웨어의 품질이 더욱 향상되었음을 알 수 있다. 계속해서 차년도에 핵심과제에서 지속적으로 수행되는 소프트웨어 테스팅 자동화도구의 연구내용을 지속적으로 본 과제에 활용하여 소프트웨어 품질 확보를 통한 평가용 대상 열차제어시스템의 안전성을 확보할 수 있는 방안을 지속적으로 모색한다.



1. 전체 요약

프로그램 정보	언어	C/CPP
	검사 대상 파일 공통 경로	C:\Tornado221\target\proj\new\Testing\
	전체 파일 개수	9 개 (입력파일 4 개 / 포함파일 5 개)
	전체 라인 수	4906 라인
	주석 라인 수(%)	1045 라인(21.30%)
	함수 개수	63 개
검사 수행 정보	선택 규칙 모음	IEC 61508, IEC 62279, MISRA 2004, SureSoft Basic Rules
	검사 대상 프로젝트 경로	C:\Program Files\SureSoftTech\CodeScroll Inspector for Administrator 2.3\working_directory\test7
결과 요약 정보	총 규칙 위배 수	1337 개
	규칙을 위배한 파일 개수 / 전체 파일 개수	7 / 8 개
	위배한 규칙 개수 / 전체 규칙 개수	53 / 175 개
	전체 규칙 준수율	69.71%

그림 3.4.7 최초 소스코드 분석 결과



1. 전체 요약

프로그램 정보	언어	C/CPP
	검사 대상 파일 공통 경로	C:\Tornado221\target\proj\new\Testing\
	전체 파일 개수	8 개 (입력파일 4 개 / 포함파일 4 개)
	전체 라인 수	4985 라인
	주석 라인 수(%)	884 라인(17.73%)
	함수 개수	63 개
검사 수행 정보	선택 규칙 모음	IEC 61508, IEC 62279, MISRA 2004, SureSoft Basic Rules
	검사 대상 프로젝트 경로	C:\Program Files\SureSoftTech\CodeScroll Inspector for Administrator 2.3\working_directory\test7
결과 요약 정보	총 규칙 위배 수	890 개
	규칙을 위배한 파일 개수 / 전체 파일 개수	7 / 8 개
	위배한 규칙 개수 / 전체 규칙 개수	38 / 175 개
	전체 규칙 준수율	78.29%

그림 3.4.8 1차 수정 후 소스코드 분석 결과

(4) 안전성 평가용 대상 열차제어시스템 시험 방법 및 결과

(가) 시험계획서

안전성 평가용 대상 열차제어시스템과 관련된 기능 및 운용시험을 위한 전반적인 시험 프로그램의 원칙과 범위 등을 정의한 문서로서, 시험 전략, 시험 조직 및 시험 계층 구조, 시험 단계, 시험 순서 및 시험 단계별 선행 조건 등을 제시하고 시험항목별로 필요한 자료 내역들을 제시한 문서이다. 문서의 구조와 내용은 다음과 같다.

① 시험 항목

- 안전성평가용 대상 열차제어시스템 구성 및 정의
- 안전성평가용 대상 열차제어시스템 아키텍쳐 정의
- 시험 분류
- 시험은 장치별 기능 및 인터페이스 시험으로 분류

표 3.4.5 장치별 기능시험 분류 내용

구분		내용
CRD	ICM	· 선로전환기 정/반위 제어 · 진로 설정/취소 · 전체진로취소 · 블록쇄정 · 보류쇄정 · 진로쇄정 · 위치검지쇄정
	DCM	· 블록 개방/폐쇄 · 열차 위치 추적 · PMA 생성 · 열차 위치 적합성 검사 · 임시제한속도 지정
	EIM	· 데이터 비교 · 계 절체
ATS시뮬	표시	· Login기능 · L/S표시

레이터		· 열차표시 · 통신이상표시 · PMA표시 · 진로설정,해정표시
	제어	· 진로설정제어 · 블록개방/폐쇄제어 · 선로전환기 전환제어 · 플랫폼제어 · 열차제어 · 임시속도제한설정
차상시뮬레이터	ATP	· 블록 임시제한속도 확인 · 블록 PMA 확인 · 열차위치정보전송
	ATO	· 출입문개방/폐쇄 제어 · 플랫폼 정지/대기 확인 · 속도제어 · 비상정지

표 3.4.6 인터페이스 시험 분류 내용

구분	내용
CRD-ATS시뮬레이터	· 통신개시 테스트 · 기능 테스트 · CRC 테스트 · Sequence 테스트 · 데이터 오류 테스트
CRD-차상ATP 시뮬레이터	· 통신개시 테스트 · 기능테스트 · CRC테스트 · Sequence 테스트 · 데이터 오류 테스트
CRD-신호설비 제어시뮬레이터	· 통신개시 테스트 · Sequence테스트 · 데이터 오류 테스트
ATS시뮬레이터 -차상ATO시뮬	· 통신개시 테스트 · 기능 테스트

레이터	· CRC 테스트 · Sequence 테스트 · 데이터 오류 테스트

② 시험 전략 및 방법

- 시험절차 정의
- 시험레벨 정의
  - · 단위 테스트 : 테스트 가능한 (최소)단위로 분리된 소프트웨어(모듈,프로그램 등)내에서 결함을 찾고 그 기능을 검증
  - · 통합 테스트 : 소프트웨어 통합 테스트는 모듈간의 인터페이스를 테스트 하는 것은 물론, OS, 파일시스템, 하드웨어, 시스템간 인터페이스와 같은 시스템의 각기 다른 부분과 상호 연동하는 동작을 테스트
  - · 시스템 테스트 : 프로젝트 차원에서 정의된 전체 시스템/제품의 동작 관련 테스트, 시스템이 설치될 환경과 동일하게 하여 테스트 환경 제한적 장애 관련 리스크를 최소화하기 위해서 가능한 실제 최종 사용 환경과 유사해야 함

③ 시험 성공/실패 기준

각 장치별 테스트 성공 및 실패의 기준을 제시한다.

- CRD
  - · ICM

표 3.4.7 ICM시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	선로전환기 전환 제어	1)ATS 제어 명령을 수신한다.	제어명령을 전송하면 OK	
		2)신호제어시뮬레이터에 제어 명령 전송		
2	선로전환기 블록쇄정	1)선로전환기 블록에 열차 점유	선로전환기가 전환 되지 않으면 OK	
		2)선로전환기 전환 제어		
3	선로전환기 진로 쇄정	1)선로전환기가 포함된 진로를 설정	선로전환기가 전환 되지 않으면 OK	
		2)선로전환기 전환 제어		
4	선로전환기 위치 검지 쇄	1)신호제어시뮬레이터에 선로전환기 정보 수신	선로전환기 고장 상태로 변경되면 OK	

	정	2)전환되지 않은 선로전환기 검지		
5	진로 설정/취소	1)진로 설정 명령 수신 2)블록에 진로 예약	진로가 설정된 블록에 열차아이디,진로아이디가 저장되면 OK	
6	진로취소	1)진로 취소 명령 수신 2)진로 취소가 된 블록에 예약 해제	진로가 설정된 블록이 예약해제 되고 60초간 진로가 설정되지 않으면 OK	
7	전체 진로 취소	1)전체 진로 취소 명령 수신 2)설정 된 진로 및 저장된 진로가 취소	모든 진로가 취소가 되고 열차들은 비상정지 되면 OK	

· DCM

표 3.4.8 DCM시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	블록 폐쇄	1)ATS에서 블록폐쇄 명령 2)블록 폐쇄 설정	시험 블록은 폐쇄 되고 인접블록에 PMA가 RED로 설정되면OK	
2	블록 개방	1)ATS에서 블록 개방 명령 2)블록 개방 설정	폐쇄된 블록은 개방되고 인접블록에 PMA가 GREEN으로 설정되면 OK	
3	임시제한속도 설정	1)ATS에서 블록에 임시제한속도 설정 명령 2)블록에 임시 제한속도 설정	열차가 해당 블록 진입시 제한 속도 보다 초과하지 않으면 OK	
4	열차 위치 추적	1)ATP에서 열차 정보 수신 2)열차 점유 위치를 ATS에 전송	ATS에 열차 점유 위치가 현재 열차 위치와 동일하면 OK	
5	열차 분실	1)ATP 열차 정보 미 수신 2)열차 추적 실패	PW,SW구역 블록 폐쇄되면 OK	
6	검지손실	1)열차 위치 적합성 검사 실패 2)점유 블록 검지 손실 설정	블록에 검지손실 설정되면 OK	

- ATS시뮬레이터

· 표시기능

표 3.4.9 ATS시뮬레이터 표시기능 시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	Login 기능	1)Console Computer에서 ATS 시뮬레이터 실행 아이콘을 마우스로 더블 클릭한다.	Login 화면이 표시되면 OK	
		2)Login 화면이 모니터에 표시되는지 확인		
2	L/S표시	1)로그인 시 모니터에 L/S가 연동 도표와 일치하게 그려지는지 확인한다.	L/S가 나타나면 OK	
3	열차표시	1)차상시뮬레이터에서 정보 수신	L/S에 열차의 표시 위치가 차상 정보와 동일하면 OK	
		2)L/S에서 현재 열차 위치 표시 확인		
4	진로설정표시	1)진로 명령을 CRD로 송신한다	예약된 블록에 진로가 표시되면 OK	
		2)CRD에서 해당 블록의 정보를 받는다.		
5	블록상태표시	1)블록 개방/폐쇄 명령을 CRD로 전송	블록 폐쇄 표시 PMA표시되면 OK	
		2)CRD에서 블록 정보 수신.		

· 제어기능

표 3.4.10 ATS시뮬레이터 제어기능 시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	진로설정제어	1)진로에서 진로 설정을 클릭한다.	진로 설정을 Click시 연동 도표의 해당 진로가 표시되면 정상	
		2) 진로를 설정 한다.		
2	진로취소제어	1) 진로를 설정 한다.	진로 취소 시 블록의 PMA가 RED로 설정되면 OK	
		2) 진로가 설정된 후 진로취소 제어		
3	선로전환기 제어	1)선로전환기 제어 명령을 전송	요청 방향에 따라 전환되면 OK	
		2)선로전환기 정보 수신		
4	블록 개방/폐쇄	1)블록 제어 명령을 전송	요청 명령에 따라 수행되면 OK	
		2)블록 정보 수신		
5	임시속도제한	1) 비상정지를 Click한다.	비상 정지 설정시 설정	

		2) 제어를 행한다.	Box가 표시되면 정상. 비상정지 적색이면 정상.	
6	열차 제어	1)열차 제어 명령을 전송한다.	열차 표시 장치에 열차 상태가 명령에 대한 결과가 표시되면 OK	
		2)열차 정보를 수신한다.		

- 차상시뮬레이터

· ATP

표 3.4.11 차상시뮬레이터(ATP) 시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	블록PMA확인	1)블록 PMA정보를 수신	PMA RED 설정 지역에 진입하지 않으면 OK	
		2)블록에 접근 허용 여부 결정		
2	임시제한속도	1)블록 정보를 수신	지정된 블록에 제한속도로 진행하면 OK	
		2)ATO장치에 속도 제한 명령		
3	열차위치전송	1)현재 열차 위치를 전송	열차 위치와 ATS L/S 표시 위치가 동일하면 OK	

· ATO

표 3.4.12 차상시뮬레이터(ATO) 시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	출입문 개방/폐쇄 제어	1)출입문 개방/폐쇄 명령수신	ATS에 열차 출입문 개방/폐쇄 표시되면 OK	
		2)열차 정보 송신		
2	플랫폼 정지/통과/대기 제어	1)플랫폼 정지/통과/대기 제어 명령 수신	ATS에 열차 플랫폼 정지/통과/대기 수행되면 OK	
		2)열차 정보 송신		
3	열차 출발/정지	1)열차 출발/정지 명령 수신	ATS에 열차가 위치 표시가 서서히 진행하면 OK	
		2)열차 정보 송신		

- 인터페이스

예시로서 각 장치별 통신개시테스트에 대한 기준을 설명한다.

표 3.4.13 장치별 통신개시 시험 기준

순번	시험 항목	실시 단계	판정기준	비고
1	ATS시뮬레이터-CRD(ICM)	1)ICM에서RFC메시지를 전송 2)ATS에서 RFC 메세지 수신 후 Polling 메시지 전송	ATS에서 POLL전송 후 시퀀스 번호가 증가하며 ICM정보를 수신하면 OK	
2	ATS시뮬레이터-CRD(DCM)	1)DCM에서 RFC메시지를 전송 2)ATS에서 RFC 메세지 수신 후 Polling 메시지 전송	ATS에서 POLL전송 후 시퀀스 번호가 증가하며 DCM 정보를 수신 하면 OK	
3	CRD(DCM)-차상ATP시뮬레이터	1)ATP에서 RFC메시지를 전송 2)CRD(DCM)에서 RFC메세지 수신 후 Polling 메시지 전송	CRD(DCM)에서 POLL 전송 후 시퀀스 번호가 증가하며 열차 정보를 수신 하면 OK	
4	CRD(ICM)-신호설비제어시뮬레이터	1)SEC에서 RFC메시지를 전송 2)CRD(ICM)에서 RFC 메시지 수신 후 Polling 메시지 전송	CRD(DCM)에서 POLL 전송 후 시퀀스 번호가 증가하며 스위치 정보를 수신하면 OK	
5	ATS시뮬레이터-차상ATO시뮬레이터	1)ATO에서 RFC메시지를 전송 2)ATS에서 RFC메시지 수신 후 Polling 메시지 전송	ATS에서 POLL전송 후 시퀀스 번호가 증가하며 열차 정보를 수신하면 OK	
6	ICM-DCM	1)ICM에서 POLL메시지 전송 2)DCM에서 POLL메시지 전송	ICM은 DCM에게 DCM은 ICM에게 각각의 정보를 전송하면 OK	

④ 재시험 정의

단계별 시험중에 오류가 발견될 경우, 해결책을 제시, 논증하기 위해 재시험을 요구 될 수 있다.

시험 중 결함이 발생하여 검사를 더 진행하기 어렵다고 판단 될 경우 , 총괄 책임자와 협의하여 해당 시험의 검사를 중단하며, 나머지 다른 시험 케이스 항목을

시험한다.

모든 시험 케이스가 종료 된 후, 재시험 일자를 지정하여 ,재시험 항목을 취합하여 오류를 해결해야 한다.

⑤ 시험 진행

- 진행용 기초 문서 리스트 정의
- 시험 요원 제한 사항 정의 및 의무사항 정의
- 시험관련 문서 작성 방안 정의

⑥ 시험 환경

- 인터페이스 환경 정의
- 시험 작업 환경 정의

⑦ 책임

- 시험 조직 및 임무 정의
  - 프로젝트 관리자
  - 시험 관리자
- 시험 단계별 임무 정의
  - 시험 설계
  - 시험 실행
  - 시험 검증

⑧ 시험 일정 정의

⑨ 승인

- 승인 기준 정의
- 제출서류 정의

(나) 체크리스트

위와 같이 전년도에 수립한 시험계획서, 시험절차서, 시험항목에 따라 테스트를 수행하였으며, 테스트에 적용한 체크리스트에는 장치 및 기능별로 시험이 수행되어

야 할 시험번호, 시험항목과 시험내용이 다음과 같이 정의된다.

표 3.4.14 장치별 통신개시 시험 기준

장치 분류	시험번호	시험항목	시험내용
지 상 설비	D201.001	선로전환기 전환제어	CRD 시스템의 선로전환기 전환 테스트
	D201.002	선로전환기 진로쇄정	CRD 시스템의 진로 설정 시 선로전환기의 쇄정 테스트
	D201.003	선로전환기 보류쇄정	CRD 시스템의 진로 취소 시 선로전환기의 쇄정 테스트
	D201.004	선로전환기 블록쇄정	CRD 시스템의 선로전환기 관련 블록의 열차 점유 시 쇄정 테스트
	D201.005	선로전환기 위치검지 쇄정	CRD 시스템의 선로전환기 전환 완료 오류 시 블록 폐쇄 테스트
	D201.006	진로 설정	CRD 시스템의 진로 설정 테스트
	D201.007	진로 취소	CRD 시스템의 진로 취소 테스트
	D201.008	진로설정에 대한 PMA정보전송	CRD 시스템의 진로 설정 시 열차의 PMA 정보 전송 테스트
	D201.009	블록폐쇄	CRD 시스템의 블록 폐쇄 설정 테스트
	D201.010	열차 위치 확인	CRD 시스템의 열차 이동 및 위치 확인 테스트
	D201.011	열차 분실	CRD 시스템의 열차 분실 시 블록의 검지 손실 테스트
	D201.012	블록 속도 제한	CRD 시스템의 블록 임시 제한 속도 설정 테스트
사 령 설비	D401.001	선로전환기 제어 표시	ATS 시뮬레이터의 선로전환기 전환 제어 및 표시 확인 테스트
	D401.002	진로설정 제어 및 표시	ATS 시뮬레이터의 진로 설정 및 표시 확인 테스트
	D401.003	진로취소 제어 및 표시	ATS 시뮬레이터의 진로 취소 및 표시 확인 테스트
	D401.004	블록제어 및 표시	ATS 시뮬레이터의 블록 제어 및 표시 확인 테스트
	D401.005	열차 출입문 제어	ATS 시뮬레이터의 열차 출입문 제어

			및 표시 확인 테스트
	D401.006	열차 점유 표시	ATS 시뮬레이터의 열차 점유 표시 확인 테스트
	D401.007	블록 속도 제한	ATS 시뮬레이터의 블록 임시 제한 속도 제어 및 표시 확인 테스트
	D401.009	열차 출발 제어	ATS 시뮬레이터의 열차 출발 제어 및 열차 진행 확인 테스트
	D401.010	열차 플랫폼 대기	ATS 시뮬레이터의 열차 플랫폼 대기 제어 및 표시 확인 테스트
	D401.011	열차 플랫폼 제어	ATS 시뮬레이터의 열차 플랫폼 개방/폐쇄 제어 및 표시 확인 테스트
	D401.012	열차 플랫폼 정차시간 제어	ATS 시뮬레이터의 열차 플랫폼 정차시간 제어 및 표시 확인 테스트
	D401.013	열차 속도 제어	ATS 시뮬레이터의 열차 속도 제어 확인 테스트
차상설비	D501.001	열차 출입문 제어	차상시뮬레이터의 열차 출입문 상태 변환 테스트
	D501.002	열차 출발	차상시뮬레이터의 열차 출발 제어 테스트
	D501.003	블록 속도 제한	차상시뮬레이터의 임시제한속도 적용 테스트
	D501.004	열차 플랫폼 제어	차상시뮬레이터의 플랫폼 개방/폐쇄 적용 테스트
	D501.005	비상 제동	차상시뮬레이터의 비상제동 해제 설정 테스트
	D501.006	열차 속도 제어	차상시뮬레이터의 열차 속도 변환 테스트
인터페이스	D601.001	ATS-CRD(ICM)인터페이스	ATS시뮬레이터-CRD(ICM)의 통신 연결 확인 테스트
	D601.002	ATS-CRD(DCM)인터페이스	ATS시뮬레이터-CRD(DCM)의 통신 연결 확인 테스트
	D601.003	ATS-ATO인터페이스	ATS시뮬레이터-차상시뮬레이터(ATO)의 통신 연결 확인 테스트
	D601.004	CRD(DCM)-ATP 인터페이스	CRD(DCM)-차상시뮬레이터(ATP)의 통신 연결 확인 테스트

	D601.005	CRD(ICM)-SEC 인터페이스	CRD(ICM)-신호설비제어시뮬레이터(SEC)의 통신 연결 확인 테스트
	D601.006	CRD(ICM)-CRD(DCM)인터페이스	CRD(ICM)-CRD(DCM)의 통신 연결 확인 테스트
시나리오(통합)	D701.001	TURN-BACK 테스트	열차의 턴백의 모든 설정 과정을 테스트
	D701.002	최초 운행 개시	열차의 최초 운행 개시 시 설정되는 모든 과정을 테스트
	D701.003	ATS 통신 장애시 반응	ATS시뮬레이터의 통신 장애 시 CRD시스템과 열차가 행해지는 모든 설정 과정을 테스트
	D701.004	CRD 통신 장애 시 반응	CRD 통신 장애시 ATS시뮬레이터와 열차간 행해지는 모든 설정 과정을 테스트
	D701.005	차상장치 통신 장애시 반응	차상시뮬레이터의 통신 장애시 CRD 시스템과 ATS시뮬레이터에서 행해지는 모든 설정 과정을 테스트
	D701.006	진로 큐 테스트	진로의 중복 설정 및 진로 대기 상태를 테스트

체크리스트 항목에 정의된 각각의 항목별로 실제 시험을 수행하기 위한 문서로서 다음과 같은 구조로 이루어진다.

- 시험 번호
- 시험 목적
- 시험 필요사항
- 시험 조건
- 시험 순서
- 시험 범위
- 시나리오별 시험 절차, 이상 결과, 확인
- 시나리오별 시험케이스와 내용, 단계, 결과
- 시험 결과 보고서

(다) 안전성 평가용 대상 열차제어시스템에 대한 시험 결과

다음은 시험절차서에 의해 수행된 안전성 평가용 대상 열차제어시스템에 대한 시험 결과 내용이다.

① 지상설비

- 선로전환기 전환 제어(D201.001)

선로전환기 정위 및 반위 전환 제어가 ATS명령에 따라 이루어지는지 확인한 시험 내용이다.

시험번호 D201.001
(선로전환기 전환 제어)
[Switch Direction Change]

시험 목적 :		
선로전환기의 정/반위 제어가 ATS 명령에 따라 이루어지는지 확인한다.		
시험 필요 사항 :		
- 동작중인 CRD 시스템 - 동작중인 ATS 시뮬레이터 - 동작중인 신호제어/설비 시뮬레이터		
초기 조건 :		확인 √
01	ATS시뮬레이터 와 CRD 시스템은 통신 연결 상태 유지	
02	CRD시스템은 신호제어/설비 시뮬레이터와 통신 연결 상태 유지	

시험 순서 :	
ATS에서 선로전환기 정/반위 제어 명령을 전송한다. 제어 명령을 수신한 CRD시스템이 신호설비/제어 시뮬레이터에 전송하여 선로전환기의 위치가 명령에 따라 전환한다. CRD 시스템은 선로전환기의 정보를 수신하여,ATS 시뮬레이터에 전송한다. ATS시뮬레이터는 현재 선로전환기의 위치를 표시한다.	
시험자 기록 사항 :	
01	선로전환기의 각 방향 제어 시 선로전환기는 다른 방향으로 설정되어야 한다 (예)선로전환기 정위 제어 테스트 : 선로전환기 방향은 반위상태
02	시험할 선로전환기는 현재 정상 상태이며, 선로 전환기 포함 블록 또한 정상이며, 진로 설정 상태는 미설정 상태이다.

03	
04	

시험 범위 :
시험의 범위, 영역을 구분한다. 이 절차는 다음의 시험 케이스를 검증한다. 시험 시나리오(Test Scenario;TS),2: 1)선로전환기의 정위 제어명령을 수행한다. 2)선로전환기의 반위 제어명령을 수행한다. 선로전환기의 개수는 15개 시험케이스는 30개이다.

시험 절차 단계		예상 결과	확인
시나리오 01: 선로전환기의 정위 제어 명령을 확인한다.			시험케이스 목록 TestCase 01-12
1.1	ATS 시뮬레이터에서 선로전환기 제어 명령을 선택하여 시험 대상의 선로전환기를 선택하고 정위 명령을 전송한다.	ATS에서 CRD시스템으로 선로전환기 제어 명령을 전송한다.	이 단계에서 ATS 선로전환기 제어 및 표시 과정을 따른다.
1.2	CRD시스템에서 선로전환기의 제어 명령을 수신하여 신호제어시뮬레이터로 제어 명령을 전송한다.	CRD에서 신호제어시뮬레이터로 정위 명령을 전송한다.	
1.3	신호제어시뮬레이터에서 정위 명령을 수행한다.	선로전환기는 정위 상태가 되며, CRD로 선로전환기 정보 전송	
1.4	CRD에서 선로전환기 정보를 수신하여 현재 정보를 업데이트 하고 ATS시뮬레이터로 선로전환기 정보를 전송	ATS로 선로전환기 정보 전송	
시나리오 02: 선로전환기의 반위 제어 명령을 확인한다.			
2.1	ATS 시뮬레이터에서 선로전환기 제어 명령을 선택하여 시험 대상의 선로전환기를 선택하고 반위 명령을 전송한다.	ATS에서 CRD시스템으로 선로전환기 제어 명령을 전송한다.	이 단계에서 ATS 선로전환기 제어 및 표시 과정을 따른다.
2.2	CRD시스템에서 선로전환기의 제어 명령을 수신하여 신호제어시뮬레이터로 제어 명령을 전송한다.	CRD에서 신호제어시뮬레이터로 반위 명령을 전송한다.	
2.3	신호제어시뮬레이터에서 반위 명령을 수행한다.	선로전환기는 반위 상태가 되며, CRD로 선로전환기 정보 전송	
2.4	CRD에서 선로전환기 정보를 수신하여 현재 정보를 업데이트 하고 ATS시뮬레이터로 선로전환기 정보를 전송	ATS로 선로전환기 정보 전송	

다음과 같은 나머지 지상설비에 대한 시험도 위의 내용(D201.001 선로전환기 전환 제어)과 같은 시험 시험절차서에 의해 수행되었다

- 선로전환기 진로 쇄정(D201.002)

- 선로전환기 보류 쇄정(D201.002)
- 선로전환기 블록 쇄정(D201.003)
- 선로전환기 블록쇄정(D201.004)
- 선로전환기 위치검지쇄정(D201.005)
- 진로 설정(D201.006)
- 진로 취소(D201.007)
- 진로설정에 대한 PMA정보전송(D201.008)
- 블록폐쇄(D201.009)
- 열차 위치 확인(D201.010)
- 열차 분실(D201.011)
- 블록 속도 제한(D201.012)

② 사령설비

- 선로전환기 제어 및 표시(D401.001)

ATS 시스템에서 선로전환기의 전환 표시를 확인한다.

시험번호 D401.001
(선로전환기 제어 및 표시)
[Control Switch & Direction Change]

시험 목적 : 선로전환기 제어 화면이 표시 되는지 확인		
ATS시뮬레이터에서 선로전환기 전환 제어 할 컨트롤이 정확히 수행되는지를 확인.		
시험 필요 사항 :		
- 동작중인 ATS 시스템 - CRD시스템		
초기 조건 :		확인 √
01	ATS시뮬레이터와 CRD시스템은 통신 연결됨.	
02	진로 및 열차가 없는 시험 영역을 선택.	

03		

시험 순서 :	
ATS시뮬레이터 MMI화면에서 현장 버튼을 클릭한 뒤 선로전환기 버튼를 클릭한다.	
시험자 기록 사항 :	
01	ATS시뮬레이터는 로그인 과정을 수행하였다.
02	이 테스트는 이후 지상설비 선로전환기 전환 제어와 연관 되어 진다.
03	
04	

시험 범위 :
이 절차는 다음 15개의 시험케이스를 갖는다,. 시험 시나리오(Test Scenario;TS),1 1) 선로전환기 정위 전환 제어 표시 조건을 확인한다. 2) 선로전환기 반위 전환 제어 표시 조건을 확인한다. 그외 사실 진로(Route)의 개수는 76개이다, 시험 케이스는 다음과 같다 1(TS) X 156(RT) = 152 시험케이스의 상세 목록은 아래 상세 시험 케이스 목록과 같다.

시험 절차 단계		예상 결과	확인
시나리오 01: 선로전환기 정위 전환 제어 표시 조건를 확인한다.			시험케이스 목록 TestCase 01-60
1.1	ATS시뮬레이터 MMI화면에서 현장제어 버튼을 클릭한다.	ATS시뮬레이터 MMI화면에서 선로전환기 제어가 나타난다.	
1.2	ATS시뮬레이터 MMI화면에서 선로전환기 제어 버튼을 클릭한다.	ATS시뮬레이터 메인 화면에 선로전환기 전환제어 다이얼로그 팝업 창이 생성된다.	
1.3	ATS시뮬레이터 선로전환기제어 팝업창이 생성되면 시험할 선로전환기를 찾아서 선택한 뒤 정위 설정을 한다.	시험할 선로전환기가 표시된다.	
1.4	확인 버튼을 클릭한다.	ATS시뮬레이터에서 선로전환기 번호와 전환 방향의 메시지가 전송된다.	
1.5	CRD로 부터 선로전환기 정보 수신을 완료한다.	선로전환기는 명령에 따라 정위 상태를 나타낸다.	이 단계에서 지상 선로전환기 전화 제어 단계가 완료 시 확인한다.
시나리오 02: 선로전환기 반위 전환 제어 표시 조건를 확인한다.			
2.1	ATS시뮬레이터 MMI화면에서 현장 버튼을 클릭한다.	ATS시뮬레이터 MMI화면에서 선로전환기가 나타난다.	
2.2	ATS시뮬레이터 MMI화면에서 선로전환기 버튼을 클릭한다.	ATS시뮬레이터 메인 화면에 선로전환기 전환제어 다이얼로그	

		팝업창이 생성된다.	
2.3	ATS시뮬레이터 선로전환기제어 팝업창이 생성되면 시험할 선로전환기를 찾아서 선택한 뒤 반위 설정을 한다.	시험할 선로전환기가 표시된다.	
2.4	확인 버튼을 클릭한다.	ATS시뮬레이터에서 선로전환기 번호와 전환 방향의 메시지가 전송된다.	
2.5	CRD로 부터 선로전환기 정보 수신을 완료한다.	선로전환기는 명령에 따라 반위 상태를 나타낸다.	이. 단계에서 지상 선로전환기 전화 제어 단계가 완료 시 확인한다.

시험 케이스	시험 케이스 내용	단계					양호/불량		비 고
		x.1	x.2	x.3	x.4	x.5			
시나리오 01: 선로전환기 제어 표시를 확인한다.									
01	선로전환기 - 선로전환기명 #S_SW21 정위	√	√	√	√	√	P	F	성공적으로 수행된 단계의 각각의 항목에 체크 마크 (√)를 표시하고 실패한 단계에는 "X"를 표시한다. 만약 한 시험 케이스의 모든 단계가 통과되었으면, 시험 케이스의 양호/불량란에서 "P"에 붉은색을 그린다. 만약 한 시험 케이스의 하나 이상의 단계가 실패했으면, 그 시험 케이스의 양호/불량란에서 "F"에 붉은색을 그리고, 여기에 해당하는 SCR 번호를 적는다..
02	선로전환기 - 선로전환기명 #S_SW22 정위	√	√	√	√	√	P	F	
03	선로전환기 - 선로전환기명 #S_SW51 정위	√	√	√	√	√	P	F	
04	선로전환기 - 선로전환기명 #S_SW52 정위	√	√	√	√	√	P	F	
05	선로전환기 - 선로전환기명 #K_SW21 정위	√	√	√	√	√	P	F	
06	선로전환기 - 선로전환기명 #K_SW51 정위	√	√	√	√	√	P	F	
07	선로전환기 - 선로전환기명 #Y_SW21 정위	√	√	√	√	√	P	F	
08	선로전환기 - 선로전환기명 #Y_SW51 정위	√	√	√	√	√	P	F	
09	선로전환기 - 선로전환기명 #O_SW21 정위	√	√	√	√	√	P	F	
10	선로전환기 - 선로전환기명 #O_SW22 정위	√	√	√	√	√	P	F	
11	선로전환기 - 선로전환기명 #O_SW23 정위	√	√	√	√	√	P	F	
12	선로전환기 - 선로전환기명 #O_SW51 정위	√	√	√	√	√	P	F	
13	선로전환기 - 선로전환기명 #O_SW52 정위	√	√	√	√	√	P	F	
14	선로전환기 - 선로전환기명 #O_SW53 정위	√	√	√	√	√	P	F	
15	선로전환기 - 선로전환기명 #O_SW54 정위	√	√	√	√	√	P	F	
							P	F	
시나리오 02: 선로전환기 반위 전환 제어 표시를 확인한다.									

1	선로전환기 - 선로전환기명 #S_SW21 반위	√	√	√	√	√	P	F	
2	선로전환기 - 선로전환기명 #S_SW22 반위	√	√	√	√	√	P	F	
3	선로전환기 - 선로전환기명 #S_SW51 반위	√	√	√	√	√	P	F	
4	선로전환기 - 선로전환기명 #S_SW52 반위	√	√	√	√	√	P	F	
5	선로전환기 - 선로전환기명 #K_SW21 반위	√	√	√	√	√	P	F	
6	선로전환기 - 선로전환기명 #K_SW51 반위	√	√	√	√	√	P	F	
7	선로전환기 - 선로전환기명 #Y_SW21 반위	√	√	√	√	√	P	F	
8	선로전환기 - 선로전환기명 #Y_SW51 반위	√	√	√	√	√	P	F	
9	선로전환기 - 선로전환기명 #O_SW21 반위	√	√	√	√	√	P	F	
10	선로전환기 - 선로전환기명 #O_SW22 반위	√	√	√	√	√	P	F	
11	선로전환기 - 선로전환기명 #O_SW23 반위	√	√	√	√	√	P	F	
12	선로전환기 - 선로전환기명 #O_SW51 반위	√	√	√	√	√	P	F	
13	선로전환기 - 선로전환기명 #O_SW52 반위	√	√	√	√	√	P	F	
14	선로전환기 - 선로전환기명 #O_SW53 반위	√	√	√	√	√	P	F	
15	선로전환기 - 선로전환기명 #O_SW54 반위	√	√	√	√	√	P	F	

다음과 같은 나머지 사령설비에 대한 시험도 위의 내용(D401.001 선로전환기 제어 및 표시)과 같은 시험 시험절차서에 의해 수행되었다

- 선로전환기 제어 및 표시(D401.001)
- 진로설정 제어 및 표시(D401.002)
- 진로취소 제어 및 표시(D401.003)
- 블록제어 및 표시(D401.004)
- 열차 출입문 제어(D401.005)
- 열차 점유 표시(D401.006)
- 블록 속도 제한(D401.007)
- 열차 출발 제어(D401.008)

- 열차 플랫폼 대기(D401.009)
- 열차 플랫폼 제어(D401.010)
- 열차 플랫폼 정차시간 제어(D401.011)
- 열차 속도 제어(D401.012)

③ 차상설비

- 열차 출입문 제어(D501.001)

차상 장치의 출입문 개방 및 폐쇄가 정확히 이루어지는 확인한다.

시험번호 D501.001
(열차 출입문 제어)
[Train Doors Control]

시험 목적 : 열차 출입문 제어 확인		
열차 출입문 개방 및 폐쇄가 정확히 이루어지는지 확인한다.		
시험 필요 사항 :		
- 동작중인 ATS시뮬레이터 - 동작중인 차상시뮬레이터		
초기 조건 :		확인 √
01	ATS시뮬레이터와 차상시뮬레이터는 인터페이스 절차에 따라 연결됨.	

시험 순서 :	
ATS시뮬레이터에서 열차 출입문 개방 및 폐쇄 명령을 수신하면 열차 출입문 개방 및 폐쇄를 수행한다.	
시험자 기록 사항 :	
01	

02	
03	
04	

시험 범위 :
이 절차는 다음의 시험 케이스를 검증한다. 시험 시나리오(Test Scenario;TS), 1) 열차 출입문 개방 명령을 수행하는 조건을 확인한다. 2) 열차 출입문 폐쇄 명령을 수행하는 조건을 확인한다. 그외의 사실 플랫폼의 개수 5(BK)이다 열차 방향 2(TR)이다. 2(TS) X 5(BK)X2(TR) = 20개 이 시험의 테스트 케이스는 20개이다.

시험 절차 단계		예상 결과	확인
시나리오 01: 열차 출입문 개방 명령을 수행하는 조건을 확인한다.			시험케이스 목록 TestCase 01-12
1.1	ATS시뮬레이터에서 출입문 개방 명령을 수신한다.		이 단계에서 사령설비 열차 출입문제어 시나리오1.열차 출입문 개방조건 절차 단계를 따른다.
1.2	출입문 개방 제어 가능한 상태인지 확인한다.		
1.3	현재 열차의 출입문 상태를 전송한다.	ATS 시뮬레이터에 출입문 상태를 전송한다.	

시험 케이스	시험 케이스 내용	단계				양호/불량		비 고
		x.1	x.2	x.3	x.4			
시나리오 01: 열차 출입문 개방 명령을 수행하는 조건을 확인한다.								성공적으로 수행된 단계의 각각의 항목에 체크 마크 (√)를 표시하고 실패한 단계에는 "X"를 표시한다. 만약 한 시험 케이스의 모든 단계가 통과되었으면, 시험 케이스의 양호/불량란에서 "P"에 원을 그린다. 만약 한 시험 케이스의 하나 이상의 단계가 실패했으면, 그
01	출입문 개방 – 수서 상	√	√	√	√	P	F	
02	출입문 개방 – 수서 하	√	√	√	√	P	F	
03	출입문 개방 – 경원 상	√	√	√	√	P	F	
04	출입문 개방 – 경원 하	√	√	√	√	P	F	
05	출입문 개방 – 모란 상	√	√	√	√	P	F	
06	출입문 개방 – 모란 하	√	√	√	√	P	F	
07	출입문 개방 – 야탑 상	√	√	√	√	P	F	
08	출입문 개방 – 야탑 하	√	√	√	√	P	F	
09	출입문 개방 – 오리 상	√	√	√	√	P	F	

10	출입문 개방 – 오리 하	√	√	√	√	P	F	시험 케이스의 양호/불량란에서 "F"에 원을 그리고, 여기에 해당하는 SCR 번호를 적는다.
시나리오 02: 열차 출입문 폐쇄 명령을 수행하는 조건을 확인한다.								
01	출입문 폐쇄 – 수서 상	√	√	√	√	P	F	
02	출입문 폐쇄 – 수서 하	√	√	√	√	P	F	
03	출입문 폐쇄 – 경원 상	√	√	√	√	P	F	
04	출입문 폐쇄 – 경원 하	√	√	√	√	P	F	
05	출입문 폐쇄 – 모란 상	√	√	√	√	P	F	
06	출입문 폐쇄 – 모란 하	√	√	√	√	P	F	
07	출입문 폐쇄 – 야탑 상	√	√	√	√	P	F	
08	출입문 폐쇄 – 야탑 하	√	√	√	√	P	F	
09	출입문 폐쇄 – 오리 상	√	√	√	√	P	F	
10	출입문 폐쇄 – 오리 하	√	√	√	√	P	F	

다음과 같은 나머지 차상설비에 대한 시험도 위의 내용(D501.001 열차 출입문 제어)과 같은 시험 시험절차서에 의해 수행되었다

- 열차 출입문 제어(D501.001)
- 열차 출발(D501.002)
- 블록 속도 제한(D501.003)
- 열차 플랫폼 제어(D501.004)
- 비상 제동(D501.005)
- 열차 속도 제어(D501.006)

④ 인터페이스 테스트

- ATS-CRD(ICM) 인터페이스(D601.001)

ATS시스템과 CRD(ICM) 간 통신 데이터 확인 및 인터페이스 조건을 확인한다.

시험번호 D601.001
(ATS-CRD(ICM) 인터페이스)
[ATS-CRD(ICM) Interface]

시험 목적 :		
ATS-CRD(ICM)과 통신 연결 조건 및 상태를 확인한다.		
시험 필요 사항 :		
- 동작중인 CRD 시스템 - 동작중인 ATS시뮤레이터		
초기 조건 :		확인 √
01	시스템은 하드웨어 결함이 전혀 없다.	

시험 순서 :	
ATS시뮬레이터 실행을 시켜 메시지 수신 대기 상태에서 CRD 시스템이 시작되면 CRD(ICM)에서 RFC메시지를 전송한다. 이후 시퀀스 넘버가 증가하며 핸드쉐이크 하듯 메시지를 주고 받는다.	
시험자 기록 사항 :	
01	이 시험은 모든 시험 케이스의 선행 조건이다.
02	
03	
04	

시험 범위 :
이 절차는 다음의 시험 케이스를 검증한다. 시험 시나리오(Test Scenario;TS),1: 1) 통신 초기 연결 조건을 확인한다. 2) 통신 초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류 처리를 확인한다. 3) ATS시뮬레이터 응답 미처리 시 반응을 확인한다. 4) CRD(ICM)의 응답 미처리시 반응을 확인한다. 5) 시퀀스 오류 시 반응을 확인한다.

시험 절차 단계	예상 결과	확인
시나리오 01: 통신 초기 연결 조건을 확인한다.		시험케이스 목록

			TestCase 01-12
1.1	ATS시뮬레이터 프로그램을 실행한다.		이 단계는 사령설비 로그인 절차 단계를 수행한다.
1.2	CRD(ICM)시스템을 실행한다.	CRD(ICM)시스템에서 초기 연결 조건의 RFC메시지를 주기적으로 전송한다.	
1.3	ATS시뮬레이터에서 RFC메시지 확인 후 시퀀스 넘버 증가 후 Poll 메시지를 전송한다.		
1.4	CRD(ICM)시스템에서 Poll 메시지 수신 후 진로예약정보, 선로전환기상태정보 등을 전송한다.	주기적으로 Poll 메시지 수신되고, 진로정보 선로전환기정보를 송신한다.	
시나리오 02: 통신 초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류처리를 확인한다.			
2.1	ATS시뮬레이터 프로그램을 실행한다.		이 단계는 사령설비 로그인 절차 단계를 수행한다.
2.2	CRD(ICM)시스템에서 RFC메시지를 전송한다. (이때 RFC 메시지의 수신자 시퀀스 넘버가 '0'이 아님)	ATS시뮬레이터는 통신 실패로 간주하고,3초간 연결을 중단한다.	
2.3	CRD(ICM)시스템에서 RFC메시지를 재전송한다. (이때 RFC 메시지의 수신자 시퀀스 넘버는 '0'이다)	ATS시뮬레이터는 RFC메시지를 확인하고 POLL메시지를 전송한다.	
2.4	CRD(ICM)시스템에서 Poll 메시지를 수신하면,진로 정보, 선로전환기 상태 정보를 전송한다.	이후 주기적으로 메시지를 주고받는다.	
시나리오 03: ATS시뮬레이터 응답 미처리 시 반응을 확인한다.			
3.1	ATS시뮬레이터에서 명령메시지를 전송한다.		
3.2	CRD(ICM)시스템에서 응답메시지를 전송한다.		
3.3	ATS시뮬레이터에서 응답 메시지를 수신되지 않아 처리가 되지 않았다.		
3.4	ATS시뮬레이터에서 이전 수신자 시퀀스 넘버와 송신자 시퀀스 넘버에 1을 증가 시켜 재전송한다.		
시나리오 04: CRD(ICM)의 응답 미처리시 반응을 확인한다.			
4.1	ATS시뮬레이터에서 명령메시지를 전송한다.		
4.2	CRD(ICM)시스템에서 ATS시뮬레이터 명령메시지를 수신하지 못하였다. 미처리가 됨.		
4.3	ATS시뮬레이터에서 송신자 시퀀스 넘버를 1증가시켜 재전송한다.		
4.4	CRD(ICM)시스템에서 메시지를 처리한다.		
시나리오 05: 시퀀스 오류 시 반응을 확인한다.			
5.1	ATS시뮬레이터에서 명령 메시지를 전송한다. (수신자 시퀀		

	스 넘버 오류발생)		
5.2	CRD(ICM)시스템에서 시퀀스 오류 탐지 후 본래 시퀀스 넘버로 응답한다.	연속 3회 이상 시퀀스 오류를 발견하면, 3초간 통신을 중단한다.	
5.3	CRD(ICM)시스템에서 RFC메시지를 생성하여 ATS시뮬레이터로 전송한다. (수신자 시퀀스 넘버는 '0'이다)		
5.4	ATS 시뮬레이터에서 RFC메시지를 확인하여 명령(Poll)메시지를 전송한다.	주기적으로 Poll전송 후 응답메시지를 수신하면 재 연결 상태가 된다.	

시험 케이스	시험 케이스 내용	단계 x.1	x.2	x.3	x.4	양호/불량		비 고
시나리오 01: 통신 초기 연결 조건을 확인한다.								성공적으로 수행된 단계의 각각의 항목에 체크 마크 (√)를 표시하고 실패한 단계에는 "X"를 표시한다. 만약 한 시험 케이스의 모든 단계가 통과되었으면, 시험 케이스의 양호/불량란에서 "P"에 원을 그린다. 만약 한 시험 케이스의 하나 이상의 단계가 실패했으면, 그 시험 케이스의 양호/불량란에서 "F"에 원을 그리고, 여기에 해당하는 SCR 번호를 적는다.
01	ATS-CRD(ICM)	√	√	√	√	P	F	
시나리오 02: 통신 초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류 처리를 확인한다.								
04	ATS-CRD(ICM)	√	√	√	√	P	F	
시나리오 03: ATS시뮬레이터 응답 미처리 시 반응을 확인한다.								
07	ATS-CRD(ICM)	√	√	√	√	P	F	
시나리오 04: CRD(ICM)의 응답 미처리시 반응을 확인한다.								
10	ATS-CRD(ICM)	√	√	√	√	P	F	
시나리오 05: 시퀀스 오류 시 반응을 확인한다.								
13	ATS-CRD(ICM)	√	√	√	√	P	F	

다음과 같은 나머지 인터페이스에 대한 시험도 위의 내용(D601.001 ATS-CRD(ICM)인터페이스)과 같은 시험 시험절차서에 의해 수행되었다.

- ATS-CRD(ICM)인터페이스(D601.001)
- ATS-CRD(DCM)인터페이스(D601.002)
- ATS-ATO인터페이스(D601.003)
- CRD(DCM)-ATP 인터페이스(D601.004)
- CRD(ICM)-SEC 인터페이스(D601.005)
- CRD(ICM)-CRD(DCM)인터페이스(D601.006)

⑤ 시나리오 테스트

- TURN-BACK (D701.001)

열차의 TURN-BACK 조건을 확인하며, 시스템간 수행 되어야 할 기능들을 확인한다.

시험번호 D701.001
(TURN-BACK)
[TURN-BACK]

시험 목적 :		
열차의 Turn-back 에 관련된 모든 제어 시스템이 시나리오대로 진행 절차가 이루어지는지 확인한다..		
시험 필요 사항 :		
- 동작중인 CRD 시스템 - 동작중인 ATS시뮬레이터 - 동작중인 차상시뮬레이터		
초기 조건 :		확인 √
01	ATS-CRD-차상장치-신호제어설비시뮬레이터가 인터페이스 절차에 따라 연결됨.	

시험 순서 :	
열차가 회차 지점에 정차 한 후 Turn-Back #1 진로를 설정한다. 열차가 끝지점에 도착한 뒤 열차의 이동방향이 변경 되어 Turn-Back #2진로가 설정된다. 열차가 플랫폼에 정차 하면 이로서 Turn-Back이 종료 된다.	
시험자 기록 사항 :	
01	이 시험은 열차의 진로, PMA설정,이동방향 변경 등 복합 시험 테스트이다.
02	이 시험은 시스템의 기능 시험이 완료 된 후 테스트 된다.
03	
04	

시험 범위 :
이 절차는 다음의 시험 케이스를 검증한다. 시험 시나리오(Test Scenario;TS),1: 1) Turn-Back 시나리오를 확인한다. 이외의 사실, Turn-Back 지점 2가지 시험 케이스는 2개이다.

시험 절차 단계		예상 결과	확인
시나리오 01: 열차의 Turn-Back 시나리오를 확인한다.			시험케이스 목록 TestCase 01-12
1.1	열차의 위치 확인(회차 지점의 플랫폼에 정차하고 있다)	ATS에서 현재 열차 위치를 확인한다.	
1.2	Turn-Back 진로 #1을 설정한다	진로가 설정 되고, 열차에 PMA 정보가 전송된다.	
1.3	열차를 턴 할 회차 지점에 정차한다.	열차의 진행방향을 변경한다. (차상장치 열차 절체 수행)	
1.4	Turn-Back 진로 #2을 설정한다.	진로가 설정된다. 열차에 PMA정보가 전송된다.	
1.5	열차가 진로 끝 지점에 정차한다.	열차가 출발 위치에 정차된다.	

시험 케이스	시험 케이스 내용	단계					양호/불량		비 고
		x.1	x.2	x.3	x.4	x.5			
시나리오 01: 열차의 Turn-Back 시나리오를 확인한다.									성공적으로 수행된 단계의 각각의 항목에 체크 마크 (√)를 표시하고 실패한 단계에는 "X"를 표시한다. 만약 한 시험 케이스의 모든 단계가 통과되었으면, 시험 케이스의 양호/불량란에서 "P"에 원을 그린다. 만약 한 시험 케이스의 하나 이상의 단계가 실패했으면, 그 시험 케이스의 양호/불량란에서 "F"에 원을 그리고, 여기에 해당하는 SCR 번호를 적는다.
01	수서역 – 상행->하행 turn-back	√	√	√	√	√	P	F	
02	오리역 – 하행->상행 turn-back	√	√	√	√	√	P	F	
03									
04									
05									
06									
07									
08									
09									
10									
11									
12									
13									

다음과 같은 나머지 시나리오에 대한 시험도 위의 내용(D701.001 TURN-BACK)과 같은 시험 시험절차서에 의해 수행되었다.

- TURN-BACK 테스트(D701.001)

- 최초 운행 개시(D701.002)
- ATS 통신 장애시 반응(D701.003)
- CRD 통신 장애 시 반응(D701.004)
- 차상장치 통신 장애 시 반응(D701.005)
- 진로 큐 테스트(D701.006)

제5절 평가대상시스템을 통한 적용성 기술 개발

검증계획서 **(Verification Plan)**	**ID No :** **TC - SR07 - SSR03 - 2010** 작성일 : 2010. 06. 18 수정일 :

7. 프로젝트는 열차제어시스템 안전성 평가 및 사고방지기술개발을 위한 모의열차제어 시스템을 설계제작하여야 한다

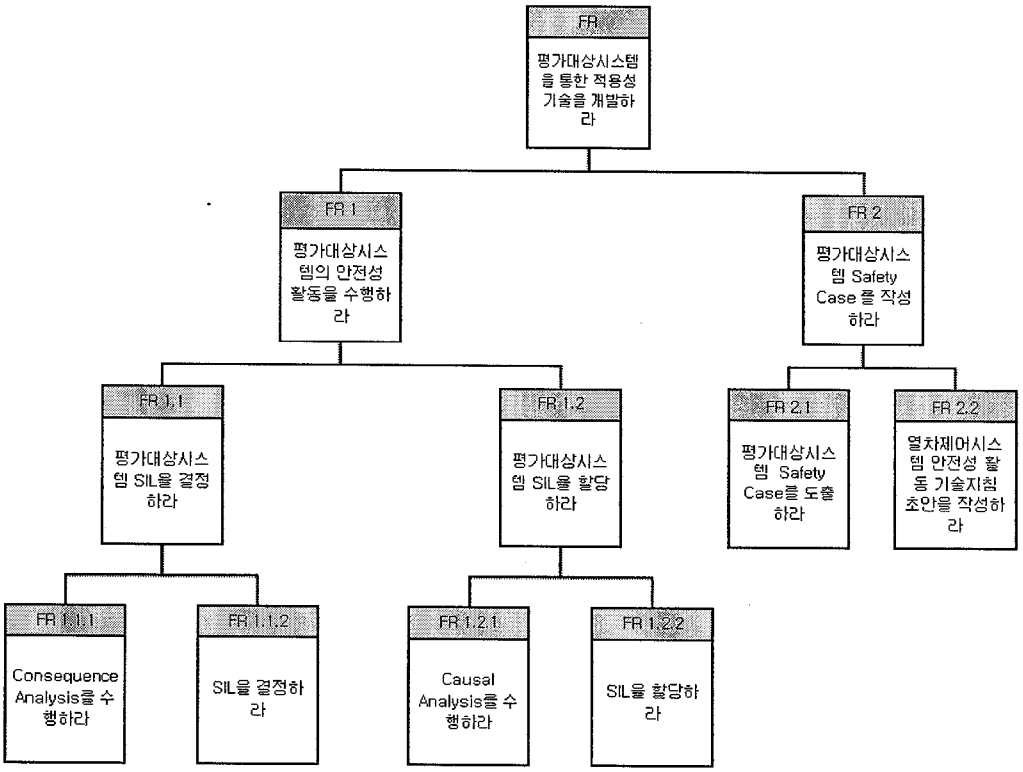
7.3 프로젝트는 평가대상시스템을 통한 적용성 기술을 개발하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 평가대상시스템 안전성활동 문서 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 2.1 단순 상황분석, 3.3 전문가 검토	- SE 검증	- 수정 VRTM - 검증결과표 3.5.

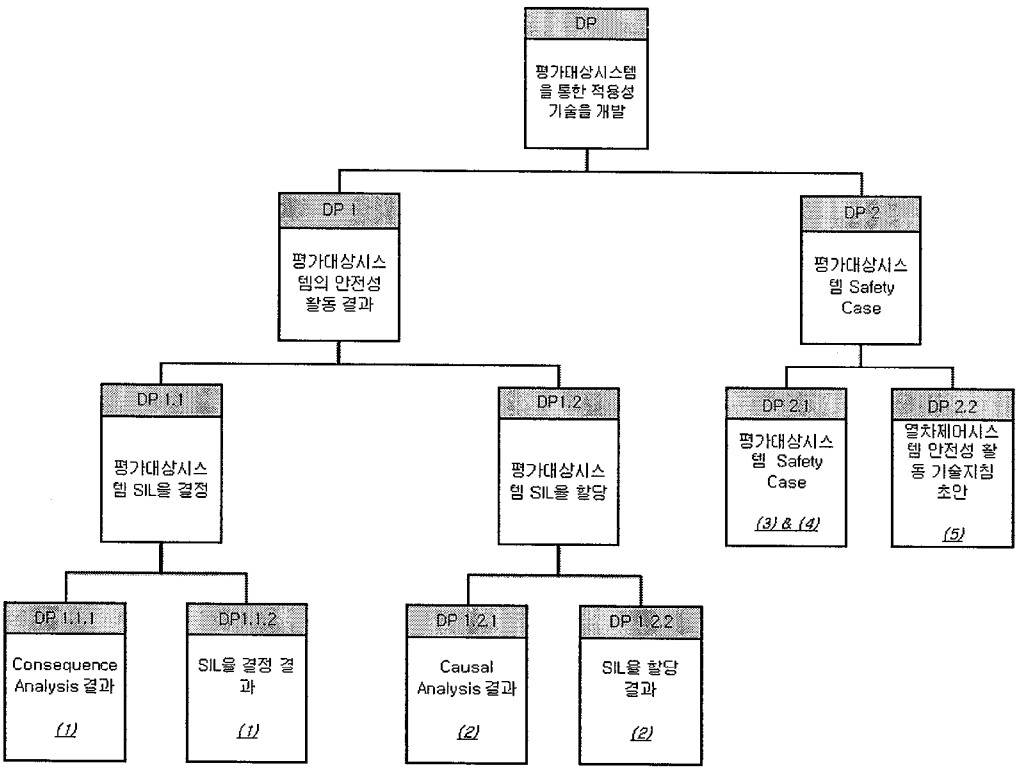
Verification Specification (검증기준) :

1. 평가대상시스템에 대한 안전성 활동이 적절히 수행되었는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

기 설계된 mock-up 시스템의 안전성 평가기술 적용성 기술 개발은 『SR 7. 프로젝트는 열차제어시스템 안전성 평가 및 사고방지기술 개발을 위한 모의열차제어시스템을 설계 제작하여야 한다.』 중 **『SSR. 7.3. 프로젝트는 모의 열차제어장치 설계 및 제작을 위한 적용성 기술을 개발하여야 한다.』**에 해당하는 내용이다. 본 절에서는 평가대상시스템의 안전성 활동 및 문서작업에 대해 제시하였다. 이러한 안전성 활동은 Risk Analysis, Hazard Control이 수행되어야 한다. 또한 이러한 결과들이 전년도에 작성한 Safety Case 작성 가이드라인 초안에 기반하여 평가대상시스템에 대한 Safety Case라는 문서로 정리되어져야 한다. 당해연도에는 이러한 안전성 활동 수행하였으며, 또한 그 결과물을 Safety Case라는 문서 형태로 작성하였다. 또한 Safety Case 작성 가이드라인의 구체화 및 개발기술의 구체화를 위해 기술지침서 형태인 '안전성 활동 기술 지침서' 초안을 작성하였다.

나. 설계기준

○ 평가대상 시스템의 잠재된 Hazard의 도출, Risk 분석, Hazard의 대처방안 및 저감대책을 마련하고 평가대상 시스템의 안전무결성 레벨에 따른 설계와 구현을 수행하였다.

○ 다음과 같은 철도 안전성 관련된 국제규격 및 참고문헌을 참고하였다.

- IEC61508, "Functional safety of electrical/electronic/programmable electronic safety - related systems", 2004.
- IEC 62279, "Railway Applications : Communications, Signalling and Processing Systems - Software for Railway Control Protection Systems", 2004.
- IEC 62425, "Railway Applications : Safety related electronic systems for signalling", 2005.
- IEC 62280, "Railway Applications : Communications, Signalling and Processing Systems - Safety-related Communication in Closed/Open Transmission Systems", 2004.

- IEC 61882, "Hazard and operability studies(HAZOP Studies)-Application guide", 2001.

○ 평가대상 시스템의 안전성 활동을 국제규격에 따라 수행하며, 이에 따라 산출된 문서는 철도시스템 안전 인증기관(TUV SUD)과의 기술자문을 통해 적용성을 평가받았다.

다. 검증 방법에 따른 증거 자료

열차제어시스템의 안전성 평가기술 적용성 연구를 위하여 앞 절에서 수행한 Mock-up 열차제어시스템 설계 결과를 활용하여, 당해연도에 전년도에 이어서 평가대상시스템의 SIL 결정 및 할당, V&V를 수행하였으며, Safety Case 일부를 작성하였다. Safety Case 문서는 전년도에 작성한 Safety Case 작성 가이드라인 초안을 기반으로 하여 당해연도부터 작성이 시작되어 차년도에 완료될 예정이다. 또한 Safety Case 작성 가이드라인의 구체화 및 개발 기술의 실용화를 위해 안전성 활동기술 지침 초안을 작성하였으며, 차년도에 최종안이 제시될 예정이다. 안전성 활동 수행 및 Safety Case 작성은 해외 안전성 평가 전문기관인 TUV SUD 기관으로부터 수개월 간의 기술자문을 통해 보완 작성되었다.

○ 평가대상 시스템 Safety Plan
- IEEE 1228에 따른 Safety Plan 작성
- Safety Plan에 대한 평가

○ 평가대상 시스템의 잠재적 Hazard 도출
- 타 시스템 Hazard 분석
- 평가대상 시스템의 Hazard 도출 방법 비교
- 평가대상 시스템의 Hazard 결과

○ 평가대상 시스템의 Risk 분석
- Risk 분석에 대한 개요
- Risk 분석 기법 비교
- Risk 평가 기법 비교
- 평가대상 시스템의 Risk 결과

○ 평가대상 시스템의 Hazard 관리

- Hazard 관리 기법 비교
- 평가대상 시스템의 FTA 결과

○ 평가대상 시스템의 Verification/Validation 계획
- IEEE 1012에 따른 Verification/Validation 계획 작성
- Verification/Validation 평가

○ Safety Case Guideline
- EN 50129에 따른 Safety Case 연구
- 기존연구에서의 Safety Case 분석
- 평가대상 시스템의 Safety Case guideline 연구

라. 성과물의 내용 및 결과

(1) 평가대상시스템 SIL 결정

(가) 평가대상시스템 위험원 도출

위험원 도출은 시스템 내부 또는 개발동안 발생할 수 있는 잠재적으로 비정상적인 상황을 야기시켜 인명피해, 시스템(시설)손실, 환경적 피해, 경제적인 손실을 가져오는 상황을 결정하는 초기단계이다. 시스템의 위험원 도출은 일반적으로 두 가지 단계를 거쳐 수행된다.

- 경험적 단계
- 창조적 단계

경험적 단계는 잠재적 위험원을 발견하기 위해 과거의 경험과 지식에 기반한다. 경험적 위험원 도출이 일반적으로 충분할 수 있지만, 새로운 시스템 또는 변경되는 시스템에서는 창조적으로 위험원을 도출해야 할 경우가 발생한다. **창조적** 위험원 도출은 풍부한 상상력을 바탕으로 사고를 예측할 필요가 있다. 하지만, 경험적 단계나 창조적 단계 모두 가장 우선적으로 고려해야 할 사항이 해당 시스템의 명확한 범위를 정의해야 한다.

본 과제에서는 지난 차년도까지 다양한 방법으로 평가대상시스템의 위험원을 도출하였다. CRD시스템의 잠재적인 위험원 도출은 이전 차년도 과제에서 수행된 바

와 같이 다양한 방법과 관점에 따라 각기 다른 결과가 도출됨을 알 수 있었다. 그 이유로는 엔지니어에 의한 경험적 그리고 창조적으로 위험원이 도출되었기에 그 생각의 차이와 범위가 다르기 때문이다. 본 연구에서는 이에 위험원 도출에 체계적으로 접근하기 위한 방법을 고려하게 되었으며, 철도시스템에서 발생할 수 있는 사고유형의 분류에 따라 관련 위험원을 도출하게 되었다. 우선 CRD시스템에서 발생할 수 있는 사고를 유형별 사고에서 표 3.5.1과 같이 선별하였다.

표 3.5.1 CRD시스템 사고 분류

사고1	사고2	사고3	CRD관련 설명
운전 사고	열차 사고	열차충돌	CRD시스템의 열차간격제어 실패로 인해 선후행 열차간 충돌이 발생할 수 있음.
		열차탈선	선로전환기 위로 열차주행 중 선로전환기 전환.
		열차접촉	CRD시스템의 열차진로제어 오류로 인해 두대의 열차가 동일 진로로 진입할 수 있음.
	운전장애 사고	이선진입	CRD시스템의 오류로 열차진로와 선로전환기의 방향이 상이함.
		폐색취급 위반	CRD시스템 허용이동권한 설정 실패.
		열차정지	CRD시스템의 오류로 인해 열차위치 정보처리 실패시 열차정지.

CRD 시스템의 특성상 사상사고, 설비사고 그리고 화재사고와는 거리가 멀어 운전사고에서만 도출하여 총 6가지의 사고유형을 도출하였다. 표 3.5.2에서 기술된 CRD관련 설명으로부터 사고가 발생되기까지의 위험상황 즉 위험원을 도출하였으며, 위험 원인은 CRD시스템에서 발생 가능한 결함 및 오류로 도출되었다.

표 3.5.2 CRD 시스템 위험원 도출

사고3	Accident	위험상황 (Hazard)	위험 원인	위험요소
열차충돌	열차충돌	동일블록에 두대의 열차가 존재함.	열차 허용이동권한 설정 오류	열차간격
			열차진로 및 선로전환기 방향 오류	열차진로
			알려지지 않은 열차 존재(투입)	미확인열차
			열차위치 확인 실패	열차위치
			후행열차의 과속주행	열차속도
열차탈선	열차탈선	비정상적인 진로로 열차	열차진로 설정 오류	열차진로
			선로전환기 방향전환 실패	선로전환기

		진입	열차진로 취소 설정 실패	선로전환기
		최대운행 제한속도를 초과하여 과속주행 중인 열차	임시속도제한명령 오류	임시속도
			열차상태 확인 불가	인터페이스
폐색취급 위반	열차정지	허용이동권한 없이 이동중인 열차	열차 허용이동권한 설정 실패	허용이동권한
			허용이동권한 열차로 전송 실패	인터페이스

CRD시스템에서 발생가능한 최상위 위험원은 총 4가지로 다음과 같이 도출되었다.

- Hazard-1 동일블록에 두 대의 열차가 존재함
- Hazard-2 비정상적인 진로로 열차진입
- Hazard-3 최대운행 제한속도를 초과하여 과속주행중인 열차
- Hazard-4 허용이동권한 없이 이동중인 열차

(나) 평가대상시스템 Consequence Analysis

위험원에 적용되는 Consequence Analysis는 '위험원이 발생한다면, 어떻게 될까?'라는 질문에 의해 수행된다. Consequence Analysis의 목적은 위험원에서 제외될 수 있는 가능한 결과들을 추가적으로 도출, 기록, 정량화하는 것이다. Consequence Analysis에서 가장 중요한 사항은 위험원의 잠재적인 증대를 억제할 수 있는 다음과 같은 구체적인 방어 대책의 도출이다.

- 기술적 진단, 경고, 제어, 보호 시스템들과 같은 물리적인 대책
- 규칙, 절차, 운영자의 프로세스 지식과 같은 절차 엔지니어링 대책
- 의도되지 않은 사고를 방어할 수 있는 환경 도출

Consequence Analysis의 개념을 표현하면 표 3.5.1과 같다.

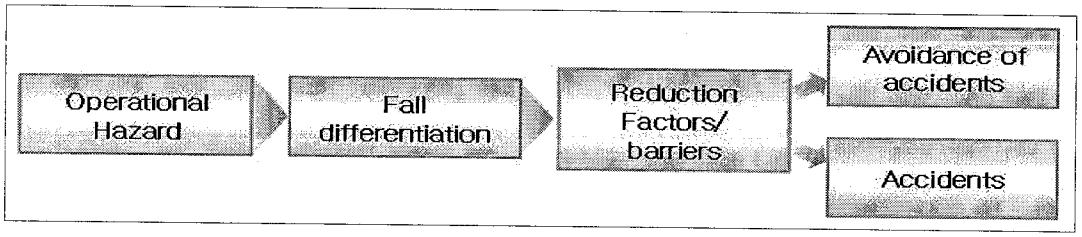


그림 3.5.1 결과분석 개념

CRD시스템의 위험원별 Consequence Analysis 수행 결과는 다음과 같다.

○ Hazard-1 동일블록에 두 대의 열차가 존재

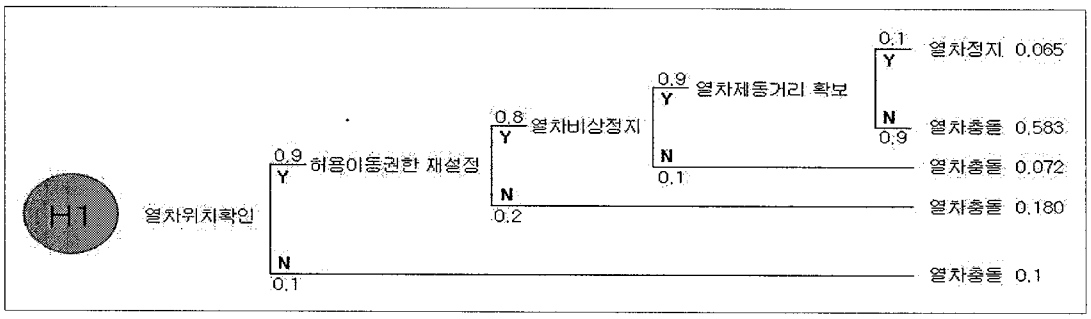


그림 3.5.2 연구대상 시스템 Hazard-1 Consequence Analysis

CRD시스템 Hazard-1에 대한 Consequence Analysis은 열차충돌이 0.935로 확률상 93.5%의 매우 높은 비율로 열차간 충돌이 발생함을 알 수 있다. 따라서 Hazard-1이 발생했을 경우, 특별한 시스템적인 방어대책이 수립되어 있고 더불어 환경적인 조건이 모두 만족해야만 열차충돌을 막을 수 있게 된다. Hazard-1은 위험원이 발생하기 전에 CRD시스템 내부에서 이를 원천적으로 차단할 수 있는 방안을 마련해야 한다.

- 열차위치 분실에 대한 대책
- 허용이동권한 설정에 대한 대책
- 진로설정에 대한 대책
- 최후 대책으로 ATS 대응책 마련

○ Hazard-2 최대운행 제한속도를 초과하여 과속주행중인 열차

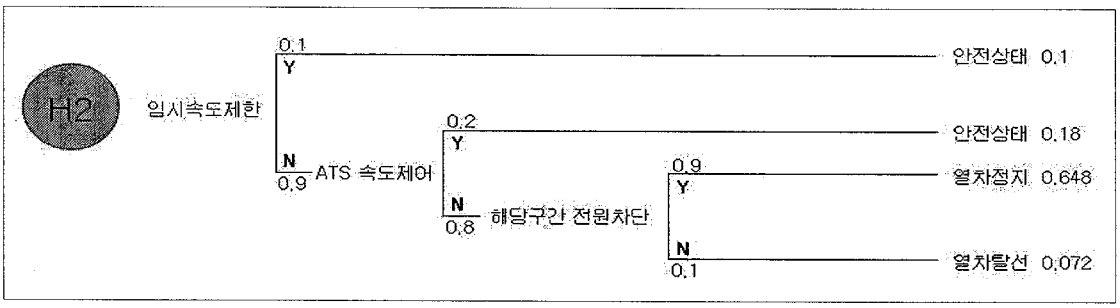


그림 3.5.3 연구대상 시스템 Hazard-2 Consequence Analysis

CRD시스템 Hazard-2에 대한 Consequence Analysis은 열차정지가 64.8%로 가

장 높은 비율을 보였으며, 과속으로 인한 탈선은 비교적 낮은 수치(7.2%)를 보였다. 그러나 Consequence Analysis의 그림에서와 같이 CRD시스템에서는 우선적으로 임시속도를 제한할 수 있는 대책만이 존재하며, 2단계부터는 ATS범위로 넘어가게 된다. 무인운전열차에서 열차가 과속주행중이라는 뜻은 열차의 고장 또는 열차와 제어시스템간 인터페이스가 안되는 상황이기 때문에 CRD시스템에서 임시속도를 제한한다고 해도 10%의 확률로 안전을 확보할 수 있다. 그러므로 보다 구체적이고 다각적인 대책을 마련해야 한다는 결론을 도출할 수 있다.

○ Hazard-3 비정상적인 진로로 열차진입

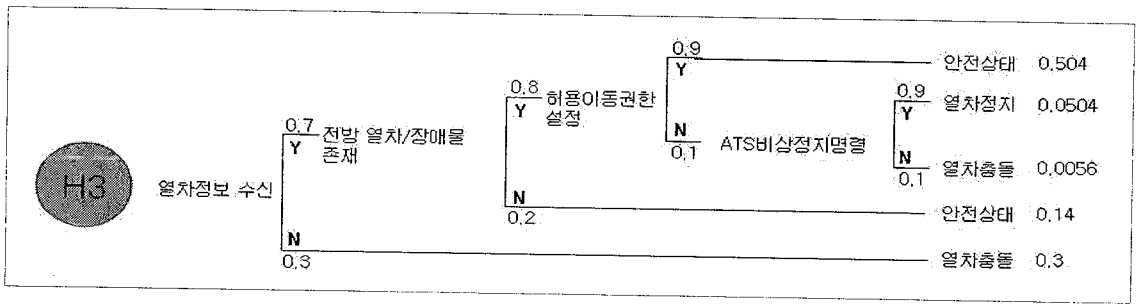


그림 3.5.4 연구대상 시스템 Hazard-3 Consequence Analysis

CRD시스템 Hazard-3에 대한 Consequence Analysis은 열차충돌이 30.5%, 열차정지가 5% 그리고 안전상태가 64.4%의 비율로 결과가 도출되었다. 즉, 비정상적인 진로로 열차가 진입한다 하더라도 열차로부터 속도, 위치, 상태정보 등을 수신하여 시스템적으로 대응할 수 있다면 70%수준의 안전을 보장할 수 있다. 따라서 Hazard-3에서 가장 중요한 사항은 열차와의 인터페이스를 최대한 확보할 수 있는 방안을 마련해야 한다.

○ Hazard-4 허용이동권한 없이 이동 중인 열차

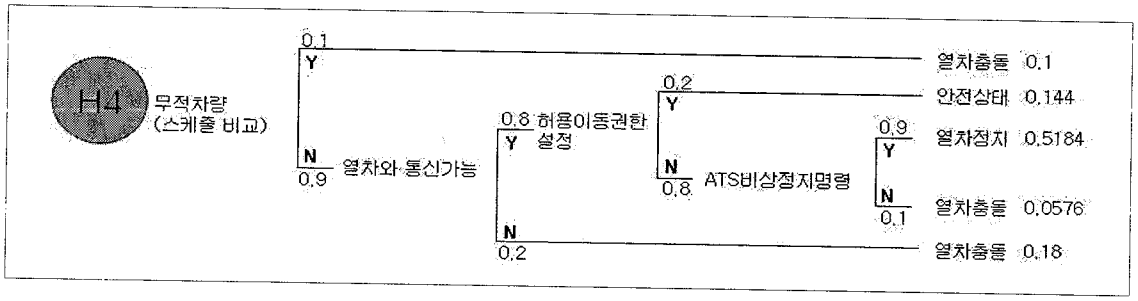


그림 3.5.5 연구대상 시스템 Hazard-4 Consequence Analysis

CRD시스템 Hazard-4에 대한 Consequence Analysis은 아무런 손실없이 운행을 유지할 수 있는 비율이 14.4%로 매우 낮은 수준이며, 열차충돌은 33.7%로 비교적 높게 나타났다. Hazard-4는 크게 열차와의 통신이 단절된 경우와 스케줄 또는 아무런 통보 없이 무적열차가 투입된 경우로 볼 수 있다. 후자의 경우 매우 특별한 상황으로 CRD시스템에서는 이에 대해 대응할 수 없기 때문에 전자의 경우에 대해서만 대책을 수립하여야 한다. Hazard-3와 마찬가지로 열차와의 인터페이스를 최대한 확보할 수 있는 방안이 마련되어야 한다.

(다) 평가대상시스템 PHA

PHA 분석기법은 각 시스템에서 발생 가능한 Hazard를 분석하고, 추가적인 Hazard를 찾아내는 것이 목적이다. PHA는 안전성 분석 기법으로 Hazard, 원인, risk 수준, 완화방법 등을 기재하게 된다. 또한 설계 초기에 시스템 안전요구사항을 도출할 수 있다. PHA는 앞서 작성된 PHL을 기반으로 Hazard의 사고 위험 정도를 평가하며, 예비설계단계에서 도출되는 추가적인 위험원을 도출하여 시스템에서 발생할 수 있는 잠재적인 위험원을 분석하게 된다. PHA는 주요 설계가 시작되기 전인 프로젝트 시작시점에 수행해야 하는데, 이는 변경작업으로 발생된 위험도 범위와 폭을 측정하기 위함이다. 분석을 하기 위해서는 시스템의 기능과 구성 그리고 사람과 타 시스템과의 인터페이스 전체에 대한 상위 레벨 설명서가 필요하다. PHA 과정동안 수행되는 위험원 분석 활동은 도출된 위험원에 대한 심각도 및 발생빈도의 초기평가를 수행해야 한다. 결과는 향후에 어디에서 정량화된 분석이 필요한지를 결정하는데 사용되고, 시스템의 상세설계가 진행됨에 따라 반복하고 보완되어서 완전한 분석과 위험도 평가가 수행될 수 있도록 한다.

PHA는 대상시스템의 기능요구사항 및 운영시나리오를 바탕으로 철도에서 발생할 수 있는 위험원 데이터를 바탕으로 실행한다. PHA의 목적은 일반적인 철도관련 위험원에서 대상 열차제어시스템의 안전성 활동을 통해 위험원을 인한 위험도의 크기를 감소시킬 수 있는 위험원을 분류하는 것이다. PHA는 대상시스템과 관련하여 기존 위험원 데이터 및 철도시스템에 일반적으로 내재되어 있는 위험원 중 대상 시스템 내부에 안전대책을 적용하여 위험도를 완화시킬 수 있는 위험원을 도출하여 목록화 한다. 따라서 PHA 보고서를 통해 대상 열차제어시스템으로 인해

발생할 수 있는 시스템 수준의 위험원을 도출하고, 도출된 위험원의 위험도를 예측하여, 위험도 완화를 위한 안전대책을 통해 대상시스템의 수명주기별 안전요구사항을 제시할 수 있다.

PHA의 시작점은 확인된 위험원의 수집물인 PHL이다. PHA은 이러한 위험원들을 좀 더 세부적으로 분석한다. 추가적으로, 분석가는 사전에 예측하지 않은 위험원을 확인하기 위하여 설계정보를 위험원 체크리스트와 비교한다. 이것은 분석가가 가능성 있는 위험원을 예상하거나 가정하도록 한다. PHA로부터의 출력결과는 확인되고 짐작된 위험원, 사고의 현황, 사고의 심각도 등을 포함한다. PHA출력물은 또한 확인된 위험원을 제거하거나 경감시키기 위해 수립된 설계 방법과 시스템 안전 요구사항을 포함한다. PHA는 설계 단계의 프로젝트 초기단계에 시작되기 때문에 사용할 수 있는 자료는 불완전한 수준이다. 이러한 불완전한 자료가 수정되고 보충될 경우 PHA도 마찬가지로 이에 따라 수정 및 추가 되어야 한다.

CRD시스템의 PHA는 총 8회에 걸쳐 다양한 방법적용과 수정이 이루어졌다. 방법의 차이는 크게 없으나 worksheet의 변경으로 인한 수정작업이 대부분이었으며, PHL에 따른 변경도 이루어졌다. 위험원을 도출하고 난 후, 이에 대한 원인과 대책을 수립하는 과정을 수행해야 한다. 이 단계에서는 아직 구체적으로 시스템에 설계가 이루어지기 전이기 때문에 수립되는 대책 또한 상세화 될 수 없다. 그렇기 때문에 시스템에 대한 구체적인 분석이 수행되기 전에 이루어지는 분석이기 때문에 예비위험원 분석이 수행된다. 본 연구에서는 위험원 도출에 따라 결과에 대한 시나리오 흐름이 결과분석을 통해 완성된 상태이기 때문에 Risks/Hazards analysis기법을 적용하고, 이에 Risk assessment를 통합하여 수행하였다. CRD시스템의 Risk assessment에 대해 기술하면 다음과 같다.

○ Risk assessment

본 연구에서의 위험도 평가의 목적은 크게 두 가지로 분류하였다. 첫 번째로 PHA단계에서 Risk analysis 결과로 THR(Tolerable Hazard Rate)을 산출하여 위험도수용기준과 SIL을 결정하기 위해 수행되며, 두 번째로 Causal analysis 단계에서 수행된 분석에 적용되어 Subsystem에서 발생되는 각 원인들이 위험도수용기준을 만족하는지 확인하기 위해 수행된다. 즉, 위험에 대한 THR을 시스템 한계에 가깝게 규명하고 각각의 Risk가 허용 가능한지 여부를 검토하기 위해 수행된다.

철도시스템에 적용할 수 있는 위험도평가를 위한 접근법으로 여러 가지 기법들이 있지만 시스템의 특성 등을 고려하여 알맞은 사항을 적용할 수 있다. 대부분의 Risk Assessment 방법은 고유의 장점을 가지고 있어 철도시스템에 적용되었으나, 적용하는 매개변수들의 모호한 분류로 인해 철도시스템에 해박한 전문가를 필요로 하기에 많은 비용과 시간을 소요하게 된다. 최근 독일 철도시스템엔 이러한 단점을 보완하여 개발된 BP-risk방법을 철도신호시스템에 적용하고 있다. BP-risk의 적용 절차는 대략적으로 다음 그림과 같다.

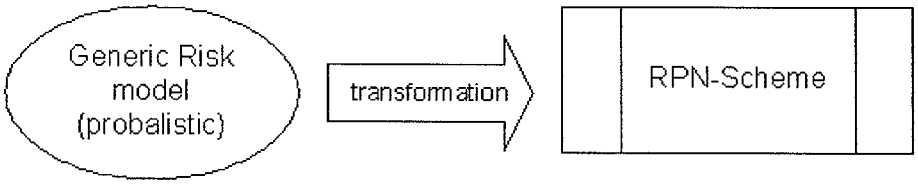


그림 3.5.6 BP-risk 개념도

- 1단계 : 일반적 확률적 Risk model 정의.
- 2단계 : 확률적 모델에 수학적인 변환을 통해 정성적인 모델 RPN에 기인한 정량적인 매개변수를 선택.
- 3단계 : 에러를 최소화 할 수 있고 의미가 명확한 매개변수 범위를 조정.

BP-risk는 독일 철도시스템에서 시작되고 적용된 시점이 짧다는 단점을 제외하면 다음과 같은 장점을 지니고 있다.

표 3.5.3 BP-risk 장점

장점
- 시스템 엔지니어링 규칙에 따라 명확한 요구사항으로 구성되었으며, 이해가 쉽다. - 정량적 방법에 비해 약 40%가량의 작업량 및 시간을 단축할 수 있어 효율적이다. - Risk평가 공식의 모든 매개변수들이 사용되어, 보다 정확한 평가가 가능하다.

○CRD시스템 BP-risk 적용

BP-risk를 적용하기 위한 원칙은 모든 컴포넌트들과 기능적인 인터페이스를 설명하는 정확한 시스템 정의에 있다. 시스템의 기능들은 인간과 기술의 상호작용에 의해 공급되는 것으로 간주된다. 시스템 기능에서 생긴 부분적인 Risk들이 첨가될 수 있고, 다음의 식(1)과 같이 전체 Risk는 부분적인 Risk를 모두 합한 것보다 더 크지 않다는 사실이 가정된다.

$$R \leq \sum_{i=1}^{n} R_i \qquad (1)$$

접근법은 고장이 발생한 경우에 각 시스템 기능의 영향을 평가하는 것이다. 일반적인 영향, 상태, 회피 확률들이 고려되어야만 한다. 부분 Risk의 경우 가장 간단한 접근법이 선택된다. 부분 Risk는 아래 식(2)에 있는 Parameter의 곱에 의해 좌우된다.

$$R_i = f_i \cdot g_i \cdot s_i \qquad (2)$$

여기서, f는 발생빈도, g는 검출되지 않거나 회피되지 않을 확률, s는 손상의 심각도를 나타내는 것으로 RPN과 같은 공식으로 접근하게 된다. 그러나 RPN과 달리 매개변수들을 세분화할 수 있다. BP-risk의 매개변수의 세분화와 절차는 다음의 그림과 같다.

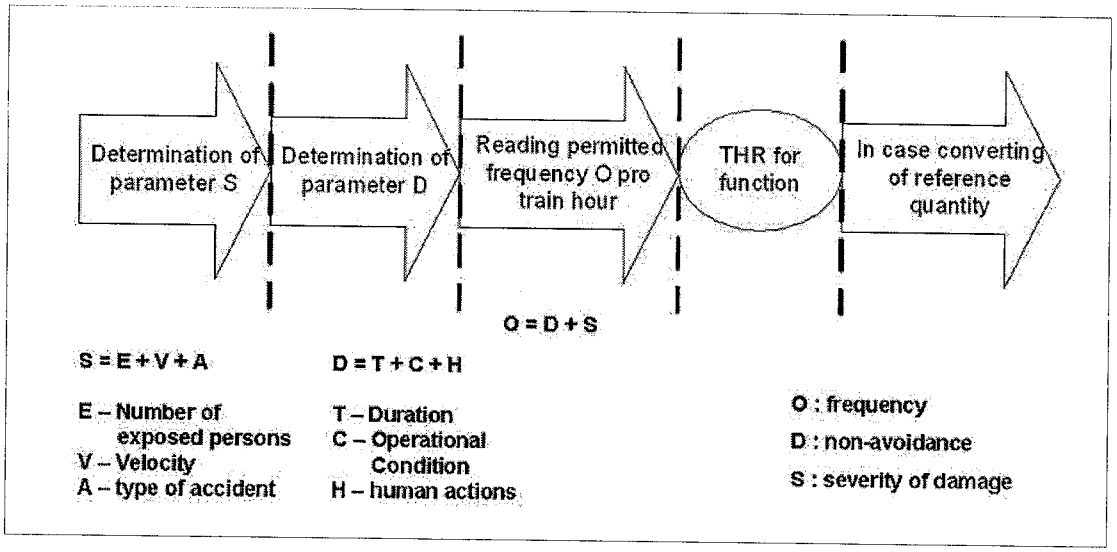


그림 3.5.7 BP-risk 수행절차

매개변수 S는 다음 표와 같이 세가지 부분변수로부터 구할 수 있다.

표 3.5.4 BP-risk S 결정 파라메터

$S = E + V + A$		
E	**V**	**A**
노출된 사람의 수	열차 속도	사고 유형

매개변수 D는 다음 표 3.5.5와 같이 세가지 부분변수로부터 구할 수 있으며, D는 시스템 경계를 벗어난 환경적 조건임을 주의한다.

표 3.5.5 BP-risk D 결정 파라메터

$D = T + C + H$		
T	***C***	***H***
위험 지속시간	운영 조건	인간 조정행위

BP-risk에서는 S+D를 통해 THR를 도출할 수 있지만, THR을 도출하기 전에 열차에 지속적인 영향을 미치는지에 대한 조정값을 추가하게 된다. 조정값 U는 다음과 같이 정의할 수 있다.

표 3.5.6 BP-risk U 파라메터

U	Type of Function	Type of Impact
-1	열차에 지속적으로 영향을 미치는 경우	중앙 제어적 기능
0		차상에서 작동되는 기능 (열차설비/기능)
0	열차에 비지속적으로 영향을 미치는 경우	드문 경우(선로차단기)
1		주기적인 경우(건널목)
2		종종 영향을 미치는 경우(선로전환기, 신호기)

최종적 BP-risk의 공식은 다음과 같이 정의된다.

$$R = S + D + U \qquad (3)$$

표 3.5.7 BP-risk 파라메터 정의

S					
E	노출된 사람의 수	***V***	열차속도	***A***	사고 유형
1	1인	1	very low	1	collision
2	few people			2	impact
3	several people	3	low	3	derailment
4	many people	4	moderate	4	crash
5	very many people	5	medium		
		6	high		
		7	very hige		

D					
T	위험 검지시간	C	운영 조건	H	인간 조정행위
1	very short	1	very low density	1	always possible
2	short	2	low density	2	often possible
3	medium	3	medium density	3	possible
4	long	4	high density	4	barely possible

표 3.5.8 BP-risk THR에 따른 SIL

S+D+U	THR (per train and per function)	Value	SIL
13	Once in 1 year	10^{-4}/h	0
14	Once in 3 year	4 x 10^{-5}/h	0
15	Once in 10 year	10^{-5}/h	0
16	Once in 30 year	4 x 10^{-6}/h	1
17	Once in 100 year	10^{-6}/h	1
18	Once in 300 year	4 x 10^{-7}/h	2
19	Once in 1,000 year	10^{-7}/h	2
20	Once in 3,000 year	4 x 10^{-8}/h	3
21	Once in 10,000 year	10^{-8}/h	3
22	Once in 30,000 year	4 x 10^{-9}/h	4
23	Once in 100,000 year	10^{-9}/h	4

BP-risk를 적용한 CRD시스템의 PHA는 전년도 보고서에 설명되어져 있다.

(라) 평가대상시스템 SIL 결정

CRD시스템의 SIL은 PHA 수행 결과 산출된 THR로부터 결정된다.

표 3.5.9 연구대상 열차제어시스템 SIL결정

Hazard	Cause	THR	SIL	System SIL
Hazard-1	1-1	1.00E-09	4	
	1-2	1.00E-08	3	
	1-3	1.00E-09	4	
	1-4	1.00E-08	3	
Hazard-2	2-1	1.00E-08	3	
	2-2	4.00E-09	4	4
Hazard-3	3-1	4.00E-09	4	
	3-2	1.00E-08	3	
	3-3	4.00E-09	4	
Hazard-4	4-1	1.00E-09	4	
	4-2	1.00E-09	4	

표 3.5.9에서와 같이 각 위험원에서 발생할 수 있는 원인별 THR과 이에 따른 SIL이 제시되었다. 따라서, CRD 시스템은 SIL-4에 대한 요건을 충족하기 위한 설계와 대책이 마련되어야 한다.

(마) 평가대상시스템 안전 요구사항

CRD 시스템의 PHA 및 SIL 결정 후, 시스템에 대한 안전요구사항이 도출된다. 본 연구에서는 안전요구사항을 두 가지로 분류하여 정리하였다.

- Functional Safety Requirements
- Technical Safety Requirements

CRD 시스템의 Functional Safety Requirements는 다음의 표 3.5.10과 같다.

표 3.5.10 Functional Safety Requirements

No.	Functional Safety Requirements
FR-1	* CRD시스템은 블록에 따른 적합한 열차 이격을 확보하여 열차간 충돌을 방지하여야 한다. - 허용이동권한 설정을 위한 블록의 적합성 검증 수행 - 열차 현재 위치에 대한 검증 수행
FR-2	* CRD시스템은 블록폐쇄 및 개방에 대한 검증을 수행하여 안전성을 확보하여야 한다. - ATS시스템의 블록 폐쇄/개방 명령에 대한 유효성 검증 수행
FR-3	* CRD시스템은 열차상태에 대한 정보를 ATS로 통보하여 관제사가 실시간으로 이에 대한 확인이 이루어질 수 있어야 한다.
FR-4	* CRD시스템은 열차와의 통신두절로 인한 영향을 최소화 하기 위해 열차검지 손실에 대한 검증을 수행한다.
FR-5	* CRD시스템은 열차진로설정 및 이에 따른 선로전환기 전환에 대한 제어명령을 검증/처리하여 안전성을 확보하여야 한다. - ATS 진로설정 명령에 대한 유효성 검사 - 연동처리 검증 - 선로전환기 방향전환에 대한 검증
FR-6	* CRD시스템은 다음의 설비에 대한 상태정보를 수집하여 관리하여야 한다. - 열차 상태정보 - 선로전환기 상태정보

FR-7	* CRD시스템은 다음의 사항에 대해 ATS로 알람 이벤트를 통보한다. - 열차와 통신두절 - 열차 고장 - 선로전환기와 통신두절 - 선로전환기 고장 - 열차과속 주행 시, - CRD시스템 계절체 시, - ATS 제어명령 부적합 및 오류 발생 시,

CRD시스템의 Technical Safety Requirements는 다음의 표 3.5.11과 같다

표 3.5.11 Technical Safety Requirements

No.	Technical Safety Requirements
TR-1	* CRD시스템은 SIL4를 만족하여야 한다
TR-2	* 하부시스템 또는 모듈에 대해 다음과 같은 분석을 수행하여 SIL4을 할당한다. - SSHA(Subsystem Hazard Analysis) - IHA(Interface Hazard Analysis) - OSHA(Operating & Support Hazard Analysis) - FTA(Fault Tree Analysis)
TR-3	* 허용이동권한 관련 모듈을 CRD시스템의 하부시스템에 독립적으로 구성한다.
TR-4	* 허용이동권한 관련 모듈의 결함 및 고장으로 인해 기능을 수행하지 못할 경우를 대비하여, 이중계로 구성한다.
TR-5	* 열차와의 무선통신에 대한 가용성 및 신뢰성을 확보하기 위해, 이에 대한 분석을 수행하여 그 결과가 SIL을 만족할 수 있어야 한다.
TR-6	* EN50129에서 권고하는 SIL4에 따른 소프트웨어 기술적 요구사항들을 만족함을 증명하여야 한다.
TR-7	* 열차진로 및 선로전환기 제어 관련 모듈을 CRD시스템의 하부시스템에 독립적으로 구성한다.
TR-8	* 열차진로 및 선로전환기 제어 관련 모듈의 고장으로 인해 기능을 수행하지 못할 경우를 대비하여 이중계로 구성한다.
TR-9	* 선로전환기와의 인터페이스에 대한 가용성 및 신뢰성을 확보하기 위해, 이

	에 대한 분석을 수행하여 그 결과가 SIL을 만족할 수 있어야 한다.
TR-10	* CRD시스템과 ATS간 인터페이스에 대한 가용성 및 신뢰성을 확보하기 위해, 이에 대한 분석을 수행하여 그 결과가 SIL을 만족할 수 있어야 한다.
TR-11	* CRD시스템과 열차간 무선통신의 오염 및 방해에 대한 구체적인 방어대책을 수립하여야 한다.
TR-12	* CRD시스템은 외부시스템과의 직접적인 인터페이스를 담당하는 모듈을 독립적으로 구성하여야 한다.
TR-13	* 또한 인터페이스 모듈의 고장으로 인해 기능을 수행하지 못할 경우를 대비하여 이중계로 구성한다.

(2) 평가대상시스템 SIL 할당

(가) Failure 분류

본 연구에서는 CRD시스템에서 발생할 수 있는 위험원은 Subsystem에서의 결함, 오류에서 비롯된 하드웨어적인 고장(Failure) 또는 소프트웨어적인(SW 코딩, 절차, 기타) 장애(Failure)에서 발생하기에 이에 대한 관계를 적용하였다. 고장 또는 장애(Failure)는 시스템의 레벨에 따라 상위레벨의 원인이 될 수 있음을 그림 3.5.8에서 확인할 수 있다.

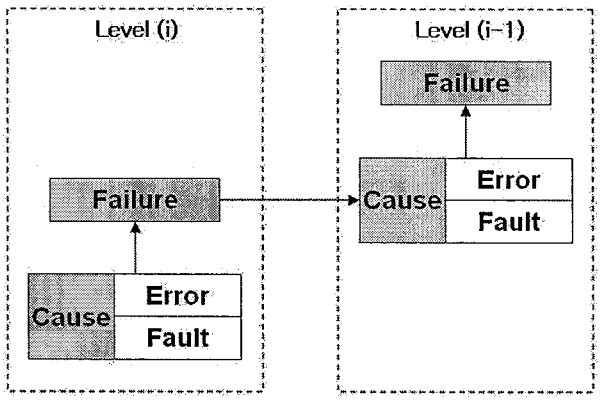


그림 3.5.8 Failure 정의

그림 3.5.8에서 i레벨에서 Cause(원인)는 그 자체가 해당 i레벨의 Error(오류) 또

는 Fault(결함)이 되지만, 이러한 Error나 Fault가 제어되지 않을 경우 이는 Failure(고장)을 발생시킨다. 이 경우, i레벨의 Failure는 i-1레벨에서 Cause가 되어 i-1레벨에 Failure를 발생시키게 된다. 전성활동 중 초기에 수행되는 Risk analysis는 Hazard를 도출하고 이에 대한 영향 및 결과에 대한 분석을 통해 위험정도를 판단하게 되고, 이렇게 정의된 위험정도에 따라 안전을 위한 요구사항을 산출하게 된다. Hazard의 분석에서 많이 발생하는 오류 중의 하나가 앞서 배경에서 기술된 바와 같이 무분별한 원인(Cause)을 도출하는 것이다. 그림 3.5.9에서와 같이 시스템을 구성하는 레벨에 따른 고장, 결함, 오류를 명확히 할 필요가 있다. 이에 대해 EN 50129에서는 그림 3.5.9와 같이 정의하고 있다.

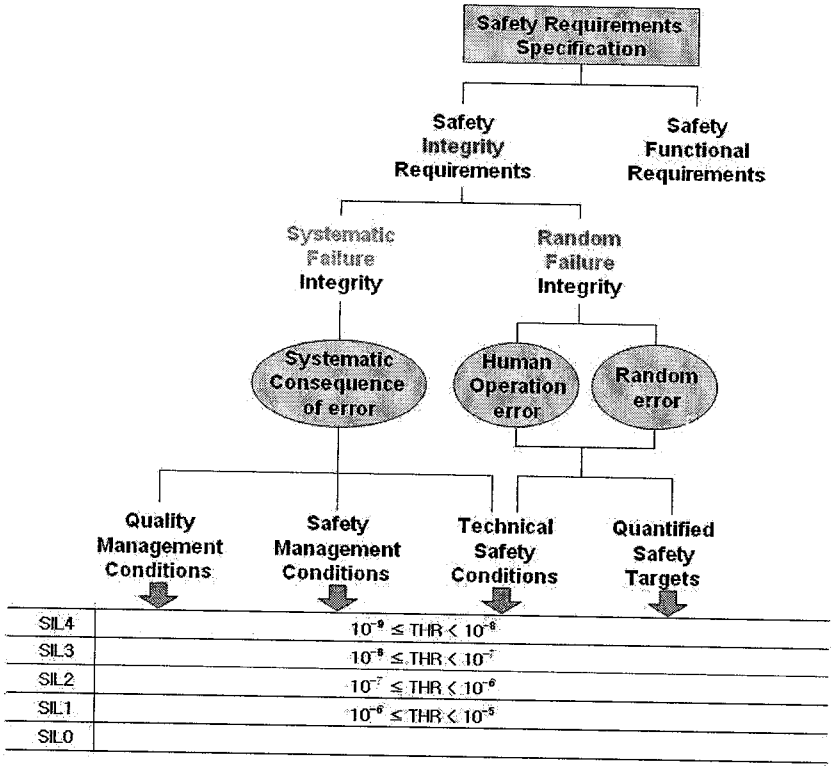


그림 3.5.9 Safety Integrity Requirement 정의

EN50129 규격에서는 안전요구명세서는 Safety Integrity Requirements와 Safety Functional Requirements로 크게 분류하였다. 그러나 분류된 요구사항은 분리될 수 없는 관계를 가지고 있다. Safety Functional Requirements는 개발하고자 하는 철도시스템에 필수적, 경험적으로 들어가야 할 안전과 관련된 기능(Safety Function)을 의미하지만, Safety Integrity Requirements는 철도시스템 또는 하부시스템(장

치)의 안전기능(Safety Function)의 수행능력을 분석하여 정량적, 정성적 확률을 도출하게 된다. Safety Integrity Requirements는 다음과 같이 분류된다.

- Systematic Failure Integrity
- Random Failure Integrity

하나의 하부시스템(장치)이 가져야 할 안전기능은 정의된 안전정도를 달성하기 위해서는 Systematic failure Integrity와 Random Failure Integrity 모두를 만족해야 한다. 즉, Systematic Failure Integrity는 인적오류와 관련되어 정량화 할 수 없는 다음과 같은 시스템적 (하드웨어/소프트웨어)오류 및 결함에 대해 분석이 이루어진다.

- Specification errors
- Design errors
- Manufacturing errors
- Installation errors
- Operation errors
- Maintenance errors
- Modification errors

위와 같은 오류 및 결함을 제거하기 위해 문서화, 체계화, 운영절차를 수립할 수 있는 품질관리, 안전관리 및 기술적인 안전조건이 적용된다. 시스템의 안전무결성 레벨(SIL)의 안전성 관리 절차에서 시스템/서브시스템의 Systematic failure는 가급적 피하고 Random failure를 제어하기를 권고하고 있으며, 이에 대한 구조/기법/수단을 규격 및 표준에서 제시하고 있다. 그 이유는 Systematic failure는 모든 원인을 도출하고 기록하는 것이 사실상 불가능하고 이를 저감시키고 회피하기 위한 정량적인 분석 또한 매우 어렵기 때문이다. 따라서 가능하다면 Random failure에 의한 정량적인 분석과 대책을 수립하도록 하여야 한다. Random Failure Integrity는 소프트웨어를 제외한 하드웨어의 정량적인 값을 도출하게 된다. 정량적인 값은 하드웨어 부품의 고장율, MTBF 등의 데이터에 의해 확률적으로 계산된다. 본 연구에서는 SSHA와 FTA를 통해 Systematic failure와 Random failure의 분석을 수행하였다.

(나) 평가대상시스템 Causal Analysis

SSHA기법은 Safety analysis를 위한 방법으로 Hazard, 원인, 영향, Risk 수준, 설계를 통한 저감방법 등을 도출하게 된다. SSHA는 상세설계 단계에서 이루어지는 기법이며, 기존에 수행된 PHA보다 더 상세한 원인에 대해 분석하게 되며, 보다 상세한 안전요구사항을 도출할 수 있다. SSHA는 PHL과 PHA에서 도출된 위험원에 대해 보다 상세하게 분석할 수 있다는 점이 장점이라고 할 수 있다. 즉, FMEA나 HAZOP과 같이 새로운 방법으로 위험원을 도출할 필요 없이 PHA의 위험원을 그대로 적용하여 보다 심도 깊은 원인 및 결과를 분석할 수 있다.

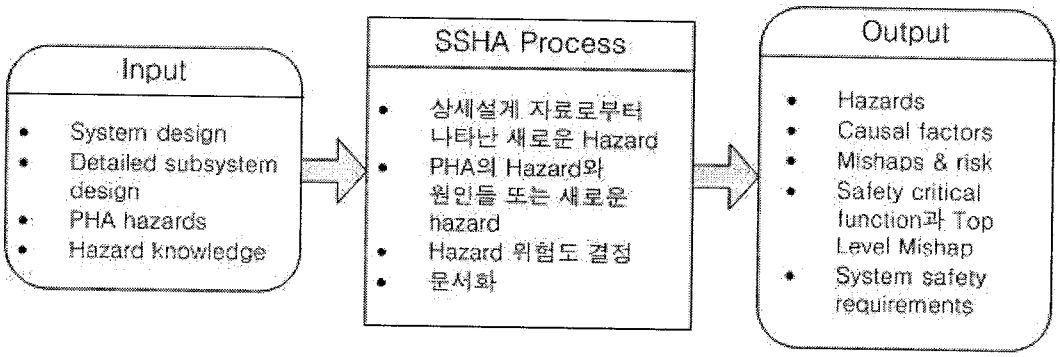


그림 3.5.10 SSHA 절차

○ SSHA 방법

SAHA의 방법론은 다음의 그림과 같이 Subsystem의 상세설계 관련 문서와 기존에 도출된 PHA hazards, Hazards Checklists 그리고 TLMs(Top Level Mishap)과 SCF(Safety Critical Function) 정보가 입력되어야 하며, 입력된 자료를 기반으로 관련 엔지니어간 회의를 통해 SSHA worksheet가 작성된다.

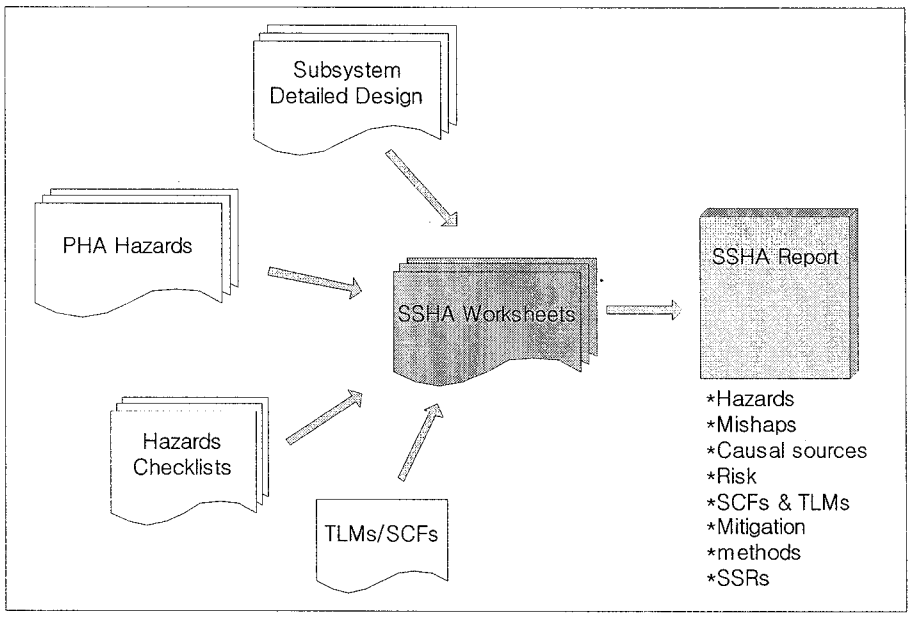


그림 3.5.11 SSHA 방법

SSHA의 Worksheet는 PHA Worksheet와 동일하다. 그 차이점은 다음의 그림과 같이 원인이 Subsystem레벨에서 도출된다는 것이다. 이러한 워크쉬트에 따른 결과는 전년도까지에 수행되었다.

Preliminary Hazard Analysis									
System : CRD System Subsystem/Function : DCM subsystem						Date : Version :			
No.	Hazard	Cause	Effect	mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-5	PMA 설정 오류	프로그램 오류, 로직 오류	열차충돌	Auto	1C	시스템 이중계 구성, Black Box Test 수행	1E		

Subsystem Hazard Analysis									
System : CRD System Subsystem/Function : DCM subsystem						Date : Version :			
No.	Hazard	Cause	Effect	mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-5	PMA 설정 오류	이동권한의 마지막 블록의 적합성 검사 오류	열차충돌	Auto	1C	시스템 이중계 구성, Black Box Test 수행	1E		

CRD 시스템의 Causal Analysis단계는 Consequece Anlysis단계와 PHA단계에서

분석된 위험원과 원인 그리고 1차적으로 제시된 대책과 안전관련 요구사항들에 대해 확인 및 구체화 시키는 단계라 할 수 있다. 이에 Causal Analysis는 다음과 같은 형식으로 진행되었다.

- Subsystem Hazard Analysis(SSHA) - Systematic failure
- Fault Tree Analysis(FTA) - Random failure

Systematic failure와 Random failure에 대해 IEC61508에서는 다음과 같이 정의하고 있다.

- Random failure : 이는 안전관련 하드웨어어의 SIL을 달성하는 것은 합리적 수준의 정확도로서 측정될 수 있으며, 따라서 SIL에 따라 확률의 조합을 위해 Subsystem에 할당될 수 있다.
- Systematic failure : Systematic failure는 평균 고장률(mean failure rate)로 측정될 수는 있지만, 결함과 고장에 대한 관련데이터를 이용한 정량적인 측정은 어렵다.

위에서 정의한 바에 따라 예를 들면, Redundant 채널은 Random failure를 제어 및 감소하기 위해서는 매우 효과적이지만 Systematic failure엔 거의 적용되지 않는다. 두 가지 형식으로 진행되는 Causal Analysis는 우선적으로 SSHA를 수행하여 PHA에서 다루어진 위험원에 대한 분석을 Subsystem에서 다음의 사항에 대해 구체적으로 다루게 된다.

- 원인 : Failure, Fault 그리고 Error 관계 적용
- 고장/장애 : Systematic Failure와 Random failure 적용
- 저감대책 및 활동 : Subsystem에서 적용할 수 있는 대책 및 활동

○ Subsystem Hazard Analysis(SSHA)

SSHA에서는 위험원에 대한 모든 원인을 기술하게 되며, 각 원인을 Systematic failure와 Random failure로 구분하여 Systematic failure사항에 대해서만 PHA에서와 동일한 BP-risk를 적용하여 THR을 도출하게 된다. 나머지 Random failure는 FTA에서 적용하게 되지만, SSHA sheet에는 해당되는 각 설비의 고장율을 입력하였다. CRD시스템의 SSHA 결과 중 BP-risk를 적용한 Systematic failure에 대한

결과는 다음과 같다. CRD시스템의 SSHA 결과 부록B 에서 기술한다.

표 3.5.12 연구대상 열차제어시스템 SSHA 결과

Hazard-1			
Subsystem	SSHA No.	THR	SIL
DCM	1.1.1.1	1.00E-09	4
	1.1.1.2	1.00E-09	4
	1.1.2.1	1.00E-09	4
	1.1.2.2	1.00E-09	4
ICM	1.3.1.1	4.00E-08	3
	1.3.1.2	4.00E-08	3
	1.3.4.1	4.00E-07	2
	1.3.4.2	4.00E-07	2

Hazard-2			
Subsystem	SSHA No.	THR	SIL
DCM	2.1.1	4.00E-08	3
	2.1.2.1	4.00E-08	3
	2.1.2.2	1.00E-08	3

Hazard-3			
Subsystem	SSHA No.	THR	SIL
ICM	3.1	4.00E-08	3
	3.2.1.1	4.00E-08	3
	3.2.1.2	4.00E-08	3
	3.2.4.1	4.00E-07	2
	3.2.4.2	4.00E-07	2

Hazard-4			
Subsystem	SSHA No.	THR	SIL
DCM	4.1.1.1	1.00E-09	4
	4.1.1.2	1.00E-09	4
	4.1.2.1	1.00E-09	4
	4.1.2.2	1.00E-09	4

○ Subsystem Fault Tree Analysis(FTA)

CRD 시스템의 FTA를 수행하기 위해 우선적으로 표 3.5.13과 같은 CRD시스템의 하드웨어 구성 및 이에 대한 입력 데이터를 필요로 한다.

표 3.5.13 연구대상 열차제어시스템 하드웨어 구성 및 데이터

	Failure rate	수량	MTBF	MTTR
CRD system	62.9818 E-06		15877.6	0.94
EIM 모듈	5.2490 E-06	2	95254.5	1
ICM 모듈	8.1645 E-06	2	61240.0	1
DCM 모듈	8.1645 E-06	2	61240.0	1
비교처리 모듈	6.0977 E-06	2	81997.5	1
네트워크 스위치	2.1479 E-06	1	465570.0	0.5
광스위치	2.1377 E-06	1	467784.0	0.5
UPS	0.1100 E-06	1	9090909.0	1
분전반	0.0034 E-06	1	286979000.0	0.5
무선AP	3.1746 E-06	1	315000.0	0.5
DCM-EIM 케이블	0.0176 E-06	1	56818180.0	0.5
ICM-EIM 케이블	0.0176 E-06	1	56818180.0	0.5
광스위치간 케이블 (차상)	0.0176 E-06	1	56818180.0	0.5
광스위치간 케이블 (선로전환기)	0.0036 E-06	1	2794333333.0	0.5
전원공급 케이블	0.0029 E-06	1	349212600.0	0.5

각 위험원별 Subsystem에 대한 FTA결과는 다음의 표 3.5.14와 같다.

표 3.5.14 Subsystem별 FTA결과

		Hazard-1	Hazard-2	Hazard-3	Hazard-4
	F	**0.031897**	**0.0149131**	**0.0238305**	**0.0280559**
	Q	**5.10808e-04**	**1.27717e-05**	**2.10407e-05**	**2.6277e-05**
DCM	F	0.0135046	0.00534237	-	0.0134306
	Q	1.35373e-05	5.25787e-06	-	1.35055e-05
ICM	F	0.00911911	-	0.0143635	0.0052585
	Q	4.89749e-04	-	1.35355e-05	5.25787e-05
EIM	F	0.00442772	0.0096221	0.00960502	0.0096221
	Q	2.27377e-06	7.51385e-06	7.50523e-06	7.51385e-06

위의 분석 결과 각 위험원별 Subsystem의 가용도는 표 3.5.15와 같다.

표 3.5.15 Subsystem별 가용도

	Hazard-1	Hazard-2	Hazard-3	Hazard-4
System	99.9489%	99.9987%	99.9978%	99.9973%
DCM	99.9986%	99.9994%	-	99.9986%
ICM	99.9510%	-	99.9986%	99.9947%
EIM	99.9997%	99.9992%	99.9992%	99.9992%

(다) 평가대상시스템 Subsystem SIL할당

CRD시스템은 최초 PHA에 의한 분석 결과 SIL4를 도출하였으며, 각 Hazard별 SIL은 다음의 표 3.5.16과 같다.

표 3.5.16 연구대상 열차제어시스템 PHA 결과

Hazard	Cause	THR	SIL
Hazard-1	1-1	1.00E-09	4
	1-2	1.00E-08	3
	1-3	1.00E-09	4
	1-4	1.00E-08	3
Hazard-2	2-1	1.00E-08	3
	2-2	4.00E-09	4
Hazard-3	3-1	4.00E-09	4
	3-2	1.00E-08	3
	3-3	4.00E-09	4
Hazard-4	4-1	1.00E-09	4
	4-2	1.00E-09	4

SSHA에 의해 Systematic failure에 대한 분석 결과 다음의 표 3.5.17과 같다.

표 3.5.17 연구대상 열차제어시스템 SSHA결과

Hazard	Subsystem	THR	SIL
Hazard-1	DCM	1.00E-09	4
	ICM	4.00E-08	3
Hazard-2	DCM	1.00E-08	3

Hazard-3	ICM	4.00E-08	3
Hazard-4	DCM	1.00E-09	4

FTA에 의해 Random failure에 대한 분석 결과 다음의 표 3.5.18과 같다.

표 3.5.18 연구대상 열차제어시스템 FTA결과

Hazard	Unreliability	Unavailability	availability(%)
Hazard-1	0.031897	5.10808E-04	99.9489%
Hazard-2	0.0149131	1.27717E-05	99.9987%
Hazard-3	0.0238305	2.10407E-05	99.9978%
Hazard-4	0.0280559	2.62770E-05	99.9973%

위의 분석 결과에 의해 CRD시스템 Subsystem별 SIL은 다음과 같이 할당된다.

표 3.5.19 연구대상 열차제어시스템 Subsystem별 SIL

Subsystem	SIL
DCM	4
ICM	3
EIM	4

표 3.5.20 위험원별 Subsystem 가용도

	Hazard-1	Hazard-2	Hazard-3	Hazard-4
System	99.9489%	99.9987%	99.9978%	99.9973%
DCM	99.9986%	99.9994%	-	99.9986%
ICM	99.9510%	-	99.9986%	99.9947%
EIM	99.9997%	99.9992%	99.9992%	99.9992%

DCM subsystem은 SSHA에서 Systematic failure분석에 의해 SIL4에 해당하는 THR값이 산출되었으며, Random failure분석에 의해 해당되는 위험원별 각 신뢰도는 99.99%를 나타내었다. ICM subsystem은 SSHA에서 Systematic failure분석에

의해 SIL3에 해당하는 THR값이 산출되었으며, Random failure분석에 의해 해당되는 위험원별 각 신뢰도의 최하위 값이 99.95%를 나타내었다. EIM subsystem은 SSHA에서 Systematic failure분석에 의해 SIL이 도출되지는 않았지만, DCM과 ICM을 지원하는 시스템으로서 DCM의 안전무결성과 동일해야 하기에 SIL4로 정의하였으며, Random failure분석에 의해 해당되는 위험원별 각 신뢰도는 99.99%를 나타내었다. 앞서 정의된 CRD시스템 안전요구사항에 다음의 사항이 추가된다.

- DCM subsystem은 SIL4를 만족하여야 한다.
- ICM subsystem은 SIL3를 만족하여야 한다.
- EIM subsystem은 SIL4를 만족하여야 한다.
- DCM subsystem은 99.99%의 가용도를 만족해야 한다.
- ICM subsystem은 99.95%의 가용도를 만족해야 한다.
- EIM subsystem은 99.99%의 가용도를 만족해야 한다.

따라서 CRD system(DCM, ICM, EIM subsystem)은 SIL3과 SIL4에 적합한 다음과 같은 기법 및 수단이 Safety Requirements에 추가되어 설계에 적용되어야 한다.

표 3.5.21 연구대상 열차제어시스템 기법 및 수단 요구사항

기법/수단	SIL3/4
안전성과 관련없는 시스템과 안전성 관련 시스템의 분리	CRD시스템과 외부 인터페이스 되는 시뮬레이터간 인터페이스 정의 및 분석
검사항목	모든 안전성 Lifecycle단계에 대한 상세한 검사
Hazard Log	전체 시스템 Lifecycle동안 작성되고 관리됨.
fail-safe구조	DCM, ICM, EIM에 대한 fail-safe 구조 확립
단일결함의 검지	Random failure분석에 따른 단일 결함의 검출 및 회피에 대한 시간 확보
동적 결함 검출	온라인 동적 시험을 통한 안전성 확인
소프트웨어 구조	EN50128(IEC62279)에 따른 소프트웨어 구현 및 시험
고장율 계산	하드웨어 최악의 조건에 근거를 둔 고장율 설계에 반영
신뢰성 확보	Random failure분석에 의한 신뢰성 값 유지를 위해 설계에 반영
유지보수 수행	Random failure분석에 의해 각 설비에 대한 유지보수 계획 수립 및 시행

(라) Risk Analysis 결과

결과로는 시스템의 SIL 정의와 이에 해당되는 Subsystem 또는 안전관련 기능에 대한 SIL이 할당되었다. 전체적인 구조는 다음과 같다.

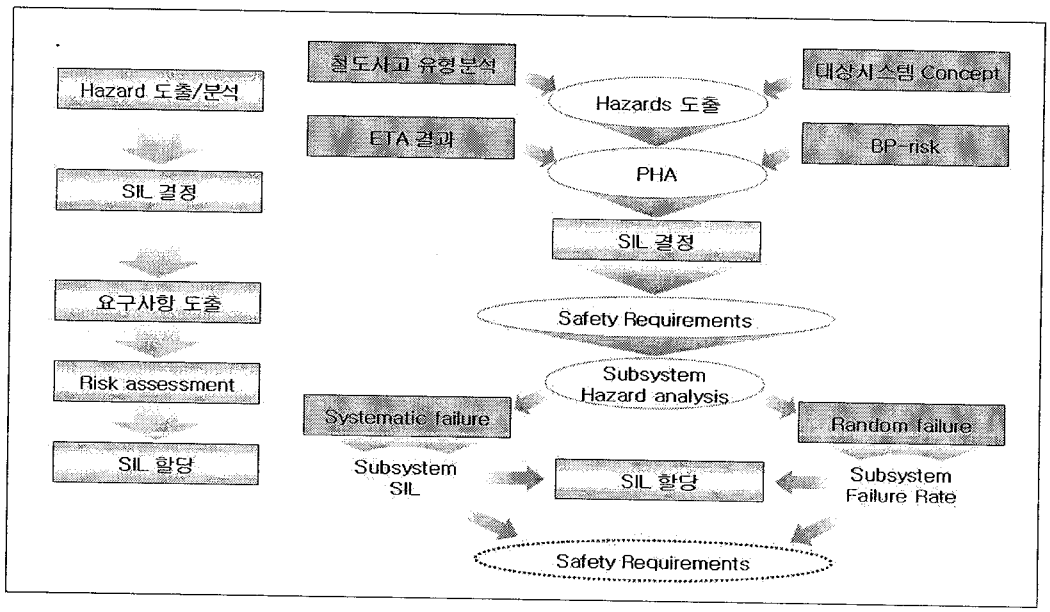


그림 3.5.12 연구 프로세스 도식

표 3.5.22 연구내용 및 연구결과

연구내용	연구결과
연구대상시스템 정의 -시스템 Concept -시스템 구성	1. 연구대상시스템 Concept - 열차제어시스템(열차진로 및 간격제어) 정의 - 기존 시스템 개념 적용 2. 연구대상시스템 구성 - 연구대상시스템의 Subsystem(Module)정의 - 외부 인터페이스 시스템 정의
철도사고 수집 및 유형별 분류 -철도사고 자료수집 -철도사고 유형별 분류	1. 철도사고 유형별 자료수집 - 충돌사고 빈도 및 유형 - 탈선사고 빈도 및 유형 2. 철도사고 유형별 분류
연구대상시스템 Hazard 도출/분석	1. Hazard 도출 - 철도사고에 기인한 연구대상시스템 Hazard 도출 2. Hazard 분석 - PHA 수행 시, BP-risk방법론 적용으로 THR산출

SIL정의	1. PHA결과 THR에 따른 전체 시스템의 SIL정의-SIL4
연구대상시스템 요구사항 제시	1. 연구대상시스템 요구사항 제시 - Functional Safety Requirements 제시 - Technical Safety Requirements 제시
Hazard별 Risk assessment -Subsystem Hazard analysis -Fault Tree analysis	1. Risk assessment 수행 - SSHA 수행 시, Systematic failure는 PHA에서 적용된 동일한 BP-risk방법론 적용 - SSHA 수행 시, Random failure는 FTA적용
SIL할당 및 요구사항 갱신	1. SIL할당 및 요구사항 갱신 - Rsik assessment 수행 결과, 각 Subsystem별 SIL할당 및 요구사항 갱신

(3) Verification & Validation

(가) V&V 목적

V&V는 결함을 찾고, 요구된 기능과 속성이 소프트웨어와 시스템에 제대로 반영되어 있는가를 알아보는 것이다. V&V 목적은 다음과 같다.

- 운영 특성, 기능 및 물리적인 구조를 설명하는 모든 문서를 검토하여 제안된 요구사항과 시스템 설계와 Software 개발이 타당한지 Verification하고, 만일 차이가 존재할 경우 이를 규명하고 보완하여 최종적으로 시스템이 요구사항에 부합함(Validation)을 검사하기 위함이다.
- 시스템의 성능과 설계 구조를 Verification하기 위함이다.
- 시스템 통합을 통해 하부시스템을 Verification하고 시스템에 대한 Validation 하기 위함이다.
- 외부 시스템과의 시스템 통합을 Verification하기 위함이다.
- 공급자의 환경에서 개발된 시스템이 시스템 사양에 따라 운영됨을 입증하기 위함이다.
- 소프트웨어 오류들을 초기에 검증하고 교정하는 것을 용이하게 한다.
- 프로세스와 산출물 리스크에 대한 관리를 강화한다.

- 프로그램 성능, 일정, 예산 요구사항들을 충족시키기 위해 소프트웨어 생명주기 프로세스를 지원한다.
- 소프트웨어와 시스템 성능에 대한 초기 평가를 제공한다.
- 소프트웨어와 시스템 성능에 대한 객관적 증빙을 제공하여 공식적인 인증절차를 지원한다.
- 소프트웨어 개발과 유지보수 절차를 향상시킨다.

통합된 시스템 분석 모델을 위한 프로세스 개선을 지원한다.

(나) V&V 원칙

V&V 활동은 시스템과 소프트웨어 개발 산출물에 대해 적용되며 다음 사항을 지원한다.

- 각 생명주기 단계에서의 산출물에 대한 아래 사항의 검증
  - 이전의 생명주기 단계에서 나타난 요구사항에 대한 적합성(정확성, 완전성, 일관선, 타당성등)
  - 각 단계의 표준, 실무, 규약에 대한 만족
  - 생명주기 다음 단계의 활동을 위한 기초 마련
- 최종 완성 제품이 설정된 시스템 및 소프트웨어 요구사항을 준수하고 있는 지 확인

V&V 작업은 설계 및 개발 조직과 분리된 회사 내 프로젝트 조직으로서 독립성이 보장된 RAMS팀과 품질보증팀에 의해 수행된다. Verification은 RAMS팀에 의해 수행되고, Validation은 품질보증팀에 의해 수행된다. 시스템 수명 주기의 단계별 검증 활동을 통해 각 단계의 결과가 입력사항과 부합하는지가 Verification될 것이다. Verification 활동은 분석/조사 및 입증/시험으로 분류된다.

- 분석/조사: 기능적 및 물리적인 구조, 내부 및 외부 인터페이스, 및 이러한 사항들에 대한 관계를 확인하고, 요구사항 할당을 제어 관리하고, 요구사항을 통해 추후 개발될 시스템에 대한 일치성 및 무결성을 verification하기 위함이다.
- 입증/시험: 입증과 시험은 시뮬레이션이나 실행을 포함한다.

시스템 통합과 시스템 설치, 그리고 이에 대한 기능 및 성능을 확인하기 위해 기

능 및 구조 시험을 실시한다. 시스템 통합 단계 후 시스템 설치 후 현장에서 실시되는 Validation 활동을 통해 시스템이 주어진 요구사항에 부합하는가가 검사될 것이다. 현장에서의 시스템 Validation는 실제 환경에서 구현되는 시스템 시험을 포함한다. 시뮬레이터는 단지 시스템 기능 및 성능 시험만을 위해 사용될 것이다.

(다) Verification

○ 요구사항 단계

- 추적성 분석 : 소프트웨어 요구사항 및 안전 요구사항과 시스템 요구사항 간의 양방향 추적성을 밝혀낸다.
- 요구사항 평가 : 소프트웨어 요구사항(기능, 인터페이스, 안전성, 사용자 운영 등)에 대하여 정확성, 일관성, 가독성, 시험가능성 등을 평가한다.
- 인터페이스 분석 : 소프트웨어 요구사항이 정확하고, 일관성 있고, 시험 가능한지 확인한다.
- 시험 계획 : 시스템 시험 계획을 수립하고, 검증한다.
- 위험 분석 : 위험을 분석, 검토하고 갱신한다. 위험요소를 제거, 감소, 약화하기 위한 권장사항을 제시한다.

○ 설계 단계

- 추적성 분석 : 설계 문서와 요구사항 간의 추적성을 분석한다.
- 설계 평가 : 설계 문서의 정확성, 일관성, 가독성, 시험 가능성 등을 평가한다.
- 인터페이스 분석 : 설계 인터페이스의 정확성, 일관성, 시험 가능성을 검증한다.
- 시험 계획 : 모듈 요구사항을 만족하기 위한 모듈시험과 통합시험 계획 및 검증과 시험 설계 및 검증을 수행한다.
- 위험 분석 : 이전의 작업 보고서를 이용하여 위험 분석을 검토하고 갱신한다. 위험요소를 제거, 감소, 약화시키기 위한 권장사항을 제시한다.

○ 제작/구현 단계

- 추적성 분석 : 원시 코드와 설계 명세서 간의 추정성을 분석한다.
- 원시코드 평가 : 원시 코드와 문서에 대하여 정확성, 일관성, 가독성, 시험 가

능성을 평가한다.

- 인터페이스 분석 : 원시 코드 인터페이스의 정확성, 일관성, 시험 가능성을 검증 및 확인한다.
- 시험 : 모듈시험, 통합시험, 시스템시험을 위한 시험 사례와 절차를 개발한다. 모듈시험을 수행하고, 설계대로 구현되었는지를 분석한다.
- 위험분석 : 이전의 작업 보고서를 이용하여 위험 분석을 검토하고 갱신한다. 위험요소를 제거, 감소, 약화시키기 위한 권장사항을 제시한다.

○ 시험 단계

- 추적성 분석 : 시험 계획, 설계, 사례, 절차 사이에 정확한 관계가 존재하는지 검증한다. 모든 시험 절차로 시험 계획을 유추할 수 있는지 검증한다.
- 시험 : SW 통합 시험을 수행하고 검증한다. 시스템 시험을 수행하고 검증한다.
- 위험 분석 : 이전의 작업 보고서를 이용하여 위험 분석을 검토하고 갱신한다. 위험요소를 제거, 감소, 약화시키기 위한 권장사항을 제시한다.

○ 설치 단계

- 설치 형상 감사 : 소프트웨어가 정확하게 설치되고 운영되기 위하여 요구되는 모든 소프트웨어 산출물이 설치 패키지 안에 모두 있는가 확인한다. 공급되는 파라미터 값이 정확한지 검증하기 위해서 운영환경에 의존되는 조건을 확인한다.
- 설치 점검 : 설치된 소프트웨어가 V&V를 실시했던 소프트웨어와 일치하는지 검증하기 위하여 분석이나 시험을 수행한다.
- 위험 분석 : 이전의 작업 보고서를 이용하여 위험 분석을 검토하고 갱신한다. 위험요소를 제거, 감소, 약화시키기 위한 권장사항을 제시한다.

○ Verification Task

표 3.5.23 Verification 업무

Task No.	Verification task description	Input documents	Output documents
Software Requirements Phase			
1	Software requirements test specification	- SQAP - Software Requirements Specification	- Software Requirements Test Specification
2	Software requirements verification	- SQAP - System Safety Requirements Spec. - Software Requirements Specification	- Software Requirements Specification Verification Report
3	Safety Requirements(by PHA) verification	- System Safety Requirements Spec. - Software Requirements Specification	- Software Requirements Specification Verification Report
4	Software Requirements Review	- Software Requirements Specification	- Review Report
Software Architecture Design Phase			
5	Interface verification	- Software Requirements Specification - Software Design & Architecture Specification	- Software Design & Architecture Verification Report
6	Software Architecture Design verification	- Software Requirements Specification - Software Design & Architecture Specification	- Software Design & Architecture Verification Report
7	Safety Requirements verification	- System Safety Requirements Spec. - Software Requirements Specification	- Software Requirements Specification Verification Report
8	Software / Hardware Integration Test generation	- Software Design & Architecture Specification	- Software / Hardware Integration Test Plan/Specification
9	Software Architecture Design Review	- Software Design & Architecture Specification - Software / Hardware Integration Test Plan/Specification	- Review Report
Software Design Phase			
10	Software Module Test Specification generation	- Software Module Design Specification	- Software Module Test Specification
11	Software Integration Test Plan generation	- Software Design & Architecture Specification	- Software Integration Test Plan/Specification
12	Final Software Design Review	- Above + Software Module	- Review Report

		Design Specification	
13	Final Software Design verification	- Software Design & Architecture Specification - Software Module Design Specification	- Software Design & Architecture Verification Report
Software Implementation Phase			
14	Code Walkthrough/Review	- Software Source code - Software Module Test Specification - Coding Standard	- Source code Verification Report
15	Software module test	- Software Module Test Specification	- Software Module Test Report
16	SW Data test	- Data Test Specification	- Software Data Test Report
Software Integration Test Phase			
17	Test Planning Review	- Software Module Test Report - Software / Hardware Integration Test plan - Software Integration Test Plan	- Review Report
18	Software integration test	- Executable Files - Software Integration Test Plan	- Software Integration Test Report
Software/Hardware Integration Test Phase			
19	Software / Hardware integration test	- Executable Files - Software / Hardware Integration Test Plan	- Software / Hardware Integration Test Report
20	Integration Tests Review	- Software Integration Test Report - Software / Hardware Integration Test Report	- Review Report
Installation Phase			
21	Installation Verification	- Installation Specification	- Installation Verification Report
System Integration Test Phase			
22	System Integration tests	- Executable Files - System Integration Test Plan	- System Integration Test Report
23	External System Interface Tests	- Executable Files - System Integration Test Plan	- System Integration Test Report
24	Software Function Review / Software Physical Review	- Software Integration Test Report - Software / Hardware Integration Test Report - System Integration Test Report	- Review Report

(다) Validation

○ Validation Task

표 3.5.24 Validation 업무

Task No.	Validation task description	Input documents	Output documents
System Validation Phase			
1	Software Acceptance/Validation Test	- Software Requirements Test Specification - Software Requirements Specification - Software Design & Architecture Specification - Software Module Design Specification - Software Source Code - Software Module Test Report - Software Integration Test - Report - Software / Hardware Integration Test Report - Software Verification & Validation Plan	- Software Validation Report
2	Interface validation test	- Software Requirements Test Specification - Software Requirement Specification - CTC-External system I/F Specification - Interface simulator	- Software Validation Report

(4) 평가대상시스템 Safety Case

평가대상시스템에 대한 Safety Case 문서는 안전성 활동 수행결과를 포함해서, 시스템의 전체적인 안전성 입증문서를 의미한다. 본 과제에서의 평가대상시스템의 Safety Case 문서는 당해연도에 작성을 시작하여 차년도에 완료될 예정으로 작성 중에 있으며, 문서의 주요한 부분에 대해서는 해외 안전성 전문 기관의 기술자문의 수행을 통해 보완되었다.

당해연도에는 Safety Case 문서 중 '시스템 정의', '품질안전 보고서', '안전관리 보고서'에 대해 작성되었으며, '기술안전보고서'에 대한 일부분이 수행 되었다. 이에 대한 자세한 내용은 본 절의 부록 A에 정리되어 있다.

(5) 열차제어시스템 안전성 활동 기술 지침서

본 절의 적용성 기술 개발은 대상시스템에 적용을 통한 안전성 활동 수행기술 연구 및 기술개발에 목적이 있다. 당해연도에는 이러한 기술개발 결과들의 실용화와 전년도에 작성한 Safety Case 작성 가이드라인 초안의 구체화를 위해 당해연도에 '열차제어시스템 안전성 활동 기술 지침서 초안'을 작성하였다. 본 지침서는 안전성 활동을 수행하기 위한 절차 및 방법을 설명한 것으로, 이 지침서를 통해 안전성 활동의 수행 및 Safety Case 작성에 활용될 수 있을 것으로 예상한다. 또한 본 기술지침은 본 과제를 통해 개발된 연구결과의 산업계 보급 및 전파를 목적으로 하고 있다. 당해연도에 작성한 초안은 차년도의 연구를 통해 보완되어 최종적으로 작성될 예정이다.

■ *1. 개요*

지침서의 목적

본 지침서는 열차제어시스템 개발 시 안전성 활동을 수행하기 위한 절차와 방법을 제공한다.

본 지침서는 CENELEC, IEC를 기반으로 국제규격에 준한 세부적인 활동에 대해 기술한다.

본 지침서는 System Engineering을 기반으로 하는 안전성 활동에 대해 기술한다.

본 지침서의 최종적인 목적은 열차제어시스템의 안전을 확보하여 인적피해, 재산상의 피해를 최소화하고자 한다.

지침서의 범위

본 지침서는 열차제어시스템에 포함되는 지상장치 및 차상장치를 대상으로 전반적인 안전성활동에 적용된다.

본 지침서는 열차제어시스템을 개발하는 모든 기관에서 적용할 수 있다.

본 지침서는 국제규격을 준수하는 일반적인 안전성 활동에 적용할 수 있으나, 국제규격 범위를 벗어난 안전성 활동에는 부분적으로 제외 및 제한될 수 있다.

System Engineering

System Engineering

System Engineering은 고객 요구를 만족하는 통합된 수명주기 균형시스템 해결책을 발전시키고 검증하는 다분야 학문의 엔지니어링 프로세스로서, 열차제어시스템 개발 프로세스에 적용된다.

System Engineering 활동은 시스템 분석 및 통제로 요건분석(Requirement Analysis), 기능분석(Functional Analysis) 및 할당(Allocation) 그리고 설계조합(Design Synthesis)로 이루어지며, System Engineering 통제는 의사결정과 요건을 추적하고, 기준을 유지하며, 인터페이스 및 위험을 관리하는 반복적이고 순환적인 활동이다.

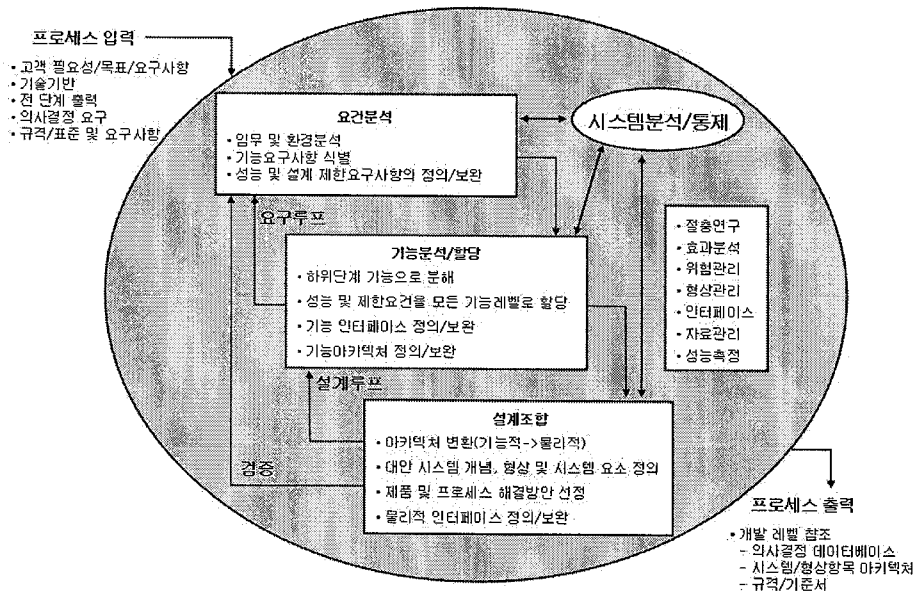


그림 1. System Engineering 개요

요건분석

System Engineering 프로세스의 첫 단계로 입력 자료를 분석하는 것이다. 요건분석은 기능 및 성능요건을 개발하는데 적용된다. 즉 고객요건은 시스템이 무엇을 어떻게 수행할 것인지를 정확하게 나타내는 요건 설정으로 변환된다.
System Engineer는 요건들이 명확하고 완전하며 간결한지 검증해야 한다.
요건분석은 기능요건과 설계 제약사항을 명확하게 정의해야 한다.

- 기능요건은 수량, 품질, 적용범위, 기간, 유용성에 대해 정의
- 설계제약사항은 설계의 유연성을 제한할 수 있는 환경조건, 한계, 위협으로부터의 보호, 규격등으로 정의

기능분석/할당

기능은 요건분석을 통해 식별된 상위 레벨 기능을 하위 레벨 기능으로 분해함으로써 분석된다. 상위 레벨에 관련된 성능요건은 하위레벨 기능으로 할당되며, 그 결과 기능 아키텍처가 산출된다.
기능분석 및 할당은 시스템이 무엇을 해야 하고, 어떤 방법으로 할 수 있는지, 그리고 하위 레벨 기능과 관련하여 우선순위 및 불일치가 어느 정도인지에 대한 정보가 제동되며, 물리적인 해결책을 최적화하는데 필수적인 정보를 제공한다.

요건루프

기능분석 및 할당은 보다 나은 요건의 이해를 가져오며, 요건분석의 재고를 활성화 시킨다. 식별된 기능은 반드시 요건을 역 추적할 수 있어야 한다. 기능 분석 및 할당의 결과로서 재 요건분석의 반복적인 수행이 이루어지며, 이와 같은 프로세스를 요건루프라고 한다.

설계조합

설계조합은 품목을 함께 구성하고 나타내는 물리적 및 소프트웨어적 요소의 관점에서 제품 또는 품목을 정의하는 프로세스이다. 이러한 결과를 물리적 아키텍처라 한다. 각 부품은 적어도 하나의 기능요건을 충족시켜야 하며, 어던 부품은 많은 기능을 지원하기도 한다. 물리적 아키텍처는 사양서와 기준을 만들기 위한 기본 구조이다.

설계루프

요건루프와 비슷하게 설계루프는 조합된 물리적 설계가 요구되는 성능레벨의 요구기능을 수행할 수 있는지 검증하기 위해 기능 아키텍처로 되돌아오는 프로세스이다. 설계루프는 시스템이 어떻게 임무를 수행할 것인지를 재고하게 하며, 조합된 설계의 최적화를 돕는다.

검증

System Engineering 프로세스의 적용에 대한 해결책은 요건과 비교된다. 프로세스의 이 부분을 검증루프 또는 검증이라 한다. 각각의 개발 레벨에서 각 요건은 검증되어야 한다. System Engineering 프로세스를 통해 만들어진 기준 문서화에 의해 각각의 요건에 대한 검증 방법이 수립되어야 하며, 적용 가능한 검증 방법은 실험, 시연, 분석 및 시험이 있다.

시스템 분석 및 통제

시스템 분석 및 통제는 진도 측정, 대안평가 및 선정 그리고 문서자료 및 의사결정에 요구되는 기술관리 활동을 포함한다. 이러한 활동은 프로세스 모든 단계에 적용된다. *분석활동은 효과분석 및 설계분석을 포함하며, 통제활동은 위험관리, 형상관리, 데이터관리 등으로 구성된다.*

수명주기 기능이란 시스템 수명주기와 연관된 제반 특성 활동을 의미하며, 이러한 활동은 8가지 주요 기능으로 구성된다. 안전성활동은 수명주기 동안 8가지 기능에 대해 분석되고 관리되어야 한다.

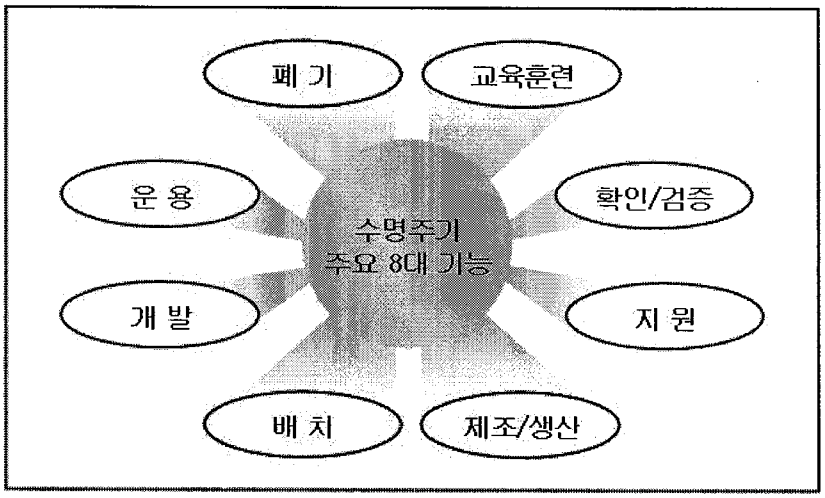


그림 2. 수명주기 기능

개발은 고객의 요구로부터 제품 또는 프로세스 해결책까지 시스템을 진화시키는데 요구되는 활동을 포함한다.

제조/생산은 엔지니어링 시험모델 및 실험모델 제작, 소량 초도생산, 시스템 및 최종 제품의 양산, 또는 대형/단일 시스템 또는 하부 시스템을 포함한다.

배치는 완전한 운용능력을 갖도록 하기 위하여 시스템을 처음 만들어 운송, 인수, 처리, 조립, 점검, 교육훈련, 운용, 수용, 저장하는데 필요한 활동을 포함한다.

운용은 사용자 기능으로 평시 및 전시 환경 하에서 정해진 운용 목적과 과업을 만족시키기 위하여 필요한 활동을 포함한다.

지원은 운용지원, 정비, 물류 및 자재관리에 필요한 제반 활동을 말한다.

폐기는 모든 적용 규정과 훈령에 의해 퇴역, 파손, 또는 수리불가 시스템 구성품의 폐기를 보장하는데 필요한 활동을 말한다.

교육훈련은 운용지원 기능의 효율적이며 효과적인 수행에 필요한 지식과 기술수준을

획득하고 유지하는데 필요한 활동을 포함한다.

검증은 발전하는 시스템 제품과 프로세스의 진행과 효과도를 평가하고, 사양과 일치성을 측정하는데 필요한 제반 활동을 포함한다.

System Engineering 관련 규격

System Engineering 흐름

Lifecycle(수명주기)

> *시스템 수명주기는 초기의 개념부터 폐기처분까지 시스템의 전체 수명주기를 포함하고, 각 업무를 포함하는 일련의 단계이다. 수명주기는 동의된 시간 다위 내에 정당한 가격으로 정당한 제품을 제공할 수 있도록, 시스템이 각 단계를 통해서 진행함에 따라서 RAMS를 포함한 시스템의 모든 측면을 계획하고 관리하고 제어하고 감시하는 구조를 제공한다.*
>
> *- IEC 62278 5.2.1 -*

시스템 수명주기 (IEC 62278)

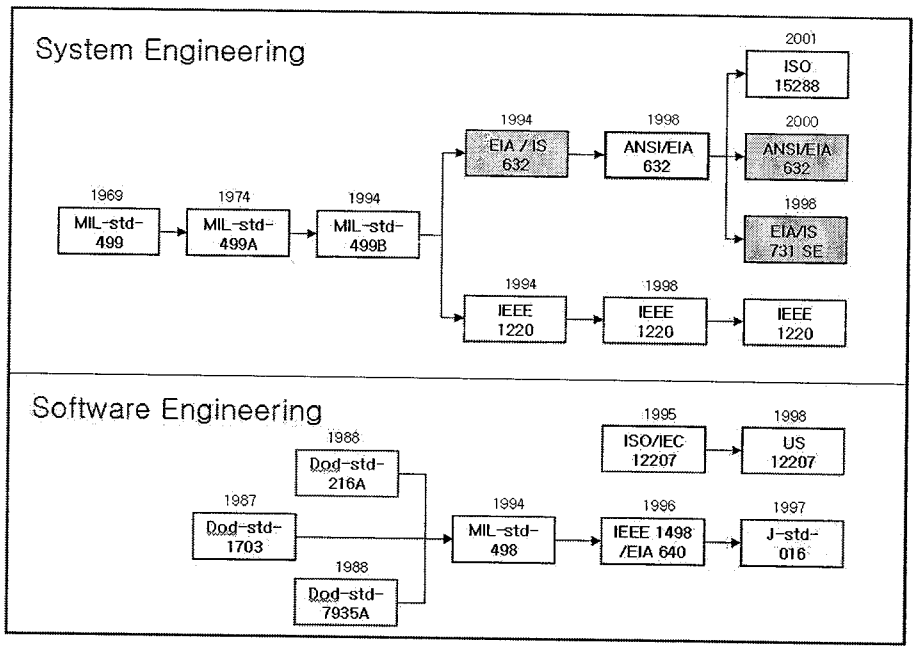


그림 3. System Engineering 흐름

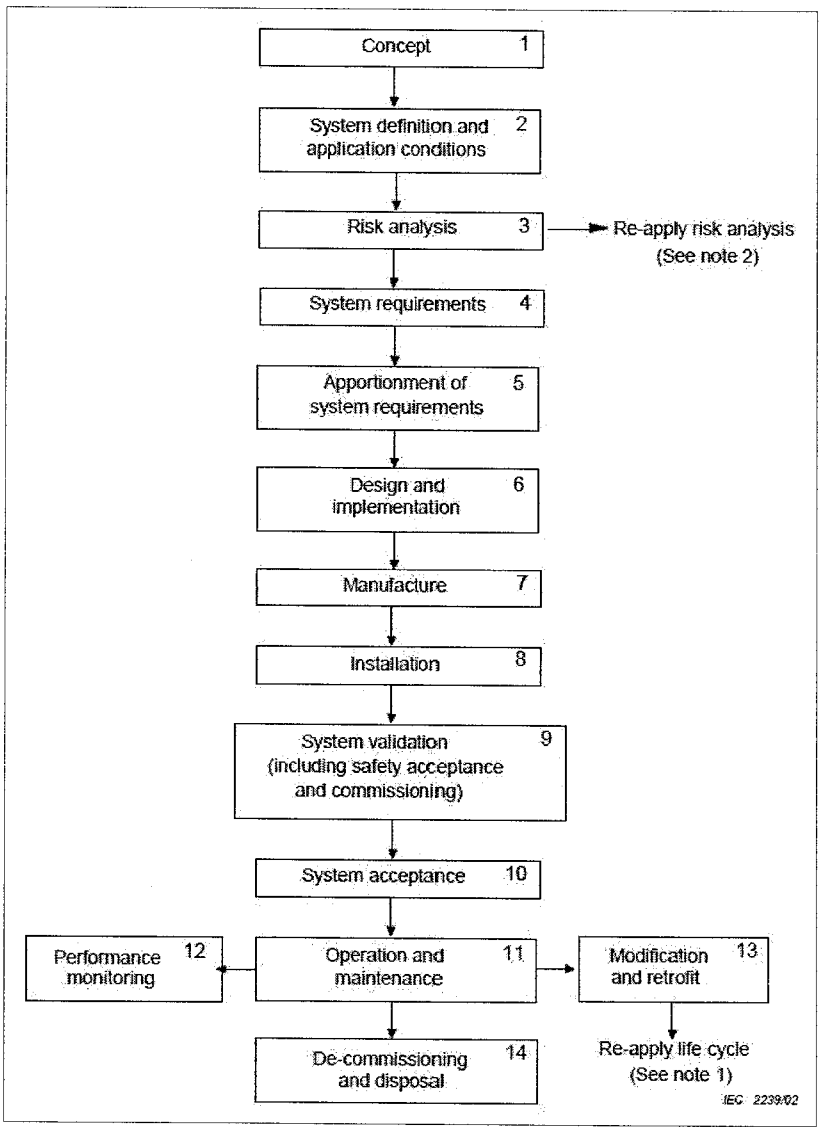


그림 4. 시스템 수명주기

수명주기 'V모델'은 Top-down(왼쪽)은 일반적으로 개발(Development)이라 하며, 시스템 부품의 제조를 위한 절차이며, Bottom-up(오른쪽)은 조립, 설치, 인수 그리고 전체 시스템의 운영과 관련된다.

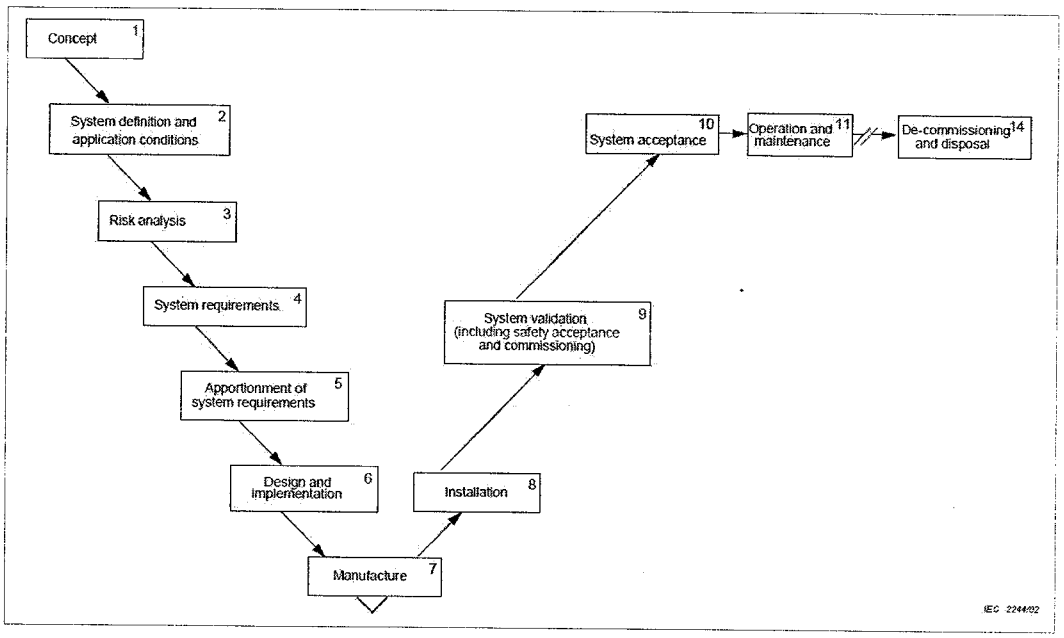


그림 5. 시스템 수명주기 'V모델'

표 1. 시스템 수명주기별 활동

	RAM	Safety
1	· 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	· 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 · Safety Plan 구축 · 위험도 기준의 허용도 정의 · 기존 설비의 제약조건의 안전성에 관한 영향 확인
3	-	· 시스템 위험상태와 안전성위험도 분석수행 · 위험상태 기록의 설정 · 위험도 평가(Risk Assessment) 수행
4	· 시스템 RAM 요구사항의 구체화 · RAM 수용기준(전체)의 정의 · 시스템의 기능적 구조의 정의 · RAM 프로그램의 수립 · RAM 관리의 수립	· 시스템 안전성 요구사항의 구체화 · 안전성 수용기준(전체)의 정의 · 안전성에 관련된 기능적인 요구사항 정의 · 안전성관리의 수립
5	· 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	· 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	· 다음을 언급하는 검토, 분석, 시험, 데이터 평가에 의한 Safety Plan 구현 - 위험상태 기록 - 위험분석 분석과 위험도 평가 · 안전성 관련된 설계 의사결정 정당화 · 다음을 포함하는 프로그램 제어 착수 - 안전성 관리 - 하부계약자 또는 공급자의 관리

	- 하부계약자 또는 공급자들의 관리	· 일반적인 안전성 증빙문서(Generic Safety Case) 마련 · 일반적인 응용안전성 증명의 준비 마련(필요시)
7	· 환경 응력 적격심사 수행 · RAM 개선 시험 수행 · 고장보고분석 및 수정활동 시스템(FRACAS)	· 검토, 분석, 시험, 데이터 평가에 의한 안전성계획을 구현 · 위험상태를 사용
8	· 유지보수자 훈련 시작 · 예비 부품과 공구 공급 구축	· 설치 프로그램 구축 · 설치 프로그램 구현
9	· RAM 입증 수행	· 시운전 프로그램 구축 · 시운전 프로그램 구현 · 특정적용 Safety Case 마련
10	· RAM 입증 평가	· 특정적용 Safety Case 평가
11	· 예비품과 공구의 상시 조달 · 상시 신뢰성중심의 유지보수 세부계획 지원실행	· 상시 안전성 중심의 유지보수 착수 · 상시 안전 성능 감시 및 Hazard Log 유지보수 수행
12	· 성능과 RAM 통계량 수집, 분석, 평가,사용	· 성능과 안전성 통계량 수집, 분석, 평가와 사용
13	· 변경과 개선을 위한 RAM 관련사항 고려	· 변경과 개선을 위한 안전성 관련사항 고려
14	· RAM에 해당하는 활동 없음	· 안전성 계획 수립 · 위험요소 분석과 위험도 평가 수행 · 안전성 계획 구현

수명주기 'V모델'은 증명(Verification)과 검증(Validation) 업무를 나타내는데 효과적이다. 증명의 목적은 특정한 입력에 대해서 각 단계의 이행 가능성이 그 단계의 요구 사항을 모든 측면에서 만족함을 입증하는 것이다. 검증의 목적은 시스템의 모든 개발 단계 및 설치 후에 고려 중인 시스템이 모든 측면에서 요구 사항을 만족함을 입증하는 것이다.

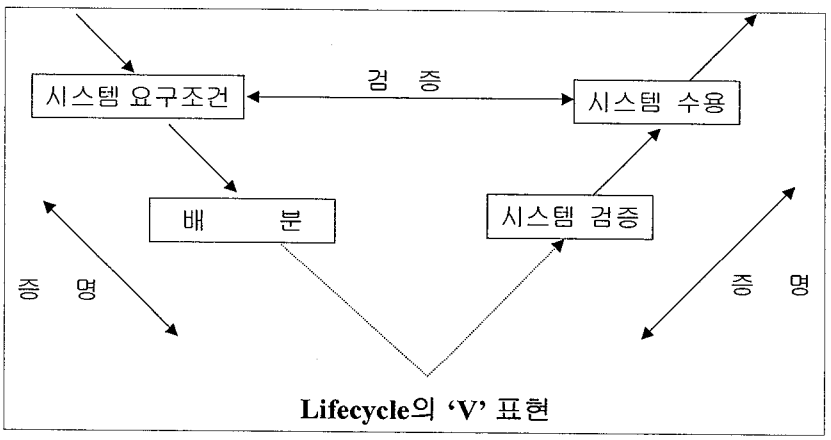


그림 6. 수명주기 증명과 검증 체계

소프트웨어 수명주기 (IEC 62279)

소프트웨어 개발에 사용되는 수명주기 모델이 선정되어야 한다.

- *품질보증 절차는 수명주기의 수행과 동시에 수행되어야 하고 공통의 용어를 사용해야 한다.*
- *모든 행위는 시작 단계부터 수행되어야 하고, 각각의 소프트웨어 수명 주기에 해당하는 단계들은 요소별로 나뉘어져 각각의 단계에 해당하는 입력과 출력 그리고 각 단계에서의 행위가 정의되어야 한다.*

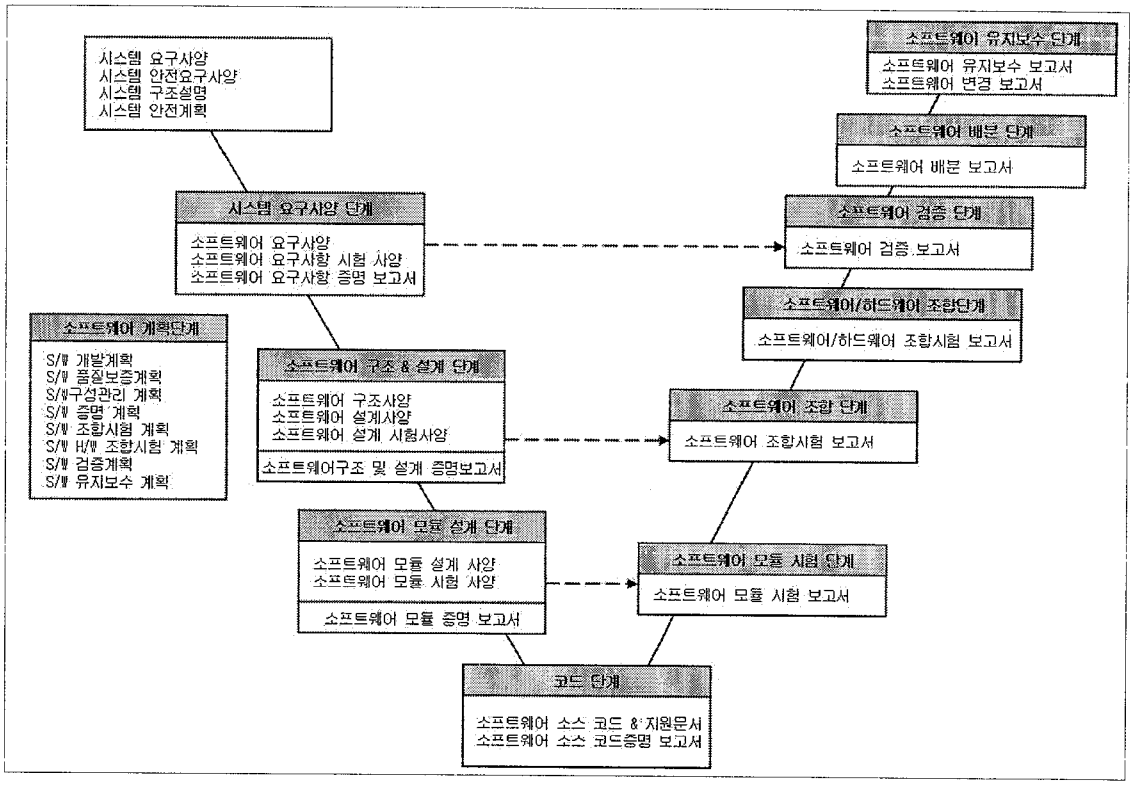


그림 7. 소프트웨어 수명주기

Safety 활동

Safety 관련 규격

철도시스템의 안전성을 확보하기 위해 관련규격을 준수하여야 하며, 규격에서 요구하는 사항에 대해 안전성 평가에서 증명할 수 있어야 한다.

철도시스템 및 탑재되는 소프트웨어의 안전성 확보와 관련된 규격은 다음과 같다.

표 2. 안전성 규격

규격	번호	규격명	분야
IEC	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	일반 전기/전자 안전
IEC	62278	**Railway applications-** Specification and demonstration of reliability, availability, maintainability and safety(RAMS)	철도 RAMS
EN	50126		
IEC	62279	**Railway applications-** Communications, signalling and processing systems- Software for railway control and protection systems	철도 SW 안전
EN	50128		
IEC	62280	**Railway applications-** Communication, signalling and processing systems- Safety related communication in close/open transmission systems	철도 통신 안전
IEC	62425	**Railway applications-** Communications, signalling and processing systems- Safety related electronic systems for signalling	철도 시스템 안전
EN	50129		

위에서 제시된 규격을 만족하기 위해 추가적으로 참고할 수 있는 규격은 다음과 같다.

표 3. 기타 관련 규격

규격	번호	규격명	분야
IEEE	730	Software Quality Assurance Plans	SW 품질보증
	828	Software Configuration management plan	SW 형상관리
	829	Software Test documentation	SW 시험
	830	Software Requirement Specification	SW요구사항
	1012	Software Verification & Validation	SW 증명 및 검증
	1074	Software Lifecycle Process	SW수명주기
	1228	Software Safety Plan	SW안전계획
	16085	Lifecycle Process-Risk management	수명주기-안전관리
	1413	Reliability Predictions	신뢰성 예측
KS	A3112	FRACAS	고장관리
	60812	FMEA	고장분석
	61025	FTA	고장분석
	61165	Malov기법	고장분석
	61713	SW수명주기 신뢰성	신뢰성
	61882	HAZOP	고장분석
Yellow Book		Engineering Safety Management	안전성

***Safety* 활동 프로세스**

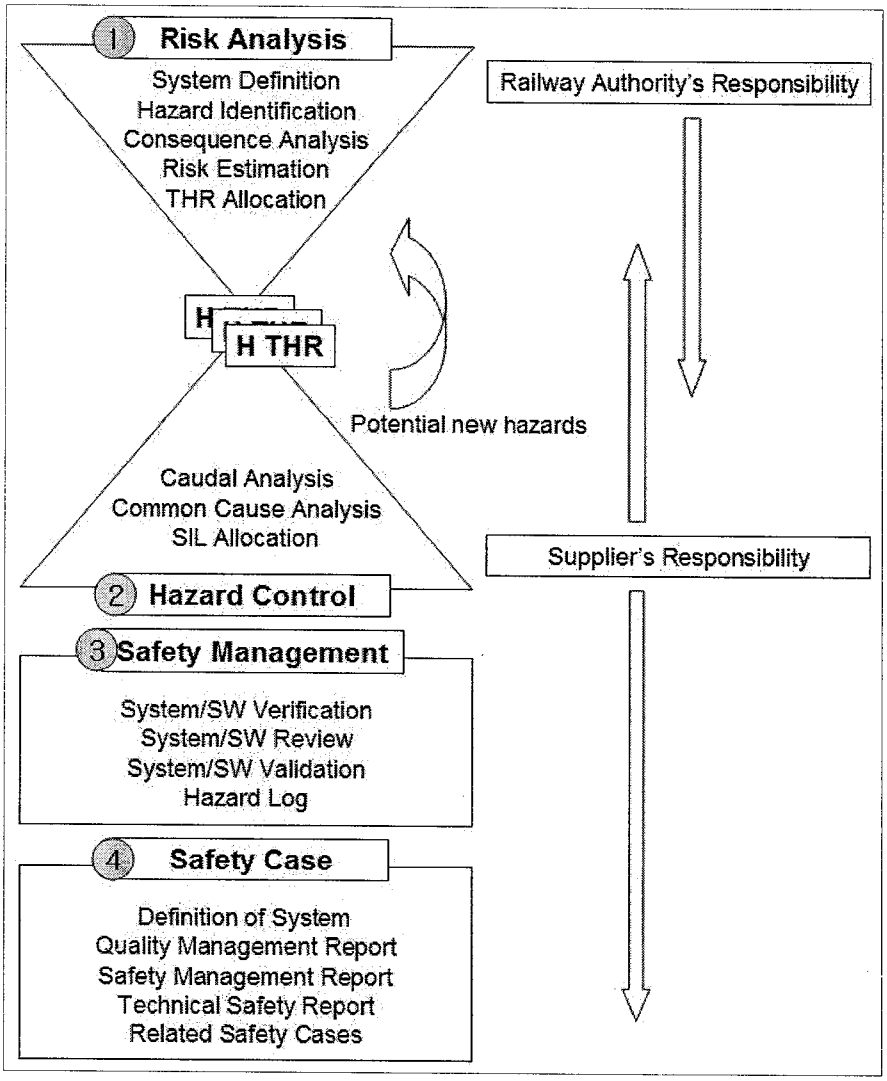


그림 8. Safety 활동 프로세스

Safety Plan

안전성 활동을 수행하기 위한 전반적인 프로세스와 세부적인 업무에 대해 상세한 계획을 수립해야 한다.

일반적으로 안전성 계획은 다음과 같이 구성된다.

표 4. Safety Plan 구성

단계	업무
서론	프로젝트에 대한 전반적인 배경 및 안전성 활동 사항을 간략히 기술한다.
과업범위	본 장에서는 다음을 포함해야 한다. ● Safety 요구사하아 ● 과업(시스템)범위
안전성 목적	본 장에서는 다음을 포함해야 한다. ● 개요 ● 수행원칙 ● 위험도 분류 - 위험원 심각도 - 위험원 발생빈도 - 위험도 등급 ● SIL
시스템 개요	본 장에서는 해당되는 시스템에 대한 설명이 기술되어야 한다.
안전성 조직	본 장에서는 다음을 포함해야 한다. ● 조직구성도 ● 안전성 활동 역할 및 책임 ● 조직간 인터페이스
시스템 수명주기별 안전성 업무	본 장에서는 다음을 포함해야 한다. ● Hazard Analysis 단계 및 방법론 ● Verification 및 Validation 프로세스 ● Audit 및 평가 프로세스
안전성 산출물	본 장에서는 안전성 활동으로 인한 산출물List를 제시하여야 한다.
품질관리	본 장에서는 품질관리 시스템에 대한 내용을 기술하며, 모든 산출 문서들이 품질관리에 따라 관리됨을 기술하여야 한다.

Hazard Analysis

위험원 분석은 4.2절의 Safety활동 프로세스에서 정의한 그림 중 Risk Analysis와 Hazard Control을 포함하는 개념이다. Hazard analysis는 다음 그림과 같이 표현된다.

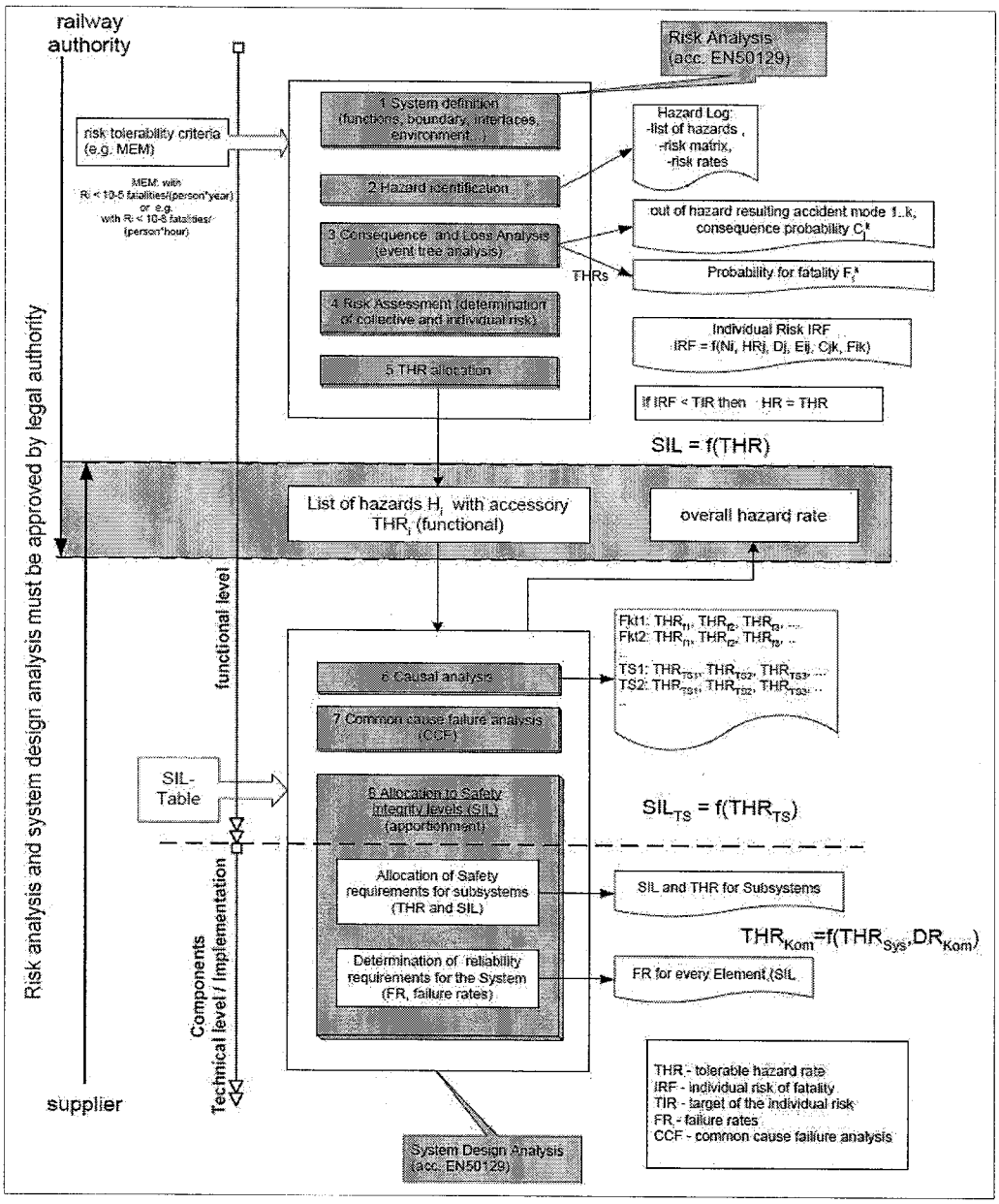


그림 9. Hazard Analysis 프로세스

위의 그림에서 제시되는 각 단계별 분석들은 수명주기 동안 반복적으로 수행될 수 있으며, 분석은 다음과 같이 상세하게 분류될 수 있다.

표 5. EN50129 분석 단계

Analysis phase	System development phases	Used methods
PHA	System specification phase	• Top-down analysis • HAZOP
SHA	System design phase	• Risk/Hazard analysis • FMECA
SSHA	Subsystem specification and design	• FMECA
IHA	Interface specification and design	• FMECA
OSHA	Initial system design phase (together with the SHA)	• FMECA • HAZOP
Specific Safety Studies	all phases	• FMECA • Top-down analysis • Simplified FTA • Markov simulations
Safety Principles assessment	Initial design phase	• FMEA • Simplified FTA • Markov simulations
HW Safety Analysis file	HW specificatio and design phases	• FMEA • Scenarios analysis
HW test/simulation file	HW design phase	• Tests and simulation
SW Error Effects analysis	SW specification and design	• FMEA on SW functions
Critical Code Review	SW coding phase	• Verification • Traceability verification
Overall Safety Validation Report		• Traceability verification • Verification

각 단계에서 적용 가능한 기법은 다음과 같다.

표 6. EN50129 분석 기법

Method	Title/Detail	Type
FMEA	Failure Mode Effect Analysis	Bottom-up
FMECA	Failure Mode Effect and Criticality Analysis	Bottom-up
FTA	Fault Tree Analysis	Top-down
Risks/Hazard analysis	Hazards/Accidents table analysis	Top-down
Markov	State transition computation using matrix differential computation	Tool
HAZOP	Hazard and Operability Study	Collegial method
Field return from experience	Existing reliability data	Reliability computation
Failure tests	HW failure tests	Tests
Failure simulation	HW failure simulation	Tests
Fault injection	Failure/error injection in HW simulators	Tests
Traceability	Traceability completeness verification	Verification

System Definition

이 단계는 모든 후속 RAMS 수명주기 업무가 만족할 정도로 충분히 수행 가능하도록 시스템에 대한 필요한 모든 관련 정보 및 필요 데이터가 확보되어야 한다.

System Definition단계에서 확보되어야 할 관련 정보 및 필요 데이터는 다음과 같다.

- 시스템의 범위, 내용 및 목적
- 시스템 환경조건
- 안전성에 영향을 줄 수 있는 다른 시스템과의 상호관계 및 인간과의 상호관계
- 유사한 관련시스템의 안전성 관련 자료 확보
- 안전성 법령

Hazards Identification

이 단계는 System Definition에서 정의된 시스템 범위, 환경조건 등에 따라 시스템의 잠재적인 위험원을 도출하여야 한다.

위험원 식별은 생명주기동안 발생할 수 있는 위험원들을 결정하기 위하여, 제품, 절차, 시스템 또는 기업에 대한 체계적인 분석을 포함한다. 위험원들은 인명 피해, 환경 피해 또는 경제적인 손실을 초래할 가능성이 있다.

위험원에 대한 체계적인 식별은 일반적으로 다음의 두 단계를 포함한다.

- *경험적인(Empirical) 단계 (과거의 경험을 이용하는 것, 예를 들어, 체크리스트)*
- *창조적인(Creative) 단계 (사전 예측, 예를 들어, 브레인스토밍, 구조적인What-If 연구)*

위험원 식별의 경험적인 단계와 창조적인 단계는 서로를 보완하며, 잠재적인 위험원를 다루고 모든 중요한 위험원들을 식별해서 신뢰성을 향상시킨다.
위험원들은 시스템 정의에 의존하고, 특히 시스템 경계는 시스템과 하부시스템에 관해 위험원들의 계층적 구조를 참작한다. 이것은 또한 위험원 식별과 원인 분석이 시스템 개발 동안 여러 단계의 항목에서 반복하여 수행되어야 한다는 것을 의미한다.
그림은 위험원 도출을 위한 범위를 제시하고 있다.

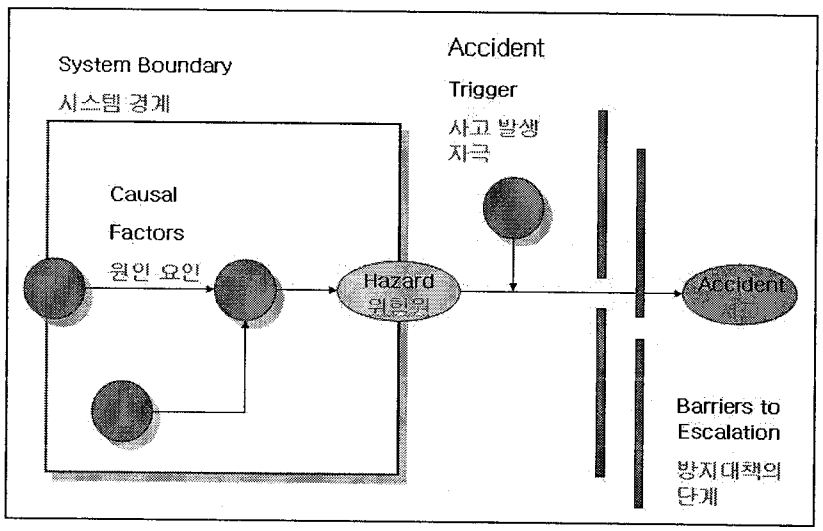


그림 10. 위험원의 정의

Consequence analysis, Risk Estimation and THR allocation

요구사항은 결과에서 도출된 THR이 위험도 허용 기준을 고려하여 도출하며, 허용기준은 각 프로젝트에서 정의되어야 한다.

- *Consequence Analysis의 목적*
  도출된 위험원으로부터 발생한 상황에 따른 최종적인 결과를 파악하기 위해 수행된다.
- *접근법*
  - *도식으로 표현*
  - *정략적인 확률값 도출*
- *적용 기법*
  - *원인-결과 다이어그램*
  - *ETA*

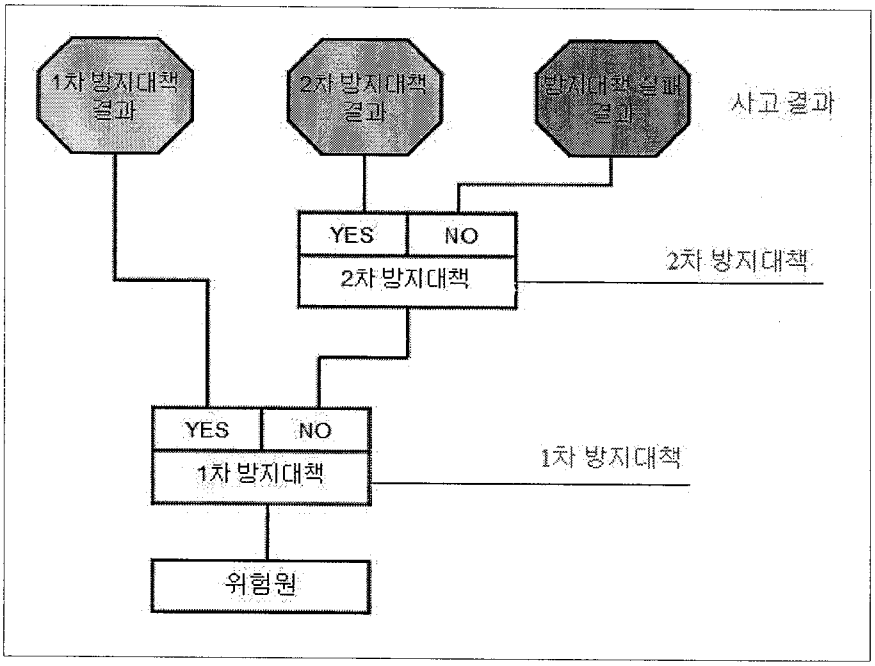


그림 11. 원인-결과 다이어그램 예

그림은 원인-결과 다이어그램으로 위험원을 야기 시키는 원인과 그에 따른 결과를 모두 표현할 수 있는 장점이 있다.

Causal Analysis

Causal Analysis는 두 단계로 구성된다.

- 각 위험원에 대한 THR이 기능레벨(Functional Level)에서 할당된다. THR은 SIL 테이블을 이용하여 SIL로 변경된다. SIL은 기능을 구현하는 하부시스템의 기능레벨에서 정의된다. 만약, 위험원과 안전기능들에 대해 THR이 정의되어 있으면, 원인분석의 첫 번째 단계를 생략하고 요구되는 THR을 기반으로 SIL을 할당한다.
- 하부시스템에 위험율(HR)이 할당되며, 물리적인 또는 구현 레벨에서 SIL은 변경되지 않고 유지된다. IEC62279에서 정의되는 소프트웨어 SIL은 예외적인 경우를 제외하고 하부시스템 SIL과 동일하다.

위에서 언급된 할당 절차는, 신뢰성 블록 다이어그램(Reliability Block Diagram), 결함트리(Fault Tree), 이진 결정 다이어그램(Binary Decision Diagrams), 마코프 모델 등과 같이 조합논리(Combination Logic)에 적합한 표현을 허용하는 임의의 방법에 의해 수행될 수 있다.

첫 번째 단계에서는 기능적인 독립성이 요구되는 반면, 두 번째 단계에서는 물리적인 독립성으로 충분하다.

공통원인 고장 분석(Common Cause Failure Analysis)

CCF는 다음의 사항에 대해 분석된다.

- 물리적인 독립성
- 기능적인 독립성
- 절차적인 독립성

물리적인 독립성

임의의 영향들에 대하여 AND 게이트를 사용하여 신뢰성 있는 결함 트리 계산(Fault Tree Calculations)을 수행하기 위해서 물리적인 독립성이 반드시 필요하다. 이를 위해 CCF 분석을 수행하기 위해 독립성을 가정하는 것이 필요하다.

CCF 물리적인 독립성에 대한 상세한 설명은 EN50129 부록 A.4.2.2.1을 참조한다.

기능적인 독립성

기능적 독립성은 기능의 고장을 야기하는 Random failure 및 Systematic failure가 없음을 의미한다. 따라서 기능들이 독립적임을 보여주기 위하여 CCF분석이 수행된다.

기능적인 독립성은 Random failure 및 Systematic failure 요구사항이 기능적 독립성이 보장된다면, 하위레벨에만 할당될 수 있다.

CCF 기능적인 독립성에 대한 상세한 설명은 EN50129 부록 A.4.2.2.2를 참조한다.

절차적인 독립성

시스템은 일반적으로 수명주기 절차들에 의해 최종 결과에 중요한 영향을 미친다. 절차적인 독립성은 수명주기 절차를 수행하는 동안 잠재적인 계통적 오류들이 발생하기 때문에 각 절차간 독립성이 유지되어야 한다.

안전무결성 레벨(SIL:Safety Integrity Level)

안전 무결성은 4개의 이산 수준들(Discrete Levels) 중 하나로 기술된다. 4등급이 최고 안전 무결성이고, 1등급이 가장 낮은 등급이다. 0등급은, 아무런 안전 요구사항들이 없음을 나타낸다. SIL은 품질 및 안전 관리와 같은 요소들에 대한 정성적인 평가를 수행해야 한다(Systematic failure).

시스템과 관련된 위험원들은 시스템 수명주기의 위험도 분석 단계 동안 잠재적인 결과들에 대하여 식별되고 평가되며, 결과적으로 요구되는 THR이 달성됨을 보장해야 한다.

시스템 요구사항 및 요구사항 할당 단계 동안에, THR은 시스템 기능들과 하부-시스템에 할당된다.

이들 기능들은 할당된 정성적 및 정량적 안전 목표를 가져야 한다. 정성적 목표는 계통적 고장 무결성(Systematic Failure Integrity)인 안전 무결성 등급(Safety Integrity Level)의 형태여야 하며, 정량적 목표는 임의 고장 무결성(Random Failure Integrity)인 수치적인 고장율(Numerical Failure Rate)의 형태여야 한다.

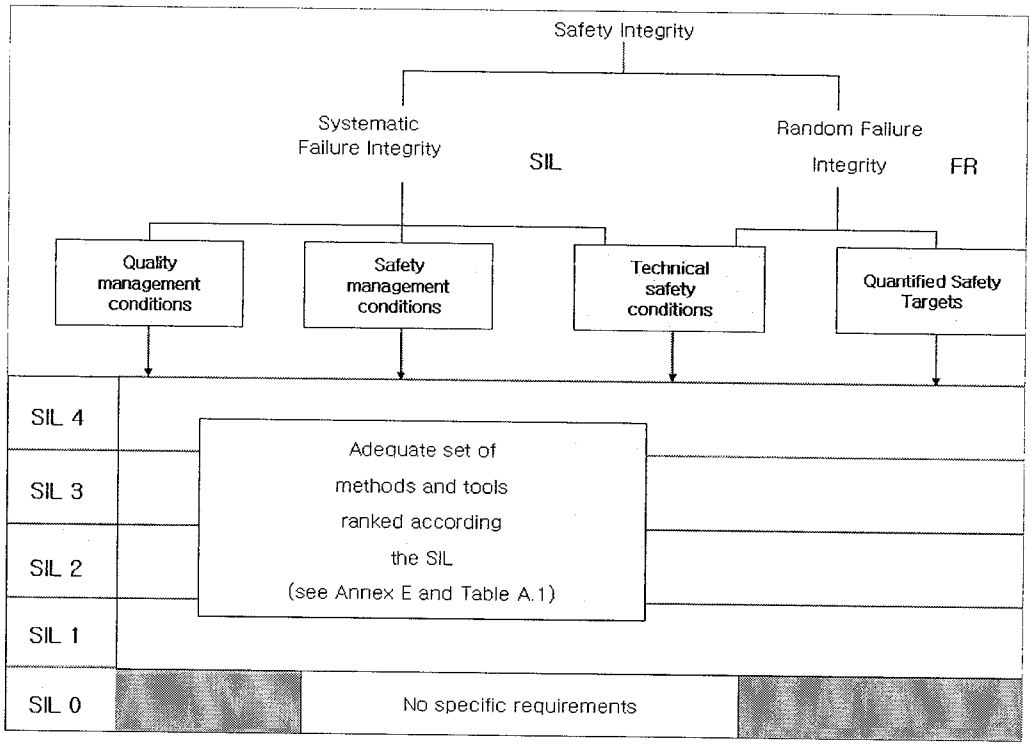


그림 12. SIL 구성

EN50129는 '안전성(Safety)은 결함들을 회피하거나 허용할 수 있는 적절한 방법들(계통적 고장에 대한 안전여유 같은 것)과 임의고장들을 제어하기 위한 적합한 방법들 모두에 의존한다'라는 가정에 기반을 두고 있다. 두 종류의 고장 모두에 적용을 위한 방법들은 시스템의 최적 안전성능을 얻기 위하여 균형을 잡아야 한다. 이를 성취하기 위하여 안전 무결성 등급(SIL)개념이 사용된다. SIL은 정성적인 접근방법들(계통적인 고장을 회피하기 위한)과 정량적인 접근법(임의 고장을 제어하기 위한)을 매칭시키기 위한 수단으로 사용되는데, 이는 계통적 고장을 정량화할 수 없기 때문이다.

SIL 테이블은 안전관련 기능들 또는 이러한 기능들 중 하나 이상을 구현하고 있는 하부시스템들에 적용가능하다. 각 SIL등급에 요구되는 수단 또는 방법들에서는, THR이 달성되었음을 입증할 때 시스템적 고장을 고려하도록 요구하지 않는다.

SIL 테이블은 THR로부터 도출되는 안전관련 기능에 요구되는 SIL과 동일하다. 그래서 만약 기능 'F'의 THR이 정량적 방법에 의해 도출되면, 요구되는 SIL은 다

음의 표를 사용하여 결정하여야 한다.

표 7. SIL 테이블

THR/hour/function	SIL
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Safety Case

안전성 수용을 위한 다음의 조건들이 만족되어야 한다.

- *품질관리에 대한 근거 확보*
- *안전관리에 대한 근거 확보*
- *기능적/기술적 안전에 관한 근거확보*

안전관련 시스템이 적절한 안전을 받아들일 수 있기 위해서는, 장치나 하부시스템, 또는 시스템 레벨에서 이러한 모든 조건들을 만족해야 한다.

이와 같은 조건들을 만족하는 문서화된 근거자료는, 종합안전대책기술서(Safety Case)이라고 알려져 있는, 구조화된 안전성 입증 문서 내에 포함되어야만 한다. 종합안전대책기술서은 일반제품, 응용제품 혹은 특정응용에 대한 안전성 승인을 얻기 위해서 안전인증기관에 제출된 모든 문서화된 근거자료들로 구성되어 있다.

종합안전대책기술서에는 시스템, 하부시스템 혹은 장치의 요소들에 대하여 문서로 된 안전성 근거자료를 포함하며, 다음과 같은 구조로 되어야 한다.

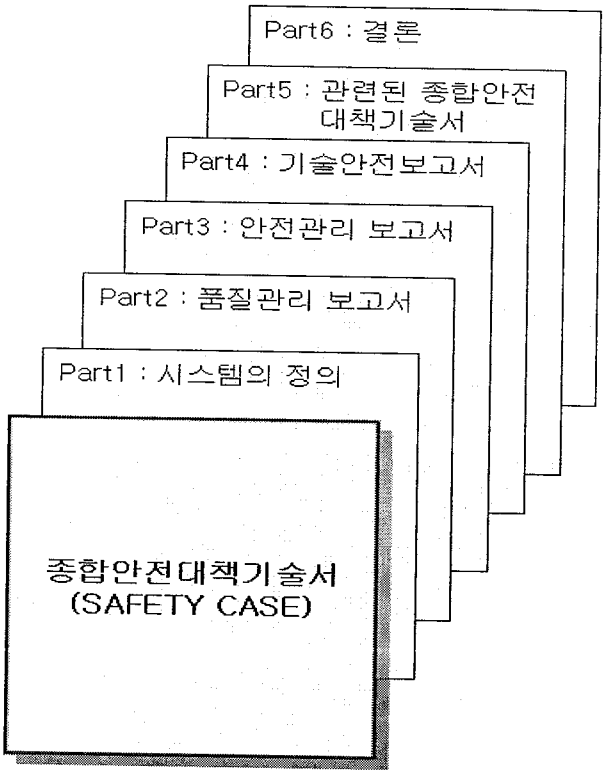


그림 13. Safety Case 구성

품질관리 보고서

안전성 수용을 위하여 만족되어야 할 첫 번째 조건은, 시스템/하부시스템/장치의 품질이 수명주기 동안 효과적인 품질관리 시스템에 의해 통제되어 왔는가 및 지속되어져야 한다는 것이다. 이를 입증하는 문서화된 증명이 품질관리 보고서로 제공되어야만 한다. 그리고 이는 종합안전대책기술서 문서의 Part 2에 해당한다.
품질관리 시스템의 목적은 수명주기 동안 각 단계에서 인위적인 오류 발생을 최소화하고자 하는데 있다. 그럼으로써 시스템, 하부시스템 혹은 장치의 계통적인 결함발생 위험을 줄이고자 하는 것이다.

품질관리 시스템은 EN 50126에 나타낸 바와 같이 시스템/하부시스템/장치의 수명주기 동안 적용이 가능해야만 한다.

품질관리는 다음의 사항에 대해 고려되어야 한다.

- *조직적인 구조*
- *품질계획 및 절차*
- *요구사양*
- *설계관리*
- *설계 검증 및 검토*
- *응용 공학*
- *조달 및 제조*
- *생산품의 확인 및 추적 가능성*
- *취급 및 저장*
- *검사 및 시험*
- *불일치와 수정작업*
- *포장 및 배달*
- *설치 및 시운전*
- *운용 및 유지보수*
- *품질 감시 및 반영*
- *문서 및 기록*
- *구성 및 변경관리*
- *요원의 능력 및 훈련*
- *품질 감시 및 추적*
- *폐기처분*

만일 품질관리와 관련된 다양한 정보를 담은 문서가 존재한다면, 품질관리 보고서는 중복된 자료와 정보를 기술할 필요는 없다.

안전 무결성 등급 1~4 모두에 대해서 품질관리를 위한 요구사항에 만족하여야 한다. 그러나 근거자료의 내용이 시스템/하부시스템/장치의 안전 무결성 등급(SIL)에 적합해야 한다.

안전관리 보고서

안전성 수용을 위한 2번째 조건은 시스템, 하부시스템 또는 장치의 안전이 만족되어야 하고, EN50126에 설명된 신뢰성(Dependability)을 위한 관리과정(RAMS)과 일치하는 효과적인 안전 관리과정에 의해 관리되고 유지되어져야 한다. 이 과정의 목적은 수명주기를 통하여 안전관련 인적오류의 발생을 더욱 줄이기 위한 것이고, 이렇게 하여 안전과 관련된 계통적 결함의 잠재위험을 최소화하는 것이다.
*수명주기를 통한 안전관리 과정의 모든 요소들에 순응하는 것을 증명하기 위한 증거문서는 종합안전대책기술서(Safety Case)의 Part 3을 형성하는 **안전관리보고서**에 제공되어야 한다. 만약 정확한 참고문헌이 그러한 문서에 제공된다면 많은 분량의 근거와 보조문서가 포함될 필요는 없다.*

이 안전관리 과정은 안전 무결성 등급 1~4 모두에서 필수적으로 시행되어야 한다. 그러나 근거자료의 내용이 시스템/하부시스템/장치의 안전 무결성 등급(SIL)에 적합해야 한다.

모든 경우에 있어서, 각각의 특별한 상황에 대하여 안전 무결성의 요구등급을 확인하기 위하여 EN50126에 정의된 위험원 분석 및 위험평가 과정이 필요하다.

기술적 안전 보고서

*품질관리 및 안전관리의 근거확보에 부가하여 시스템, 하부시스템 또는 장치의 요소(Item)가 의도된 응용에서 충분히 안전이 공인되기 전에 3번째 조건이 만족되어야 한다. 이것은 설계의 안전에 대한 기술적인 입증으로 구성되며, 그것은 **기술안전보고서(Technical Safety Report)**에서 문서화되어야 한다. 이 문서는 5.1에 설명된 것처럼 시스템/하부시스템/장치에 대한 종합안전대책기술서(Safety Case) Part 4를 구성한다.*

기술안전보고서는 안전 무결성등급(SIL) 1~4에 대해서 필수적이다. 그러나 근거자료의 내용이 시스템/하부시스템/장치의 안전 무결성등급(SIL)을 적합해야 한다.

기술안전보고서는 모든 부가되는 근거(예, 설계원리와 계산, 시험사양과 결과, 안전 무결성 분석)를 포함하여 설계의 안전을 보증하는 기술원리들을 설명해야한다. 만약, 이러한 문헌에 정확한 참조물이 제공된다면 상당한 분량의 상세한 증명과 지원하는 서류는 포함할 필요가 없다.

Safety 관련업무간 상관관계

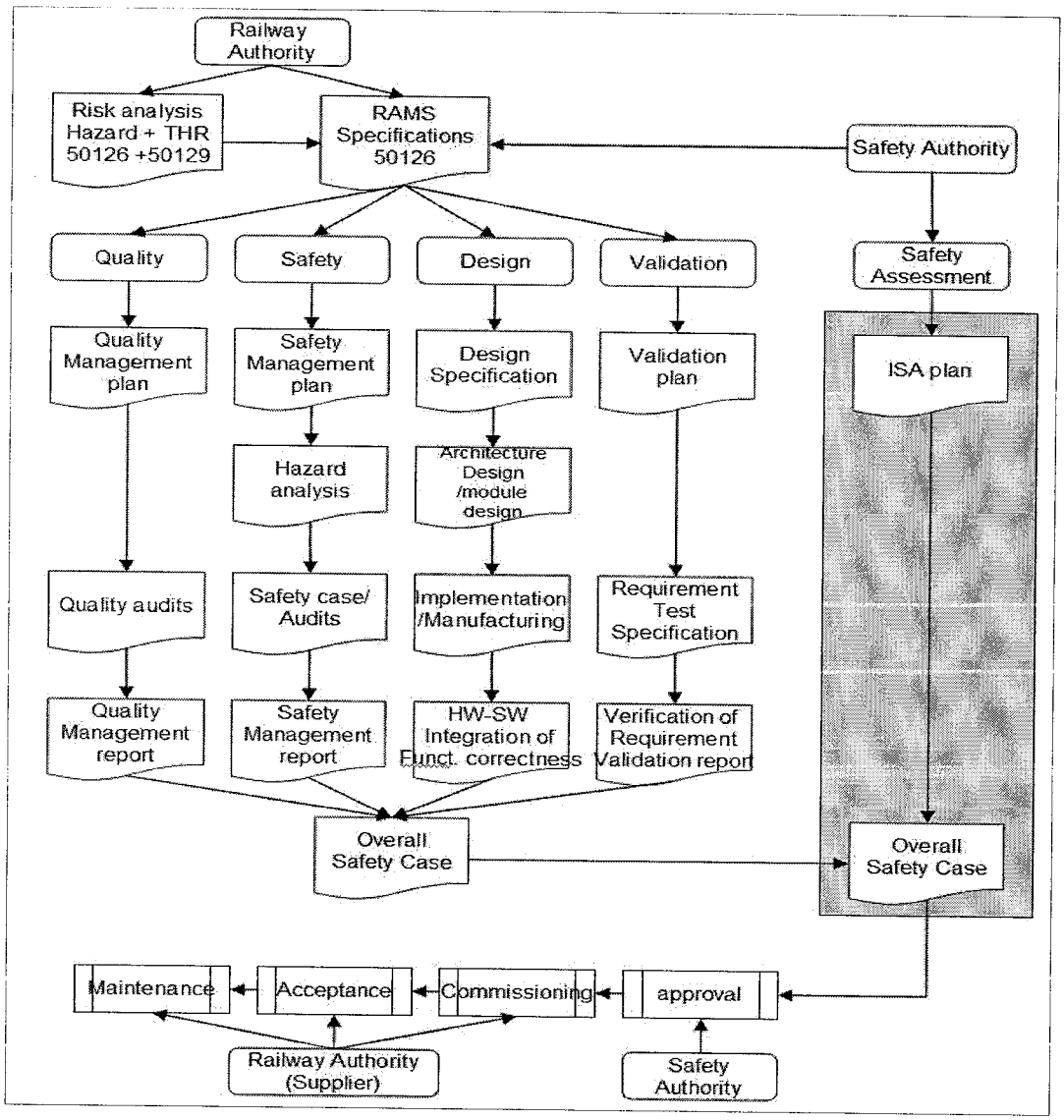


그림 14. Safety 관련업무간 상관관계

위의 그림은 안전성 활동과 그 밖의 관련 업무와의 절차들을 간략히 표현하고 있다. EN50126 (IEC62278)는 안전성 활동을 수행하기 위한 전반적인 프로세스와 세부수행 기술을 담고 있다.

앞서 기술된 Safety Case는 품질(Quality), 안전(Safety), 설계(Design), 확인(Verification) 그리고 평가(Assessment)에 대한 사항을 모두 포함하여야 하며, 안전성 활동의 궁극적인 목표는 시스템의 안전을 확보하여 안전 인증을 획득하는 것이다. ■

부 록 A

대상시스템의 Safety Case(1)

부 록 A

대상시스템의 Safety Case(1)

1.1 평가대상시스템 Safety Case

1.1.1 시스템 정의

본 장은 일반적 사항과 시스템에 대해 설명된다.

일반적 사항으로는 다음과 같은 사항들이 기술되어야 한다..

- 목적 및 범위 - 사업/제품 상황 및 적용 가능성을 포함한 항목
- 정의 및 약어 - 본 항목은 외부 문성에 의해 참조 될 수 도 있지만 개별적인 표로 나타난다. 주요 관련 항목은 본 항에 기술 된다.
  ※비고: 본 종합 안전 대책 기술서는 1장 앞에 약어표가 있다. 만약 약어표가 종합 안전 대책 기술서의 모든 약어를 포함한다면 이번 장에서 또 다시 고려할 필요는 없다. 하지만 모든 약어는 반드시 본 문서에 기록되어 있어야 한다.
- 적용 및 참고 문서 - 다음을 포함
  - 적용 가능 문서: 하위 목록에 나타나있고 그 버전 상태를 목록화한 참고사항이다. 종합 안전 대책 기술서는 목록화된 문서들 중 수정이 되어 더 이상 효력이 없는 문서들에 대해 최신화 되어야 한다. 예를 들면 업무 시작 공고, 계약 및 관련 부록과 적용 가능한 계약 문서들이 목록화 될 수 있다.
  - 적용 가능한 법적 요구사항 및 규격: 만약 기한을 가진 적용 가능 규격이 참조되어 있다면 그것에 대한 순차적인 수정 및 최신화 작업이 추후의 개정본에서도 동일하게 명백히 기술 되어 있을 때에 본 문서에 적용 될 것이다. 기한이 없는 적용 규격에 대해서는 가장 최근에 개정된 발행본이 적용 될 것이다. 목록은 CENELEC 규격, ISO 9001:2008, 그밖에 내부 절차서들이 포함된다.
  - 참고 문서 및 규격: 참고 문서 및 규격은 문서에 더 나은 이해를 위해서나 필수적이지 않은 적용 사항들에 대해서 고려 할 때에 사용되는 추가적인 정보를 제공하기 위해 인용된다. 본 목록은 안전 및 품질 매뉴얼, 내부 적용 안내서 및 EN 61508 과 같은 관련 규격들이 포함된다.

본 장의 시스템 정의는 "System Description"을 기반으로 한다.

1.1.1.1 개요

(가) 전제 조건

대상시스템의 열차운행방식은 ETCS/ERTMS Level2를 대상으로 구성해야 하며, 이를 위한 시스템 구성시의 전제조건은 다음과 같다.

첫째, 대상시스템은 기존의 물리적인 트랙을 대신하여 소프트웨어에 의해 가상으로 정의 되어지는 Logical 블록으로 구분된 가상블록을 대상으로 한다. 따라서, 대상시스템에서는 대상역을 대상으로 이러한 가상블록을 소프트웨어적으로 구분하여 구성하여야 한다.

둘째, 이러한 가상블록 시스템의 경우 실제 궤도에는 Transponder등과 같은 위치검지장치를 설치하여 차상장치로 하여금 열차위치를 검증할 수 있도록 구성되어 있다. 따라서, 차상 시뮬레이터에서는 모의열차운행 시 Transponder 등과 같은 열차위치검지장치를 인식해서 열차위치를 파악하는 것과 동일한 기능을 하도록 소프트웨어적으로 구현해야 한다.

(나) 설계 범위

대상시스템은 그 기능 구현을 위해 CRD(Control Route Distance)시스템과 ATS(Automatic Train Supervision) 시스템으로 구분되어 구성되며, 그 외에 차상장치 기능을 위한 차상설비 시뮬레이터와 현장설비 기능을 위한 신호설비 시뮬레이터로 구성된다.

본 과제에서 제작되는 시스템은 Main Line 및 Metro Line에 적용 가능하도록 설계함을 원칙으로 한다.

(다) 시스템 특징

1. 안전

CRD 시스템은 SIL4 규격을 만족하도록 구성하는 것을 원칙으로 한다.

2. 결함허용(Fault Tolerance), Availability

이중계의 REDUNDANT 시스템으로 구성하여 에러가 발생할 경우 STAND-BY 쪽으로 절체되어 안전하게 연속적인 동작이 이루어지도록 구성한다.

즉, 대상시스템인 CRD는 Hot-stand by 이중계 시스템으로 구성되며, 이러한 이중계 시스템은 입,출력 데이터를 비교하는 시스템으로 구성된다. 이중계 시스템의 결과를 비교하기 위해서는 결과를 처리하는 데이터 구조는 미리 정의되어 있어야 하고 독립적으로 실행되는 각 계의 동기화를 이루기 위한 구성과 알고리즘으로 구성된다.

3. Fail-safe

진로제어, 이동권한기능 등과 같은 CRD 시스템의 핵심기능은 Fail-Safe의 개념으

로 설계하여 시스템에 이상이 발생할 경우 안전 측으로 동작하도록 구성한다.

4.무정지, 무순단 하드웨어 구조

5.낙뢰, 서지 등 이상전압으로부터의 장치 보호

6.프로세싱 상태 감시 기능

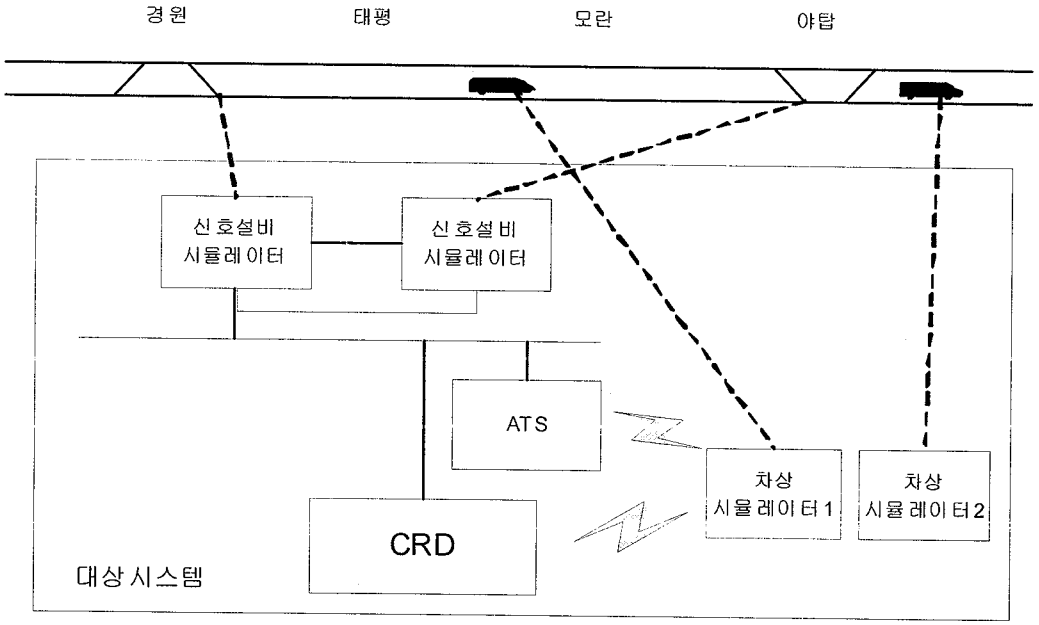
7.신뢰성 있는 고속 통신 기능 등

1.1.1.2 구성

대상시스템은 중앙의 신호기기실에 설치되어 진로제어 및 열차간격을 제어하는 시스템인 CRD와 Non-Vital 감시 기능을 가지는 ATS, 가상 열차운행을 위한 차상 시뮬레이터와 현장의 선로변에 설치되어 현장 선로전환기 등과 같은 선로변 장치를 제어하는 모의 현장신호 설비인 신호설비 시뮬레이터 시스템으로 구성된다.

(가) 다음은 시스템 전체에 대한 블록 다이아그램을 나타내었다.

그림 1. 시스템 블록 다이어그램



대상시스템을 구현하기 위한 신호설비 시뮬레이터는 선로전환기가 포함되어 있는 대상역을 구현하기 위해 2Set로 구성한다. 또한, 실제 차상 시뮬레이터를 시뮬레이션 하기 위한 차상 시뮬레이터도 2Set로 구성하여 열차 2대가 모의운행 되도록 구성한다.

(나) 다음은 대상시스템 전체에 대한 운영Level을 나타내었다.

대상시스템 중 ATS와 CRD 시스템은 각각 Center에 설치되는 개념으로 열차운행 감시와 제어를 담당하며, 신호설비 시뮬레이터는 현장에 설치되는 개념으로 현장신

호설비 기능을 담당한다. 차상 시뮬레이터는 현장 선로에서 운행되는 모의열차운행을 담당한다.

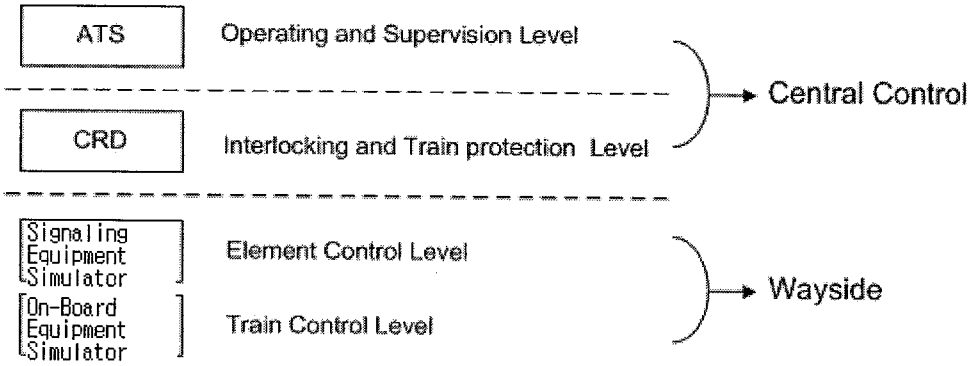


그림 2. 대상 시스템 운영 등급

(다) 다음은 대상시스템의 장치 별 인터페이스 구성도를 나타내었다.

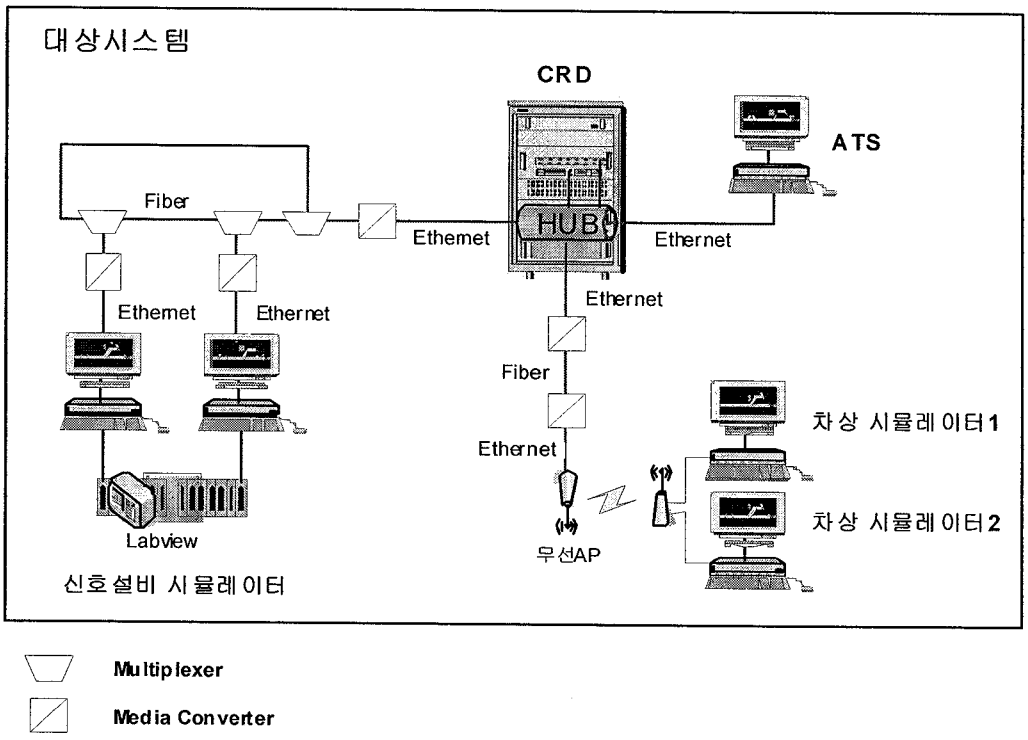


그림 3. 대상 시스템 장치별 인터페이스 구성도

CRD 시스템은 진로제어 및 열차이동권한 등의 기능을 담당하는 CPU 모듈과 외부 시스템과의 인터페이스를 담당하는 EIM(External Interface Module) 모듈과 각 모듈에 전원을 공급하는 전원부 등으로 구성된다.

CRD와 신호설비 시뮬레이터 및 무선AP(차상 시뮬레이터 인터페이스용)는 광 변환기와 같은 Media Converter를 이용해 광통신을 구현하도록 한다. 이는 외부시스템

으로부터 CRD 시스템을 보호하기 위한 절연기능과 함께 실제로 현장에 설치되는 신호설비와 무선AP의 특성을 고려하여 우수한 품질의 장거리 고속용 광통신을 구현하도록 하기 위함이다. CRD와 ATS 시스템은 Ethernet을 통한 인터페이스를 구현한다.

CRD와 차상 시뮬레이터와의 인터페이스는 무선 AP를 이용한 구성으로 한다.

(라) 다음은 Vital 기능을 포함하는 대상시스템인 CRD 시스템 기능별 Block diagram이다.

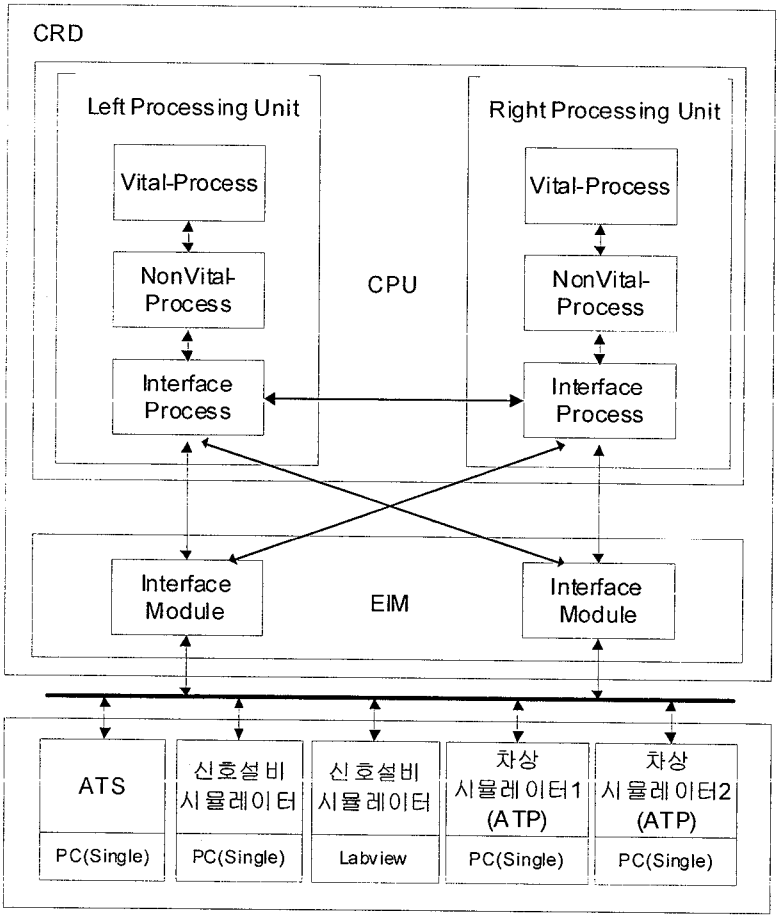


그림 4. CRD 시스템 기능별 블록 다이어그램 구성도

CRD 시스템은 두 개의 프로세스 단위로 구성된 Redundant 시스템으로서, 하나는 On-line으로 동작하고 다른 하나는 Stand-by시스템으로 동작하게 되며, 만약 On-line 시스템에 장애가 발생할 경우 Stand-by 시스템이 즉시 On-line시스템으로 절체 되어 안정적으로 연속적인 기능을 수행하여야 한다.

CPU 소프트웨어 구성은 vital과 Non-vital 기능으로 구분하며 논리적으로 구분된 두 Processor에서 각각의 기능을 담당한다. 즉, 시스템의 vital 기능은 vital processor에 의해 이루어지며, non-vital기능은 non-vital processor에서 담당하도록 구성한다. 즉, 안전과 관련된 진로제어와 같은 연동기능과 이동권한 등의 처리는

vital processor에서 이루어지며, 시스템 기동 및 관리, 로깅, 외부시스템과의 인터페이스를 위한 정보 생성 및 처리 기능 등은 non-vital processor에서 담당한다.

1.1.1.3 CRD시스템 기능

CRD시스템은 ATS로부터 수신되는 진로설정 제어명령의 처리와 현장설비 감시 등 현장 제어 정보에 대한 연동 제어를 수행하는 연동 시뮬레이터 기능과, 차상 시뮬레이터로부터의 열차운행정보 수신 처리 및 차상 시뮬레이터의 모의 열차운행을 위한 이동권한(PMA) 설정 등과 같은 열차자동방호 장치의 기능 등을 수행한다.

CRD시스템은 차상 시뮬레이터로부터 열차위치, 운행방향, 차량길이, 차량편성, 차상 시뮬레이터의 상태 등을 무선AP를 통하여 수신하여 ATS시스템으로 전송해야 한다. 또한 ATS시스템으로부터 수신된 진로설정 제어명령을 이용하여 해당 역의 진로를 설정 함으로서 열차의 진행을 할 수 있도록 한다.

다음은 CRD 시스템의 주요기능을 나타내었다.

■ 데이터 비교 입·출력

CRD 시스템은 이중계로 구성된다. 정상적인 상태에서는 1,2계가 ATS시스템으로부터 동시에 제어명령을 받아 입력 데이터를 비교한 후 CPU모듈에서 처리를 수행하여 서로의 연산결과를 확인하여 동일할 경우에만 주계에서만 출력을 해야 한다.

CRD의 이중화된 시스템은 동일하게 프로그래밍 되어 동기화된 명령에 의해 동일하게 동작한다. 구성은 2대의 독립된 마이크로컴퓨터에 의해 처리된 출력을 직렬 통신을 통해 전송한 후 비교하는 형태로 구성되며, 비교 처리된 정보가 동일할 경우에만 현재 on-line으로 동작하는 시스템이 출력을 내보내게 된다. CRD 시스템에서 연산되어 출력되는 vital 정보는 고수준의 안전성을 확보하기 위하여 On-line과 Stand-by시스템의 vital processor에서 연산된 정보를 비교하여 일치할 경우에만 정보를 출력하며, 연산된 정보가 일치하지 않을 경우는 경우 2회까지 반복 처리한 후 불일치 할 경우 해당출력에 대하여 안전측으로 제어되도록 하여야 한다.

또한, 2개 채널에 입력된 데이터도 병렬로 비교되고 처리된다. 수신된 입력정보도 마찬가지로 비교하여 동일하지 않을 경우 2회까지 반복 처리한 후 불일치 할 경우 해당입력에 대하여 안전측으로 동작되도록 하여야 한다.

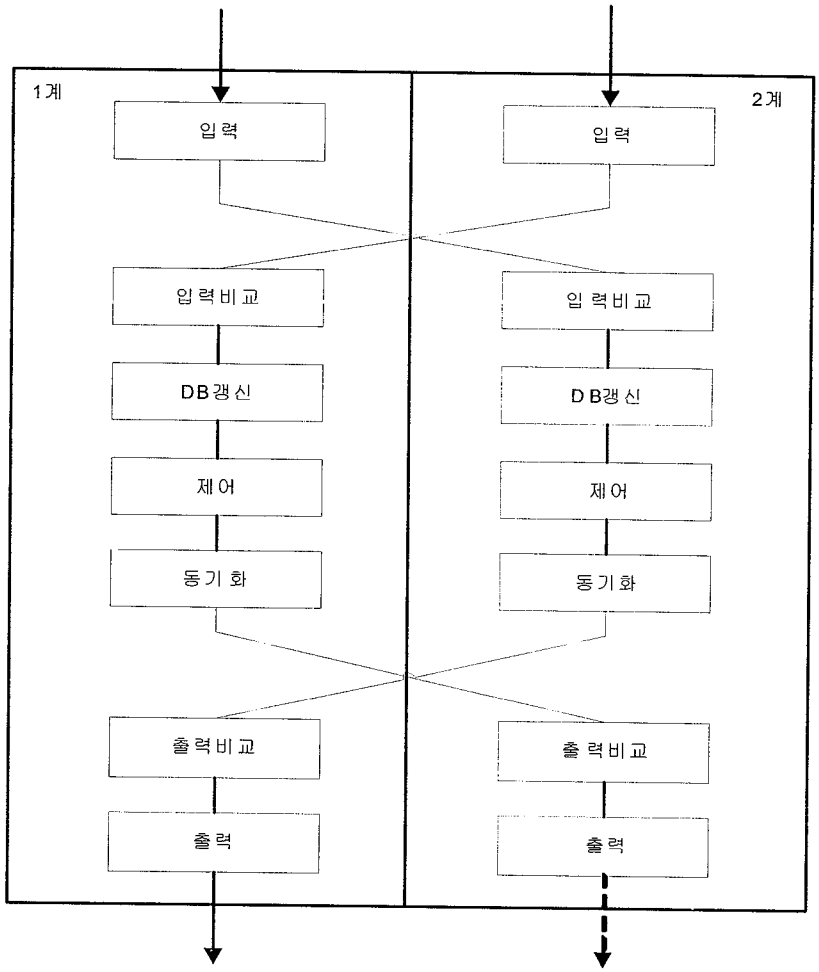


그림 5. CRD 시스템 데이터 비교처리 흐름도

운용중에 주계나 부계에서 CPU모듈 등의 고장으로 인해 더 이상 정상적인 연산을 수행할 수 없을 때, 현재 정상적인 운용이 가능한 계가 주계가 되어 기존의 출력을 그대로 유지한 채 지속적인 연동임무를 수행해야 한다

■ 연동 시뮬레이션

CRD 시스템에서의 연동 시뮬레이션 기능은 ATS시스템에서 수신되는 제어 정보의 처리 및 현장신호설비 상태변화에 따른 연동 정보의 변화를 처리하는 기능을 의미한다.

■ 진로/선로전환기 처리

진로/선로전환기 처리 기능은 Vital 기능 가운데 하나이며, CRD 시스템에 의해 처리된다. 선로전환기 감시 기능은 ATS 시스템이 고장을 일으킨 경우에도 영향을 받지 않는다.

■ 열차위치/이동/방향 감시

열차의 이동은 가상 블록 단위로 이루어 지며 CRD시스템은 차상에서 전송된 정보와 현재 시스템에서 저장하고 있는 이전 정보를 비교 분석하여 열차의 위치/이동/방향이 정

상인지 여부를 확인한다.

- 지정 열차에 대한 이동권한(PMA) 설정

  차상과의 통신을 통한 통신기반 열차운행 시스템은 열차의 이동 구간 확인을 위해 과거의 궤도 회로를 대신하여 가상 블록(Logical Block)이라는 개념을 도입하여 사용하며 이 가상 블록에 이동 권한을 부여함으로써 열차가 이동할 수 있도록 한다. 가상블록은 소프트웨어에 의해 가상으로 정의된 블록들로서 기존의 물리적인 트랙을 대신하여 정의되었다.

  CRD 시스템은 열차이동에 따라 차상으로부터 열차위치, 운행방향, 차상상태 등을 수신하여 열차의 이동에 따른 적절한 이동권한(PMA)을 설정하여 무선링크를 통해 차상 시스템으로 전달하는 기능을 한다.

- 열차간 안전한 이격 확보

  안전한 열차 이격을 확보하기 위해 최대 블록 길이를 설정하여 최악의 고장 조건 하에서도 열차를 보호할 수 있는 충분한 안전거리를 확보한다.

- 중앙 비상정지 처리

  ATS 시스템에서 중앙 비상정지(CESB) 명령이 수신되면 CRD 시스템은 제어 영역 내에 있는 모든 블록들을 폐쇄하고, 해당 구역 내에 있는 차량 이동을 금지시키게 되며, 경보가 ATS 시스템으로 전달된다. ATS 시스템 (Central Control) 내에 있는 reset 버튼을 눌러야만 CESB를 reset 할 수 있다.

- 가상블록 개/폐쇄

  궤도 유지보수와 같은 작업을 위하여 ATS 시스템에서 선로의 일정 구간에 대하여 작업구간 보호 구역 및 제한된 진로 보호 기능이 설정되어 CRD 시스템으로 전달되면, CRD 시스템은 블록 및 선로전환기 폐쇄를 이용하여 제로 속도 구역을 지정한다. 블록 보호 해제는 ATS 시스템에서 발생된 명령에 따라 이루어진다.

- 임시속도 제한

  열차가 작업구간 등과 같은 특정구간을 통과할 때 임시속도제한이 설정된다. 이러한 임시속도제한은 한 대의 열차에만 적용할 수도 있고, 특정지역내의 모든 열차에 적용할 수도 있다. ATS 시스템에서 CRD 시스템으로 임시속도제한 명령을 전송하면 CRD 시스템은 임시속도제한 명령을 차상 시뮬레이터로 전송하게 된다.

1.1.2 품질관리 보고서

안전승인을 위해 충족되어야 하는 첫째 조건은 시스템, 하위시스템 또는 장비의 품질이 그들의 수명주기(life-cycle) 동안 효력있는 품질 관리 시스템에 의해 지속적으로 관리되어야 한다는 것이다. 이를 증명하기 위해 증거문서가 품질 보고서(종합안전대책 기술서의 양식 Part2)에 제공 되어야 한다.

품질 관리 시스템의 목적은 수명 주기동안 각 단계에서 인적 오류로 인한 사고를 최소화

하여 시스템, 하위시스템 또는 장비의 체계적 고장의 위험성을 감소시키는 것이다.

품질 관리시스템은 EN 50126에 명시된 것처럼 시스템/하위시스템/장비의 수명주기동안 효력이 있어야 한다.

품질 관리는 종합안전대책 기술서에서 필수적인 사항이다. 품질 관리 보고서의 예시는 본 조항에 명시되어 있다.

품질 관리 보고서에 포함 되야하는 내용은 ISO 9001 인증을 받은 기업이라면 이미 어느 정도 수행하고 있고 만족한다고 생각 할 수 있다. 이후의 하위 항목의 대한 내용들은 각 항목의 내용으로 직접 작성 될 수도 있고 품질 매뉴얼 혹은 각 항목에 맞는 절차서를 참조함으로 종합 안전 대책 기술서의 품질 관리 보고서 장을 완성 할 수 있다. 관련 문서들은 기존의 문서를 그대로 사용 할 수 있으나 문서 고유 번호등을 고려할 때에 본 프로젝트에 적용 되는 형상 관리 계획서에 따른 작업이 이루어져야 한다.

1.1.2.1 조직구조

조직구조는 조직을 상호 관련이 있는 집단으로 분류하는 방법이다. 경영자의 관점에서 주로 고려해야 할 사항은 효과적인 의사소통 및 관리감독을 보장해야 한다는 것이다.

일반적으로, 업무(프로젝트) 부서의 조직구조는 그림형태로 나타낸다..
[품질 매뉴얼 및 관련 절차서] 참조 .

1.1.2.2 품질 계획서 및 절차서

품질 계획서에는 품질 검사 및 품질 자료가 프로젝트에 언제, 어떻게 적용되는지를 명시할 수 있다.

품질 계획서의 내용에 관한 예시는 다음과 같다

- 품질을 점검하기 위해 무엇이 필요한가?
- 품질을 점검하기 위해 가장 적절한 방법은 무엇인가?
- 언제 시행되어야 하는가?
- 누가 참여해야 하는 가?
- 어떤 품질 자료가 사용되어야 하는 가?

품질 자료는 프로젝트 책임자가 프로젝트의 품질을 향상시킬 수 있도록 지원하는 조직에서 사용한 결과물이다. 예: 견본, 표준, 점검표, 절차서 등
[품질 매뉴얼 및 관련 절차서] 참조 7

1.1.2.3 요구사양서

프로젝트의 요구사항은 고객 요구사항, 표준, 규정 등처럼 본 조항에 명시해야 한다.
[시스템 요구사양서 및 시스템 안전 요구사양서] 참조

1.1.2.4 설계 제어

설계 제어에서는 제조업체 또는 공급업체가 설계 제어를 받는 제품을 개발하는 경우, 그들이 명시된 설계 요구사항을 만족시켰음을 증명하는 적절한 문서를 작성하고 유지해야 한다고 설명한다.
[설계 계획서 및 관련 절차서] 참조

1.1.2.5 설계 검증및 검토

설계 검토 프로세스는 자격있는 검토자가 모든 문서를 검토해야 한다.
자격 있는 검토자는 회사 절차서에 명시된 요구사항 및 프로젝트 요구사항에 의거하여 설계 또는 분석을 점검할 수 있다.
[설계 계획서 및 관련 절차서] 참조

1.1.2.6 적용 공법

프로젝트 요구사항에 명시될 수 있는 장비가 언급된다.
[품질 매뉴얼 및 관련 절차서] 참조

1.1.2.7 수입 및 제조

수입 및 제조의 절차와 정책은 프로젝트 요구사항과 같이 정의되어야 한다
[품질매뉴얼 및 관련 절차서] 참조

1.1.2.8 제품 식별 및 추적성

이에 대한 정의 ISO9001에서 인용하였다.
적절한 경우, 조직은 제품을 실현하는 동안 적절한 방법으로 제품을 식별해야 한다. 조직은 감독 및 측정 요구사항에 맞게 제품 현황을 식별해야 한다. 추적성이 요구될 경우, 조직은 제품에 대한 고유의 식별법을 관리하고 기록해야 한다.
[형상 관리 계획서]참조

1.1.2.9 취급 및 저장

공급업체는 제품의 취급, 저장뿐만 아니라 보존 및 운반에 관해 문서화된 절차서를 작성하고 유지해야 한다.
[품질매뉴얼 및 관련 절차서] 참조 .

(가) 취급

공급업체는 제품의 손상 및 변질을 예방하기 위한 취급 조치(방법)를 모색한다.
[품질매뉴얼 및 관련 절차서] 참조 .

(나) 저장

공급업체는 제품의 사용 및 운반 전에 손상과 변질을 예방하기 위해 전용 저장소 및 창고를 지정해야 한다. 이와 같은 구역에서 반입 및 반출 권한을 부여하는 적절한 방법이 명기되어야 한다.

변질을 감지하기 위하여 공급업체는 적절한 간격으로 재고품의 상태를 평가하기 위한 계획서를 작성해야 한다.

[품질 매뉴얼 및 관련 절차서]참조 .

1.1.2.10 검사 및 시험

검사 및 시험의 목적과 절차가 정의되어야 한다.

공급업체는 제품에 대해 명시된 요구사항이 충족되었음을 검증하기 위한 검사 및 시험 행위에 대해 문서화된 절차서를 작성하고 유지해야 한다. 필수 검사 및 시험과 관련 기록은 품질 계획서 또는 문서화된 절차서에 상세히 명시되어야 한다.

[시험 사양서, 시험 보고서, 형식 시험 형식시험 보고서 및 관련 절차서] 참조 .

1.1.2.11 부적합 및 시정 조치

본 조항의 목적은 예방 및 시정 조치를 규명, 문서화, 분석 및 수행하기 위한 프로세스를 만들고 그 윤곽을 잡기 위함이다. 예방 또는 시정 조치는 조직에 영향을 미치는 모든 환경적 문제에 관한 절차서를 참고하여 착수될 것이다.

[품질 매뉴얼 및 관련 절차서] 참조 .

1.1.2.12 포장 및 운반

(가) 포장

공급업체는 명시된 요구사항에 대한 적합성을 보증하는데 필요한 포장 및 표기 공정(재료 용도 포함)의 관리 계획서를 작성해야 한다.

[품질 매뉴얼 및 관련 절차서] 참조 .

(나) 운반

공급업체는 최종 검사 및 시험 후, 제품의 품질을 지원해야 한다. 계약서 상에 명시된 경우, 목적지까지의 운반을 지원할 수 있는 만큼 확장 되야 한다.

[품질 매뉴얼 및 관련 절차서] 참조 .

1.1.2.13 설치 및 시운전

설치 및 시운전 방법은 자격이 있는 자에 의해 정해져야 한다.
[설치 매뉴얼, 유지보수 매뉴얼 및 관련 절차서] 참조 .

1.1.2.14 작동 및 유지보수

대게는 공급업체(개발업체)가 작동 및 유지보수에 관한 매뉴얼을 작성한다.
[사용자/유지보수 매뉴얼 및 관련 절차서] 참조 .

1.1.2.15 품질 모니터링 및 피드백

품질 모니터링은 비공식적으로 매일 행하는 것을 기본으로 하며, 설계 검토 단계에서 검증된다. 공식적인 품질 모니터링 및 피드백은 품질 심사를 통해 이행된다.
[품질 경영 계획서 및 관련 절차서] 참조 .

1.1.2.16 문서 및 기록

모든 문서는 다음 사항을 포함해야 한다:

- 품질 정책 및 품질 목적에 대해 문서화 된 보고서
- 품질 매뉴얼
- 국제표준에서 요구하는 문서화 된 절차서
- 프로세스의 효율적인 계획, 운영 및 관리를 보증하기 위해 조직이 필요로 하는 문서
- 국제 표준에서 요구하는 기록물

기록물은 실직적인 작동 및 요구사항의 적합에 대한 증거를 제공하기 위해 작성하고 유지되어야 한다.
[관련 절차서, Baseline 기록물 및 관련 절차서] 참조 .

1.1.2.17 형상관리/변경관리

형상화할 수 있는 품목은 시스템의 모든 부분을 의미하며 이는 반드시 형상 관리되어야 한다. 여기에는 시스템을 구성하는 모든 장비뿐 아니라 시스템의 구성 또는 기능을 정의하는 모든 설계 문서가 포함된다.
[변경 기록서 및 관련 절차서] 참조

1.1.2.18 자격 및 훈련

제품의 품질에 영향을 미치는 작업을 수행하는 인원은 적절한 교육, 훈련, 기술 및 경험을 기반한 자격이 있어야 한다.
조직은:

- 제품 품질에 영향을 미치는 작업을 수행하는 인원에 대해 필수 자격을 정해야 한다.

- 이러한 요구를 충족시키기 위해 훈련을 시키거나 기타 다른 조치를 취해야 한다.
- 취해진 조치의 효과를 평가해야 한다.
- 직원들이 그들의 활동의 타당성 및 중요성을 자각하고 있다는 것과 어떻게 그들이 품질 목표를 달성하는데 기여하는지를보증해야 한다
- 교육, 훈련, 기술 및 경험에 대한 적절한 기록이 남아 있어야 한다.

[품질 경영 계획서, 직원의 이력서] 참조 .

1.1.2.19 품질 심사 및 사후 조치

품질 심사는 ISO 9001 규격에 따라 완료 될 것이다. 자세한 활동은 제품의 특이성과 복잡성에 따라 달라진다. 프로젝트의 심사 일정은 품질 계획에 따라 정의될 것이며 요구되는 수명 단계에서 심사 일정에 따라 수행된다.

[품질 심사 프로토콜 및 관련 절차서] 참조 .

1.1.2.20 철회(Decommissioning) 및 철거(disposal)

공급업체(개발업체)는 철거 및 폐기에 관한 절차서를 작성하고 유지할 것을 요구한다.

[관련 가이드라인 및 관련 절차서] 참조 .

1.1.3 안전관리 보고서

안전관리 프로세스의 목적은 안전과 관련 있는 관리성 불량으로 인한 사고를 줄임으로써 체계적 고장(systematic faults)의 잔여 위험성을 최소화 하기 위해 전체 프로젝트 수명주기(life-cycle) 동안 현 기술표준에 명시된 안전 조건을 이행하였음을 보증하는 것이다.

안전관리 보고서는 다음 사항을 증명하기 위해 작성된다:

- 해당 프로젝트는EN50126에 따른 신뢰성을 가진 (RAMS)을 위한 관리 프로세스를 포함하고 있는 안전 관리 절차 시스템에 따라 정의, 개발 되었다.
- 조직 구조는 EN 50129 표준에 의거하였다.

또한 이는 EN50129의 요구사항에 따라 프로젝트의 안전을 보장하기 위해 이행된 활동에 대해 상세하게 설명한다.

프로젝트에 적용되는 안전관리 방법, 절차 그리고 조직은 프로젝트 예비단계부터 안전 계획서에 명확하게 정의되고 문서화되어야 한다.

안전 수명주기(Safety Life Cycle)

안전 수명주기는 EN 50126에 명시된 수명 주기를 충족하는 시스템 수명주기 내에서 행해지는 안전활동에 대해 상세히 설명한다. (여기에는 입력자료(Input), 산출자료(Output), 이미 작성된 또는 현재 작성 중인 문서 및 다른 단계에 대한 책임이 포함된다.)

모든 관련 행위는 안전 계획서에 의거하여 행해 졌다. 각 단계의 행위는 검증(verification) 계획서에 의거하여 검증되어야 하며 검증 보고서로 문서화 되어야 한다. 각 단계의 입력은

해당 단계와 관련된 모든 정보 및 데이터를 말한다.

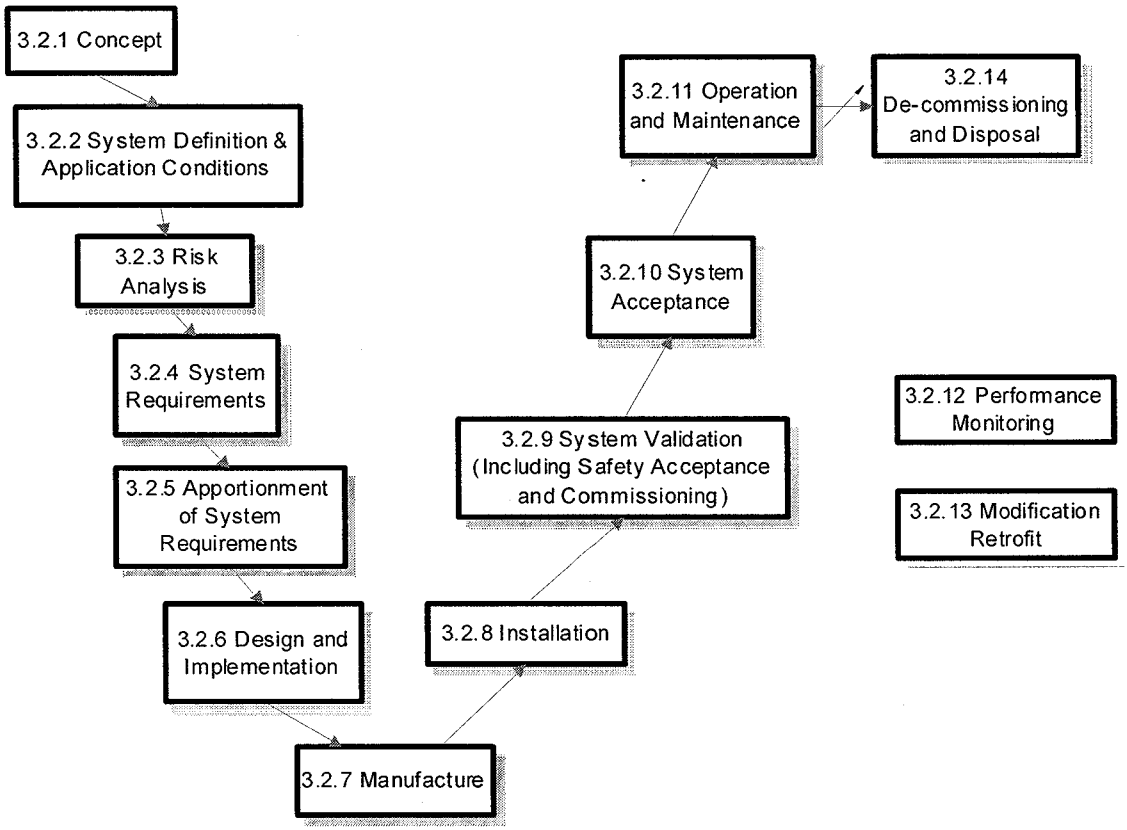


그림 6. 시스템 수명 주기

(가) 개념(Concept)

- 목표:
  - 안전 수명주기에 따라 시스템에 대한 이해를 높이기 위해
- 안전활동:
  - 사전에 성취된 유사/관련 시스템의 안전 성과/안전 요구사항과 관련된 정보를 획득
  - 기타 시스템 또는사람과 관련 있는 프로젝트의 안전 implications를 검토
  - 현 (철도당국) 안전 정책 & 안전 타겟 검토
- 결과물:
  - 참조된 문서 목록
  - 안전 조직도
  - 프로젝트 팀 인원들의 역할

(나) 시스템 정의 및 적용 조건

- 목표:
  - 시스템의 경계를 정의하기 위해

- 적용 조건을 규정
- 시스템에 대한 안전 계획서를 작성하기 위해
- 안전 기능을 규명하기 위해
- 일반적인 시스템 구성을 정의하기 위해

● 안전활동:

- 안전을 위한 과거경험 데이터 평가
- 위험원 사전 규명 수행
- (전반적인) 안전 계획서 작성
- 위험성 기준의 허용가능성에 대한 획득/정의
- 기존 사회기반기설 제약에 미치는 영향을 규명

● 결과물:

- 형상 관리 계획서
- 품질경영 계획서
- 안전 계획서(본 문서)
- 예비 위험원 분석(안전분석법 등)

(다) 위험성 분석

● 목표:

- 시스템과 연관된 위험원을 규명하기 위해
- 위험원을 초래하는 사건을 규명하기 위해
- 위험원과 연관된 위험성을 결정하기 위해
- 진행 중인 위험성 관리를 위한 프로세스를

● 안전활동:

- 시스템 위험원 및 안전 위험성 분석 수행
- 위험원 기록 Set-Up
- 위험성 평가 수행

● 결과물:

- 위험원 기록 (위험원, THR 계산, 저감 대책 등을 포함)

(라) 시스템 요구사항

● 목표:

- 시스템에 대한 전반적인 안전 요구사항을 명시하기 위해

● 안전활동:

- (전반적인) 시스템 안전 요구사항을 명시
- (전반적인) 안전 승인 조건 정의
- 기능적 요구사항과 관련된 안전을 정의
- Establish 안전 관리

● 결과물:

- 시스템 요구 사양서 (안전 관련 기능 반영)
- 검증(Verification)- 및 확인(Validation) 계획서)>
- 시스템 통합 계획서 (확인(Validation) 계획서에 통합시킬 수 있다.)
- 시스템 시험 사양서>
- 안전관리 보고서 (종합안전대책 기술서 중 일부)

(마) 시스템 요구사항의 할당

- 목표:
  - 지정된 하위 시스템, 부품 및 외부 설비에 대한 전반적인 안전 요구사항을 배분하기 위해
- 안전활동:
  - 시스템 안전 대상 및 요구사항 배분Apportion
    -하위시스템 및 부품 안전 요구사항 명시
    -하위 시스템 및 부품 안전 승인 조건 정의
  - 시스템 안전 계획서 업데이트
  - 전반적인 인터페이스 명시
- 결과물:
  - 구성 사양서
  - 하위시스템 사양서
  - 하위시스템 관련 안전 사양서
  - 하위시스템 시험 사양서
  - 확인(Validation) 계획서
  - 안전 계획서
  - 업데이트 된 시스템 요구 사양서
  - 업데이트 된 시스템 안전 요구 사양서

(마) 설계 및 실행

- 목표:
  - 안전 요구사항을 따른 하위시스템 및 부품을 생성하기 위해create
  - 하위시스템 및 부품이 안전 요구사항을 이행하였음을 증명하기 위해
  - 안전과 관련 있는 향후 수명주기 업무에 대한 계획서를 작성하기 위해
- 안전활동:
  - RAMS 요구사항을 따른 하위시스템 및 부품 생성
  - 위험원 기록 업데이트
  - 위험원 분석 완료
  - 안전 관련 설계 결정의 정당화
  - 프로그램 제어, 다음 사항 포함:
    - 안전관리 심사

- 하도급업체 및 공급업체 심사
- 일반 종합안전대책 기술서 준비
- (만약 적합할 시) 일반 적용 종합안전대책 기술서 준비
- RAMS와 관련하여 향후 수명주기 업무에 대한 계획서를 작성, 다음 항목 포함.:
  - 설치
  - 시운전
  - 운영 및 유지보수(운영, 유지보수 절차서의 정의를 포함)
  - 운영하는 동안 데이터 수집 및 평가
- 기법/대책에 따라 설계 및 실행
- 모든 문서가 상기 요구사항을 충족시키고 있음을 검증
- 일반 종합안전대책 기술서 준비

● 결과물:

- <향후 수명주기 업무에 대해 업데이트 된 또는 독립된> 확인(Validation) 계획서
- <업데이트 된> 안전 계획서
- 설계 사양서(소프트웨어: 모듈 사양서 포함)
- 시험 사양서 <예: 모듈 시험 사양서, 설계 시험 사양서>
- 부품 및 하위시스템 시험 보고서 <예: 모듈 시험 보고서>
- 심사 보고서
- 위험원 분석
- 종합안전대책 기술서 (시작)
- 소스 코드(Source code)>
- 각 문서에 대한 검증(Verification)보고서
- 업데이트 된 확인(Validation) 계획서
- 업데이트 된 종합안전대책 기술서
- 설계와 관련 있는 모든 기술 문서

(바) 제조

● 목표:

- 안전이 확인된 하위시스템(부품 포함)을 생성하는 제조 프로세스를 실행하기 위해,
- 안전 중심 프로세스 보증 방식을 To establish
- 하위시스템 및 부품 안전 지원방식을 To establish

● 안전활동:

- 하위시스템 및 부품 지원 방식 Establish

- 위험원 기록 작성

- 결과물:
  - 부품 및 하위시스템의 설치 및 유지보수 문서
  - 형상 문서
  - 사용자 매뉴얼
  - 시작 검증(verification) 보고서
  -

(가) 설치

- 목표:
  - 완성된 시스템을 형성하기 위해 요구되는 하위 시스템 및 부품의 조립 및 설치를 준비하기 위해
  - 시스템 지원 착수
- 안전활동:
  - 시스템 설치
  - 지원 방식 착수 (훈련, 지원 절차, 도구 및 여유 부품 준비)
- 결과물:
  - 설치 매뉴얼 작성
  - 설치 시험 보고서
  - 훈련 자료
  - 업데이트 된 안전 계획서
  -

(나) 시스템 확인(Validation)(안전 승인 및 시운전 포함)

- 목표:
  - 시스템이 요구사양서와 검증(verification) 및 확인(validation) 계획서를 이행하였는지 확인하기 위해
- 안전활동:
  - 하위시스템, 부품 및 외부 위험성 감소 조치가 시스템에 대한 RAMS 요구사항을 이행하였는지 확인
  - 하위시스템, 부품 및 외부 위험성 감소 조치의 종합적 시운전
  - 승인 가능한 시스템의 적용 종합안전 대책 기술서 준비.
  - 데이터 수집 및 평가
- 결과물:
  - (완성된) 종합안전대책 기술서
  - 확인(Validation) 보고서
  - 검증(Verification) 보고서
  - 시험성적서(Tests reports) ...>

- 운영 매뉴얼
-

(다) 시스템 승인

- 목표:
  - 하위시스템, 부품 및 외부 위험성 감소 조치가 완성된 시스템에 대한 모든 안전 요구사항을 이행하였는지를 평가하기 위하여
- 안전활동:
  - 종합안전대책 기술서 평가
  - 모든 프로젝트 관련 문서 준비
- 결과물:
  - 평가 보고서
  -

(라) 운영 및 유지보수

- 목표:
  - 운영자 및 유지보수 직원을 위한 관련 매뉴얼 준비
- 안전활동:
  - 진행 중인 안전 중심 유지보수 수행
  - 진행 중인 안전 성능 모니터링 및 위험원 기록 유지보수를 수행
  - 운영 매뉴얼 작성
  - 유지보수 매뉴얼 작성
  - 관계자 훈련
- 결과물 (그리고 업무):
  - 운영 매뉴얼
  - 유지보수 매뉴얼
  - 훈련
  -

(마) 성능(Performance) 모니터링

- 목표:
  - 시스템의 안전 성능에 대한 신뢰성을 유지하기 위해
- 안전활동:
  - 성능 및 안전 통계를 수집, 분석, 평가하고 사용
- 결과물 (또는 업무):
  - 기록 (데이터, 오류, 등)
  -

(바) 변경 및 보강

- 목표:

- 시스템 RAMS 요구사항을 유지하기 위한 시스템 변경 및 보강 업무를 관리하기 위해

- 안전 활동:
  - 변경 및 보강으로 인해 미치는 안전 영향을 고려
- 결과물 (또는 업무):
  - 형상 관리 계획서에 따른 변경 기록
  - 업데이트 된 위험원 기록

(사) 철거 및 폐기

- 목표:
  - 시스템의 철거 및 폐기 업무 관리를 위해
- 안전활동:
  - 안전 계획서 작성
  - 위험원 분석 및 위험성 평가 수행
  - 철거 조치
- 결과물(또는 업무):
  - 모든 철거 및 폐기 업무에 대한 기록물
  - 업데이트 된 위험원 기록

1.1.3.2 안전조직

안전 조직은 EN 50129 표준에 의거하여 하기 표와 같이 정의된다. CRD 시스템은 SIL4를 필요로 하므로 안전 조직은 SIL 3와 4를 위한 조직 구조를 따라야 한다.

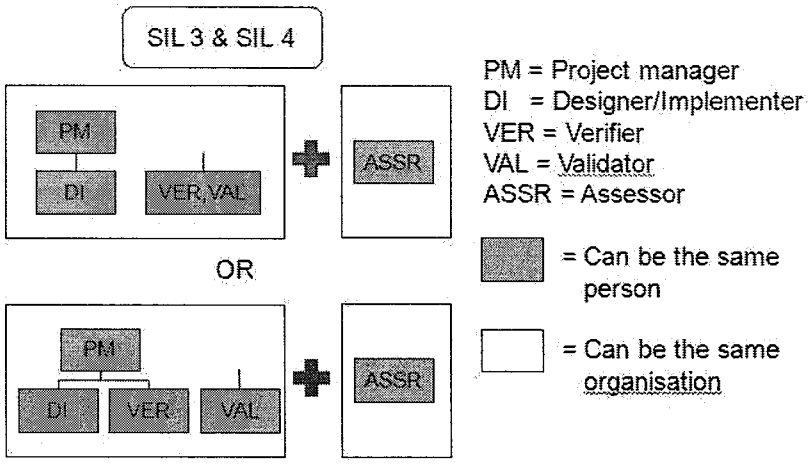


그림 7. SIL3와 SIL4 등급에서의 안전 조직

SIL 3과 4의 경우, 프로젝트 책임자는 확인자(validator)에게 명령(지시)을 할 권한이 주어지지 않는다. 확인자(Validator)와 검증인(verifier)은 동일한 인물이라도 상관없다. 단, 평가자(assessor)는 항상 독립적이어야 한다.
역할 및 권한에 대해서는 [안전 계획서] 에 상세히 설명되어 있다.

1.1.3.3. 안전계획서

본 장은 안전 계획서 작성을 위한 안내서를 포함한다. 대개, 안전 계획서는 별도의 문서로 작성된다. 대아티아이는 본 안내서나 2차년도 프로젝트 때에 발행된 템플릿을 기반으로 안전 계획서를 작성 할 수 있다.

(가) 목적

안전 계획서는 시스템 및 하위시스템의 기능적 안전의 범위, 목적 달성, 유지보수, 공급을 위한 모든 활동, 방법, 기술 및 사건에 대한 기록을 포함한다.
본 문서는 제품 수명 주기 동안에 유효하며 어제든지 최신화 될 수 있다. 안전 관리인은 본 제품의 성공적인 평가를 수행 할 때까지 본 계획서에 대한 책임을 가지고 있다.
안전 계획서는 수명주기 중 2단계인 '시스템 정의와 적용 조건"에서 작성이 시작되며, 성공적인 검증 이후에 본 단계에서 유용하다(형상 관리 계획서, 사전 위험성 분석, 시스템 검증 계획서 및 소프트웨어 검증 계획서 참조). 시작 단계에서는 순차적인 주기 단계에 따라 완전하지는 않겠지만 최종 단계에서는 본 프로젝트의 완전한 안전 관리 활동이 완성될 것이다. 안전 계획서는 본 프로젝트의 다른 계획서나 참조 문서들과 최신 버전으로 반드시 일치되어야 한다.

(나) 범위

안전 계획서는 우리가 의도하는 CRD 시스템이 CENELEC 규격인 EN 5012x 시리즈에 따라 관련 SIL 등급 획득을 고려하는데에 적용할 수 있다.

(다) 안전 수명 주기

안전 계획서는 모든 수명주기 동안의 활동을 포함하며 안전적인 측면에서 본 프로젝트를 관리한다. 수명 주기는 14단계로 되어 있다. 본 장에는 CENELEC 규격에 따라 각 단계의 목적, 활동 및 결과물에 대해서 설명한다.
안전 활동을 확인하기 위한 각 단계의 검증은 검증 보고서에 따라 수행되고 문서화되어야 한다. 모든 관련 정보들과 그 단계에 적당한 자료들이 각 단계의 입력 값으로 사용된다.
적절한 결과물을 얻기 위한 안전 활동과 문서의 성공적인 완성을 감시하기 위해 점검표가 사용 될 것이다.

(라) 안전 목표값과 안전

① 안전 목표값의 정의

각 기능들은 정성적 안전 목표값과 함께 정량적 목표값을 가져야한다. 정성적 목표값은 안전 무결성 등급으로 나타나고 체계적 장애 무결성을 담당해야 한다.

CRD 시스템의 안전 목표값은 시장 요구(고객 요구)에 의해 제안되었다. 그럼에도 불구하고 안전 목표값은 THR 값을 구하기 위해 BP리스크 (또는 다른 위험성 분석 방법)를 통해 계산되어 각 기능으로 할당 되었다. 자세한 내용은 시스템 안전 요구 사양서에 기술 되어 있다.

정의된 안전 목표값과 할당된 SIL 등급이 표 2 에 기록되어있다.

대아티아이에 의해 결정된 모든 최 상위 기능은 THR 값과 SIL 등급과 함께 표 2 에 기록되어야 한다.

표 1. 안전 목표값 및 SIL(예)

번호	최상위 기능	THR	SIL
**	기능 1	4.00E-09	4
	기능 2	4.00E-09	4
	기능 3	4.00E-08	3
	기능 *	4.00E-08	3

SIL 목표값에 도달하기 위한 기술 및 방법들에 대한 계획이 세워져야 한다. 안전 관리자가 수명주기 동안의 기술 방법에 대한 책임을 가진다. 안전 계획서에 대한 점검표가 사용될 것이다.

참고 문서들이 기술과 방법(Techniques and measures)들을 기본으로 작성 되었고 그 목록이 추산된다. 전체 수명 수명 주기 동안에 추가되거나 수정 될 것이다.

CENELEC 규격(EN 50128, EN 50129)의 부록에 보면 우리가 목표하는 SIL 등급에 따른 수행되어야 하는 기술과 방법들이 나와있다. 대아티아이에서는 시스템의 SIL 등급에 맞춰 필요한 기술과 방법들을 결정하고 또한 각 기술과 방법에 대한 올바를 숙지를 바탕으로 수행해야 한다.

아래 표 3 은 EN 50129 부록에 첨부된 기술과 방법들 중 우리가 목표하는SIL 4 등급에서의 적용 방법들에 대해서 표현한 표이다. 예시와 같은 계획이 안전 계획서에 포함되거나 첨부되어야 한다.

표 2. 기술과 방법 적용 예

Technique / Measure	SIL 4	Approach	Comments
Checklists	R	No	The verification and validation plan will be used.
Simulation	R	No	It will be not applied.
Functional testing of the system	HR	Yes	Comprehensive functional test will be recited in the test plan.
Functional testing under environmental conditions	HR	Yes	Safety-related functions under the specified environmental conditions will be depicted in the test plan.

② 시스템에 의한 위험성 및 위험원

본 시스템에서 발생 가능한 모든 위험성에 대해서 '사전 위험원 분석" 문서에 기록되어있다.

위험원 분석을 통해 확인 된 위험원들은 계산되고 분류 되었다. 그 방법과 근거들은 [시스템 안전 요구 사양서] 와 [위험원 기록] 문서에 기록되어있다.

③ 안전 개념의 기본

본 프로젝트는 일반 CRD 시스템의 SIL 인증서를 획득하는 것이다. 결국, 모든 안전 활동은 CENELEC 규격을 따라야 한다. 설계자와 독립된 검증자는 전체 수명주기에서 각 단계의 결과를 검사하고 검토 할 것이다. 모든 프로젝트 안내서는 다음과 같이 작성된다.

- 품질 관리
  - 형상 관리 계획서
  - 품질 관리 계획서

- 안전 관리
  - 시스템 검증 계획서
  - 소프트웨어 검증 계획서
  - 시스템 확인 계획서
  - 소프트웨어 확인 계획서
  - 안전 계획서 점검 표

- 내부 안전 심사 계획서
- 요구 사항 추적표

다음의 활동은 안전 계획서를 작성하는 것과는 별개로 안전 관리자가 책임을 가지고 있다.

- 전체 주명주기 동안에 안전 요구사항의 유효성에 대한 점검
- 안전 검토의 시행

④ 하위 계약자와 공급자의 관리

기본적으로 CRD 시스템은 대아 티이에 의해 설계되고 생산된다. 만약 대아 티아이에서 CRD 의 어떤 부분에 대하여 공급자를 고용한다면 그 공급자는 반드시 ISO 9001에 부합하는 품질 절차를 가지고 있어야 한다.

⑤ 종합 안전 대책 기술서 개념

일반 종합 안전 대책 기술서는 CENELEC 규격 EN 50129 에 따라서 작성 될 것이다. 안전 관련 개발 및 적용 조건 (SACs)은 특정 프로젝트에서 가정 될 것이다. (실제 프로젝트. 적용시는 목표값으로 삼아야 한다.)

⑥ 안전 관리

안전 계획서는 종합 안전 대책 기술서의 3장 안전 관리 보고서의 안내서를 제공할 것이다.

⑦ 역할과 기능

3.3.1 장 참조

⑧ 자격 요건

3.3.2 장 참조

⑨ 프로젝트 조직

SIL 프로젝트 팀이 조직 되었다. SIL 3&4 조건에 맞추기 위해 확인자는 프로젝트 관리자로부터 독립되어 있어야 한다. 팀은 CENELEC 규격에 따라 조직 될 수 있다. (그림 8참조)

다음 그림은 조직도의 한 예이다.

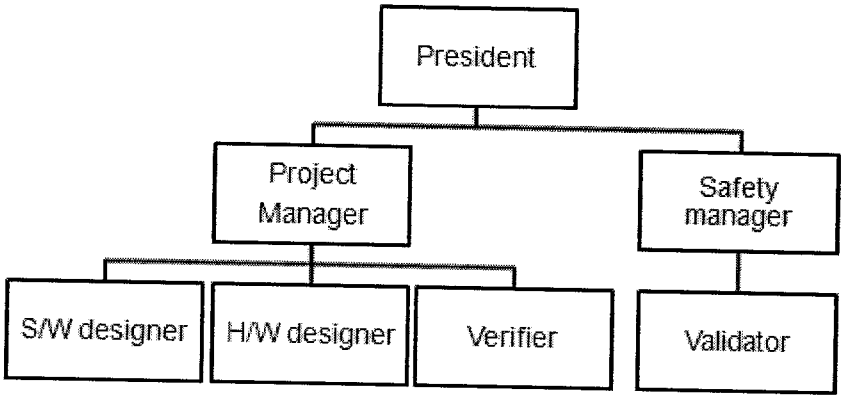


그림 8. 안전 조직도의 예

안전 조직을 구성할 때 SIL 4 등급에 맞는 조직으로 구성해야 함을 고려해야 한다. SIL 4 등급에 적용되어야 하는 조직 구성은 그림 8에 나와있다. 주요 사항은 시스템 및 소프트웨어등의 요구사항을 확인 하는 확인자 (Validator)가 반드시 프로젝트 관리자(Project Mager)와 독립되어 보고 체계에 있어서도 프로젝트 관리자 상위의 구성원에게 바로 보고가 될 수 있는 조직 구성이 이루어져야 한다.
안전 조직도에는 각 역할을 맡고 있는 구성원의 이름이 직접 조직도 안에 포함되어야 하며 추후 조직의 변경이 발생시 관련 절차서에 따른 수정이 이루어져야 한다.

⑩ 검토 / 검증

검토 및 검증은 시스템 검증 계획서 및 소프트웨어 검증 계획서에 따라 검증자에 의해 수행될 것이다. 알맞은 활동과 기술 및 방법들은 3.4.4.3장에 정의된 품질 및 안전 절차서에 기술 된 내용에 따를 것이다.

⑪ 안전 심사

안전 계획서는 담당자에 의해 작성되고 검토되고 배포될 것이다.
안전 계획서를 최신화 해야 한다면 안전 관리자의 확인을 받은 후 수정된 안전 계획서가 배포 될 것이고 즉시 프로젝트에 적용 할 것이다. 어떤 교정이라도 발생한다면 수명 주기중 적당한 시기로부터 안전에 대한 영향에 평가되어야 한다.
개발 기간 동안, 안전 관리자는 티유브이 슈드의 안전 심사 일정에 따라 내부 안전 심사를 수행해야 한다.

표 3. 내부 심사 개념

단계	대아 티아이 내부 심사	티유브이 심사
개념 단계	티유브이 심사 한 달 전	개념 단계의 마지막
상세/이행 단계	티유브이 심사 두 달 전	상세 단계의 마지막
구체적인 날짜는 양사간의 합의에 의해 결정 될 것이다.		

⑫ 배포

만약 안전 계획서에 어떤 변경이 있다면 모든 프로젝트 팀 구성원들은 그 정보를 받고 변경된 안전 계획서를 열람 할 수 있어야 한다.

표 4. 안전 계획 배포 목록

배포 받을 자	배포 형태	목적
프로젝트 관리자	E 메일 사용	정보 전달
안전 관리자	E 메일 사용	정보 전달
하드웨어 / 소프트웨어 설계자	E 메일 사용	정보 전달
확인자	E 메일 사용	정보 전달
검증자	E 메일 사용	정보 전달
평가자	E 메일 사용	정보 전달

문서 배포에 앞서 해당 문서의 배포 대상이 먼저정의 되어야 한다. 대개의 문서는 프로젝트 팀 구성원 모두를 배포 대상으로 가질 것이다. 배포 대상을 명확히 정의하여 변경 정보등에 대한 정보를 받지 못하는 구성원이 생기지 않도록 해야한다.

(가) 위험원 및 위험성 분석

① 위험성 분석 및 위험원 제어 방법

대개 위험성 분석은 운영사에 의해 수행된다: 위험성 분석은 최소한 다음 사항을 다뤄야 한다.

- 시스템 정의
- 위험원 도출
- 결과 분석
- 위험성 평가
- THR 할당

만약 해당 프로젝트에 대한 위험성 분석이 수행 되지 않았다면 그에 대한 이유가 기술 되어야한다.

본 프로젝트에 대한 위험원 분석이 수행되었다. 그것은 [관련 문서]에 문서화 되어 있다. 또한 개발 과정에 따라 지속적으로 최신화 될 것이다.

위험원 분석은 사전 위험원 도출, 인과적 분석, 공통 사항의 분석, SIL 할당 및 정량적 분석을 포함하고 있다. (본 프로젝트에서 어떠한 방법이 사용 되었는지 기술 되어야 한다.)

② 위험원 및 위험성의 추적 및 완화절차

첫 단계로, 최고 단계 위험원의 완화 대책이 위험원 기록 및 사전 위험원 분석 문서에 고려되어 있다. 개발하는 동안 모든 엔지니어들은 추적 및 추후의 완화 방법의 최신화를 위해 위험원을 열람 할 수 있다.

위험원 상태에 대한 일관성을 유지하기 위해 위험원 기록의 수정 및 최신화 절차는 형상 관리 절차서를 따른다. 위험원은 그 위험원을 감지한 프로젝트 구성원에 의해 기록 되어야 한다. 위험원 기록의 제출자는 즉각적으로 안전 관리자에게 알려야 한다. 발견된 위험원이 아직 알려지지 않은 것인지 혹은 이미 위험원 기록에 기록이 되어 있는지가 안전 관리자에 의해 점검 되어야 한다.

③ 위험원 기록

위험원 기록은 기능, 도출된 위험원, 원인, 결과, 안전 목표, 완화 대책 및 위험원의 상태를 (광범위한 안전 관리 활동) 포괄하고 있다.

위험원 기록은 작성되고 최신화 될 것이다. 그것은 시스템에서 발생 가능한 모든 위험원 목록들로 구성되어 있다. 공식적인 구조는 MS 엑셀 시트를 사용한다.

모든 프로젝트 구성원은 위험원 기록을 열람 할 수 있으며 안전 관리자만이 그 상태(완료, 진행중, 미완료)를 결정 할 수 있다.

개발의 마지막 단계에서 모든 입력은 완료 되어야 한다.

(나) 확인 및 평가

① 확인

확인은 시스템 확인 계획서 및 소프트웨어 확인 계획서에 따라 확인자에 의해 수행 될 것이다. 적당한 활동 및 기술 방법들이 3.4.4.3장의 품질 및 안전 절차서에 맞춰 수행 될 것이다.

② 평가 및 승인

평가 및 승인 절차는 평가 계획서에 따라 티유브이 슈드에 의해 완료 될 것이다.

이것은 프로젝트의 상황에 따라 조정 될 수 있다.

1.1.3.4. 위험원 기록(Hazard log)

위험원 기록에는 각 위험원에 대한 위험성 관리 정보 및 위험성 분류와 함께 규명된 위험원의 목록을 포함한다.

위험원 기록은 "live"로 고려되어야 한다. 이는 프로젝트 수명 동안 위험원 기록에 등재된 인원이 변경될 수 있음을 의미한다. 또한, 위험원 기록에 등재된 인원은 live 상태여야 한다. 그래서 수명주기 동안 위험원은 프로젝트와 관련된 모든 변경사항에 의해 재개(reopen)될 수 있다.

위험원 기록에는 각종 기록이 나열되어 있다. 이는 시스템에 의해 수시로 업데이트 되어야 하기 때문에 쉽게 관리되어야 한다. 위험원 관리를 위한 기록물은 완벽하게 설명되어야 하며 문서화되어야 한다.

다음 사항이 보고된다

- 사용된 방법, 도구 및 기술
- 위험원 기록의 구조

다음 정보가 사용된다

- 독특한 식별번호 : 식별번호는 독특하고 명확하며 추적이 가능해야 한다.
- 기록일자
- 고안자
- 각각의 위험한 경우 (위험원에 대한 간략한 설명)
- 관련 부품들. (타입 및 버전에 영향을 받는 시스템, 하위시스템 또는 장비);
- 상세 설명 및 분석의 상호참조 (안전 검토 및 심사 포함);
- 각 위험원과 관련 있는 사건 순서의 중요도 및 빈도 및 결과
- 각 위험원의 위험성 (위험성은 명시된 위험한 사고의 결과 및 개연성의 빈도의 결과로 정의된다.;
- 각각의 위험한 사건 동안, 허용 등급을 낮추거나 위험성을 제거하기 위해 취해진 조치
- 이행된 모든 분석에 대한 상세 설명, 분석의 한계, 분석하는 동안 발생된 모든 가정 또는 분석 중에 사용된 데이터에적용하는 모든 신뢰성 한계
- 현황 열림 / 취소됨 / 해결됨 (검증됨) / 닫힘 (확인됨)

이미 언급된 것처럼, 위험원 기록은 생동적으로 고려되어야 하기 때문에 현황을 규명하는 것이 필수적이다. 이는 다음 항목을 포함해야 한다.

- 위험한 상태(Criticality)
- 종결을 위한 남은 조치
- 기존 저감 대책
- 모든 남은 포인트에 대한 평가

[위험원 기록_1.0]에 명시되어 있는 표 참조 바람.

1.1.3.5 안전 요구 사양서

각 시스템/하위시스템/장비에 대한 특정 안전 요구사항(안전 기능 및 안전 무결성 포함)은 안전 요구 사양서에 규명되고 문서화되어야 한다. 이는 다음과 같은 방법으로 달성 될 수 있다.

- 위험원 식별 및 분석
- 위험성 평가 및 분류
- 안전 무결성 등급 할당

EN 50126에 명시되어 있음.

(가) 적용범위

SSRS은 안전과 관련이 있는 요구사항을 포함한다. 안전 요구사항은 독립된 사양서에 작성된다.

안전 요구사항은 다음 두 가지로 고려될 수 있다

- 안전 기능 요구사항
- 안전 무결성 요구사항

안전 기능 요구사항은 시스템, 하위시스템 또는 장비가 이행해야 하는 사항으로 실제 안전과 관련이 있는 기능을 의미한다.

안전 무결성 요구사항은 각각의 안전 관련 기능에 요구되는 안전 무결성 등급에 대해 정의한다.

[시스템 안전 요구 사양서] 참조 바람.

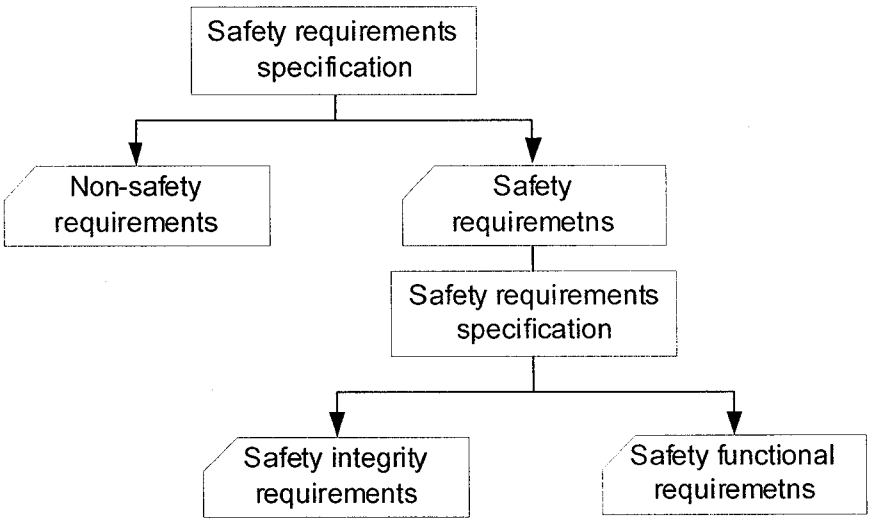


그림 9. 안전 요구사항

(나) 안전 무결성

시스템 무결성은 필수 안전 기능을 준수하기 위한 안전 관련 시스템의 성능과 관련이 있다. 안전 무결성이 높아질수록, 필수 안전 기능을 이행하지 못할 가능성이 낮아진다.

안전 무결성은 그림 10 과 같이 다음 두 항목으로 구성된다. 그림 10

- 체계적 장애 무결성
- 비체계적 장애 무결성

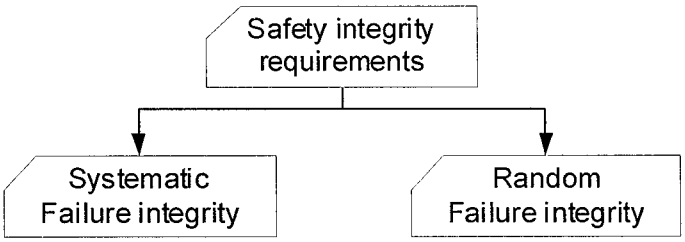


그림 10. 안전 무결성 요구사항

체계적 장애 무결성은 안전 무결성 중 정량화 할 수 없는 부분을 의미하며 위험한 체계적 고장과 관련이 있다. 체계적 고장은 수명 주기(life cycle)의 다양한 단계에서 인재로 인해 발생한다.

체계적 장애 무결성은 품질 경영과 2장 및 3장에 명시되어 있는 안전관리를 통해 획득된다.

체계적 고장에 대한 기술적인 방어책은 4장에 명시되어 있는 기술 안전 조건에 포함된다.

비체계적 장애 무결성의 achievement는 4장에 명시된 기술 안전 조건 안에 포함된다. 안전 무결성 요구사항의 할당

SIL 할당은 수행된 위험성 분석 및 시스템 구조 사양서를 바탕으로 위험원 기록에 나타내어져 있다 (참조: 위험성 분석보고서, 시스템구조사양서, 위험원기록)

1.1.3.6 시스템/하위시스템/장비 설계

명시된 요구사항에 맞게 설계되어야 한다. 상의하달식의 구조화된 설계 방법이 엄격하게 제어되고 검토된 문서와 함께 사용되어야 한다.
시스템/하위시스템/장비의 설계 단계에서는 다음 주제를 포함하는 설계 문서를 작성해야 한다.

- 시스템/하위시스템/장비 구조 기술서
- SW 요구사양서
- HW 요구사양서
- 형식시험 계획서

설계의 종결단계에서는 검증(verification) 활동이 이행되어야 한다. 이 활동의 결과물로 다음 항목을 포함하는 시스템/하위시스템/장비 Architecture 검증(Verification) 보고서가 작성된다.

- 시스템/하위시스템/장비 요구사양서 및 설계 문서 간의 추적성
- 구조화를 위한 설계 방법의 상의하달식 방법. SIL등급에 따라 EN 50129, 표 E.7의 기법/대책이 적용 되었다.
- EN 50128에 의거하여 하드웨어 및 소프트웨어 간의 관련성. EN 50128의 기술/대책이 명시된 SIL 등급에 의거하여 적용되었음을 상세히 명시해야 한다
- 환경 요구사항 및 형식시험 계획/환경 연구와 관련하여 주고 받은 서신의 목록. 적용된 표준/규범의 목록을 명시해야 한다.
-

1.1.3.7 안전 검토

수명주기 중 적절한 단계에서 안전 검토가 이행 된다. 안전 검토는 안전 계획서에 의거하여 이행되며 모든 결과는 [관련 문서]에 문서화되어야 한다.
다음 항목들이 반드시 고려되고 명시되어야 한다.

- 항목(Item) 참조 번호
- 검토 된 문서의 참고 문서t
- 검토 일자
- 검토자
- 수명주기(life-cycle)의 단계 및 검토된 문서
- 검토 내용
- 권고 사항 및 행위의 상태
- 완화 대책 및 오픈 포인트의 평가

1.1.3.8 안전 검증(Verification) 및 확인(Validation)

확인 계획서로부터 최초의 안전 요구사양서에 따라 완성된 시스템/하위시스템/장치의 확인 및 검증 계획서에 따른 앞 단계에서 확인된 어떤 안전 요구 사항이 수명 주기의 각 단계에 만족 하도록 검증 하는 작업이 수행 되었다. 그리고 두 가지 계획서 모두 안전 계획서에 포함되거나 참조 되었다.

- V&V 계획서
- V&V 보고서
- SW 모듈 시험 사양서

[V&V 관련 문서] 참조 바람.

1.1.3.9 안전 타당성

종합안전대책 기술서는 CRD 시스템이 안전 목표를 만족함을 증명한다. 필요시, 타당성 보고서와 같은 관련 문서가 도움이 된다.

1.1.3.10 시스템/하위시스템/장비 양도

CRD시스템의 공식적인 양도 이전에 안전 승인 및 안전 승인에 대한 조건이 만족되어야 하며 종합안전대책 기술서 및 안전 평가 보고서를 제출해야 한다.

1.1.3.11 운영 및 유지보수

운영자 및 유지보수 직원을 위해 운영 및 유지보수 매뉴얼을 준비해야 할 필요가 있다.
[운영 매뉴얼, 유지보수 매뉴얼 외] 관련 문서 참조 바람.

1.1.3.12 철거 및 폐기 Decommissioning and disposal

적절한 철거 및 폐기를 위해, 적절한 조치가 마련되어야 한다.
[관련 문서 및 절차서] 참조 바람.

1.1.4 기술적 안전 보고서

본 장에서는 종합 안전 대책 기술서의 1장 개요 부분을 보충하는 내용을 기술한다

CRD 시스템은 다음과 같은 특징을 갖는다.

- Safety
  CRD 시스템은 SIL4 규격을 만족하도록 구성하는 것을 원칙으로 한다.
- 결함허용(Fault Tolerance), Availability
  이중계의 REDUNDANT 시스템으로 구성하여 에러가 발생할 경우 STAND-BY 쪽

으로 절체되어 안전하게 연속적인 동작이 이루어지도록 구성한다.즉, 대상시스템인 CRD는 Hot-stand by 이중계 시스템으로 구성되며, 이러한 이중계 시스템은 입,출력 데이터를 비교하는 시스템으로 구성된다. 이중계 시스템의 결과를 비교하기 위해서는 결과를 처리하는 데이터 구조는 미리 정의되어 있어야 하고 독립적으로 실행되는 각 계의 동기화를 이루기 위한 구성과 알고리즘으로 구성된다.

- Fail-safe

  진로제어, 이동권한기능 등과 같은 CRD 시스템의 핵심기능은 Fail-Safe의 개념으로 설계하여 시스템에 이상이 발생할 경우 안전측으로 동작하도록 구성한다.
- 무정지, 무순단 하드웨어 구조
- 낙뢰, 서지 등 이상전압으로부터의 장치 보호
- 프로세싱 상태 감시 기능
- 신뢰성 있는 고속 통신 기능 등

본 장에서는 EN 50129 규격에 따라 CRD 시스템의 안전에 관한 근거들을 제시한다.

1.1.4.1 정확한 기능적 운영의 보증

본 장에서는 운영 및 안전 요구 사항에 기술되어진 내용에 따라 고장으로부터 자유로운 조건에 따른 시스템의 정확한 운영을 고려한다.

다음과 같이 가용한 문서나 그 통합 문서들에 대한 기술이 필요하다.

- 필요시 이전 버전의 시스템/하위시스템/장치 평가
- 각 기능의 SIL 분류에 따른 안전 관련 기능에 대한 설명과 분석 (필요시 새로운 기능 포함)
- 관련 설계 문서에 언급된 저급 방법 운행 정의 및 관리
- 영향을 받는 구조 제시
- 사용되는 안전 원리 제시
- 재 사용되는 기능의 안전 정당성 제시
- 사용되는 규격과 기준에 따라 달성되는 안전 등급 제시
- 안전 등급을 고려한 운영 보장 조건과 사용 조건 제시

본 프로젝트에 기반하는 기술적 안전 원리에 대해서 소개해야 한다. 위의 사항들에 대해 명확히 하기 위한 블록 다이어드램이나 도표들이 유용하게 사용되어야 한다.

(가) 시스템 구조 설명서

시스템 구조에 대한 설명 혹은 관련 문서 참조를 포함한다.

CRD 시스템은 ATS로부터 받은 제어 정보와 로컬 및 차상 자료를 통한 열차 PMA를 가지고 열차를 운행한다. 이러한 목적을 위해 CRD 시스템은 VME 버스를 통한 임베디드 시스템을 구축하였다.

CRD 기능을 구현하기 위한 CPU모듈, 광통신부, Network Switch 등은 표준 19"랙

에 다음과 같이 장착되었다.

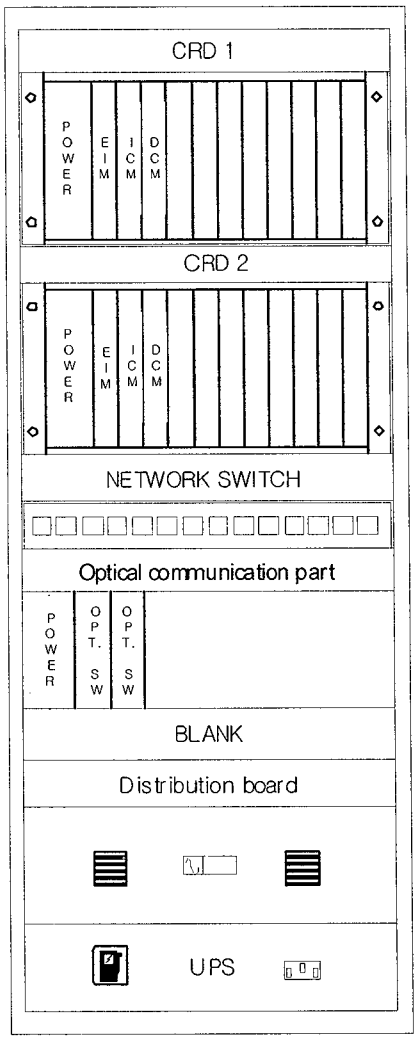


그림 11. CRD 19RAck 구조

CRD 시스템의 주요 부품과 사양은 시스템 요구사양서에 기술되어 있다.
또한 일반적인 CRD 시스템 설계의 설명을 포함하며 그것이 사용되는 원리와 기술에 대한 명확한 이해를 전할 수 있다.

(나) 인터페이스 정의

본 장에서는 우리가 고려하고 있는 시스템에 대한 인터페이스를 정의한다. 안전 문제는 내부 인터페이스 뿐만 아니라 외부 인터페이스와도 연관이 있기 때문에 외부 인터페이스에 대한 특별한 관리가 수행되어야 한다.
지상시스템(CRD, ATS시뮬레이터)과 차상시뮬레이터간에는 무선 통신방식으로 접속이 이루어지나, 실제 지상시스템은 무선전송장치와 접속 되어있는 네트워크 장비

(Network Switch)까지만 네트워크로 접속이 이루어진다. 지상시스템 상호간, 즉 CRD, ATS시뮬레이터, 신호설비제어시뮬레이터, 신호설비(선로전환기)시뮬레이터간 interface는 네트워크 접속으로 이루어진다.

인터페이스 종류는 다음과 같이 구분할 수 있다.

- CRD(ICM)과 ATS시뮬레이터
- CRD(DCM)과 ATS시뮬레이터
- CRD(ICM)과 신호설비제어시뮬레이터
- CRD(DCM)과 차상시뮬레이터(ATP)
- ICM과 DCM
- EIM과 ICM
- EIM과 DCM
- EIM(1계)과 EIM(2계)

위의 인터페이스에 대한 각각의 설명은 시스템 구조 사양서에 기술되어있다.

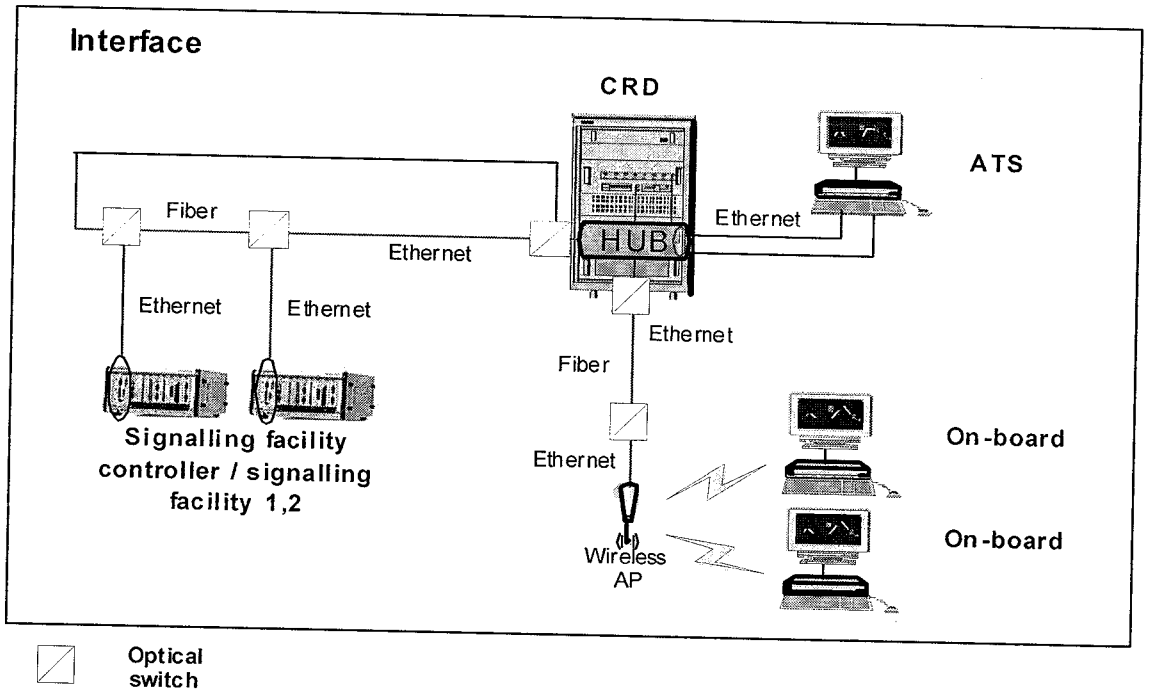


그림 12. 인터페이스 시스템의 물리적 구조

ICM과 신호설비제어시뮬레이터, DCM과 차상시뮬레이터(ATP), ATS시뮬레이터와 차상시뮬레이터(ATO) 인터페이스간에는 광 스위치와 같은 Media Converter를 이용해 광통신을 구현하도록 한다. 이는 외부시스템으로부터 CRD 시스템을 보호하기 위한 절연기능과 함께 실제로 현장에 설치되는 신호설비와 무선AP의 특성을 고려하여 우수한 품질의 장거리 고속용 광통신을 구현하도록 하기 위함이다. CRD(ICM, DCM)와 ATS시뮬레이터는 Ethernet을 통한 인터페이스를 구현한다.

본 장에서 시스템간 정보 전송 방식은 Multicast방식을 기본으로 한다. Mock-up을 구성하는 각 시스템(호스트)은 Multicast Group에 가입하여 시스템간 정보를 송·수신하게 된다. 따라서 Multicast Group은 시스템간 인터페이스에 따라 최적화되어 생성되어야 하며, 이에 따라 다음에 설명되는 Multicast Group은 mock-up 각 시스템의 최적화된 인터페이스를 위해 추후 변경 가능하다.

CRD 시스템 인터페이스의 자세한 설명은 시스템 요구사양서에 기술되어있다.

(다) 시스템 요구 사양서의 수행

본 장에서는 요구 사양서에 기술 된 운영적 기술적 요구사항이 설계에 어떻게 반영되는지에 대하여 설명한다. 그 내용은 검증 보고서와 확인 보고서에 기술되어 있다.

V&V 계획서에 따른 V&V 활동은 V&V 보고서를 통해 기록된다. 검증 활동은 현재의 상태가 이전 단계에서의 요구사항에 부합하는가의 내용을 검증한다.

검증: 각 단계에서 출력되는 결과가 이전 단계의 요구 사항에 부합하는지를 분석과 시험을 통해 결정하는 활동

확인: 제품이 기술된 요구 사항에 모든 면에 있어서 부합하는지에 대해 시험과 분석을 통해 결정하는 활동

다음의 문서들이 참조 될 수 있다.

- 소프트웨어 디자인 사양서
- 소프트웨어 모듈 설계 사양서
- 시스템 요구 사양서
- 소프트웨어 모듈 시험 사양서
- 소프트웨어 모듈 시험 보고서
- V&V 보고서

(라) 안전 요구사양서의 수행

본 장에서는 기술된 안전 기능적 요구사항이 설계에 어떻게 반영되는지에 대해서 설명한다.

안전 요구 사항 수행은 V-수명주기의 상-하행 단계에서의 위험원 분석 단계에서 정해진 다음의 두 가지 사항에 대해서 증명한다.

- 기능적 안전
  - 본 사항은 설계 방법에 대응되는 요구사항의 근거와 관련 시험방법들 및 시험 보고서를 근거로서 증명 될 수 있다.
  - 안전 시험 사양서는 체계적 접근을 기본으로 해야 한다. 예를 들면 HAZOP 과 FMECA 연구를 통한 위험원 분석을 기본으로 할 수 있다.
- 안전 무결성
  - 본 사항은 부품들의 장애율의 결합, 사고간의 간격, 안전을 위한 방법의 보

장에 대한 분석과 계산을 통해서 증명 될 수 있다.

다음의 문서들이 참조 될 수 있다.

- 소프트웨어 설계 사양서
- 소프트웨어 모듈 설계 사양서
- 시스템 안전 요구 사양서
- 안전 분석 및 결과

(마) 설치 설계

완성 된 제품을 설치하기 위한 요구사항도 고려해야 한다. 각 요구사항은 고유 번호를 두어 추적성을 확립해야 한다.

(바) 설치 시험

제품의 성공적인 설치를 확인하기 위한 시험들에 대해서 나열 한다. 입력 값에 따른 출력 값을 확인 하는 방법 등의 시험등을 고려할 수 있으며 각각의 시험을 점검하기 위한 점검 표가 사용 될 수 있다.

(사) 승인 및 시운전 시험

확인 공정 중 이 단계에서는 시스템 승인과 시운전을 위한 준수해야하는 공정 등급을 확인하고 오류와 문제를 평가한 결과를 기록한다.

(아) 정확한 하드웨어 기능의 보증

본 장에서는 하드웨어의 구조와 요구 무결성을 달성하기 위해 어떻게 설계가 되었는지에 대해 요구 사양서와 RAMS 관련 규격(EN 50126)등을 통해서 증명할 수 있다.

- RAMS

표 5. RAM 업무

수명 주기 단계	단계에 따른 RAM 업무
1	기존의 RAM 수행 자료 검토 프로젝트에 있어서 RAM 관계 고려
2	과거 경험한 RAM 자료 평가 사전 RAM 분석 수행 RAM 정책 수립 장기 운영 및 유지보수 조건 도출 기존 기반 시설의 제약에 따른 RAM 영향 도출
3	N/A
4	시스템 RAM 요구사항 열거 (전체) RAM 승인 기준 정의 시스템 기능 구조 정의 RAM 프로그램 수립

	RAM 관리 수립
5	시스템 RAM 요구사항 할당 ● 하위 시스템 및 부품의 RAM 요구사항 열거 ● 하위 시스템 및 부품의 RAM 승인 기준 정의
6	검토, 분석, 시험 및 자료 평가에 의한 RAM 프로그램 이행 ● 신뢰성 및 가용성 ● 유지보수 및 유지 보수 성 ● 최선의 유지 보수 정책 ● 물류 지원 프로그램 제어 착수 ● RAM 프로그램 관리 ● 하위 계약자와 공급자 제어
7	환경 압박 심사 수행 RAM 개선 시험 수행 장애 기록 및 정정 활동 시스템 시작
8	유지 보수자 훈련 시행 여분의 부품 및 장비 공급 확립
9	RAM 증명 수행
10	RAM 증명 평가
11	진행중인 여분의 부품 및 장비의 획득 진행중인 유지 보수와 물류 지원 중점의 신뢰성 수행
12	수집, 분석, 평가와 성과 및 RAM 통계
13	수정 및 개선에 대한 RAM 관계 고려
14	RAM 활동 없음

(자) 정확한 소프트웨어 기능의 보증

본 장에서는 EN 50128의 요구 사항을 준수했는지 증명한다. 하드웨어와 소프트웨어 간의 상호작용에 관하여 설명한다.

- EN 50128 규격에서 요구하는 모든 문서
- 소프트웨어 확인 보고서
- 소프트웨어 평가 보고서
- 하드웨어와 소프트웨어간의 상호작용

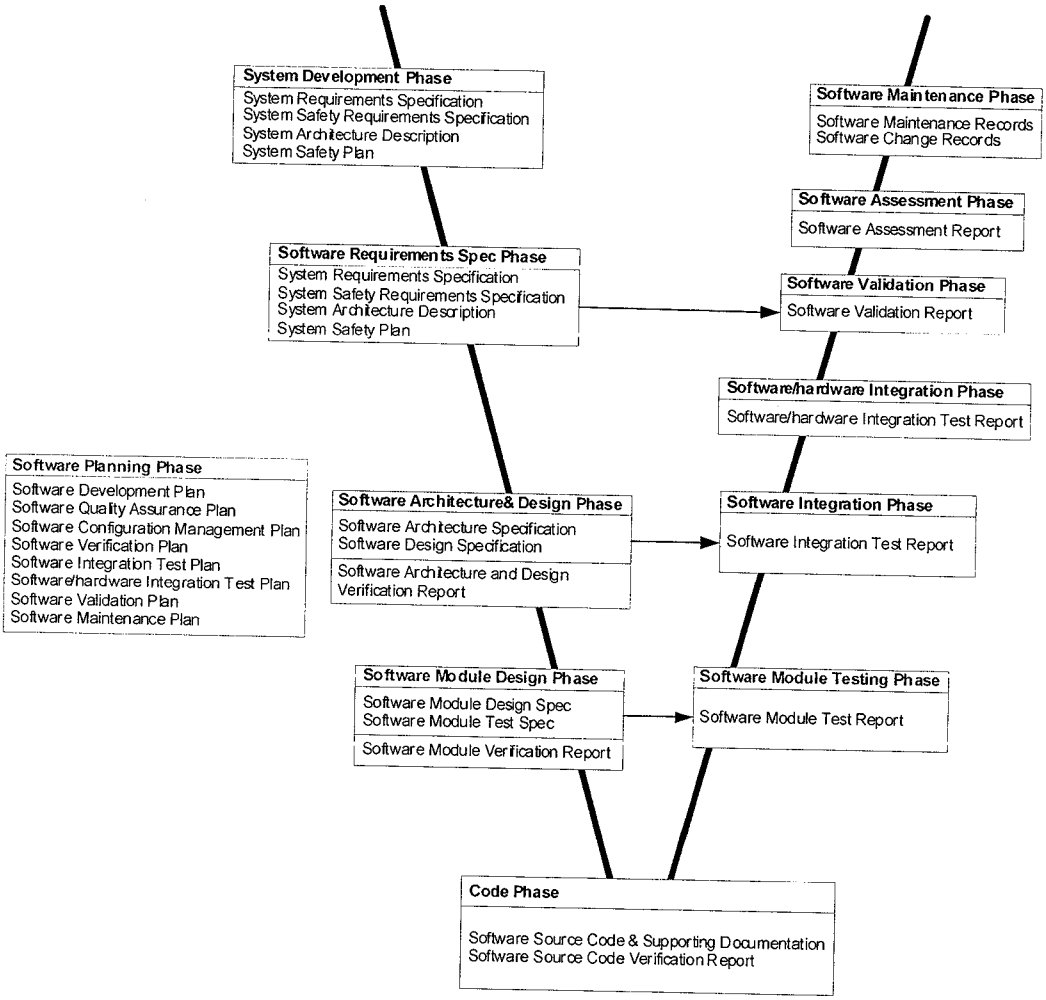


그림 13. 소프트웨어 수명 주기

1.1.4.2 고장의 영향

고장의 영향에 대해서 논하기 앞서 고장을 정의하고 또한 고장, 오류, 장애간의 관계를 설명하는 것이 필요하다. CENELEC 에서는 그 용어들을 다음과 같이 정의한다.

- 고장: 시스템에서 오류를 발생 시킬 수 있는 비 정상적인 조건. 고장은 체계적 혹은 비체계적으로 발생 될 수 있다.
- 오류: 의도하지 않은 시스템의 동작이나 장애로 인한 결과로 인한 의도된 설계로 부터의 일탈
- 장애: 시스템의 기록된 수행으로부터의 일탈. 장애는 시스템의 고장이나 오류의 결과이다
- 위험원: 사고를 일으킬 수 있는 조건

그림 14는 외부 사고, 부품 고장, 시스템과 하위시스템의 위험원이 되는 고장 및 다른 장

애들 사이의 관계를 보여주고 있다.

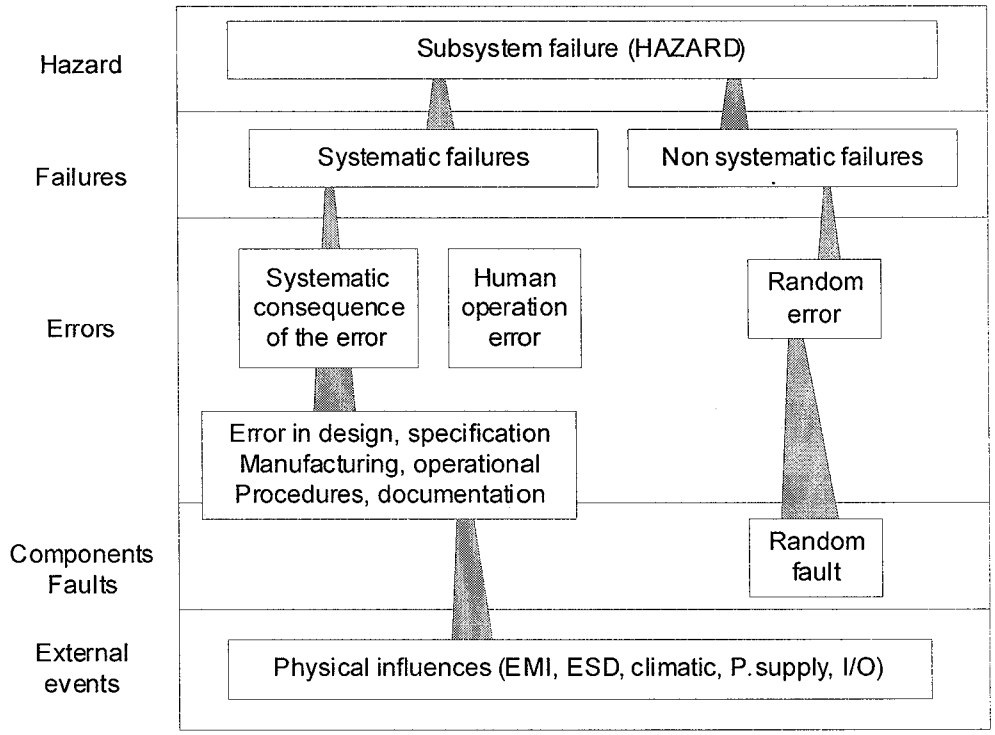


그림 14. 고장, 오류, 장애의 관계

체계적 장애는 정량화 할 수는 없지만 관련 절차와 기술적 방법들을 통해서 완벽히 측정되고 최대한 완화되어야 한다.

체계적 결함은 다음의 이유를 통해 유발 될 수 있다.

- 사양 및 설계 오류
- 기 존재하는 고장 (소프트웨어 설계 오류, 프로그램 장치의 오류 등)
- 도구 고장 (컴파일러, 개발 툴 등)
- 절차서 (설계, 개발, 운영 등) 혹은 유지 보수 오류

(가) 하나의 고장에 따른 영향

본 장은 FMEA 의 결과로서 충분히 설명 될 수 있다. CRD 안전 분석 보고서에 FMEA 의 결과값이 나타나있다.

(나) 품목별 독립성

FTA 혹은 Markov 모델이 사용된다면 그 방법들이 적용되는 동안 4.3.2, 4.3.3, 4.3.4장과 관련된 질문들에 대한 답이 제시 되어야 한다. 그것은 대개 공통 원인 장

애(CCF) 분석을 포함한다.

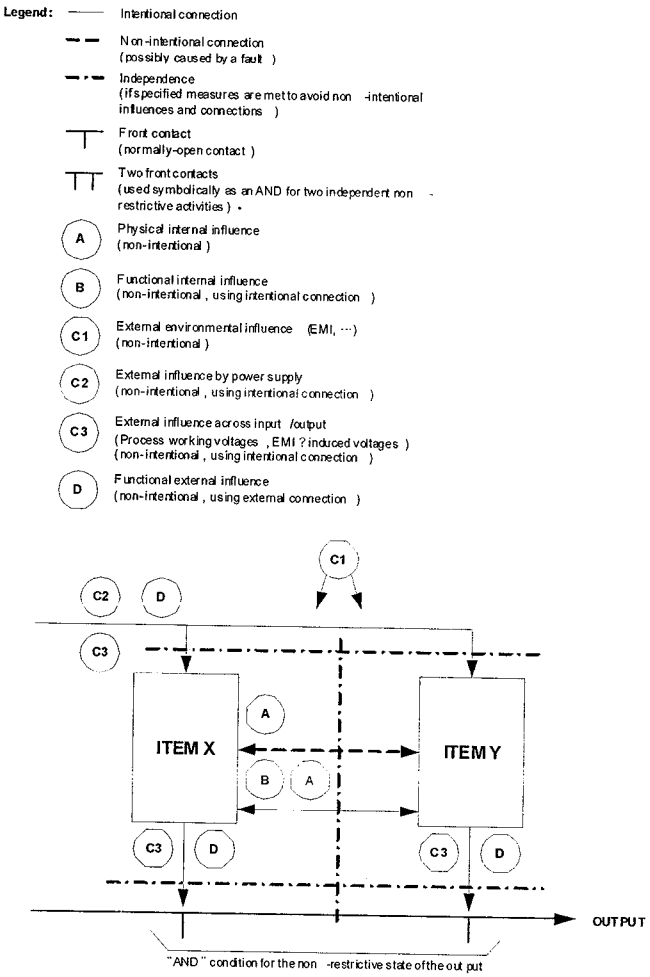


그림 15. 품목별 독립성의 영향

(다) 하나의 고장에 대한 탐지

FMEA와 비체계적 장애 무결성에 대한 평가의 조합된 방법으로 시스템이 안전 목표에 준한다는 것을 증명한다.

(라) 탐지에 따른 행동 (안전 상태의 유지 포함)

EN 50129에 기술된 방법들을 통해서 어떠한 고장이 발생하더라도 시스템은 안전한 상태로 움직인다라는 것을 증명한다.

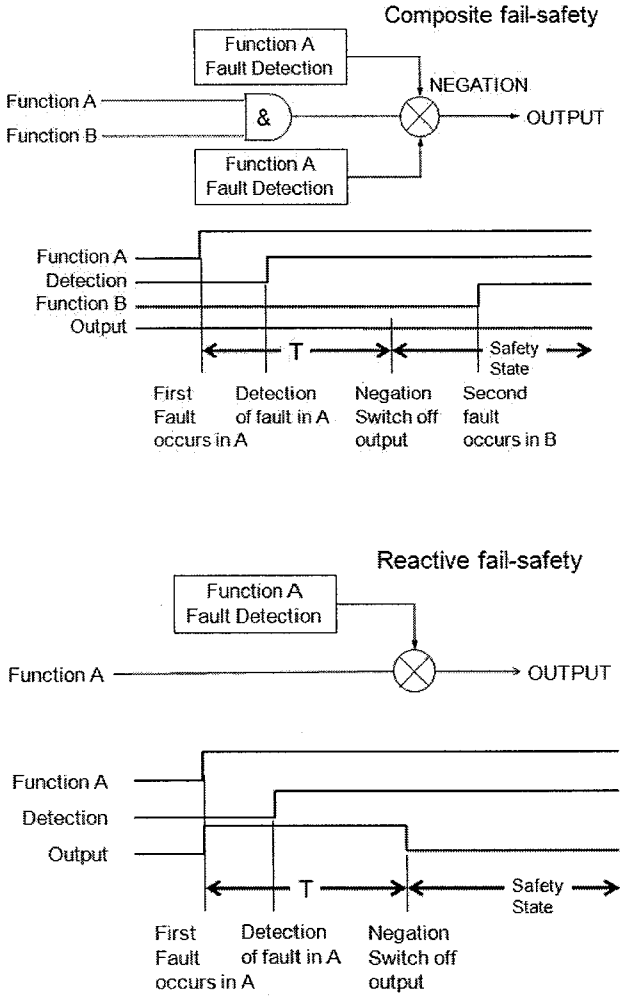


그림 16. 하나의 고장에 대한 탐지와 부정

(마) 복합적 고장에 대한 영향

복합적 고장에 따른 영향은 고장목 분석을 통해서 평가된다.

(바) 체계적 고장의 방어

전체적인 시스템의 구조는 안전하게 설계된 장치의 하위 시스템이나 아이템의 위험한 장애의 사고 중에도 사고가 발생되지 않도록 구성되어야 한다.

1.1.4.3 외부 영향에서의 운영

본 장에서는 외부 영향에 노출 되어 있을 때에 시스템의 정확하고 안전한 운영 능력을 고려한다. "정확한 운영"은 운영적, 안전적 요구사항의 수행을 모두 포함한다.

EN 50125-1 과 EN 50125-3 에 나열된 다른 조건에서의 값들을 만족해야 한다.

저장과 이동에 따른 영향도 고려해야 한다.

- 기후조건

- 기계적 조건
- 고도
- 전기적 조건 (비 차량 관련)
- 전기적 조건 (차량 관련)
- 허락되지 않은 접근으로부터의 보호
  - 접근 등급 정의
  - 보호
  - 외부 조건
  - 보호
- 보다 심각한 조건

각 시험에 대한 결과는 확인 보고서에 증명되어있다.

1.1.4.4 안전 관련 적용 조건

본 장에서는 규칙, 조건, 시스템 및 하위시스템의 적용에서 관찰이 필요한 기능적 안전 사항 관련 법 등에 대해서 정의한다.

본 장에서 다루는 일반적 사항은 다음과 같다.

- 특정 조건을 준수하기 위한 프로그램 시스템의 구성
- 제조, 설치, 시험 및 시운전 시의 예방 조치
- 유지보수 및 고장 발견을 위한 규칙과 방법
- 시스템 운영 교육
- 안전 경고 및 예방 조치
- EMC 예방조치 (영향 및 방출)
- 수정 및 철거를 고려한 정보
- 시험 장치, 유지보수 장치 및 구성 툴 과 같은 보조 장치의 안전 정당성
-

(가) 하위 시스템/장치 구성 및 시스템 조립

- 구성
- 시스템 조립
- 기능 변경

(나) 운영 및 유지보수

- 운영 상태
- 유지보수 등급
- 주기적 유지보수
- 유지보수 원조

(다) 운영적 안전 감독

안전 관련 활동들은 감독되고 기록된다

관련 문서 참조

(라) 철거 및 처분

철거 및 처분을 위한 안내서가 있어야 한다.

1.1.4.5 통합 안전 시험 (Safety Qualification Test)

시스템 운영 조건들 하에서 통합 안전 시험이 성공적으로 수행하였다는 결과를 기록하여 한다(validation report가 참조될 수 있음). 본 시험의 목적은 다음과 같다.

- 시스템이 규정된 운영 요구사항 이상을 만족하고 있다는 확인
- 규정된 신뢰성 및 안전 목표 이상을 달성하였다는 확인
- 최종 안전 승인 이전에 운행 서비스를 시행할 수 있다는 확인

부 록 B

CRD시스템 당해년도 SSHA 도출

Hazard-1 동일블록에 두 대의 열차가 존재

Hazard-1	동일블록에 두대의 열차가 존재																	
Preliminary Hazard Analysis						S			D			U	Total	THR	Failure Rate	Action	Recommended action	Remark
Subsystem	No.	Cause		Failure	Effect	E	V	A	T	C	H							
DCM	1.1	DCM 열차 허용이동권한 설정 오류																
	1.1.1	열차위치 정보 오류			열차충돌													
	1.1.1.1		열차로부터 비정상적인 열차 위치 정보 수신	Systematic		5	7	4	1	3	4	-1	23	1.00E-09		설계	* 열차위치 적합성 검사를 통한 열차위치 검증 * 지속적인 열차 상태정보 확인 필요	
	1.1.1.2		DCM 열차위치 정보 처리 오류	Systematic		5	7	4	1	3	4	-1	23	1.00E-09		설계, 테스트	* DCM이중계 구성 필요 * EIM 비교처리 기능 수행 * 열차위치 검증 수행 * EN50128에 따른 SW안전성 보증 활동 수행 * 각 테스트 수행	EN50128 부록 참조
	1.1.2	DCM 허용이동권한 처리 오류(S/W)			열차충돌													
	1.1.2.1		허용이동권한 처리 로직 오류	Systematic		5	7	4	1	3	4	-1	23	1.00E-09		설계, 테스트	* DCM이중계 구성 필요 * EIM 비교처리 기능 수행 * EN50129에 따른 SW안전성 보증 활동 수행 * 허용이동권한 처리를 위한 블록검증, 열차위치 검증 수행 * 각 테스트 수행	
	1.1.2.2		Database(memory) full	Systematic		5	7	4	1	3	4	-1	23	1.00E-09			* DCM이중계 구성 필요 * EN50130에 따른 SW안전성 보증 활동 수행 * Database 용량 확대 및 플래시 메모리 추가	
	1.1.3	DCM 전원공급 실패			DCM Down													
	1.1.3.1		UPS 고장	Random											1.10E-07	설계, 유지보수	* PSU이중계 구성 * DCM전원공급 실패 시, ATS알람 발생	Reliability Prediction 수행
	1.1.3.2		분전반 전원 분배 실패	Random											3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	Reliability Prediction 수행
	1.1.3.3		전원공급 케이블 손실	Random											2.86E-09	설계, 유지보수	* PSU이중계 구성 * DCM Down 시, ATS알람 발생	Reliability Prediction 수행
	1.1.4	DCM H/W 고장		Random	DCM Down										8.16E-06	유지보수	* HW고장으로 인해 DCM다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	Reliability Prediction 수행

	1.2	DCM 열차 허용이동권한 송신 실패			열차충돌													
	1.2.1	DCM-EIM 통신 케이블 손실		Random											1.76E-08	유지보수	* EIM 이중계 구성 필요 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.2.2	EIM H/W 고장		Random											5.25E-06	설계, 유지보수	* EIM 이중계 구성 필요 * EIM 상태정보 ATS 감시	
ICM	1.3	ICM 열차진로 및 선로전환기 방향 오류																
	1.3.1	진로제어 명령 처리 오류			열차충돌													
	1.3.1.1	- 진로설정 로직 오류		System atic		5	7	4	1	3	1	-1	20	4.00E-08		설계, 테스트	* ICM이중계 구성 * EN50130에 따른 SW안전성 보증 활동 수행 * ICM 연동처리검증 및 진로검증 수행을 통한 안전한 연동로직 구현	
	1.3.1.2	- 진로 Queueing 오류		System atic		5	7	4	1	3	1	-1	20	4.00E-08		설계, 테스트	* ICM이중계 구성 * Queue 데이터 처리 용량 확보	
	1.3.2	ICM 전원공급 실패		Random	ICM Down													
	1.3.2.1	UPS 고장		Random											1.10E-07	설계	* PSU이중계 구성 * 분전반을 통한 안정적인 전원공급 * ICM전원공급 실패 시, ATS알람 발생	
	1.3.2.2	분전반 전원 분배 실패		Random											3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.3.2.3	전원공급 케이블 손실		Random											2.86E-09	유지보수	* PSU이중계 구성 * DCM Down 시, ATS알람 발생	
	1.3.3	ICM H/W 고장		Random	ICM Down										8.16E-06	설계, 유지보수	* HW고장으로 인해 ICM 다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	Reliability Prediction 수행
	1.3.4	ICM선로전환기 상태정보처리 오류 (S/W)			열차충돌											설계, 유지보수		
	1.3.4.1	선로전환기 처리 로직 오류		System atic		5	5	4	1	3	1	-1	18	4.00E-07		설계, 테스트	* ICM이중계 구성 * EN50130에 따른 SW안전성 보증 활동 수행 * ICM 연동처리검증 및 선로전환기 전환 검증 수행	

	1.3.4.2		비정상적인 선로전환기 상태 정보	Systematic		5	5	4	1	3	1	-1	18	4.00E-07			* ICM이중계 구성 * ICM 연동처리검증 및 선로전환기 전환 검증 수행 * 지속적인 선로전환기 인터페이스 및 상태 확인 * 해당 선로전환기 자동블록폐쇄 수행 후, ATS로 통보	
	1.4	ICM 선로전환기 전환명령 송신 실패			열차충돌													
	1.4.1		ICM-EIM 통신 케이블 손실	Random											1.76E-08	유지보수	* EIM 이중계 구성 필요 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.4.2		EIM H/W 고장	Random											5.25E-06	설계, 유지보수	* EIM 이중계 구성 필요 * EIM 상태정보 ATS 감시	
EIM	1.5	EIM과 외부시스템간 인터페이스 실패																
	1.5.1		EIM전원공급 실패		열차충돌													
	1.5.1.1			UPS 고장	Random										1.10E-07	설계	* PSU이중계 구성 * 분전반을 통한 안정적인 전원공급 * EIM전원공급 실패 시, ATS알람 발생	
	1.5.1.2			분전반 전원 분배 실패	Random										3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.1.3			전원공급 케이블 손실	Random										2.86E-09	유지보수	* PSU이중계 구성 * EIM Down 시, ATS알람 발생	
	1.5.2		EIM H/W 고장		Random	열차충돌									5.25E-06	유지보수	* HW고장으로 인해 EIM다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.3		입출력 네트워크 설비 고장			열차충돌										유지보수	* CRD 시스템과 외부 시스템간 인터페이스를 담당하는 통신 담당 설비 고장 시, ATS로 통신불가 메시지를 통보하여 유지보수 수행.	
	1.5.3.1			EIM간 연결 케이블 손실	Random										1.76E-08	유지보수	* EIM 이중계 구성 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.3.2			네트워크 스위치 고장	Random										2.15E-06	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.3.3			광스위치 고장	Random										2.14E-06	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.3.4			광스위치간 케이블 손실(차상 인터페이스)	Random										1.76E-08	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	1.5.3.5			광스위치간 케이블 손실 (선로전환기 인터페이스)	Random										3.58E-10	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	

Hazard-2 최대운행속도를 초과하여 과속주행 중인 열차

Hazard-2	최대운행속도를 초과하여 과속주행 중인 열차																	
Preliminary Hazard Analysis					S			D			U	Total	THR		Action	Recommended action	Remark
Subsystem	No.	Cause	Failure	Effect	E	V	A	T	C	H							
DCM	2.1	임시속도제한명령 설정 실패															
	2.1.1	부적합한 ATS임시속도제한명령	Systematic	열차탈선	4	7	3	1	3	3	-1	20	4.00E-08		설계, 테스트	* DCM이중계 구성 * 데이터 비교 검증 수행 * DCM 입력 정보의 유효성을 판단 후 처리 수행	
	2.1.2	DCM 임시속도제한명령 처리 오류 (S/W)		열차탈선													
	2.1.2.1	임시속도제한명령 처리 로직 오류	Systematic		4	7	3	1	3	3	-1	20	4.00E-08		설계, 테스트	* DCM이중계 구성 필요 * EN50128에 따른 SW안전성 보증 활동 수행 * 허용이동권한 처리를 위한 블록검증, 열차위치 검증 수행	
	2.1.2.2	해당 열차 정보 누락	Systematic		4	7	3	1	3	4	-1	21	1.00E-08			* 반복적 열차정보 요청	
	2.2	임시속도제한명령 열차로 송신/수신 실패													설계, 유지보수	* DCM이중계 구성 필요 * EIM이중계 구성 필요 * 열차와 인터페이스 실패 시, 열차는 상용제동 체결로 안전 보장.	*IHA추가분석수행 *Reliability Prediction 수행
	2.2.1	DCM-EIM 통신 케이블 손실	Random											1.76E-08	유지보수	* EIM 이중계 구성 필요 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	2.2.2	EIM H/W 고장	Random											5.25E-06	설계, 유지보수	* EIM 이중계 구성 필요 * EIM 상태정보 ATS 감시	
EIM	2.3	EIM과 열차와의 인터페이스 실패															
	2.3.1	EIM전원공급 실패		열차탈선													
	2.3.1.1	UPS 고장	Random											1.10E-07	설계	* PSU이중계 구성 * 분전반을 통한 안정적인 전원공급 * EIM전원공급 실패 시, ATS알람 발생	
	2.3.1.2	분전반 전원 분배 실패	Random											3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	2.3.1.3	전원공급 케이블 손실	Random											2.86E-09	유지보수	* PSU이중계 구성 * EIM Down 시, ATS알람 발생	
	2.3.2	EIM H/W 고장	Random	열차탈선										5.25E-06	유지보수	* HW고장으로 인해 EIM다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	

	2.3.3		입출력 네트워크 설비 고장																
	2.3.3.1			네트워크 스위치 고장	Random											2.15E-06	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	2.3.3.2			광스위치 고장	Random											2.14E-06	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	2.3.3.3			광스위치간 케이블 손실(차상 인터페이스)	Random											1.76E-08	유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	

Hazard-3 비정상적인 진로로 열차 진입

Hazard-3	비정상적인 진로로 열차 진입																		
Preliminary Hazard Analysis						S			D			U	Total	THR		Action	Recommended action		Remark
Subsystem	No.	Cause			Failure	Effect	E	V	A	T	C	H							
ICM	3.1	ATS로부터 비정상적인 진로제어명령 수신			Systematic	열차충돌	5	7	4	1	3	1	-1	20	4.00E-08			* 진로제어명령 유효성 검사 수행	
	3.2	ICM 진로 설정 오류/실패																	
	3.2.1		진로제어 명령 처리 오류			열차충돌													
	3.2.1.1			진로설정 로직 오류	Systematic		5	7	4	1	3	1	-1	20	4.00E-08		설계, 테스트	* ICM이중계 구성 * EN50130에 따른 SW안전성 보증 활동 수행 * ICM 연동처리검증 및 진로검증 수행을 통한 안전한 연동로직 구현	
	3.2.1.2			진로 Queueing 오류	Systematic		5	7	4	1	3	1	-1	20	4.00E-08		설계, 테스트	* ICM이중계 구성 * Queue 데이터 처리 용량 확보	
	3.2.2		ICM전원공급 실패		Random	ICM Down													
	3.2.2.1			UPS 고장	Random											1.10E-07	설계	* PSU이중계 구성 * 분전반을 통한 안정적인 전원공급 * ICM전원공급 실패 시, ATS알람 발생	
	3.2.2.2			분전반 전원 분배 실패	Random											3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.2.2.3			전원공급 케이블 손실	Random											2.86E-09	유지보수	* PSU이중계 구성 * DCM Down 시, ATS알람 발생	
	3.2.3		ICM H/W 고장		Random	ICM Down										8.16E-06	설계, 유지보수	* HW고장으로 인해 ICM 다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.2.4		ICM선로전환기 상태정보처리 오류(S/W)			열차충돌													

	3.2.4.1		선로전환기 처리 로직 오류	Systematic		5	5	4	1	3	1	-1	18	4.00E-07		설계, 테스트	* ICM이중계 구성 * EN50130에 따른 SW안전성 보증 활동 수행 * ICM 연동처리검증 및 선로전환기 전환 검증 수행	
	3.2.4.2		비정상적인 선로전환기 상태 정보	Systematic		5	5	4	1	3	1	-1	18	4.00E-07			* ICM이중계 구성 * ICM 연동처리검증 및 선로전환기 전환 검증 수행 * 지속적인 선로전환기 인터페이스 및 상태 확인 * 해당 선로전환기 자동블록폐쇄 수행 후, ATS로 통보	
	3.3	ICM 선로전환기 전환명령 송신 실패			열차충돌													
	3.3.1		ICM-EIM 통신 케이블 손실	Random										1.76E-08		유지보수	* EIM 이중계 구성 필요 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.3.2		EIM H/W 고장	Random										5.25E-06		설계, 유지보수	* EIM 이중계 구성 필요 * EIM 상태정보 ATS 감시	
EIM	3.4	EIM과 선로전환기와의 인터페이스 실패																
	3.4.1		EIM 전원공급 실패		EIM Down													
	3.4.1.1			UPS 고장	Random									1.10E-07		설계	* PSU이중계 구성 * 분전반을 통한 안정적인 전원공급 * EIM전원공급 실패 시, ATS알람 발생	
	3.4.1.2			분전반 전원 분배 실패	Random									3.49E-09		설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.4.1.3			전원공급 케이블 손실	Random									2.86E-09		유지보수	* PSU이중계 구성 * EIM Down 시, ATS알람 발생	
	3.4.2		EIM H/W 고장		Random	열차충돌								5.25E-06		유지보수	* HW고장으로 인해 EIM다운 시, ATS알람 발생 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.4.3		입출력 네트워크 설비 고장															
	3.4.3.1			네트워크 스위치 고장	Random									2.15E-06		유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.4.3.2			광스위치 고장	Random									2.14E-06		유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	
	3.4.3.3			광스위치간 케이블 손실 (선로전환기 인터페이스)	Random									3.58E-10		유지보수	* 신뢰성 분석에 따른 정기적인 유지보수 수행	

Hazard-4 허용이동권한 없이 이동 중인 열차

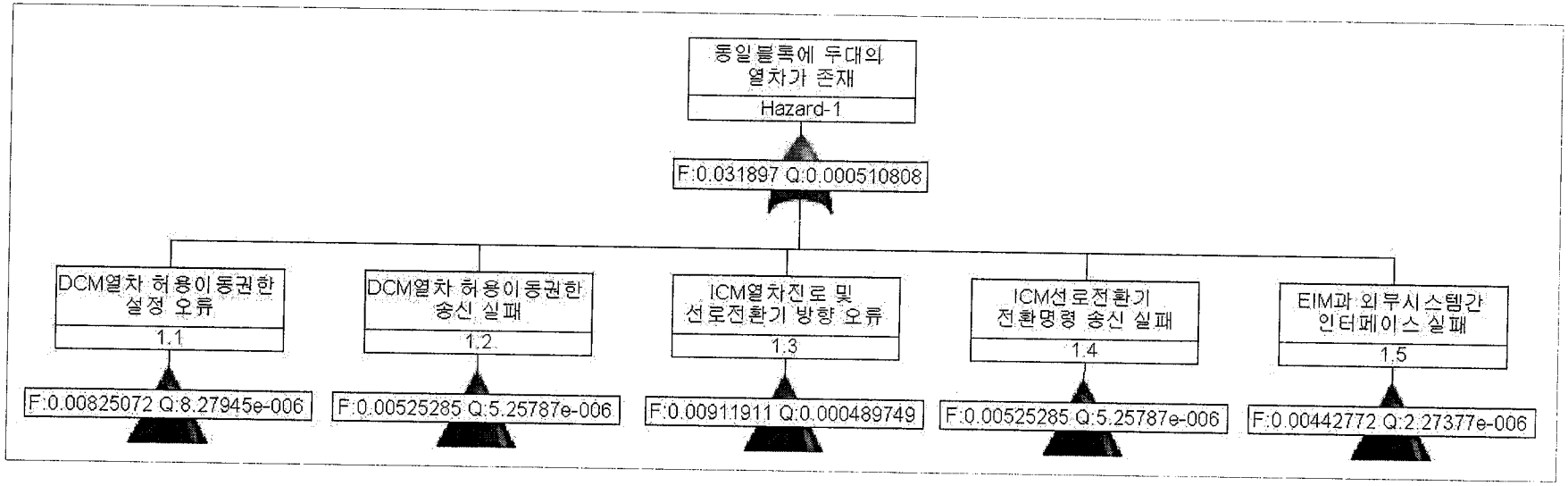
Hazard-4	허용이동권한 없이 이동중인 열차																	
Preliminary Hazard Analysis					S			D			U	Total	THR		Action	Recommended action	Remark
Subsystem	No.	Cause	Failure	Effect	E	V	A	T	C	H							
DCM	4.1	DCM 열차 허용이동권한 설정 오류															
	4.1.1	열차위치 정보 오류		열차충돌													
	4.1.1.1	열차로부터 비정상적인 열차 위치 정보 수신	System atic		5	7	4	1	3	4	-1	23	1.00E-09		설계	* 열차위치 적합성 검사를 통한 열차위치 검증 * 지속적인 열차 상태정보 확인 필요	
	4.1.1.2	DCM 열차위치 정보 처리 오류	System atic		5	7	4	1	3	4	-1	23	1.00E-09		설계, 테스트	* DCM이중계 구성 필요 * EIM 비교처리 기능 수행 * 열차위치 검증 수행 * EN50128에 따른 SW안전성 보증 활동 수행 * 각 테스트 수행	
	4.1.2	DCM 허용이동권한 처리 오류(S/W)		열차충돌													
	4.1.2.1	허용이동권한 처리 로직 오류	System atic		5	7	4	1	3	4	-1	23	1.00E-09		설계, 테스트	* DCM이중계 구성 필요 * EIM비교처리 기능 수행 * EN50129에 따른 SW안전성 보증 활동 수행 * 허용이동권한 처리를 위한 블록검증, 열차위치 검증 수행 * 각 테스트 수행	
	4.1.2.2	Database(m em ory) full	System atic		5	7	4	1	3	4	-1	23	1.00E-09			* DCM이중계 구성 필요 * EN50130에 따른 SW안전성 보증 활동 수행 * Database 용량 확대 및 플래시 메모리 추가	
	4.1.3	DCM 전원공급 실패		DCM Down													
	4.1.3.1	UPS 고장	Random											1.10E-07	설계, 유지보수	* PSU이중계 구성 * DCM전원공급 실패 시, ATS알람 발생	
	4.1.3.2	분전반 전원 분배 실패	Random											3.49E-09	설계, 유지보수	* 신뢰성/가용성 높은 분전반 설계 및 설치 * 신뢰성 분석에 따른 정기적인 유지보수 수행	
	4.1.3.3	전원공급 케이블 손실	Random											2.86E-09	설계, 유지보수	* PSU이중계 구성 * DCM Down 시, ATS알람 발생	

| | | |

부 록 C

CRD시스템 당해년도 FTA

① Hazard-1 FTA



<그림25>는 Hazard-1에 대한 FTA 1차 원인 도식이다.

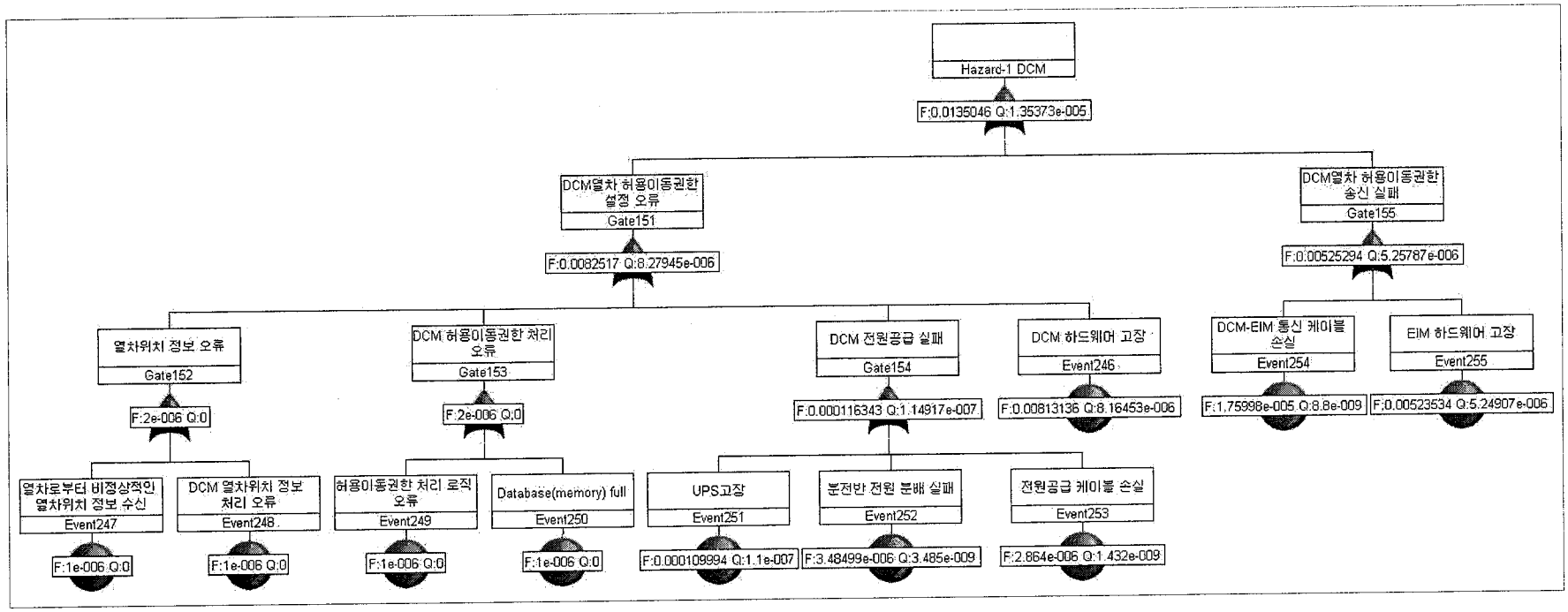
Hazard-1을 발생시키는 원인으로는 다음과 같은 총 5가지로서, 이는 SSHA sheet에서 이미 도출된 사항이다.

- DCM 열차 허용이동권한 설정 오류
- DCM 열차 허용이동권한 송신 실패
- ICM 열차진로 및 선로전환기 방향 오류
- ICM 선로전환기 전환명령 송신 실패
- EIM과 외부시스템간 인터페이스 실패

Hazard-1의 결과로는,

- Unreliability(F) : 0.031897
- Unavailability(Q) : 5.10808e-04

● Hazard-1 DCM FTA

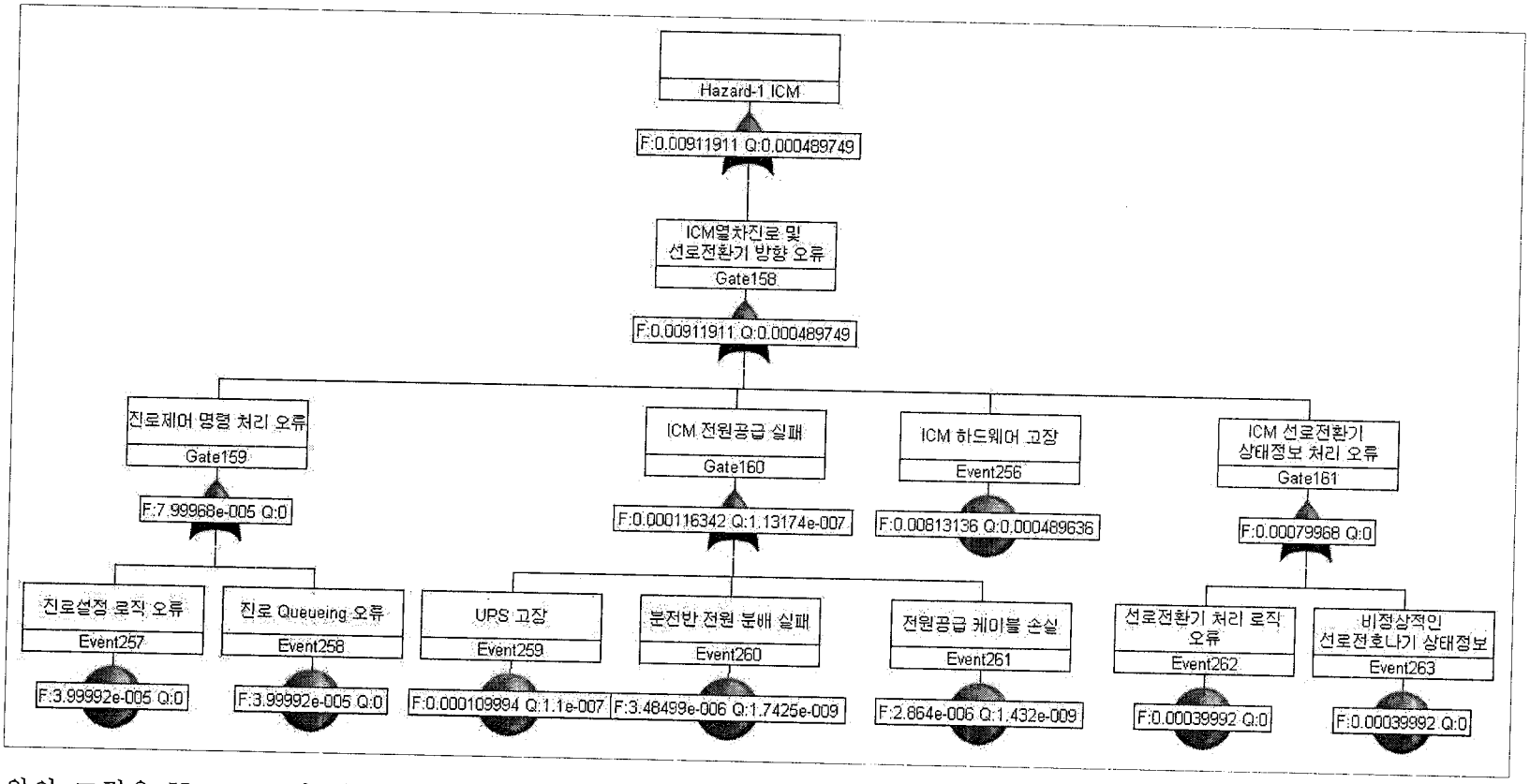


위의 그림은 Hazard-1에 대한 DCM FTA 결과 도식이다.

Hazard-1의 DCM Subsystem의 결과로는,

- Unreliability(F) : 0.0135046
- Unavailability(Q) : 1.35373e-05

● Hazard-1 ICM FTA

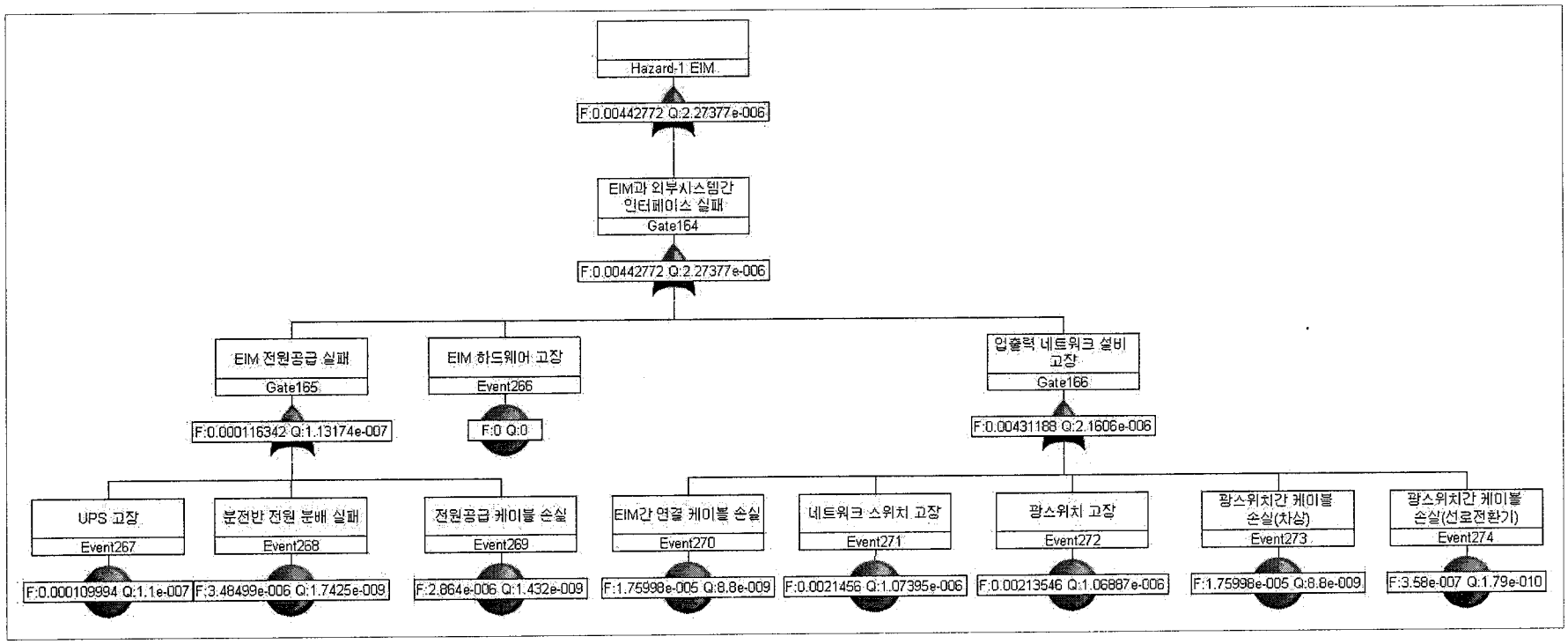


위의 그림은 Hazard-1에 대한 ICM FTA 결과 도식이다.

Hazard-1의 ICM Subsystem의 결과로는,

- Unreliability(F) : 0.00911911
- Unavailability(Q) : 4.89749e-04

● Hazard-1 EIM FTA

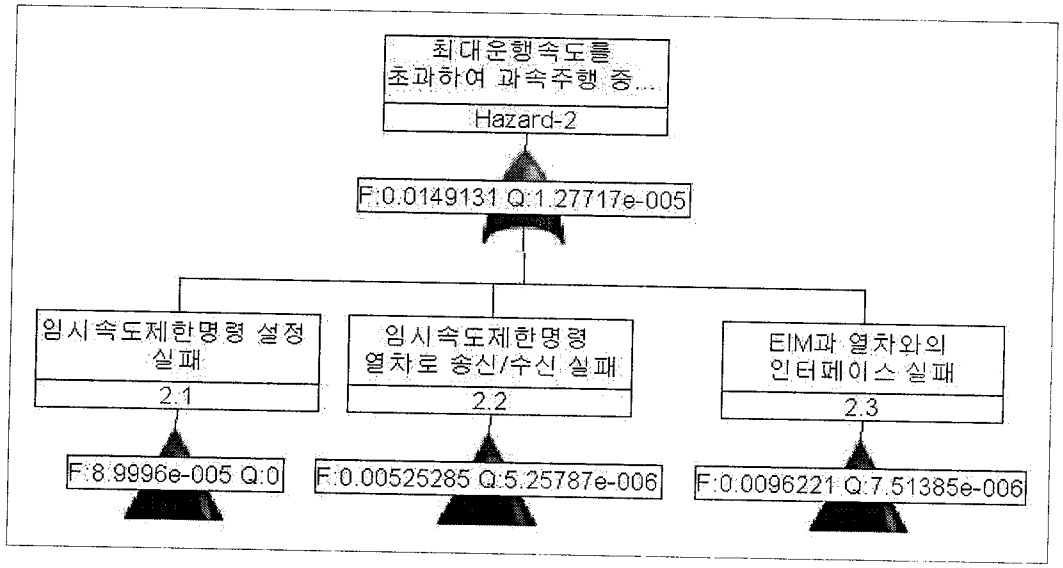


위의 그림은 Hazard-1에 대한 EIM FTA 결과 도식이다.

Hazard-1의 EIM Subsystem의 결과로는,

- Unreliability(F) : 0.00442772
- Unavailability(Q) : 2.27377e-06

② Hazard-2 FTA



위의 그림은 Hazard-2에 대한 FTA 결과 도식이다.

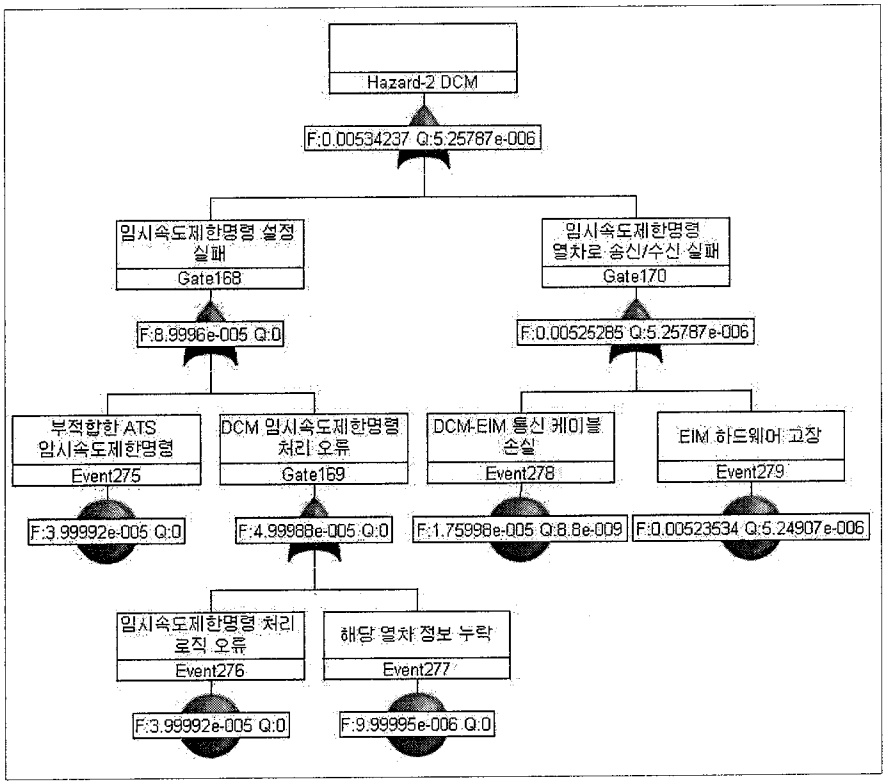
Hazard-2를 발생시키는 원인으로는 다음과 같은 총 3가지로서, 이는 SSHA sheet에서 이미 도출된 사항이다.

- 임시속도제한명령 설정 실패
- 임시속도제한명령 열차로 송신/수신 실패
- EIM과 열차와의 인터페이스 실패

Hazard-2의 결과로는,

- Unreliability(F) : 0.0149131
- Unavailability(Q) : 1.27717e-05

● Hazard-2 DCM FTA

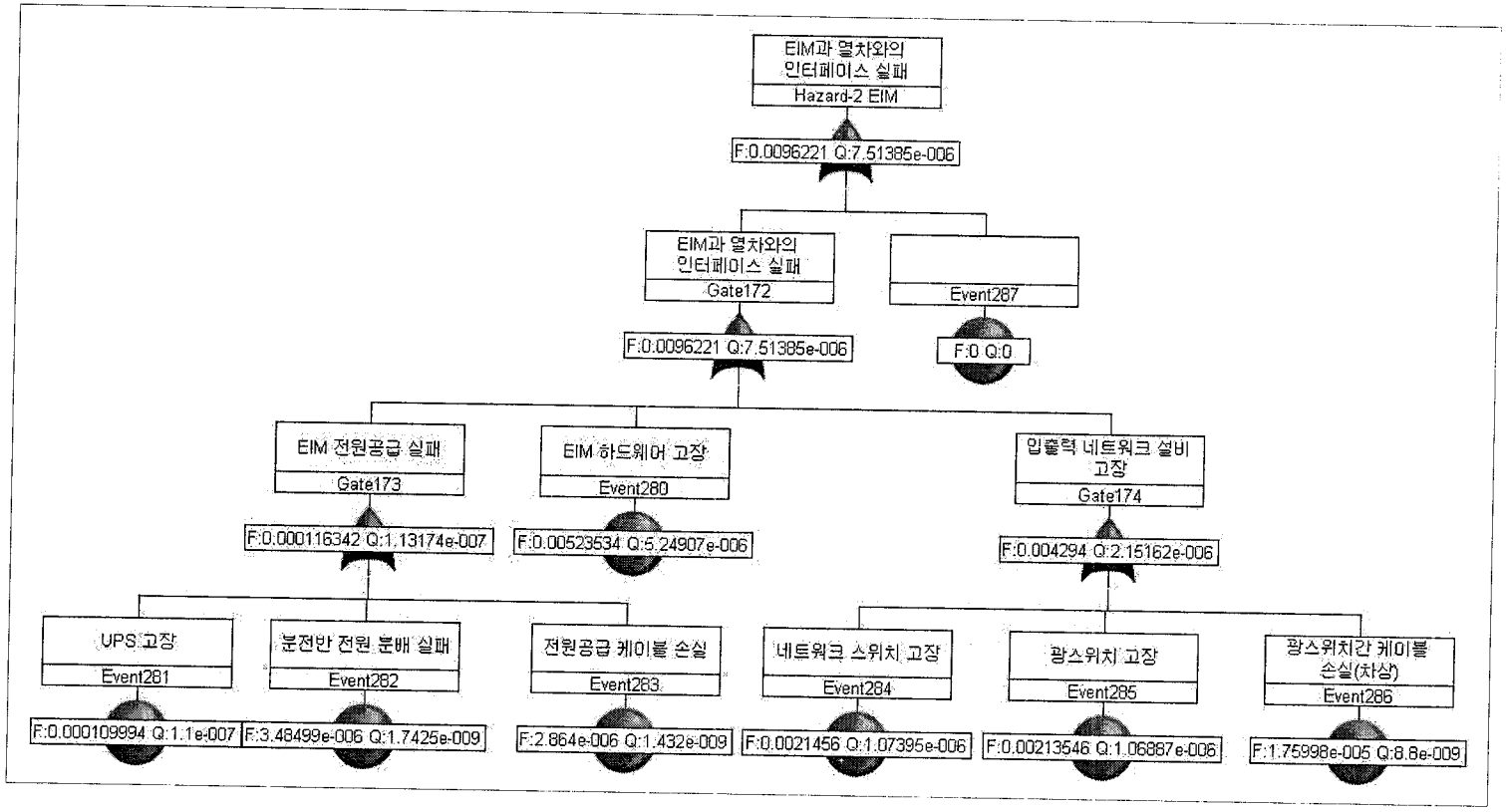


위의 그림은 Hazard-2에 대한 DCM FTA 결과 도식이다.

Hazard-1의 DCM Subsystem의 결과로는,

- Unreliability(F) : 0.00534237
- Unavailability(Q) : 5.25787e-06

● Hazard-2 EIM FTA

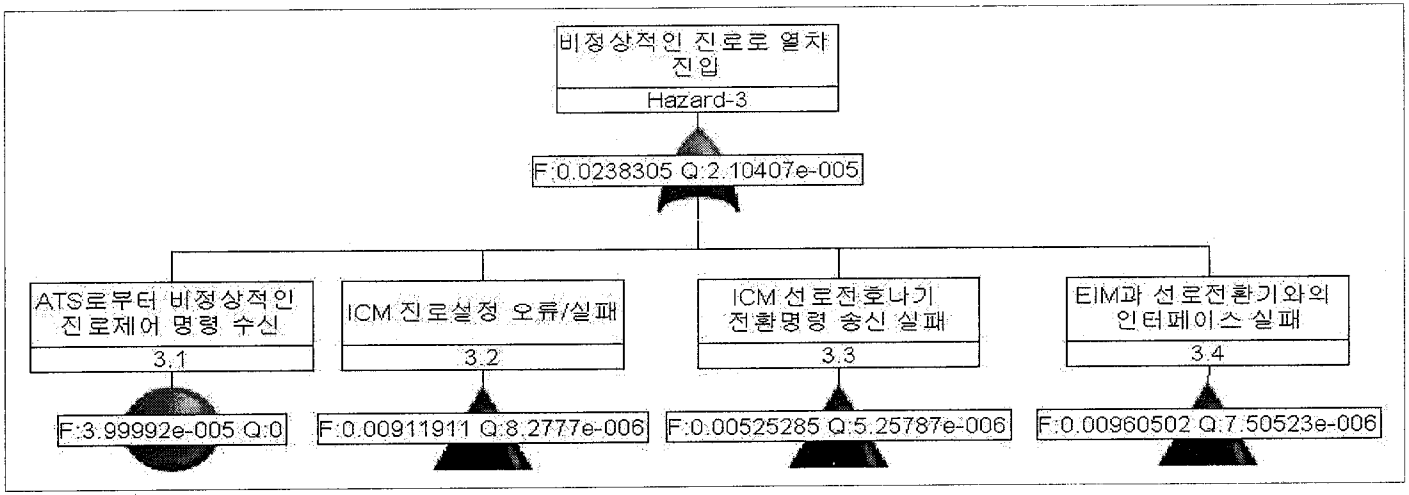


위의 그림은 Hazard-2에 대한 EIM FTA 결과 도식이다.

Hazard-1의 EIM Subsystem의 결과로는,

- Unreliability(F) : 0.0096221
- Unavailability(Q) : 7.51385e-06

③ Hazard-3 FTA



위의 그림은 Hazard-3에 대한 FTA 결과 도식이다.

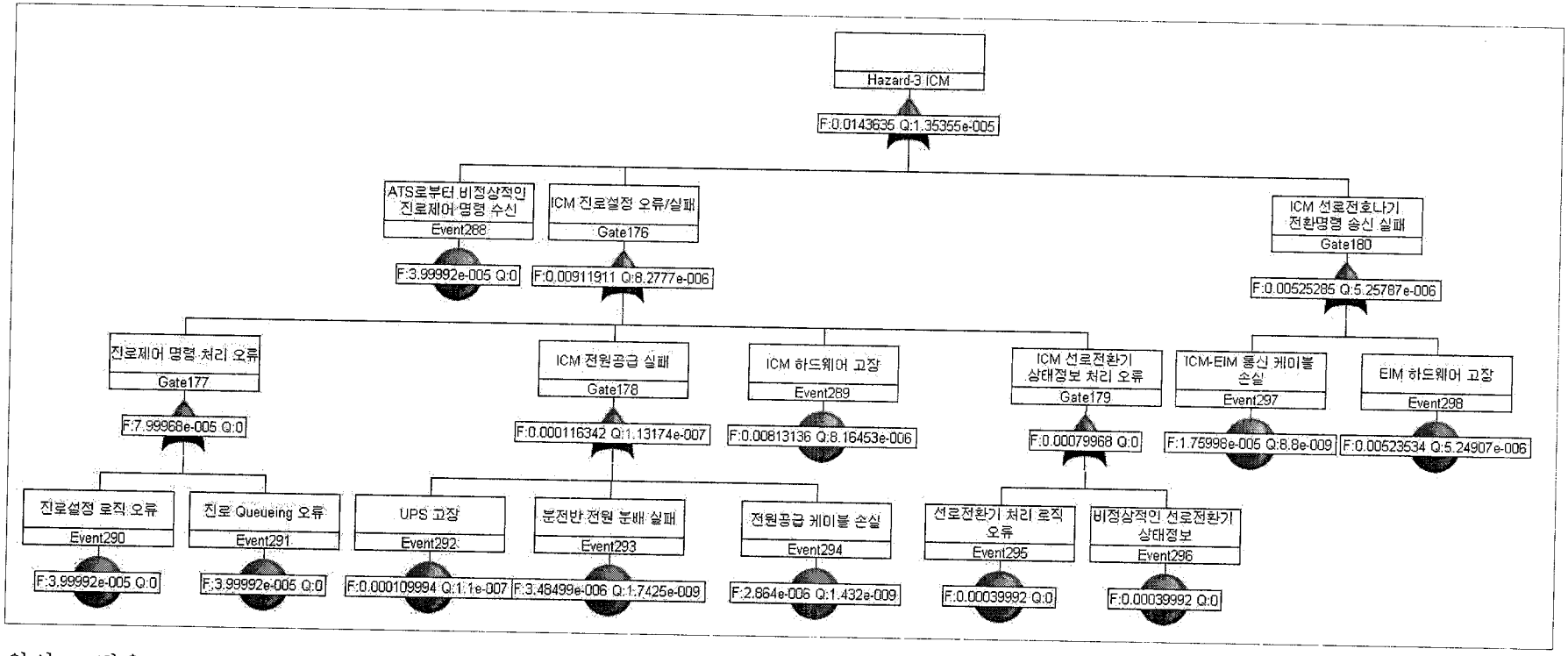
Hazard-3을 발생시키는 원인으로는 다음과 같은 총 4가지로서, 이는 SSHA sheet에서 이미 도출된 사항이다.

- ATS로부터 비정상적인 진로제어 명령 수신
- ICM 진로설정 오류/실패
- ICM 선로전환기 전환명령 송신 실패
- EIM과 선로전환기와의 인터페이스 실패

Hazard-3의 결과로는,

- Unreliability(F) : 0.0238305
- Unavailability(Q) : 2.10407e-05

● Hazard-3 ICM FTA

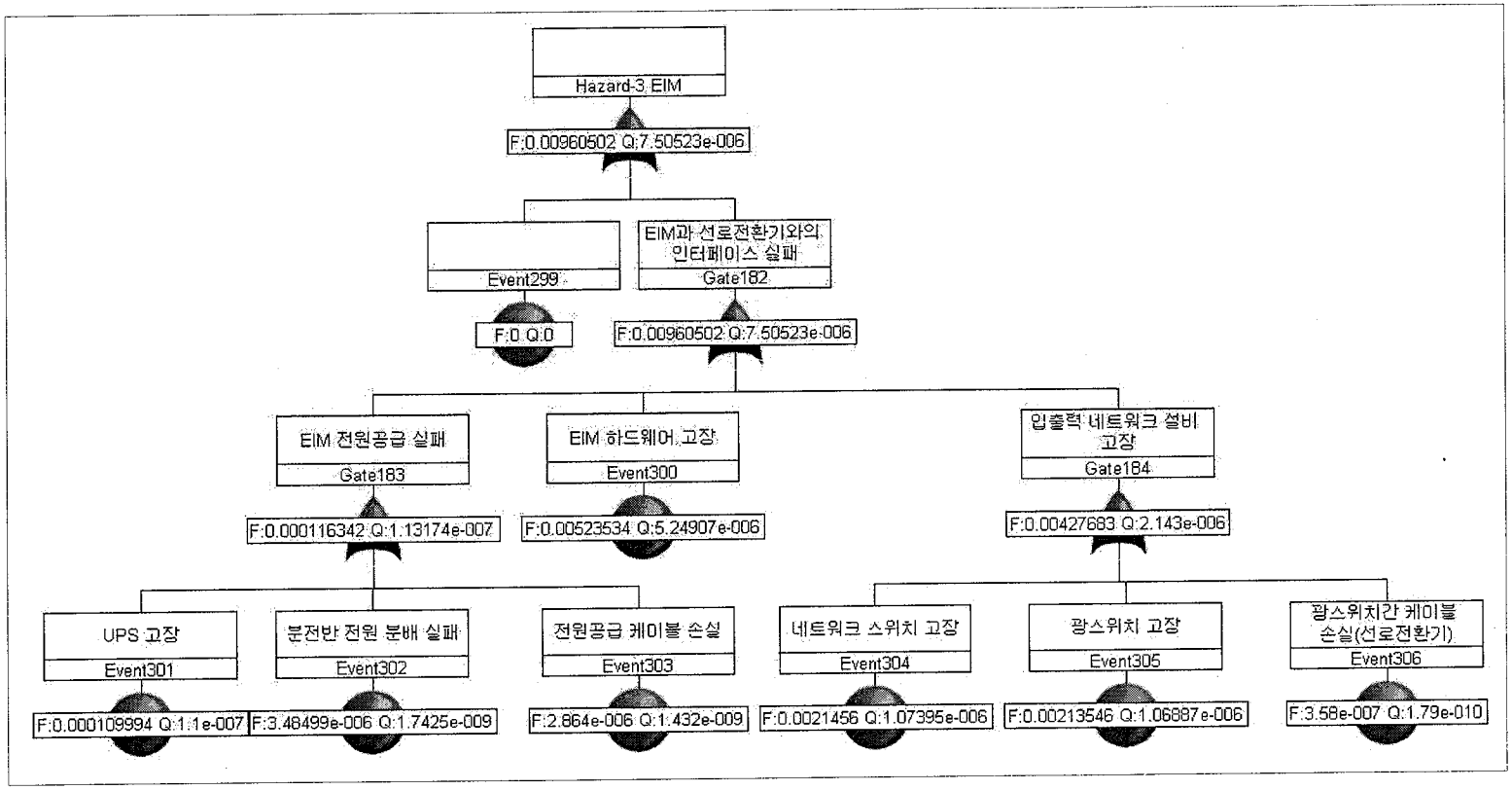


위의 그림은 Hazard-3에 대한 ICM FTA 결과 도식이다.

Hazard-1의 ICM Subsystem의 결과로는,

- Unreliability(F) : 0.0143635
- Unavailability(Q) : 1.35355e-05

● Hazard-3 EIM FTA

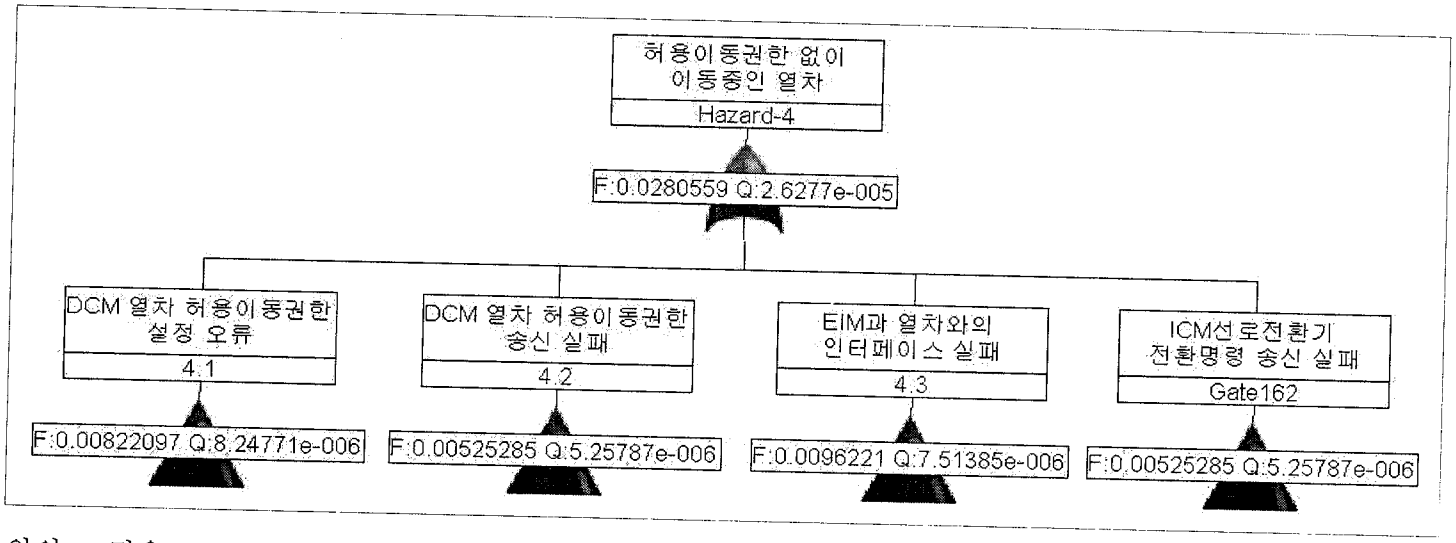


위의 그림은 Hazard-3에 대한 EIM FTA 결과 도식이다.

Hazard-1의 EIM Subsystem의 결과로는,

- Unreliability(F) : 0.00960502
- Unavailability(Q) : 7.50523e-06

④ Hazard-4 FTA



위의 그림은 Hazard-4에 대한 FTA 결과 도식이다.

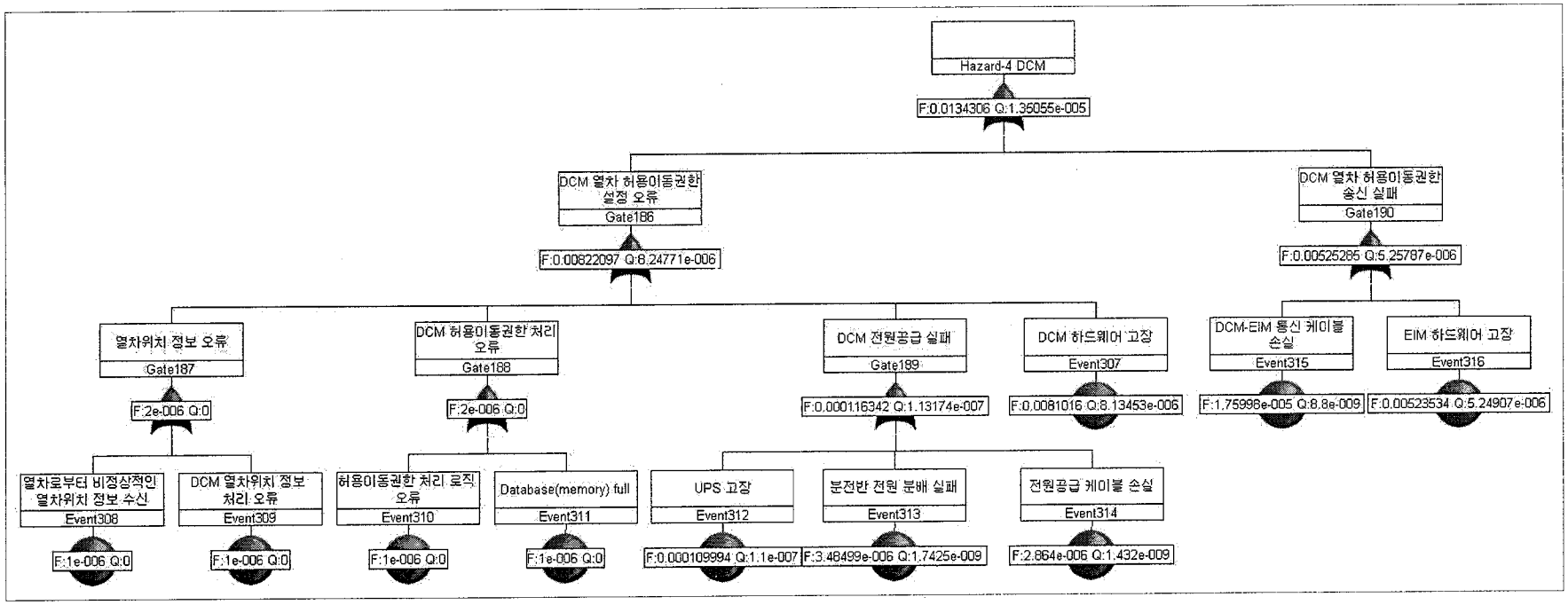
Hazard-4를 발생시키는 원인으로는 다음과 같은 총 4가지로서, 이는 SSHA sheet에서 이미 도출된 사항이다.

- DCM열차 허용이동권한 설정 오류
- DCM열차 허용이동권한 송신 실패
- EIM열차와의 인터페이스 실패
- ICM선로전환기 전환명령 송신 실패

Hazard-4의 결과로는,

- Unreliability(F) : 0.0280559
- Unavailability(Q) : 2.6277e-05

● Hazard-4 DCM FTA

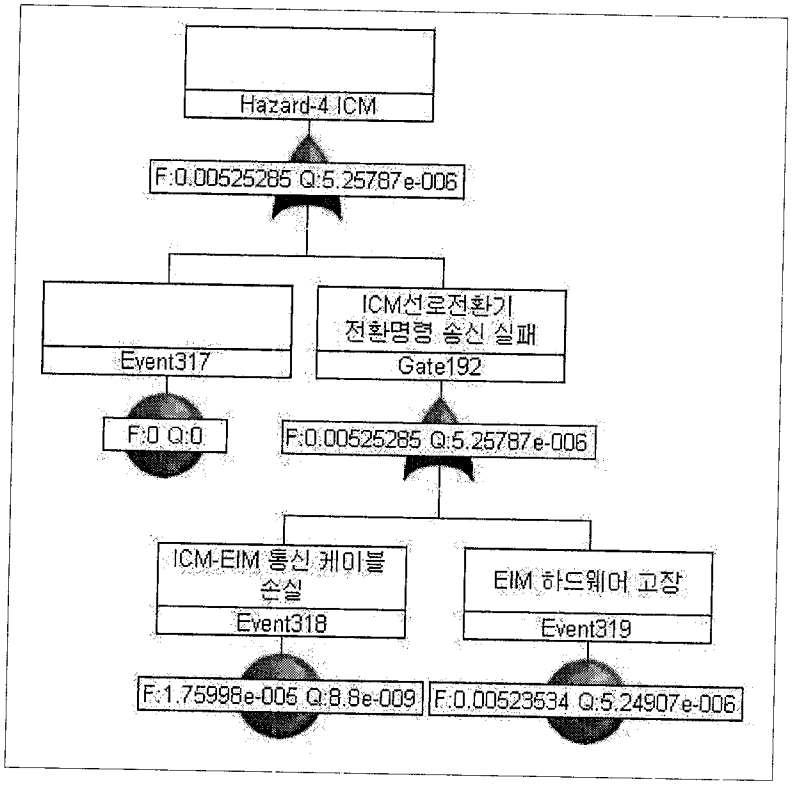


위의 그림은 Hazard-4에 대한 DCM FTA 결과 도식이다.

Hazard-4의 DCM Subsystem의 결과로는,

- Unreliability(F) : 0.0134306
- Unavailability(Q) : 1.35055e-05

● Hazard-4 ICM FTA

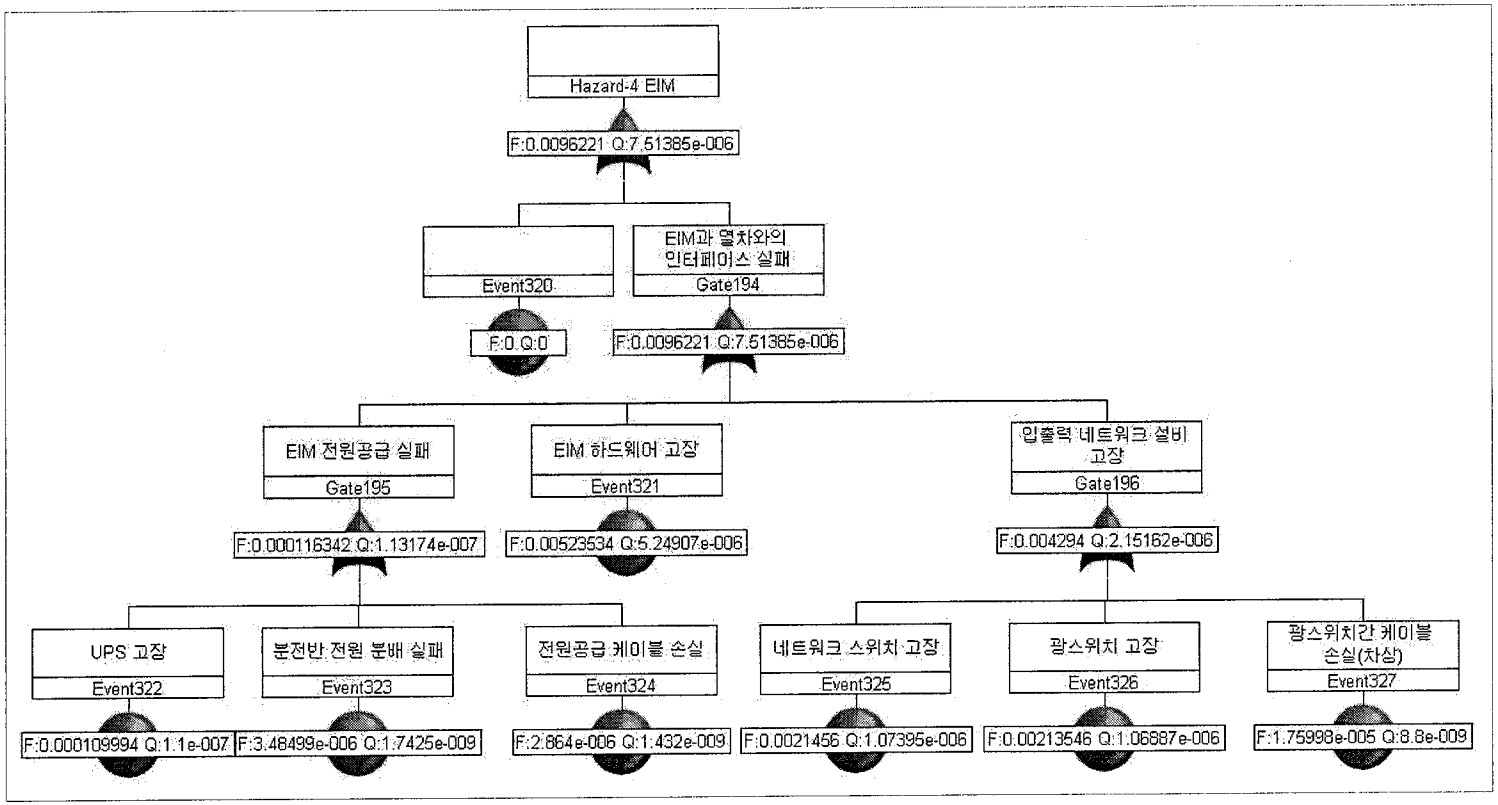


위의 그림은 Hazard-4에 대한 ICM FTA 결과 도식이다.

Hazard-4의 ICM Subsystem의 결과로는,

- Unreliability(F) : 0.0052585
- Unavailability(Q) : 5.25787e-05

● Hazard-4 EIM FTA



위의 그림은 Hazard-4에 대한 ICM FTA 결과 도식이다.

Hazard-4의 ICM Subsystem의 결과로는,

- Unreliability(F) : 0.0096221
- Unavailability(Q) : 7.51385e-06

제6절 평가대상 시스템 시뮬레이터 제작 및 시험

	검증계획서 **(Verification Plan)**	ID No : TC - SR09 - SSR02 - 2009 작성일 : 2010. 05. 04 수정일 :

9. 프로젝트는 평가대상시스템 시험을 위한 시뮬레이터를 개발해야 한다.

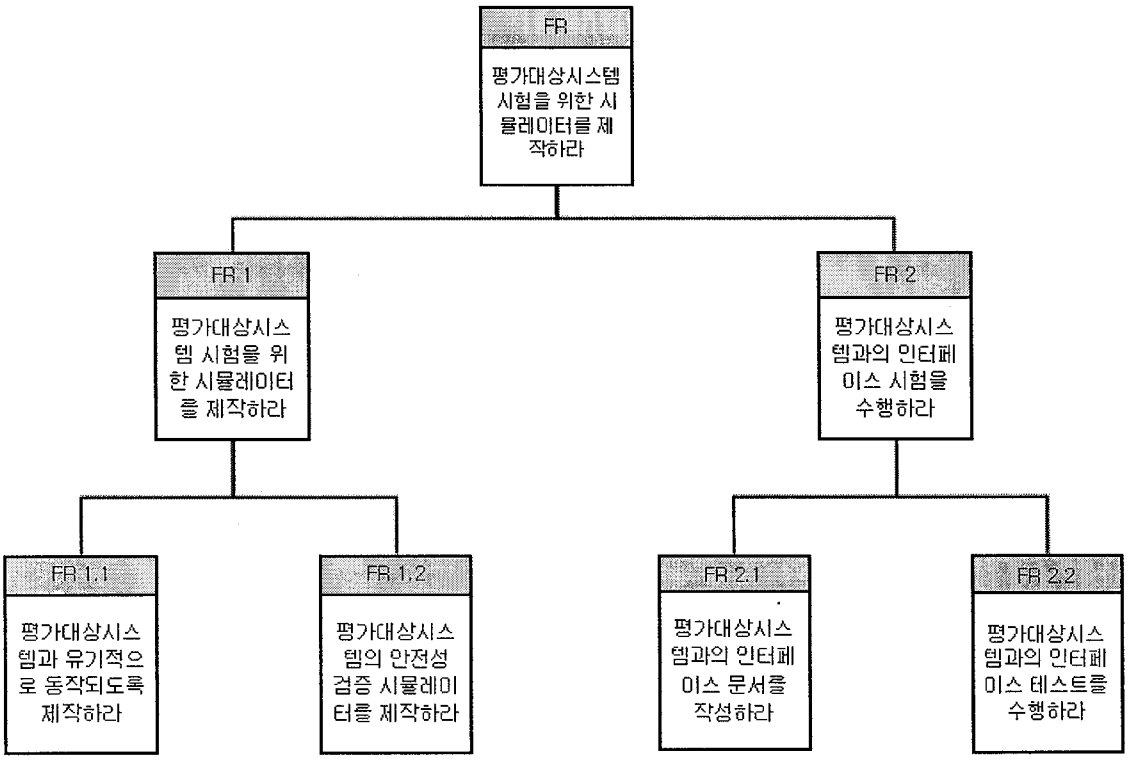
9.2 프로젝트는 평가대상시스템 시험을 위한 시뮬레이터를 제작하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 시뮬레이터 설계 문서 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 2.1 단순상황 분석 - 5.3 기능시험	- SE 검증	- 수정 VRTM - 검증결과표

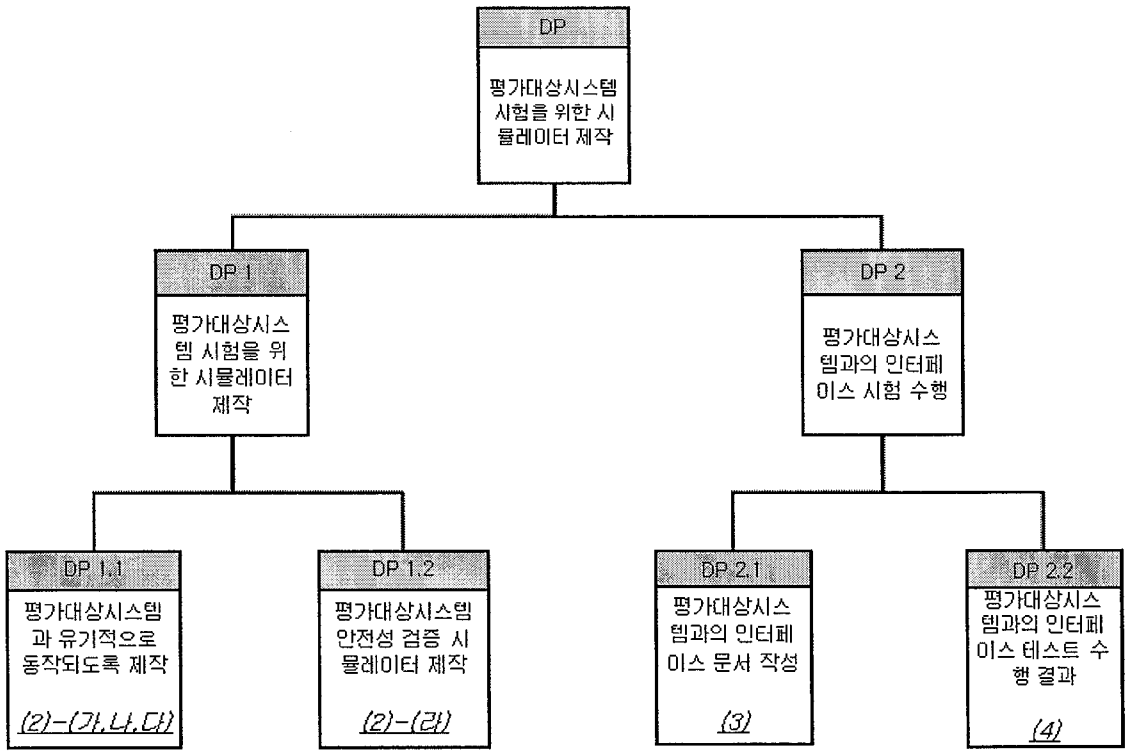
Verification Specification (검증기준) :

1. 안전성 평가용 대상 열차제어시스템의 평가가 수행될 수 있도록 대상시스템과 유기적으로 동작되도록 설계·제작되었는가?
2. 안전성 검증 시뮬레이터는 안전측 동작에 대한 요구사항을 제대로 반영하고 있는가?
3. 시뮬레이터의 시험 문서는 충실히 작성되고 수행되었는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

안전성 평가기술 적용을 위한 시뮬레이터 제작 및 시험은 『SR 9. 프로젝트는 평가대상시스템 시험을 위한 시뮬레이터를 개발해야 한다.』 중 『**SSR. 9.2. 프로젝트는 평가대상시스템 시험을 위한 시뮬레이터를 제작하여야 한다.**』에 해당하는 내용이다. 본 절에서는 전년도에 도출한 시뮬레이터의 설계 내용을 바탕으로 하여 수행한 시뮬레이터 제작 내용과 인터페이스 시험에 관한 내용을 제시하였다.

나. 설계기준

○ 안전성 평가용 대상 열차제어시스템 제작/테스트 산출 문서

○ 철도종합안전기술개발사업, '열차제어시스템 안전성능 평가 및 사고방지기술 개발 연구보고서', 2009. 8.

○ 해외 통신기반 열차제어시스템 시험사양 참조(Alcatel사)

다. 검증 방법에 따른 증거 자료

평가 대상시스템 시험을 위한 시뮬레이터 제작 및 시험을 위해 본 절에서는 시뮬레이터 제작 내용과 테스트 수행에 대한 내용을 기술하였다. 평가대상시스템 시험을 위한 시뮬레이터 제작을 위해 전년도의 설계 분석 결과를 충분히 고려한 제작이 수행되었으며 평가대상시스템과의 인터페이스 시험을 수행하였다.

○ 시뮬레이터 설계 문서

○ 테스트 수행 문서

라. 성과물의 내용 및 결과

(1) 개요

평가 대상시스템 시험을 위한 시뮬레이터는 평가용 대상 열차제어시스템 중 연동기능과 열차방호기능을 하는 CRD 시스템의 기능을 시험하기 위한 장치로서 자동열차감시 장치인 ATS 시뮬레이터, 선로전환기 기능을 하는 신호설비제어·신호설비시뮬레이터, 자동열차보호와 자동열차운행을 담당하는 차상시뮬레이터로 구성된

다. 또한 안전성 평가용 대상 열차제어시스템 중 주로 CRD 시스템의 안전측 동작에 대한 요구사항을 검증하기 위한 안전성 검증 시뮬레이터로 구성된다. 시뮬레이터 제작은 최우선적으로 본 안전성 평가용 대상 열차제어시스템에서 유기적으로 동작되도록 제작함을 원칙으로 한다.

(2) 제작

안전성 평가용 대상 열차제어시스템 보완 제작을 위한 ATS시뮬레이터, 차상시뮬레이터, 신호설비제어/신호설비 시뮬레이터의 제작 내용과 안전측 동작에 대한 기능을 검증하기 위한 안전성 검증 시뮬레이터에 대한 제작 내용을 기술한다.

(가) ATS 시뮬레이터

다음은 전년도에 수행된 요구사항 분석 및 설계내용을 바탕으로 하여 제작된 ATS 시뮬레이터 내용이다. ATS 시뮬레이터는 아래의 성능을 갖는 한대의 퍼스널 컴퓨터를 하드웨어로 사용하며 UDP/IP LAN 통신을 이용하여 CRD 시스템 및 차상시뮬레이터(ATO)와 통신한다. 프로그램 개발에 사용된 컴퓨터 언어는 Visual C++ 2003을 사용하였다.

① L/S

다음은 전년도에 요구분석된 사항을 토대로 실제 구현된 L/S Window화면이다.

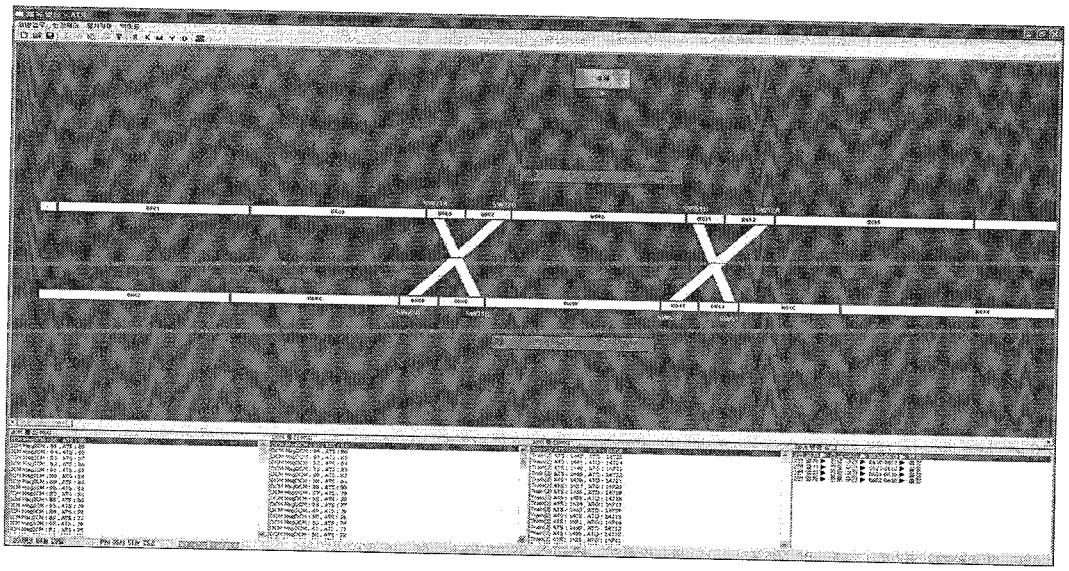


그림 3.6.1 L/S 화면

다음은 L/S 화면에 실제 구현된 내용에 대한 설명이다.

- 역 구분 표시

역 구분 표시는 L/S 화면에서 현재 화면의 위치가 어떤 역인지를 확인하기 위해 표시되는 화면이다.

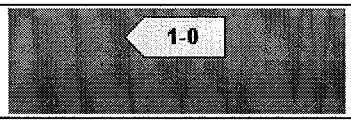
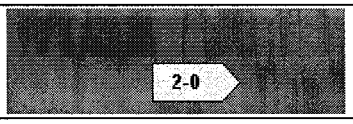
표 3.6.1 역 구분 표시

상태	수서역	경원역	모란역	야탑역	오리역
표시	수서 S	경원 K	모란 M	야탑 Y	오리 O

- 열차 기본 표시

열차를 나타내는 기본적인 표시는 열차를 나타내는 아이콘과 열차 Label로 구성된다. 열차 아이콘은 블록의 옆에 오각형 형태로 표시된다.

표 3.6.2 열차 기본 표시

상태	상행	하행
표시		

- 열차 Label 표시

열차 Label은 열차 아이콘 가운데에 텍스트로 표시된다.

표 3.6.3 열차 Label 표시

상태	표준
표시	

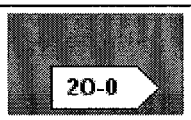
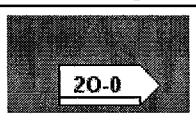
열차 Label에는 다음과 같은 열차상태가 표시된다. 예를 들어 위와 같이 열차 Label이 "2O-79"일 경우는 다음의 상태를 나타낸다.

- "2" : Train ID, ATS시뮬레이터가 차상시뮬레이터(ATO)로부터 수신한 메시지 중 차상 ATO ID를 참조하여 생성된 Train ID
- "O" : 열차의 최종 목적지 표시
- "79" : 열차의 속도 표시

- 열차 출입문상태 표시

열차출입문은 열차 아이콘 내에 사각형으로 다음과 같이 표시된다. 열차 아이콘 내에 사각형은 열차출입문 개방상태를 나타낸다. 사각형은 열차출입문이 개방되었을 경우에만 표시된다.

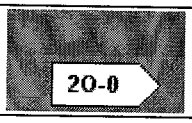
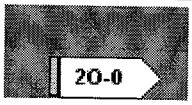
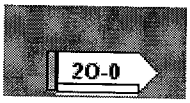
표 3.6.4 열차 출입문상태 표시

상태	출입문 Closed	출입문 Open
표시		

- 열차 대기상태 표시

열차대기상태는 열차 아이콘 내에 사각형으로 다음과 같이 표시된다. 열차 아이콘 내에 사각형은 열차 대기상태를 나타낸다.

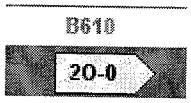
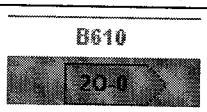
표 3.6.5 열차 대기상태 표시

상태	대기 해제	출입문 폐쇄 대기 상태	출입문 개방 대기 상태
표시			

- 열차 비상제동상태 표시

열차비상제동 상태는 열차 아이콘 색상으로 표시되며 다음과 같다.

표 3.6.6 열차 비상제동상태 표시

상태	비상제동 해지상태	비상제동 적용상태
표시		

- 열차 이동상태 및 정위치 정차 표시

열차이동 및 정지상태는 열차 Label에 표시되는 열차속도로 표시한다. 열차속도 표시가 "0"일 경우 열차 정지상태이다. 정위치 정차는 열차 icon색상으로 표시된다.

표 3.6.7 열차 이동상태 표시

상태	이동 중	정위치정차가 아닌 정지	정위치정차
표시			

- 블록 점유 표시

블록 아이콘의 색상 변화로 열차의 점유상태를 표시한다. 점유는 열차 아이콘을 반드시 필요로 하지는 않는다. CRD로부터 수신한 열차의 전방, 중앙, 후방 점유 블록의 점유상태를 표시한다. 한 대의 열차는 동시에 최대 3개 블록의 점유가 가능하

다.

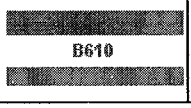
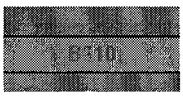
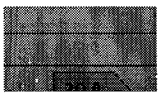
표 3.6.8 블록 점유 표시

상태	해정	점유
표시		

- 블록 개방/폐쇄/검지손실 표시

블록의 개방/폐쇄/검지손실 상태는 블록 아이콘의 색상 변화로 표시된다. 블록 점유와 폐쇄 상태가 혼합되어있을 경우에는 블록 아이콘을 새로운 색상으로 표시한다.

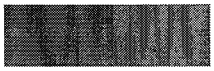
표 3.6.9 블록 개방/폐쇄/검지손실 표시

상태	개방, 미점유	폐쇄, 미점유	폐쇄, 점유	검지손실
표시				

- 진로 표시

블록 아이콘 색깔로 진로설정 상태를 표시한다.

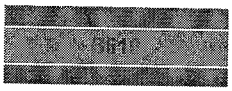
표 3.6.10 진로 표시

상태	진로 미설정	진로설정, 미점유	진로설정, 점유
표시			

- 임시속도제한 표시

블록 아이콘의 색상 변화로 블록에 설정된 임시속도제한상태를 표시한다. 블록에 설정되는 임시속도제한은 블록이 개방되어 있고 점유되어 있지 않을 때만 설정된다.

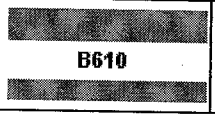
표 3.6.11. 임시속도제한 표시

상태	임시속도제한 미설정	임시속도제한 설정
표시		

- PMA 표시

블록 Label의 색상변화로 CRD로부터 수신한 블록의 PMA 상태를 표시한다.

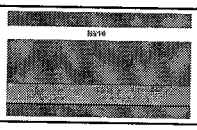
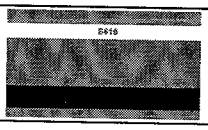
표 3.6.12 PMA 표시

상태	PMA미설정	PMA GREEN	PMA YELLOW	PMA RED
표시				

- 플랫폼 개방 및 폐쇄 표시

플랫폼 개방 및 폐쇄 상태는 플랫폼 아이콘 색상으로 표시된다.

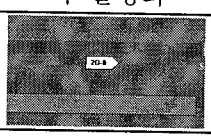
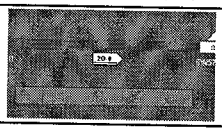
표 3.6.13 플랫폼 개방/폐쇄 표시

상태	개방	폐쇄
표시		

- Dwell Time 표시

출발 예정시간까지의 잔여 시간이 초단위로 플랫폼 아이콘 옆에 표시된다. 이 값은 매 초마다 갱신된다.

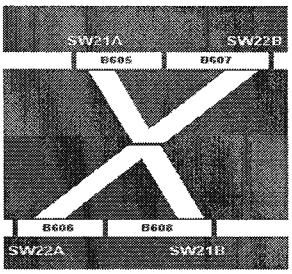
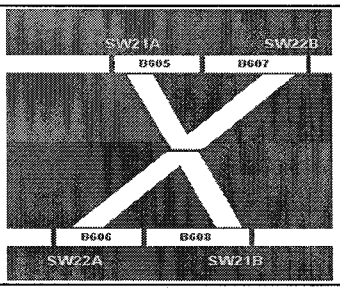
표 3.6.14 Dwell Time 표시

상태	비 활성화	출발예정 잔여시간
표시		

- 선로전환기 쇄정 표시

선로전환기 쇄정 표시는 선로전환기 명칭의 색깔로 표시된다.

표 3.6.15 선로전환기 쇄정 표시

상태	정위 해정	정위 쇄정
표시		

② MMI

다음은 전년도에 요구분석된 사항을 토대로 실제 구현된 MMI 화면이다.

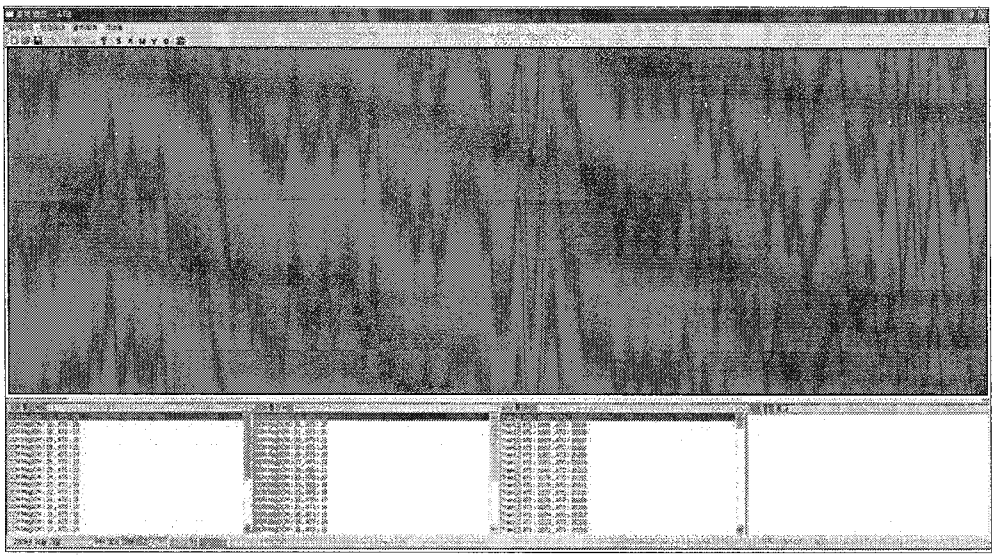


그림 3.6.2 MMI 화면

MMI 화면에는 ATS 시뮬레이터에서 열차운행과 현장설비 제어명령을 위한 명령 메뉴 표시부, 자주 사용하는 메뉴를 툴바에 아이콘 형태로 구성한 툴바 표시부, 통신 및 제어명령 표시부, Status Bar로 구성된다. 명령 메뉴 표시부에서는 ATS 시뮬레이터에서 열차운행과 현장설비 제어명령을 수행하기 위한 화면을 표시하며, 명령 메뉴 표시부의 메뉴는 다음과 같이 구성된다.

표 3.6.16 명령 메뉴 표시부 구성

1차 메뉴	2차 메뉴	3차 메뉴	화면 표시 내용
	사용자 등록		사용자 등록/제거 관리
일반업무	로그 인/아웃		사용자 로그 인/아웃 관리
	종료		ATS시뮬레이터 종료
현장제어	수동진로		개별진로설정/취소
	자동진로		자동진로설정/취소
	선로전환기		선로전환기 전환
	임시속도		블록에 임시속도제한 설정/해지
	블록개방		블록 개방/폐쇄
	플랫폼	플랫폼 개방	플랫폼 개방/폐쇄
		플랫폼 대기	플랫폼 대기 설정/해지
		플랫폼 정차시간	플랫폼 정차시간 설정
	CRD절체/RESET		CRD시스템 On-Line시스템과 Stand-by시스템 지정
열차제어	출발/정지		열차 출발/정지
	출입문 제어		열차 출입문 개방/폐쇄
	비상제동 해지		열차 비상제동 해지
	운행속도제어		열차 속도 제한
	목적지 제어		열차 운행방향 목적지 지정
역이동	역명 표시		지정역을 L/S에 표시
	Overview		모든 역을 화면에 표시

툴바 표시부에서 실제 열차운행상황 표시와 관련되어 사용되어지는 부분에 관한 내용이며, Overview 표시는 모든 역을 화면에 표시하기 위한 메뉴이다. 다음 그림은 Overview 표시 화면을 나타낸 것이다.

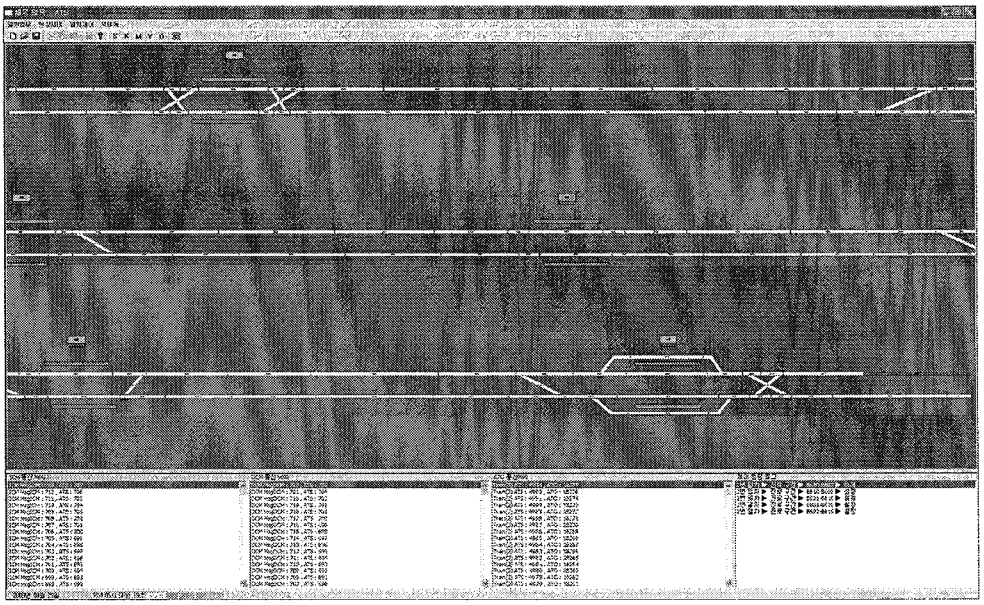


그림 3.6.3 Overview 화면

통신 표시부는 ATS 시뮬레이터와 인터페이스 되는 장치인 CRD와 차상시뮬레이터와의 인터페이스를 확인하기 위한 표시부이며, 각 장치별로 현재 송·수신되는 Sequence 번호를 표시한다. 표시되는 정보는 시간 순으로 표시되며 가장 최근의 정보가 로그창의 가장 상위에 표시되며 스크롤이 가능하다.

제어명령 표시부는 입력하는 제어명령을 표시하는 부분으로 는 창에 표시되는 제어 명령 로그는 실시간으로 표시되어야 하며 ATS시뮬레이터에서 수행되는 제어명령을 화면에 표시된다. 표시되는 화면은 다음과 같다.

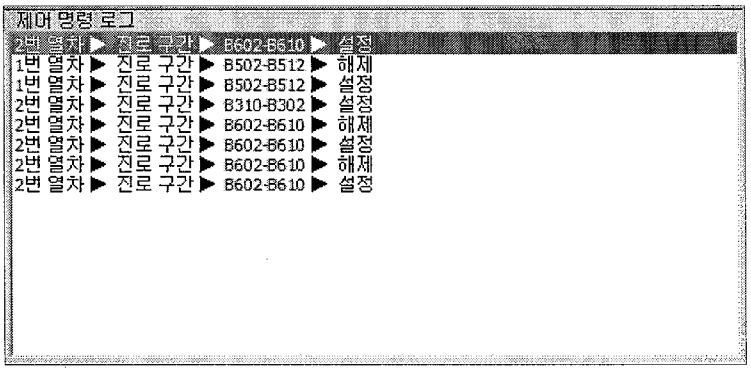


그림 3.6.4 제어명령 표시부

전체화면의 바닥을 따라 위치한 Status Bar에는 현재일자 및 시간, 통신링크 상태 등이 표시된다. 통신링크의 경우 ATS 시뮬레이터와 인터페이스되는 CRD와 차

상시뮬레이터와의 통신링크 상태를 표시하며, 녹색이 정상, 적색일 경우가 통신링크 장애의 경우에 해당한다.

(나) 차상 시뮬레이터

차상 시뮬레이터는 CRD와의 연동을 위한 ATP 차상장비와 ATS 시뮬레이터와의 연동을 위한 ATO 차상시뮬레이션을 동시에 수행한다. 차상 시뮬레이터는 아래의 성능을 갖는 한대의 퍼스널 컴퓨터를 하드웨어로 사용하며 UDP/IP LAN 통신을 이용하여 CRD 시스템 및 ATS시뮬레이터와 통신한다. 프로그램 개발에 사용된 컴퓨터 언어는 Visual C++ 2003 을 기본으로 하였으며 open GL이 그래픽 화면 구성을 위해 사용되었다.

① 초기화면

차상 시뮬레이터 사용은 매우 단순하게 설계 제작되었다. 사용자 화면을 주메뉴 화면 하나로 구성하였으며 주 화면에 필요한 모든 정보를 다 표시하도록 하였다. 다음 그림은 차상시뮬레이터의 초기 화면이다.

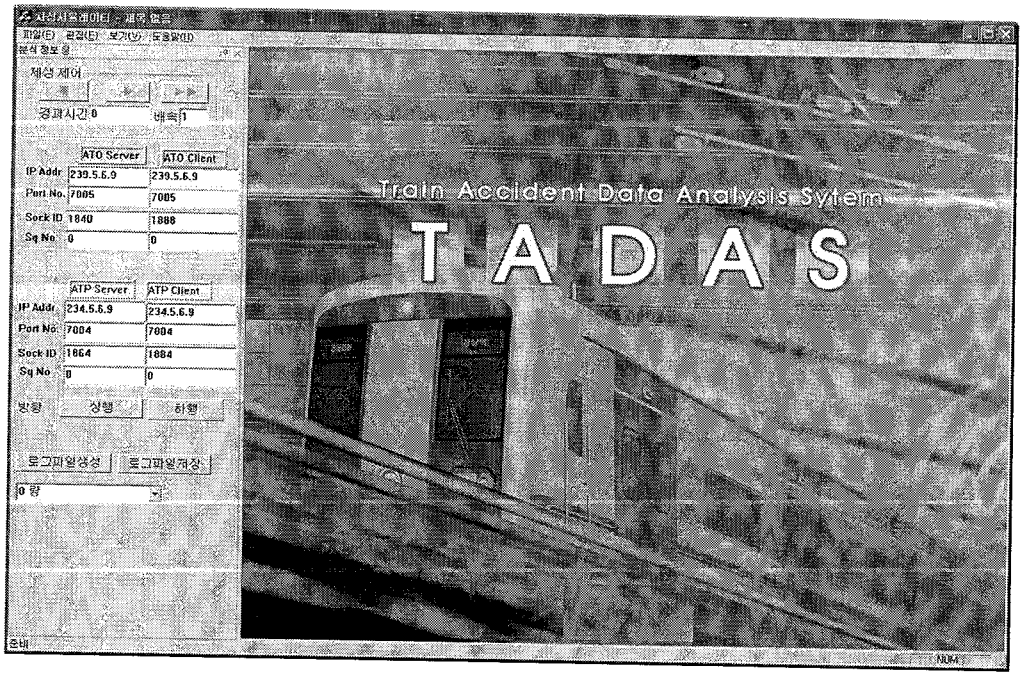


그림 3.6.5 차상시뮬레이터 초기 화면

② 시뮬레이션 화면

다음 그림은 현재 열차가 운행되는 시뮬레이션이 시작된 상태를 보여준다. 화면 중앙에 열차가 운행되는 동안 열차의 속도를 표시하는 운전선도와 실제 선로와 열차의 이동을 표현하고 현재 열차운행과 관련된 정보를 화면 하단에 표시한다.

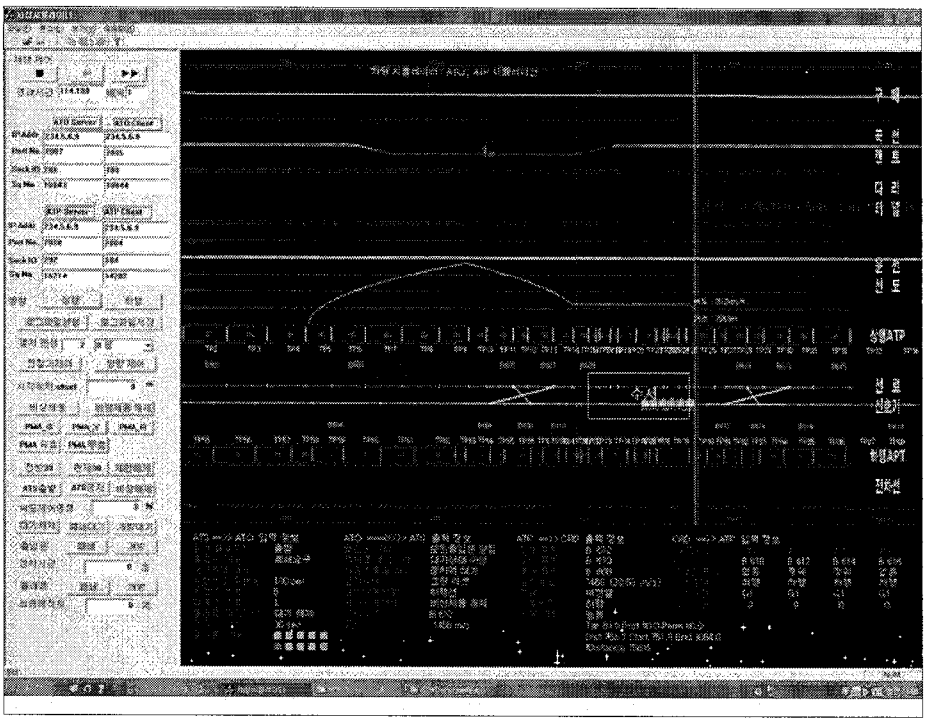


그림 3.6.6 차상시뮬레이터 시뮬레이션 화면

③ 메뉴 화면

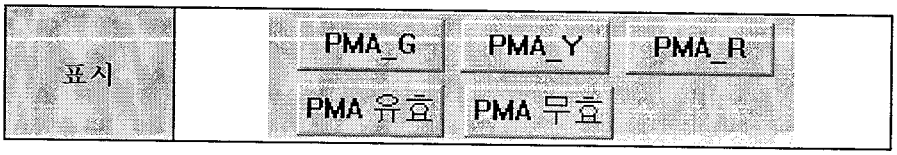
시뮬레이션 좌측에 메뉴 화면이 제공된다. 이 메뉴를 통해 시뮬레이터로서 가져야 될 차량편수 선택, 선로전환기 방향전환, 열차운행 방향제어, 열차 속도제한 등 다양한 기능들이 실행되어지게 된다. 다음은 메뉴에서 수행되는 기능 중 주요한 내용들을 나타낸 것이다.

- 재생제어 버튼 : 재생제어버튼을 통해 시뮬레이션의 시작 (▶), 일시정지(■), 배속(▶▶)을 결정할 수 있도록 하였고, 경과 시간 및 현재의 배속상태를 알 수 있다. 배속은 16 배속까지 가능 하면 배속 버튼을 누르면 2 배씩 시뮬레이션 속도가 증가하고 16 배속이상이 되면 다시 정속(1 배속)으로 변한다. 경과 시간은 최초에 재생버튼을 클릭했을 때와 상하행 노선을 바꾸는 경우에도 초

기화 된다. 이 경우에 열차는 각각 상하행 출발역 정위치 정차위치에서 운전을 시작하게 된다.

- 소켓정보 표시창 : 차상 시뮬레이터는 UDP/IP 멀티캐스팅 방식으로 통신하며 이를 위한 포트번호와 CRD, ATS 시뮬레이터의 IP 주소정보를 표시하며, Sock ID, SqNO는 메시지의 송수신횟수 등의 정보를 제공하도록 한다.
- 로그파일 버튼 : 로그파일 버튼은 차상시뮬레이터가 연동상태에서 송수신메시지의 값을 확인하기 위하여 사용된다. 로그파일생성 버튼을 클릭하면 "AutoTrainLogFile.dat"라는 이름으로 쓰기용 파일을 열고 저장버튼을 클릭하기 전까지 모든 송수신 데이터를 기록한다. 이 기록으로 시스템 운영상의 오류를 진단할 수 있도록 하였다.
- 비상제동 설정 및 비상제동 해제 : 열차의 비상제동 상태를 설정하거나 현재 비상제동 상태를 해제 하는 버튼으로서 열차의 현재 상태 값을 변경하여 ATS시뮬레이터의 열차 상태변화 및 비상제동 해제 명령을 수행하기 위해 존재한다. 비상제동 설정 상태에서 열차는 진행 할 수 없음을 나타낸다.
- PMA 설정 : 열차가 수동으로 진행하도록 설정할 것인지 또는 열차가 CRD의 PMA 정보를 획득하여 진행할 것인지를 결정하도록 하는 버튼으로 PMA 무효 버튼을 클릭하면 열차가 CRD의 PMA를 무시하여 진행하게 된다. PMA 유효 버튼을 클릭 시 CRD에서 전송해주는 블록의 PMA 정보를 획득하여 현재 블록에 진입 가능한지를 결정한다. PMA 무효 시 PMA_G 버튼을 클릭하면 전방에 GREEN 상태를 유지하여 정상 운행하게 하며 PMA_Y 버튼을 클릭하면 전방 블록이 YELLOW 상태가 되어 서행 운행으로 진행하게 된다. PMA_R 버튼을 클릭하면 PMA 상태가 RED가 되어 현재 진행 블록의 끝에서 정지하게 된다.

표 3.6.17 PMA설정 확인 버튼



- 임시제한속도 설정 : 열차의 임시 제한 속도를 설정함을 시뮬레이션 하는 버튼

이다. 전방30 버튼을 클릭 시 현재 블록의 다음 블록에서 30km/h 속도로 진행하도록 설정한다. 현재30 버튼을 클릭 시 현재 운행 속도를 줄여 30km/h가 되도록 속도를 줄여준다. 제한 해제 버튼을 클릭 시 제한 속도를 해제 하여 다시 속도가 증가하는지를 확인시켜준다.

- 열차 출발·정지 설정 : 열차의 출발·정지를 수동으로 설정하는 버튼으로 열차가 진행 중일 때 정지 버튼을 클릭하면 열차가 상용제동에 의한 정지가 이루어지도록 설정하도록 하고, 정지 후 재출발 하고자 할 때 출발 버튼을 클릭하면 열차가 다시 출발 하도록 설정하는 버튼이다.
- 열차 속도 제어 : 열차는 항시 최고 속력을 내기 위해 달린다. 하지만 어떤 임시의 작업에 의해 열차 속도를 줄여야 할 경우가 발생한다. 플랫폼을 통과하고자 하거나, 선로전환기를 지나칠 때나 속도를 줄일 수 있도록 설정하는 것이다. 열차가 진행 할 수 있는 최고속도를 100분율로 환산하여 계산하도록 한다. 100%일 때 80km/h 속도를 낼 수 있다면, 50%로 속도를 제어한다면 이 열차는 40km/h 속도로 줄여서 열차가 계속 진행하게 설정한다.
- 출입문 개방·폐쇄 설정 : 열차의 출입문 상태를 개방 할 것인지, 폐쇄 할 것인지를 결정한다. 열차가 현재 플랫폼에 정위치 정차 중일 때 열차 출입문이 폐쇄 상태이면 개방버튼을 클릭하여 열차 출입문 상태를 개방상태로 변경이 가능하다. 현재 열차 출입문이 개방 상태이면 폐쇄 버튼을 클릭하여 출입문 폐쇄 상태로 설정이 가능하다.

이러한 기능 이외에도 정차시간 제어, 플랫폼 개방·폐쇄 설정, 목적지 제어 등의 기능이 설계 및 구현되어 있다.

④ 마우스 사용

주 표시화면에 커서를 위치시키고 움직임으로써 화면을 x 축방향으로 확대, 축소, 이동시킬 수 있도록 하였다. 커서 오른쪽 버튼을 누른 상태에서 커서를 위로 움직이면 화면은 그 상태에서 확대되고 아래로 움직이면 화면이 축소되며, 커서를 오른쪽으로 움직이면 화면이 오른쪽으로 이동하고, 왼쪽으로 이동하면 왼쪽으로 이동한다. 화면은 열차의 이동에 따라 자동 스크롤 (열차위치에 따라 화면이 자동으로 좌우로 이동함)되는데, 만약 자동 스크롤을 원하지 않으면 마우스 오른쪽 버튼을 더블 클릭하면 된다. 다시 자동스크롤을 원하면 또 다시 마우스 오른쪽 버튼을 더

블 클릭하면 된다.

⑤ 송·수신 정보 표시창

시뮬레이션 화면 하단에 CRD와 ATS시뮬레이터와 송·수신 되는 데이터의 내용을 실시간으로 표시한다.

○ 차상시뮬레이터(ATP)-CRD 송·수신정보

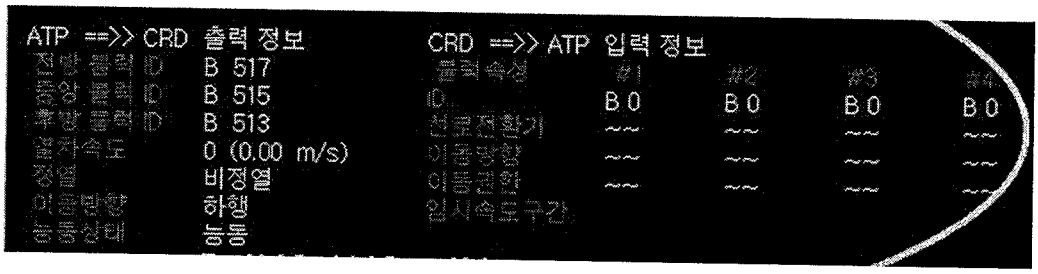


그림 3.6.7 차상시뮬레이터(ATP) 송·수신정보 표시 화면

- 차상시뮬레이터(ATP) ⇒ CRD 출력정보
  · 전방Block ID : 중앙 Block 앞쪽의 Block 인덱스 표시
  · 중앙Block ID : 열차 중앙이 점유하는 폐색구간이 속한 Block 인덱스 표시
  · 후방Block ID : 중앙 Block 진입에 의해 점유되는 폐색구간이 속한 Block 인덱스 표시
  · 열차 속도
  · 정열 : 열차의 정위치 정차 상태를 표시
  · 이동 방향
- CRD ⇒ 차상시뮬레이터(ATP) 출력정보
  · Block 속성 : 열차 전방의 4 개 Block의 Block 인덱스 및 정보 표시
  · Block ID : Block 인덱스 1, 2, 3, 4
  · 선로 전환기 · 이동 방향
  · 이동 권한 : 신호상태 R, Y1, Y2, G1, G2 표시
  · 임시속도구간

○ 차상시뮬레이터(ATO)-ATS시뮬레이터 송·수신정보



그림 3.6.8 차상시뮬레이터(ATO) 송·수신정보 표시 화면

- ATS시뮬레이터 ⇒ 차상시뮬레이터(ATO) 출력정보
  · 출발 정지 : 열차 "출발" 또는 "정지" 상태 표시 운행 중은 "출발"
  · 출입문 상태 : 출입문 "열림", 출입문 "닫힘"
  · 비상제동해제 : "해제", "체결"
  · 제한속도 적용율 : 현재 제한속도의 실 적용율 "0 ~ 100 %"
  · 종착역 번호 · 다음 역 번호
  · 플래폼 대기상태 · 정차 시간
- 차상 시뮬레이터(ATO) ⇒ ATS 시뮬레이터 출력정보
  · 출입문 상태 : "모든 출입문 열림", "오른쪽 출입문 열림 왼쪽 닫힘", "왼쪽 출입문 열림, 오른쪽 출입문 닫힘", "모든 출입문 닫힘"
  · 승강장 대기 상태 : "출입문 개방상태 대기", "출입문 폐쇄 상태 대기", "대기 중"," 대기상태 아님"
  · 다음역 통과/대기 : "대기", "통과"
  · 고장 상태 : "고장 설정", "고장해제"
  · 이동 방향 · 비상제동상태
  · 열차 위치 : 열차중앙 점유 Block 인덱스 · 열차 속도

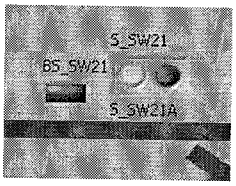
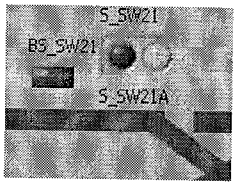
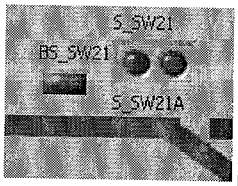
(다) 신호설비제어 · 신호설비 시뮬레이터

① 선로전환기 상태 표시

선로전환기는 Digital input 두 비트를 사용한다. 아래 그림에서처럼 LED의 상태가 왼쪽만 ON일 경우 정위 상태이고 오른쪽만 ON일 경우 반위 상태이다. LED가

둘 다 ON일 경우 현재 선로전환기의 상태는 전환 중인 상태이다. LED가 둘 다 꺼져 있을 경우는 해당 선로전환기가 고장상태임을 의미하며, 이는 Digital 입·출력이 이루어지지 않는 상태이다.

표 3.6.18 선로전환기 상태 표시

상태	정위상태	반위상태	전환 중	고장
표시				

② 선로전환기 상태 수동 설정

선로전환기는 각각의 선로전환기에 정위, 반위, 전환 중, 고장 상태를 수동으로 임의 조작이 가능하도록 하였다. 선로전환기의 상태를 임의적으로 조작하기 위해서는 실행 화면 하단에 전환버튼을 클릭하면, 선로전환기의 상태를 임의적으로 조작할 수 있는 다음과 같은 선로전환기 수동 조작화면이 표시된다.

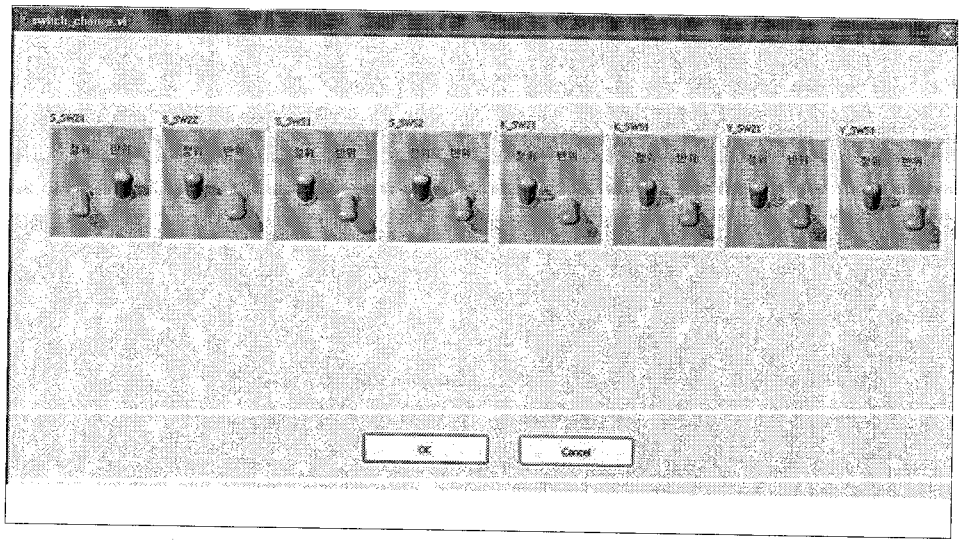
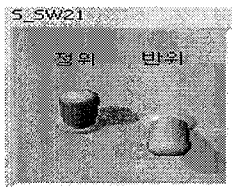
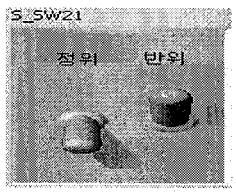
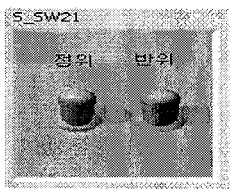
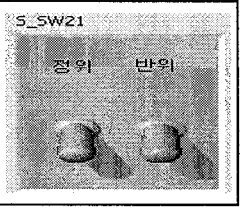


그림 3.6.9 선로전환기 수동 조작 화면

선로전환기 수동 조작화면에서 선로전환기 상태별 수동조작은 아래 표에서 보이

는 수동 설정에서 정위, 반위 스위치를 원하는 상태에 따라 ON, OFF 시킴으로써 수행된다. 선로전환기 수동 조작에 따라 실제 Digital 입·출력이 해당 조작에 따라 이루어지게 되어 선로전환기 상태를 생성한다.

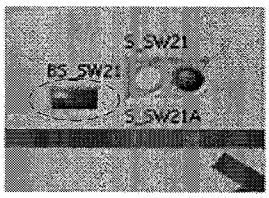
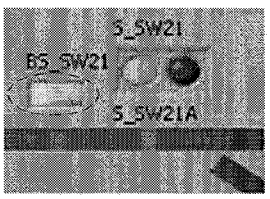
표 3.6.19 선로전환기 상태 표시

상태	정위상태	반위상태	전환 중	고장
수동 설정				

③ 선로전환기 고장 설정

선로전환기의 상태를 시뮬레이션하기 위해 임의적으로 고장 설정 정보를 생성해서 보낸다. 이는 실제 디지털 입·출력과는 상관없이 소프트웨어적으로만 해당 선로전환기 고장정보를 생성해서 CRD로 전송하게 되는 경우이다. 선로전환기 고장 설정은 선로전환기 옆에 위치한 사가형 버튼(점선 원 표시)을 클릭함으로써 설정된다. 클릭한 사가형의 버튼에 초록색이 현시되면 선로전환기 고장이 설정되었음을 의미한다.

표 3.6.20 선로전환기 고장 설정 표시

상태	정상 상태	고장 상태
표시		

④ 초기화면

신호제어설비시뮬레이터의 사용은 매우 간단하게 설계 제작되었다. 신호제어설비시뮬레이터는 현재 Digital input 정보를 수집하여 선로전환기의 상태값으로 입력받게 된다. 선로전환기 하나당 Digital 포트 2개를 사용하여 정위 포트와 반위 포트

로 나타낸다. 이는 정위 상태일 때는 정위 포트에만 Digital 출력이 이루어지고, 반위 상태 일 때는 반위 포트에만 Digital 출력이 이루어짐을 의미한다. 다음은 신호제어설비시뮬레이터 실행 전 초기화면이다.

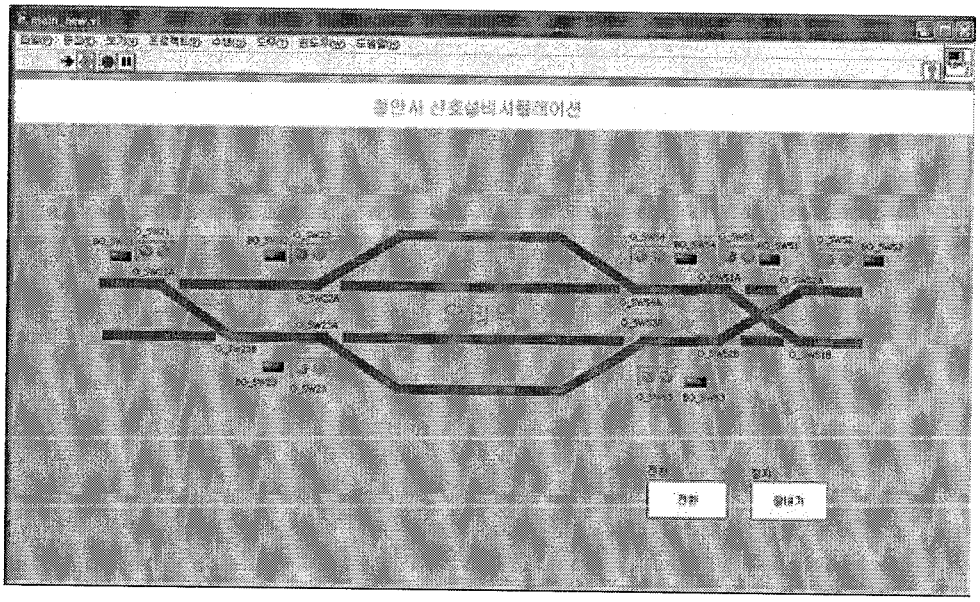


그림 3.6.10 신호설비제어시뮬레이터 초기 화면

이 그림에서와 같이 신호설비제어 시뮬레이터 실행 전에는 선로전환기의 상태는 Digital 출력 값과 입력 값이 없으므로 아래 그림과 같이 선로전환기 상태를 표시하는 LAMP에 아무것도 표시가 되지 않고 현재 모든 선로전환기가 반위 상태로 나타난다.

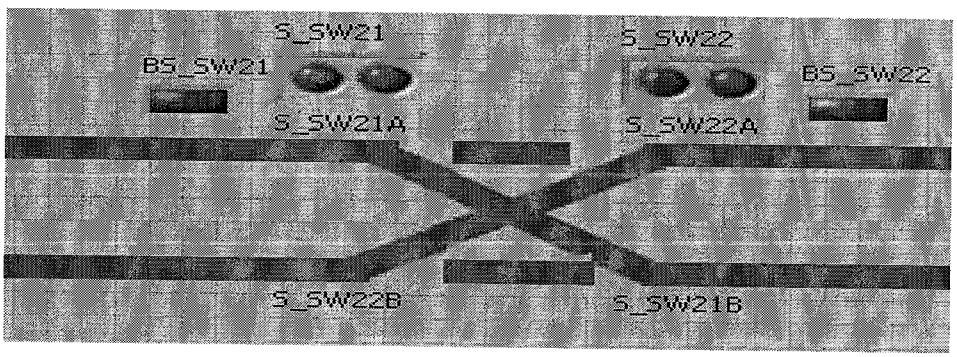


그림 3.6.11 신호설비제어시뮬레이터 실행 전 선로전환기 상태

⑤ 실행화면

신호설비제어 시뮬레이터 초기화면의 툴바에서 실행버튼을 클릭하면 신호설비제어 시뮬레이터가 실행된다. 신호설비제어 시뮬레이터 실행을 수행하면 선로전환기마다 Digital 출력 및 입력이 이루어지고 이로 인해 아래 그림처럼 모든 선로전환기의 상태가 정위로 초기화되고 선로전환기 상태를 표시하는 LAMP에 정위를 표시하게 된다. 신호설비제어 시뮬레이터 실행 시 처음에는 모든 선로전환기 상태는 정위값으로 초기화 되도록 설정되어 있다.

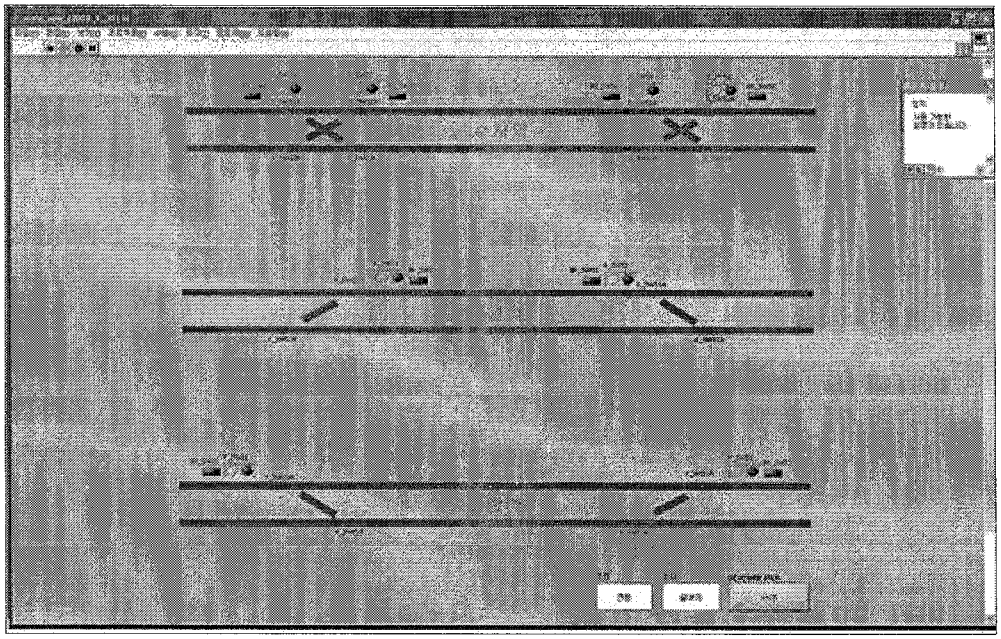


그림 3.6.12 신호설비제어시뮬레이터 실행 화면

⑥ 제어명령 수행

CRD에서 선로전환기 전환 제어 수신 시 신호설비제어 시뮬레이터는 해당 선로전환기 전환을 수행한다. 시뮬레이션을 확인한다. 만약 CRD에서 S_SW21의 반위를 설정을 수신하면 신호제어설비시뮬레이터는 Digital 반위 포트에 출력을 내보내고 정위 포트의 출력을 OFF 시켜 정지 시킨다. S_SW21은 반위 상태로 설정되고 그 상태를 CRD로 전송하게 된다. 다음 그림은 S_SW21이 반위 상태(점선 원 표시)로 전환된 것을 나타내는 화면이다.

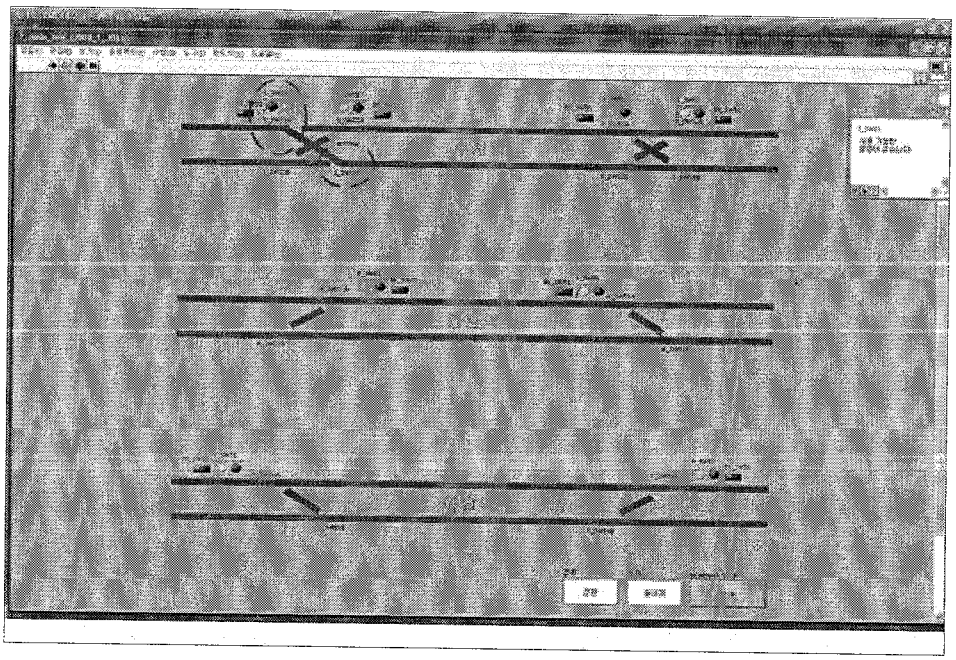


그림 3.6.13 선로전환기 반위 전환 실행 화면

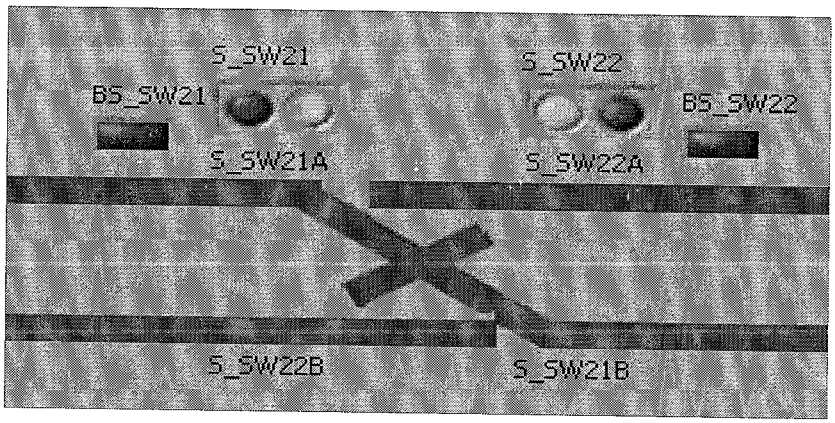


그림 3.6.14 선로전환기 S-Sw21 반위 전환 상태 표시

(라) 안전성 검증 시뮬레이터

① 개요

안전성 검증 시뮬레이터(이하 검증시뮬레이터)는 안전성평가용 대상 열차제어시스템 중 주로 CRD시스템의 기능 중 안전측 동작에 대한 요구사항을 검증하기 위한 시뮬레이터이다. 당해연도에는 이를 위해 안전성평가용 대상 열차제어시스템 기능 중 안전측 동작을 검증하기 위한 검증항목을 선별하고 이러한 검증항목을 검증하기 위한 방안을 정의한 설계문서와 이를 바탕으로 검증시뮬레이터를 제작하였다.

검증시뮬레이터는 Validation의 항목 중 일부 검증 가능한 항목에 대해서만 적용 가능한 툴이며, 안전성평가용 대상 열차제어시스템의 Validation 활동은 검증시뮬레이터의 사용 여부와 상관없이 수행되어야 한다.

② 구성

검증시뮬레이터는 안전성평가용 대상 열차제어시스템의 네트워크망에 접속되어 구성된다. 안전성평가용 대상 열차제어시스템은 진로제어 및 열차간격을 제어하는 시스템인 CRD, Non-Vital 감시 기능을 가지는 ATS시뮬레이터, 가상 열차운행을 위한 차상시뮬레이터, 현장의 선로변에 설치되어 현장 선로전환기 등과 같은 선로변 장치를 제어하는 모의 현장신호제어 설비인 신호설비제어시뮬레이터, 실제 선로전환기 기능을 담당하는 신호설비(선로전환기)시뮬레이터 시스템으로 구성된다. 안전성평가용 대상 열차제어시스템을 구성하는 서브시스템간 인터페이스는 Network Switch를 이용한 Ethernet으로 구성되며, 검증시뮬레이터도 Network Switch를 이용하여 안전성평가용 대상 열차제어시스템의 Ethernet망에 접속한다.

다음은 안전성평가용 대상 열차제어시스템을 포함한 검증시뮬레이터 시스템 전체에 대한 구성도를 나타낸다.

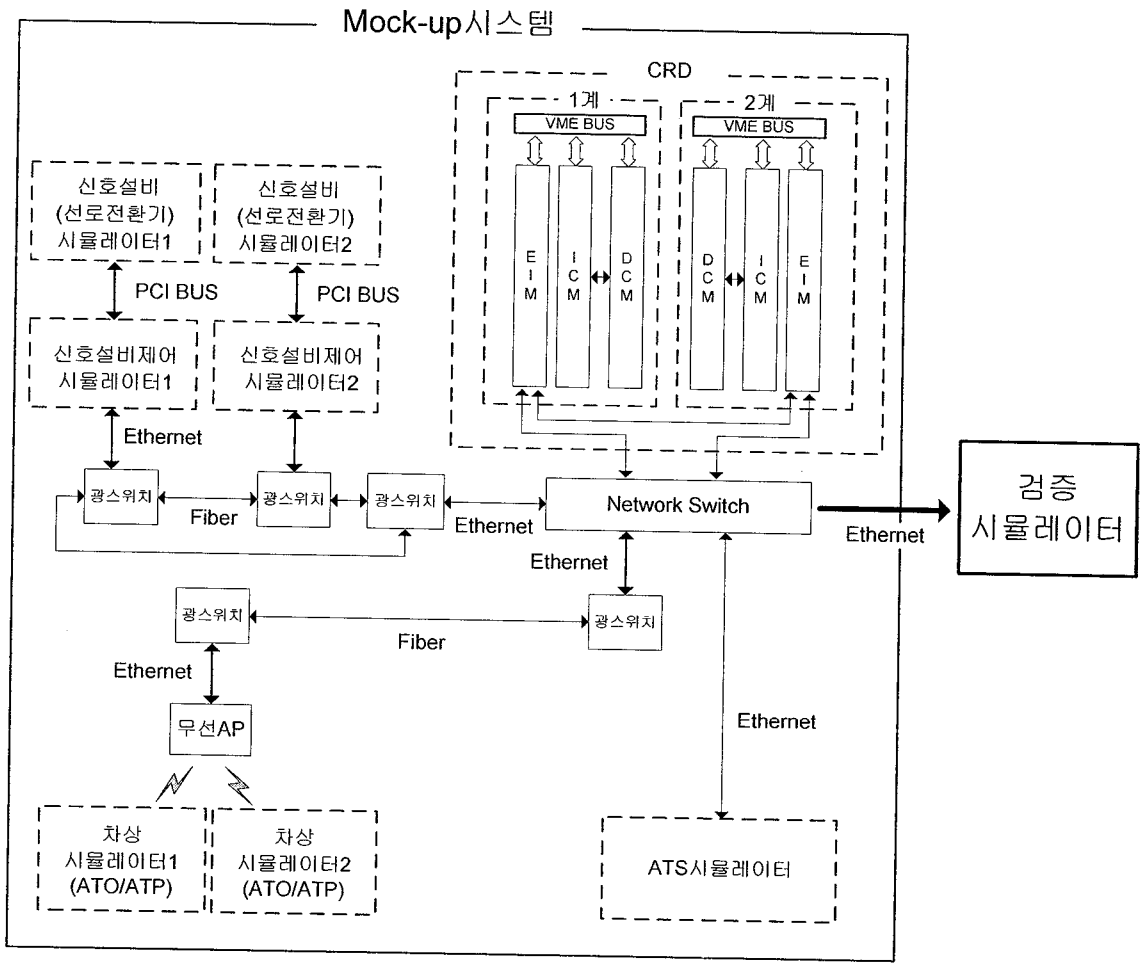


그림 3.6.15 시스템 구성도

③ 인터페이스

안전성평가용 대상 열차제어시스템을 구성하는 CRD와 주변 시뮬레이터는 Network Switch에 접속되어 상호 인터페이스 되며 장치간 사용되는 인터페이스 방식은 다음과 같다.

표 3.6.21 시스템 장치간 인터페이스 방식

장치	구분	내용
• CRD-ATS시뮬레이터 • CRD-차상ATP시뮬레이터 • CRD-신호설비제어시뮬레이터 • ATS시뮬레이터-차상ATO시뮬레이터	Protocol	UDP/IP, Multicast 방식
	접속 방법	UTP 케이블 접속 (RJ-45)

안전성평가용 대상 열차제어시스템을 구성하는 각 장치간 인터페이스는 위 표와

같이 Multicast 프로토콜을 이용하여 구현된다. 검증시뮬레이터도 안전성평가용 대상 열차제어시스템의 각 장치와 동일한 프로토콜과 접속방법을 이용하여 안전성평가용 대상 열차제어시스템의 네트워크망에 접속한다.

표 3.6.22 mock-up시스템간 인터페이스 방식

구분	내용
Protocol	UDP/IP, Multicast 방식
접속방법	UTP 케이블 접속(RJ-45)

아래 그림처럼 검증시뮬레이터는 Multicast프로토콜을 이용하여 안전성평가용 대상 열차제어시스템 장치간 상호 송/수신되는 모든 정보를 수집한다. 검증시뮬레이터는 안전성평가용 대상 열차제어시스템의 장치간 상호 송/수신되는 모든 정보를 수집만 하며 안전성평가용 대상 열차제어시스템으로 어떤 정보도 전송하지 않는다.

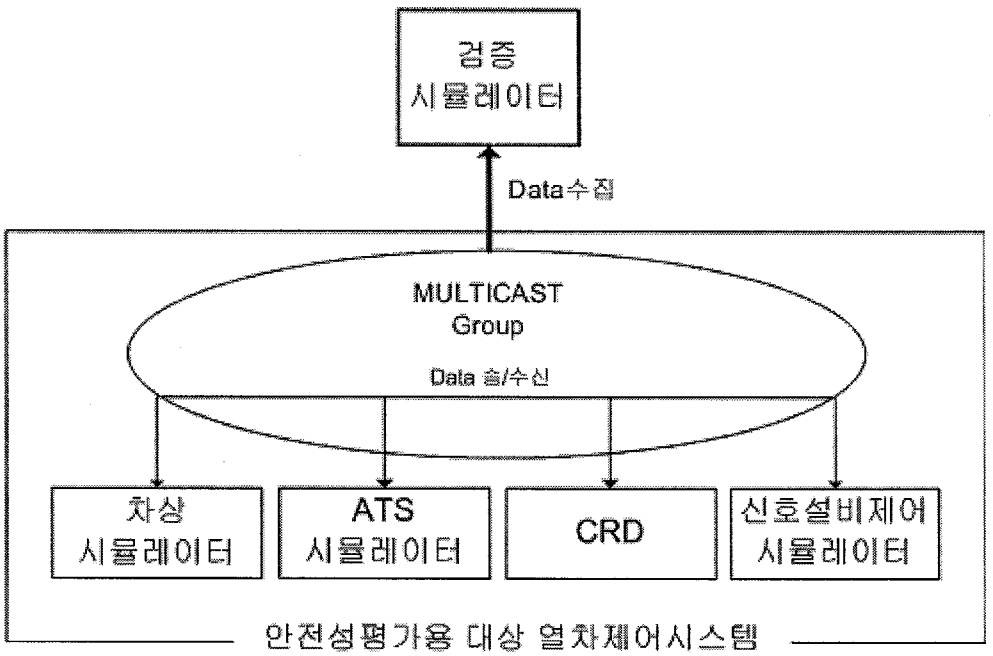


그림 3.6.16 데이터 수집 방안

④ 검증 항목

검증시뮬레이터는 주로 안전성평가용 대상 열차제어시스템의 CRD와 관련된 기

능 중 안전측 동작을 요구하는 항목 가운데 검증이 가능한 항목을 선별하여 그 기능을 구현한다. 다음은 안전성평가용 대상 열차제어시스템 기능 중 안전측 동작으로 구현되어야 하는 요구사양 중 검증시뮬레이터에서 검증 가능한 항목이다. 검증시뮬레이터는 다음의 검증항목이 아래표에서 보여지는 확인 내용대로 안전성평가용 대상 열차제어시스템에서 구현되었는지를 검증해야 한다.

표 3.6.23 검증 항목

검증항목	안전측 동작 내용	확인 내용
CRD주계에 장애가 발생될 경우	CRD부계가 주계로 자동절체되어 무중단 운영	CRD상태 확인(자동절체)
CRD부계에 장애가 발생될 경우	CRD주계 단독으로 무중단 운영	CRD상태 확인
CRD가 차상시뮬레이터로부터 3회 이상 비정상적인 메시지를 수신할 경우	열차가 점유한 블록과 관련 인접블록(PW와 SW내 모든 블록) 폐쇄	블록 상태 확인
CRD와 차상시뮬레이터와의 통신두절이 허용시간(3초)이상 발생된 경우	열차가 점유한 블록과 관련 인접블록(PW와 SW내 모든 블록) 폐쇄, 열차는 상용제동 체결하여 정지	-블록 상태 확인 -열차정지상태 확인
CRD에서 예상하는 열차위치와 다른 열차정보(위치)가 차상시뮬레이터로부터 수신된 경우	열차가 점유한 블록과 관련 인접블록(PW와 SW내 모든 블록) 폐쇄	블록 상태 확인
선로전환기 고장이 발생된 경우	관련 블록 폐쇄	블록 상태 확인
선로전환기 관련블록이 열차점유상태에서 선로전환기 전환명령을 CRD가 수신한 경우	선로전환기 전환명령 발생하지 않음	선로전환기 상태 확인
폐쇄된 블록과 관련된 선로전환기 명령을 CRD가 수신한 경우	선로전환기 전환명령 발생하지 않음	선로전환기 상태 확인
진로가 설정된 블록의 관련 선로전환기 전환명령을 CRD가 수신한 경우	선로전환기 전환명령 발생하지 않음	선로전환기 상태 확인
열차가 통과하지 않고 진로가 취소된 경우 CRD가 취소된 진로상의 선로전환기 전환명령을 수신한 경우	열차가 통과하지 않고 취소된 진로에 포함된 선로전환기는 60초 동안 쇄정(보류쇄정)되어 CRD는 선로전환기 전환명령 발생하지 않음	선로전환기 상태 확인
폐쇄된 블록에 열차가 진입한 경우	열차 비상제동	-열차비상제동확인 -열차정지상태 확인
열차가 위치한 블록에 폐쇄명령이 수행된 경우	열차 비상제동	-열차비상제동확인 -열차정지상태 확인

이동되는 열차에 대해 진로가 취소되는 경우가 발생하여 허용 이동권한이 이동중인 열차에 대해 취소되는 경우	열차 비상제동	-열차비상제동확인 -열차정지상태 확인
ATS 시뮬레이터 기능에 장애가 발생하여 차상시뮬레이터(ATO) 사이의 통신 장애가 3초 이상 발생할 경우	본선을 운행하는 모든 열차는 이동방향으로 자신과 가장 근접한 플랫폼으로 제한속도(25Km/h 이하)로 이동하여 시스템 보류 상태로 정차. 만약 플랫폼진입이 불가한 열차의 경우는 플랫폼과 가장 근접한 지점까지 제한속도로 이동한 후 정차	열차정지상태 확인
CRD 기능에 장애가 발생하여 차상(ATP)시뮬레이터 사이의 통신 장애가 발생할 경우	본선을 운행하는 모든 열차는 3초 동안 계속해서 이동. 3초 후에도 통신이 재개되지 않으면 열차는 상용제동을 체결	열차정지상태 확인
차상시뮬레이터(ATO) 기능에 장애가 발생한 경우	열차는 진행방향으로 가장 근접한 플랫폼 또는 플랫폼에 정차가 불가한 경우는 플랫폼에 접근 가능한 위치까지 서행운전 한 후 정차하여 시스템이 정상 복구될 때 까지 대기	열차정지상태 확인
차상시뮬레이터(ATP) 기능에 장애가 발생한 경우	열차 비상제동 체결하여 정지한 후 시스템이 정상 복구될 때 까지 대기	-열차비상제동확인 -열차정지상태 확인
신호설비제어시뮬레이터 기능에 장애가 발생한 경우	CRD는 해당구간폐쇄, 해당구간 열차이동 금지	-블록 상태 확인 -열차정지상태 확인

⑤ 검증 수행

검증시뮬레이터는 안전성평가용 대상 열차제어시스템의 네트워크망에 접속되어 검증항목에 대한 확인을 수행해야 한다. 이러한 검증은 안전성평가용 대상 열차제어시스템의 네트워크망에서 송/수신되는 모든 정보를 수집하고, 수집된 정보중에서 검증항목과 관련된 정보를 선별하여 검증항목의 확인을 수행하는 방식으로 한다.

㉮ 검증항목 초기 화면 구성

검증시뮬레이터에서 검증되어야 하는 검증항목은 검증시뮬레이터에서 선택이 가능하도록 화면에 다음 그림과 같이 초기화면이 표시된다.

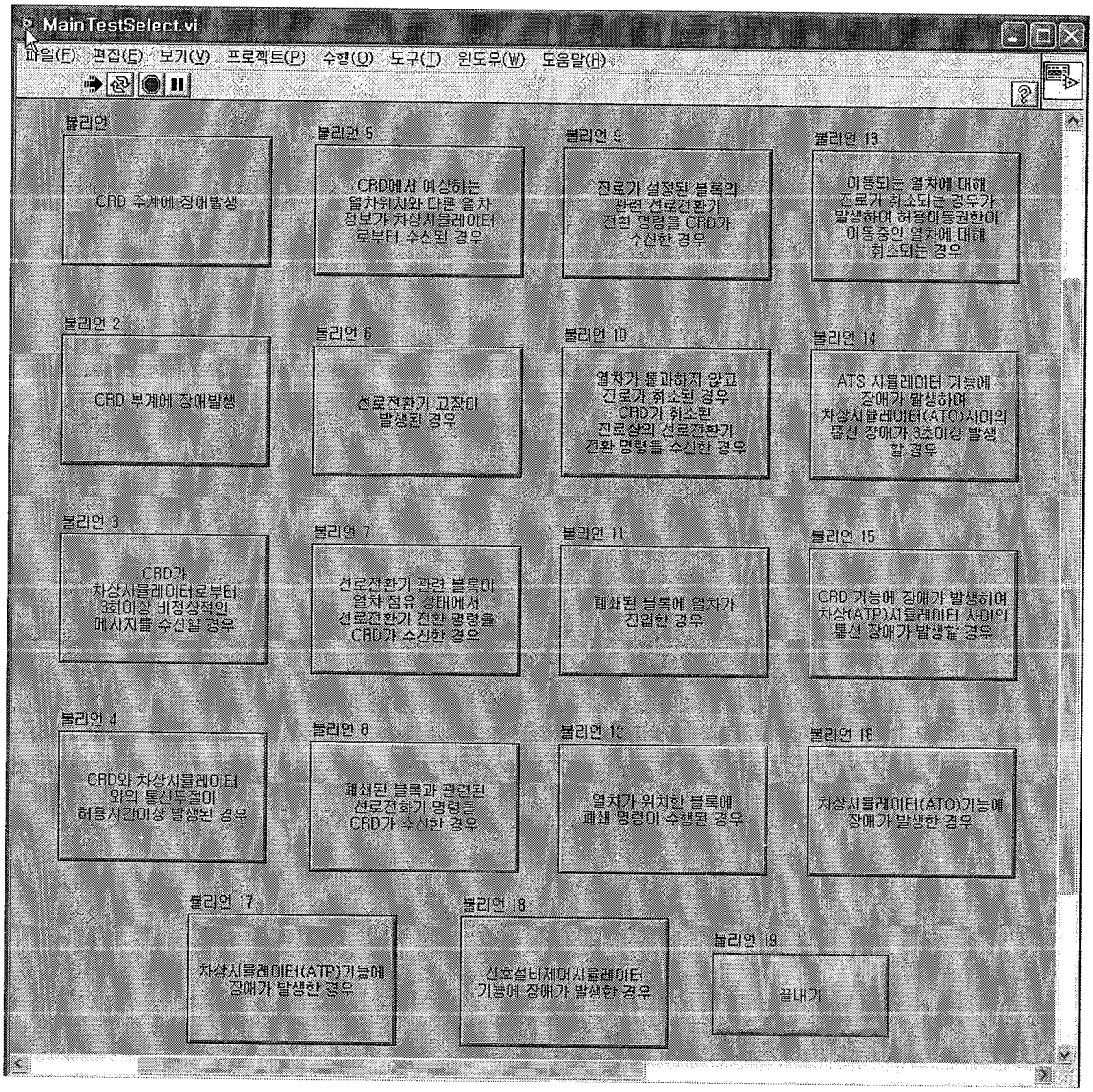


그림 3.6.17 검증 시뮬레이터 초기 화면

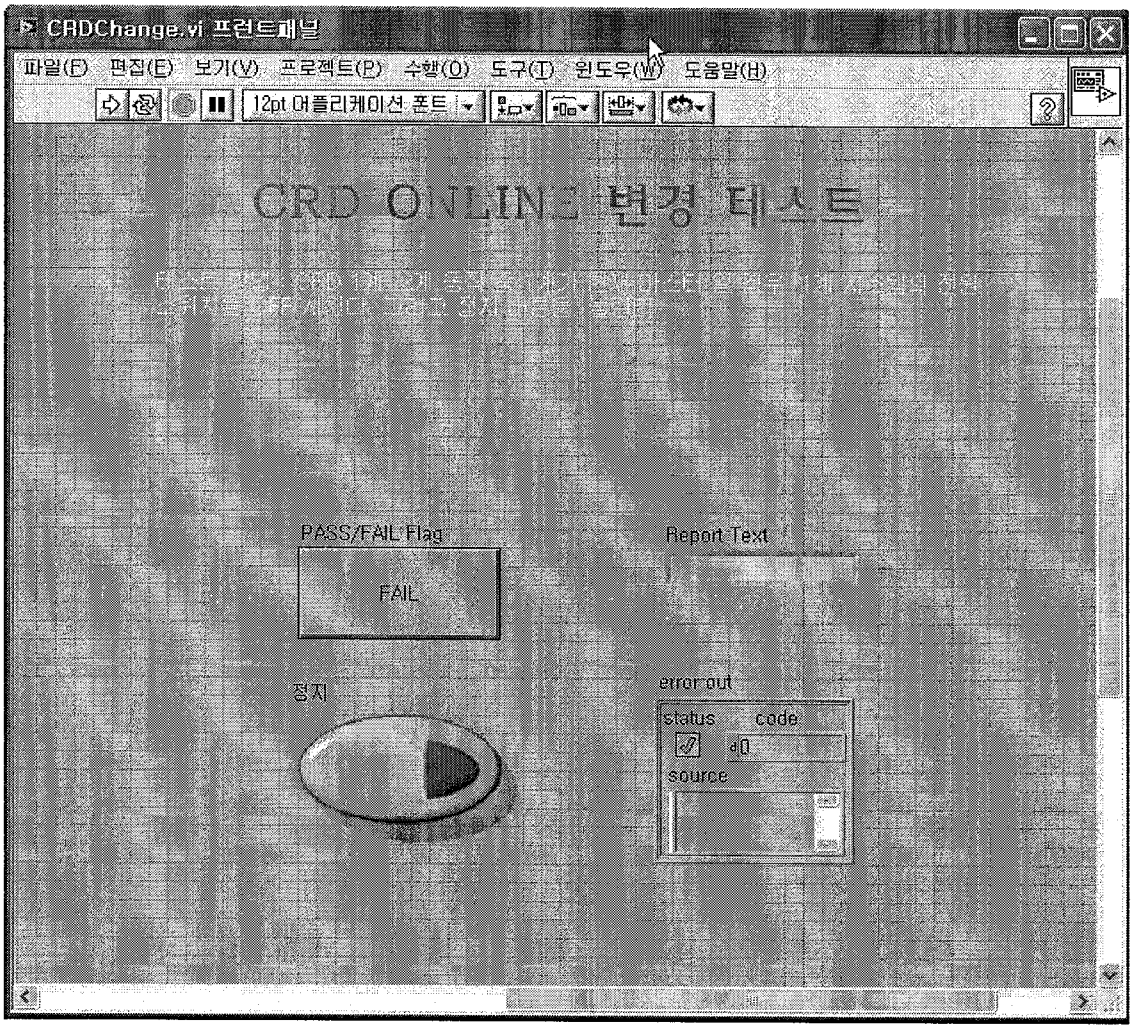
검증을 위해 초기 화면에 표시된 아이콘을 클릭하면 검증시뮬레이터는 해당되는 항목에 대한 검증결과를 확인하기 위한 기능수행을 시작한다.

㉯ 검증항목별 화면 구성 및 방안

다음은 검증항목별로 제작된 화면 구성 내용과 수행 방안 및 결과 확인 방안에 대한 설명이다.

○ CRD Online Change (케이스 명 : CRD 주계에 장애 발생)

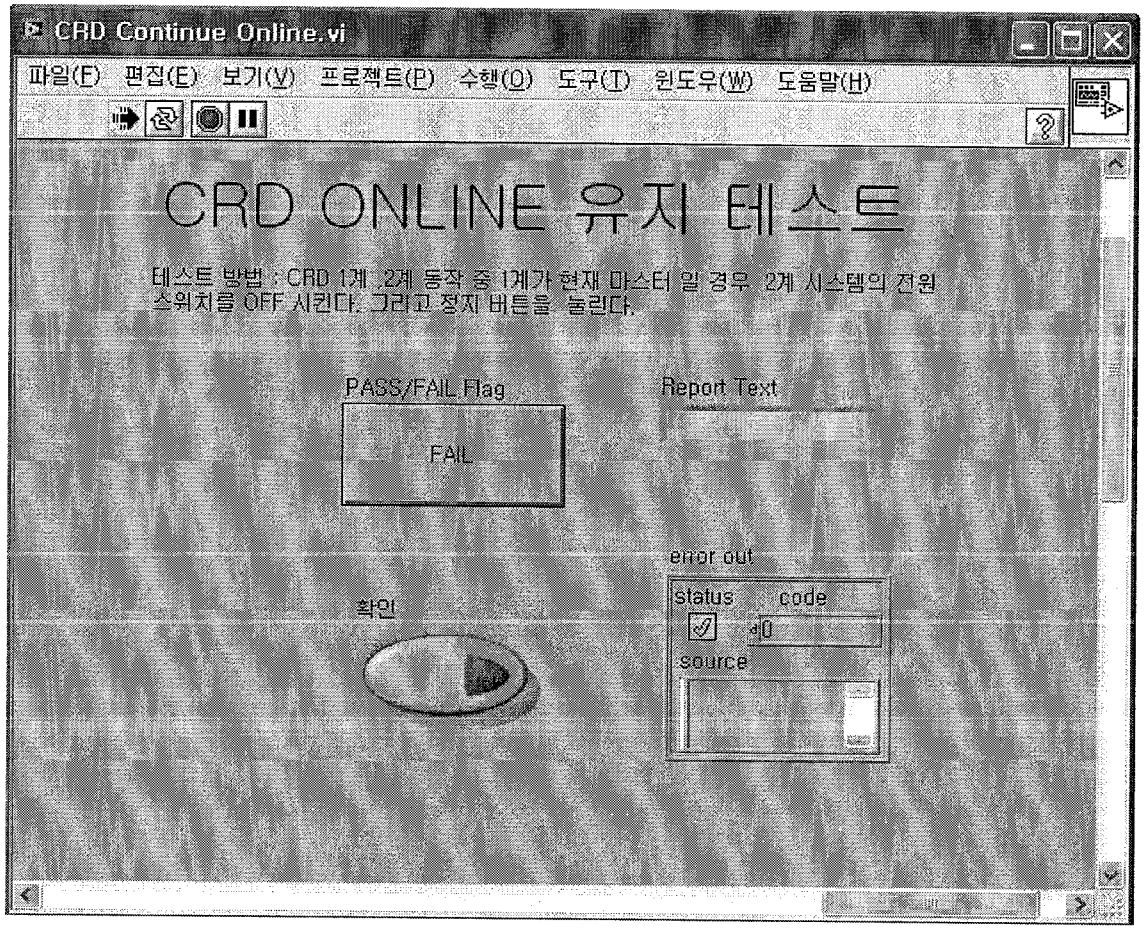
- CRD 마스터와 슬레이브 중에 마스터의 전원을 off 시키면 슬레이브 시스템이 온라인 상태로 유지됨을 확인한다. (임의로 CRD 1계를 MASTER, CRD 2계를 SLAVE로 선택함)
- STATUS : 수행 결과 (PASSED : 성공, FAILED: 실패)
- 결과 Text : CRD SLAVE



○ CRD Continue Online (케이스 명 : CRD 부계에 장애 발생)

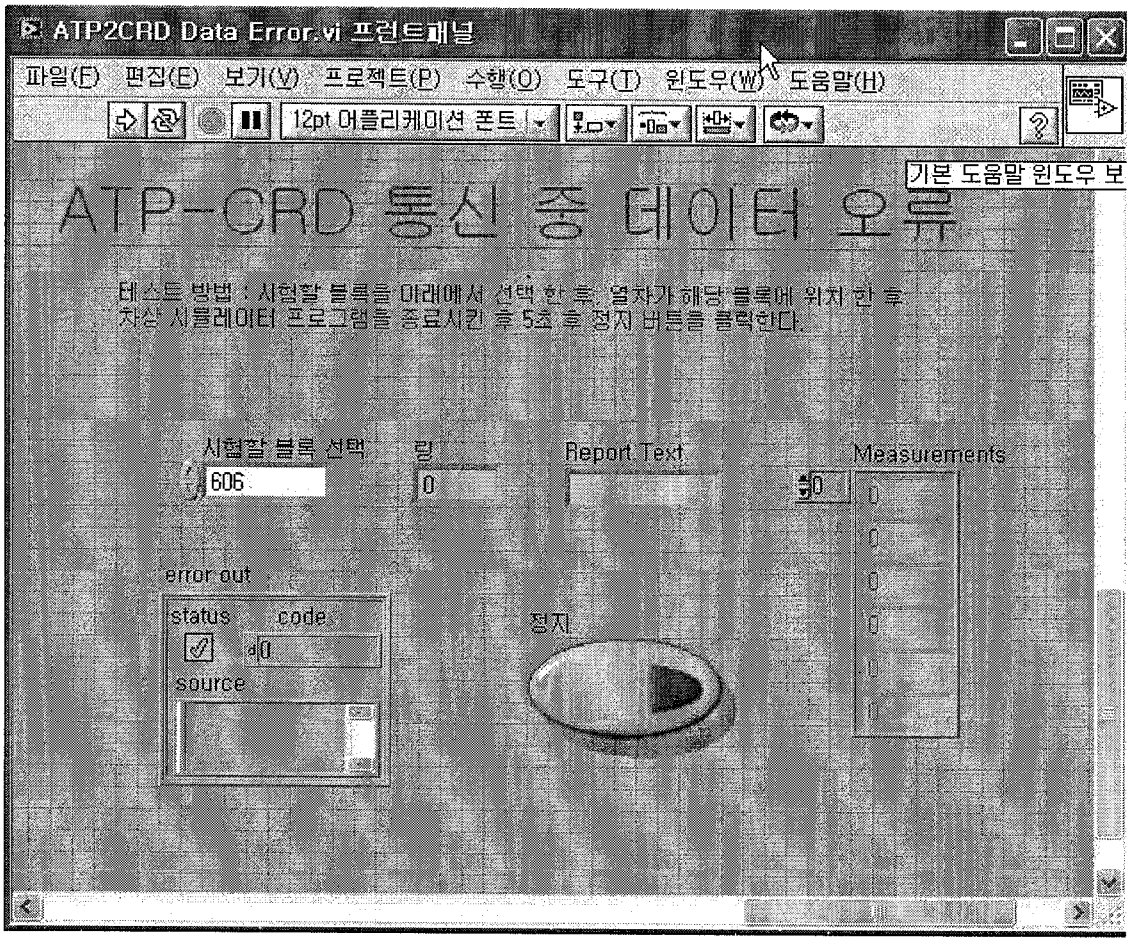
- CRD 마스터와 슬레이브 중에 슬레이브의 전원을 off 시키면 마스터가 계속해서 온라인 상태로 유지됨을 확인한다. (임의로 CRD 1계를 MASTER, CRD 2계를 SLAVE로 선택함)
- STATUS : 수행 결과 (PASSED : 성공, FAILED: 실패)

- 결과 Text : CRD MASTER



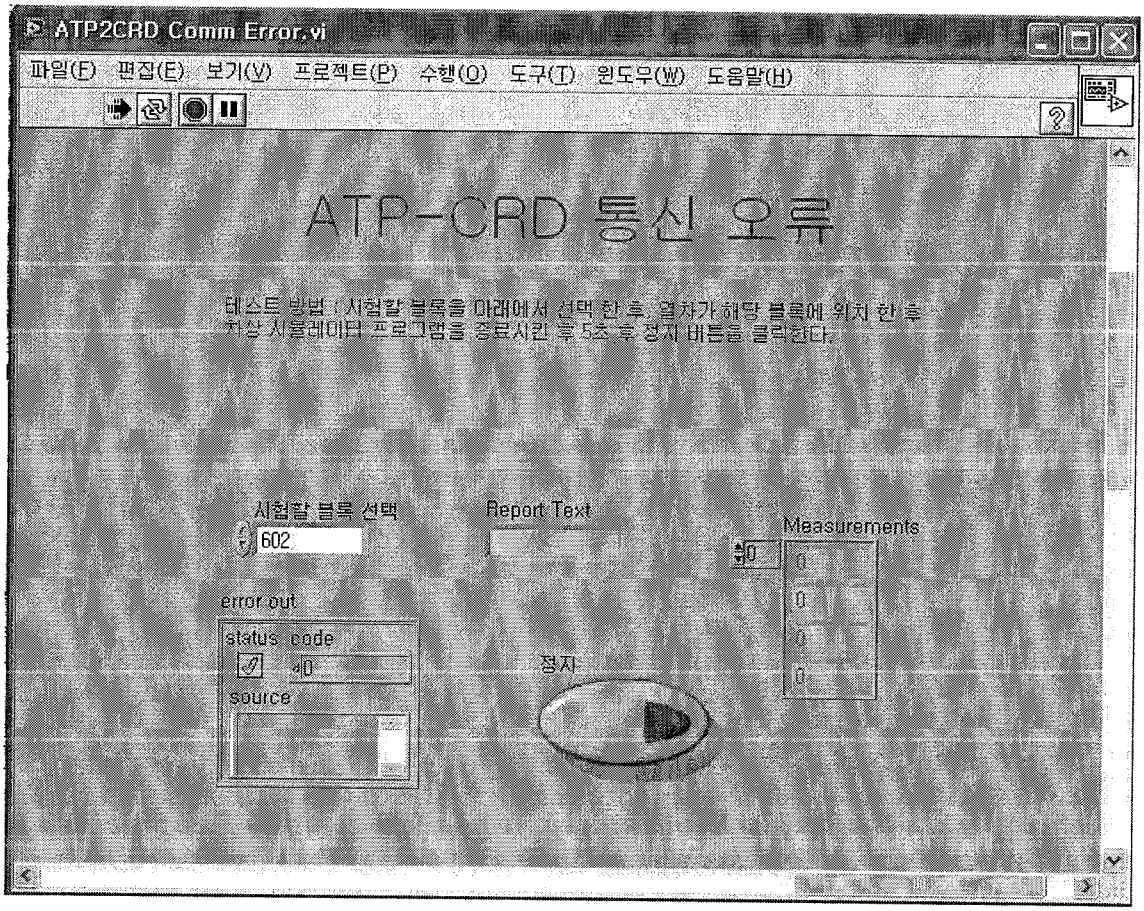
○ ATP2CRD Data Error(케이스 명 : CRD가 차상시뮬레이터로부터 3회 이상 비정상 적인 메시지를 수신할 경우)

- 데이터 오류 시 블록 폐쇄를 확인
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- Measurement : 측정한 개수(배열로 표시 됨) 여기서는 4개를 설정함
- Low : 0 측정해야할 값을 선택
- Comparison Type : EQ(==) LOW의 데이터와 같아야 함을 뜻한다.
- Data : 수신된 데이터의 값이다. 여기서는 0이다
- STATUS : LOW와 DATA 가 같으므로 성공
- 결과 텍스트 : 열차 점유 위치 : 602블록



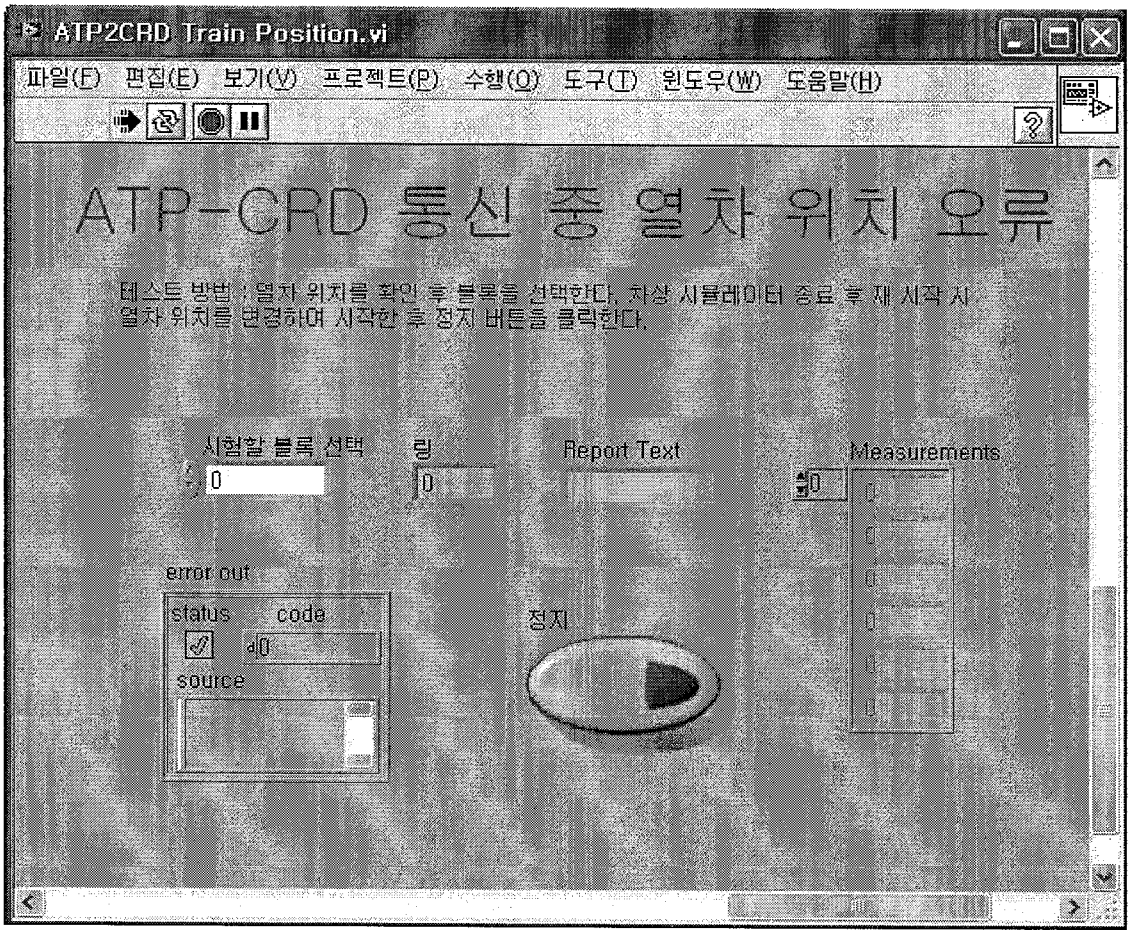
○ ATP2CRD Comm Error (케이스 명 : CRD와 차상 시뮬레이터와의 통신 두절이 허용시간이상 발생된 경우)

- 통신 두절로 인한 블록 폐쇄를 확인함.
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- Low : 0 측정해야할 값을 선택
- Comparison Type : EQ(==) LOW의 데이터와 같아야 함을 뜻한다.
- Data : 수신된 데이터의 값이다. 여기서는 0이다
- STATUS : LOW와 DATA 가 같으므로 성공
- 결과 텍스트 : 열차 점유 위치 : 602블록



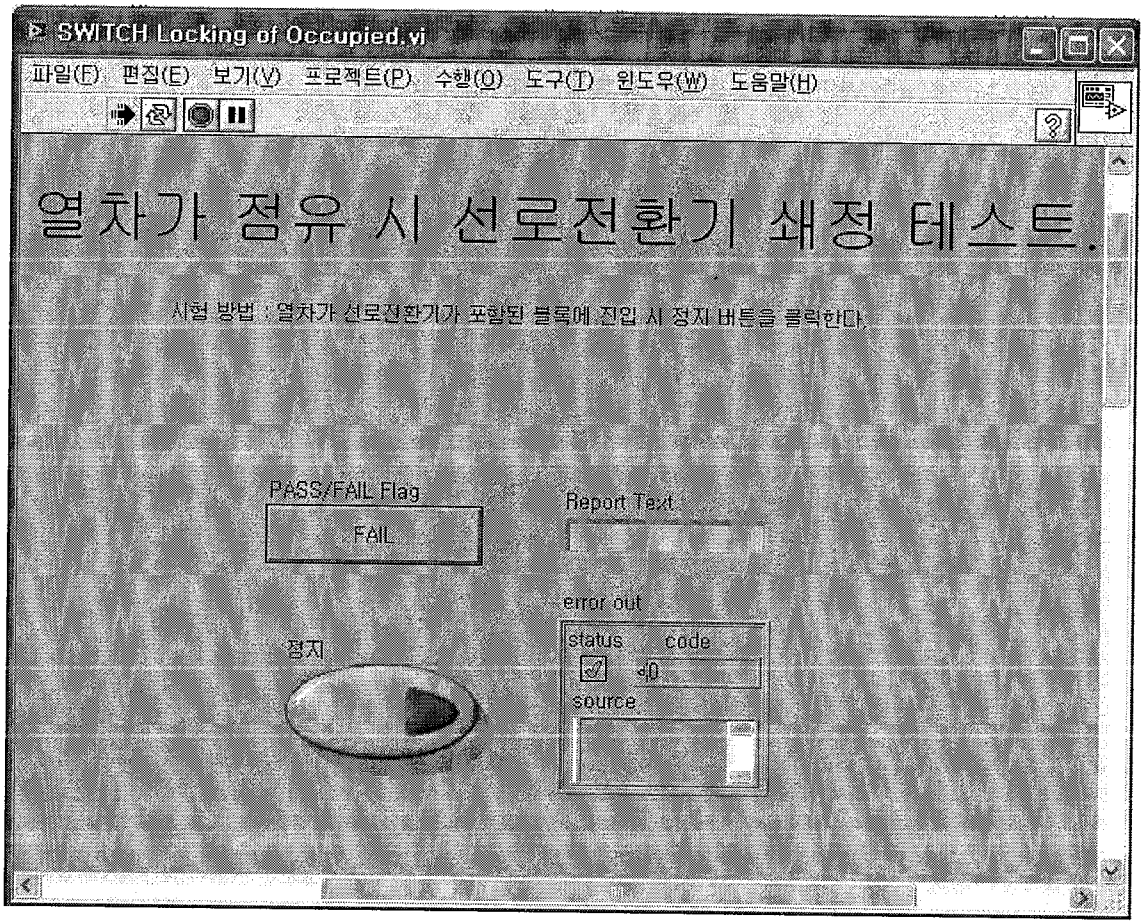
○ ATP2CRD Train Position Error (케이스 명 : CRD에서 예상하는 열차위치와 다른 열차 정보가 차상시뮬레이터로부터 수신된 경우)

- 열차 진행 중 현재 점유 블록에서 다음 블록을 점유 하지 않고 다른 블록의 정보를 수신한 경우
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- Measurement : 측정한 개수(배열로 표시 됨) 여기서는 4개를 설정함
- Low : 0 측정해야할 값을 선택
- Comparison Type : EQ(==) LOW의 데이터와 같아야 함을 뜻한다.
- Data : 수신된 데이터의 값이다. 여기서는 0이다
- STATUS : LOW와 DATA 가 같으므로 성공
- 결과 텍스트 : 열차 점유 위치 : 602블록



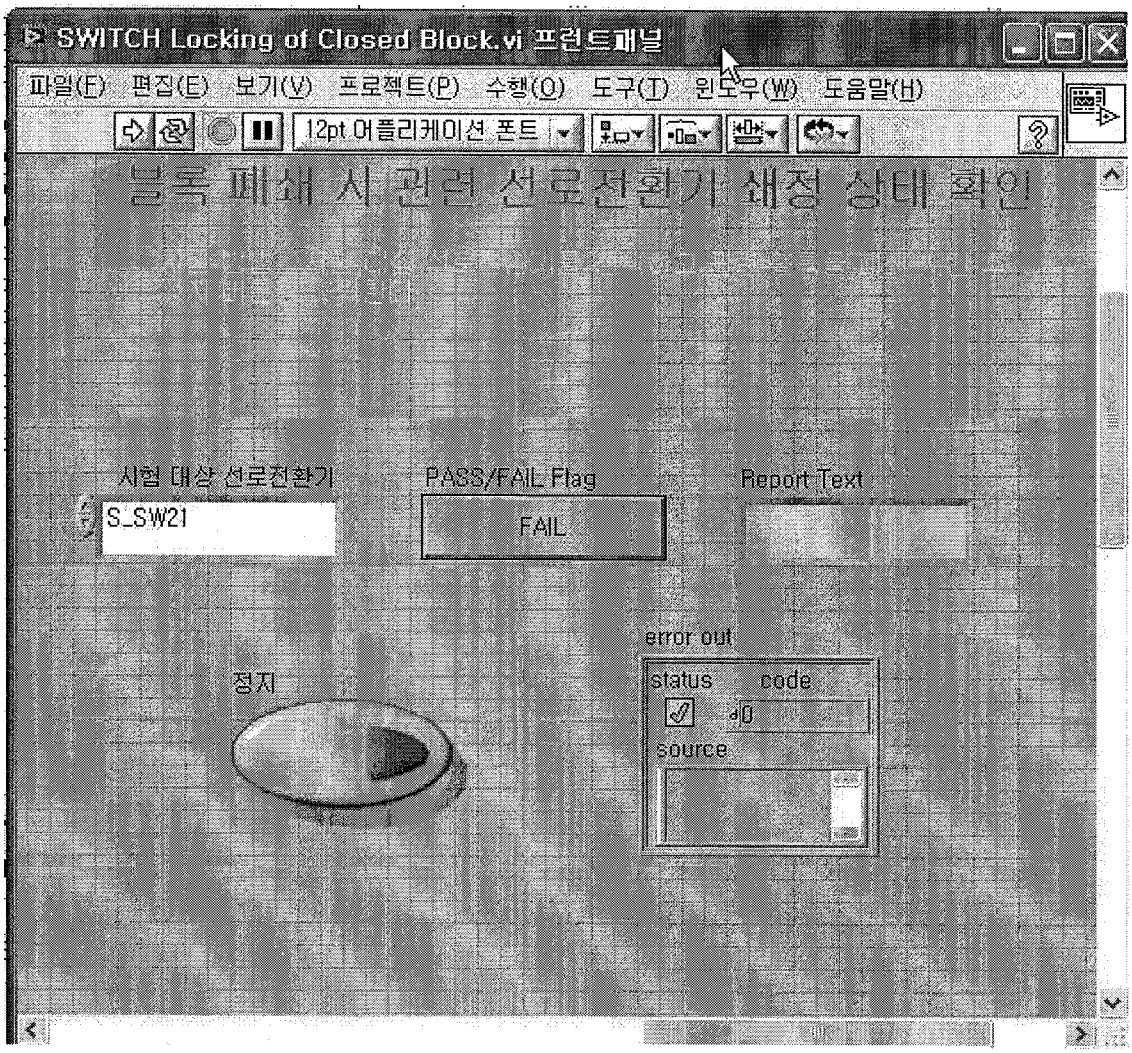
○ SWITCH Locking of Occupied Train (케이스 명: 선로전환기 관련 블록이 열차 점유 상태에서 선로전환기 전환 명령을 CRD가 수신한 경우)

- 선로전환기 포함 블록 점유 시 선로전환기 쇄정 조건을 확인
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 선로전환기 : 0 번 (S_SW21)



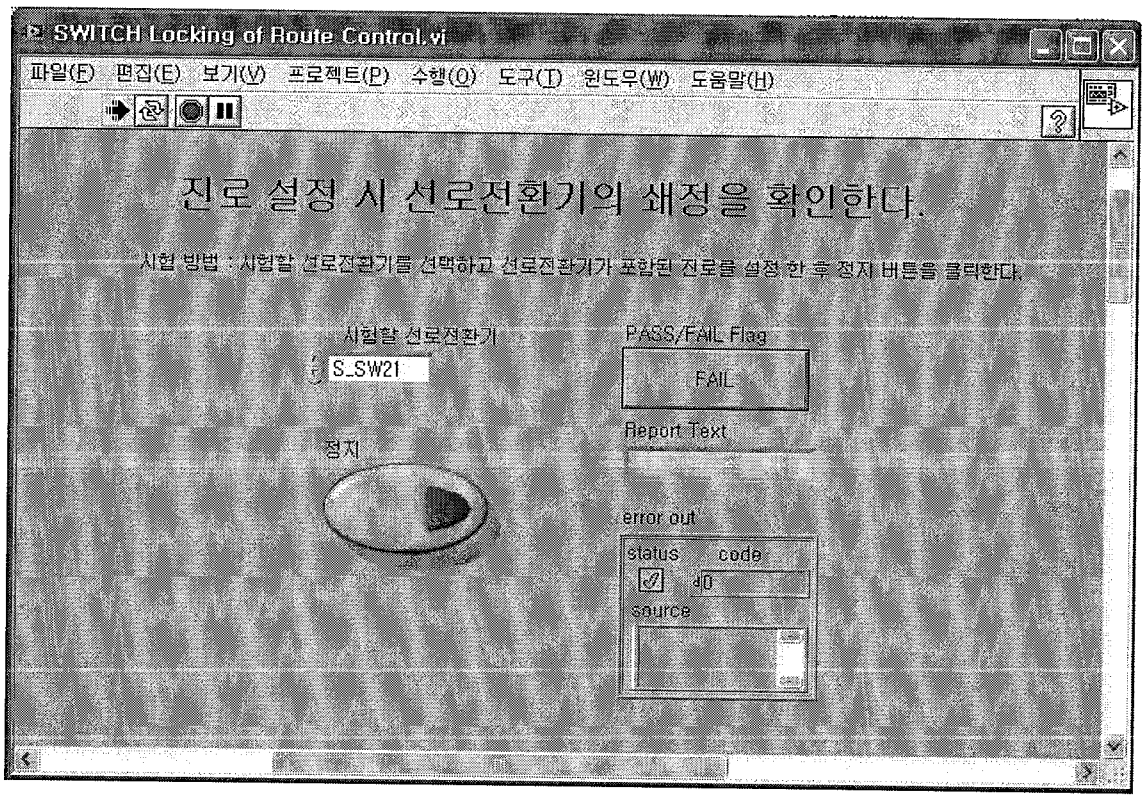
○ SWITCH Locking of Closed Block (케이스 명 : 폐쇄된 블록과 관련된 선로전환기 명령을 CRD가 수신한 경우)

- 선로전환기가 포함된 블록이 폐쇄 상태 일 경우 선로전환기 쇄정 조건을 확인
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 선로전환기 : 0 번 (S_SW21)



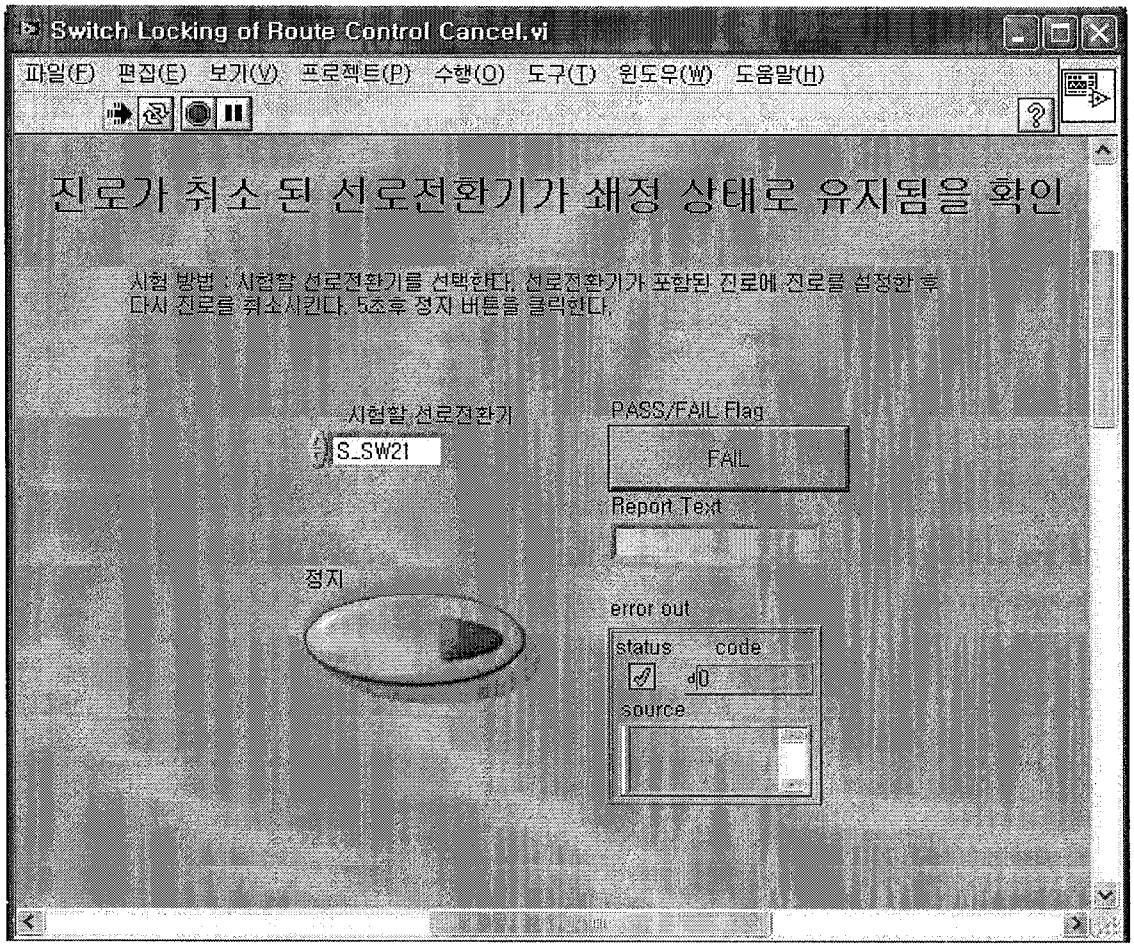
○ SWITCH Locking of Route Control(Switch Change Command) (케이스 명 : 진로가 설정된 블록의 관련 선로전환기가 전환 명령을 CRD가 수신한 경우)

- 선로전환기가 포함 된 진로를 설정 시 진로 설정이 완료 된 후 선로전환기는 쇄정 상태를 유지함을 시험한다.
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 선로전환기의 방향 : NORMAL (선로전환기의 방향이 동일하게 유지됨)



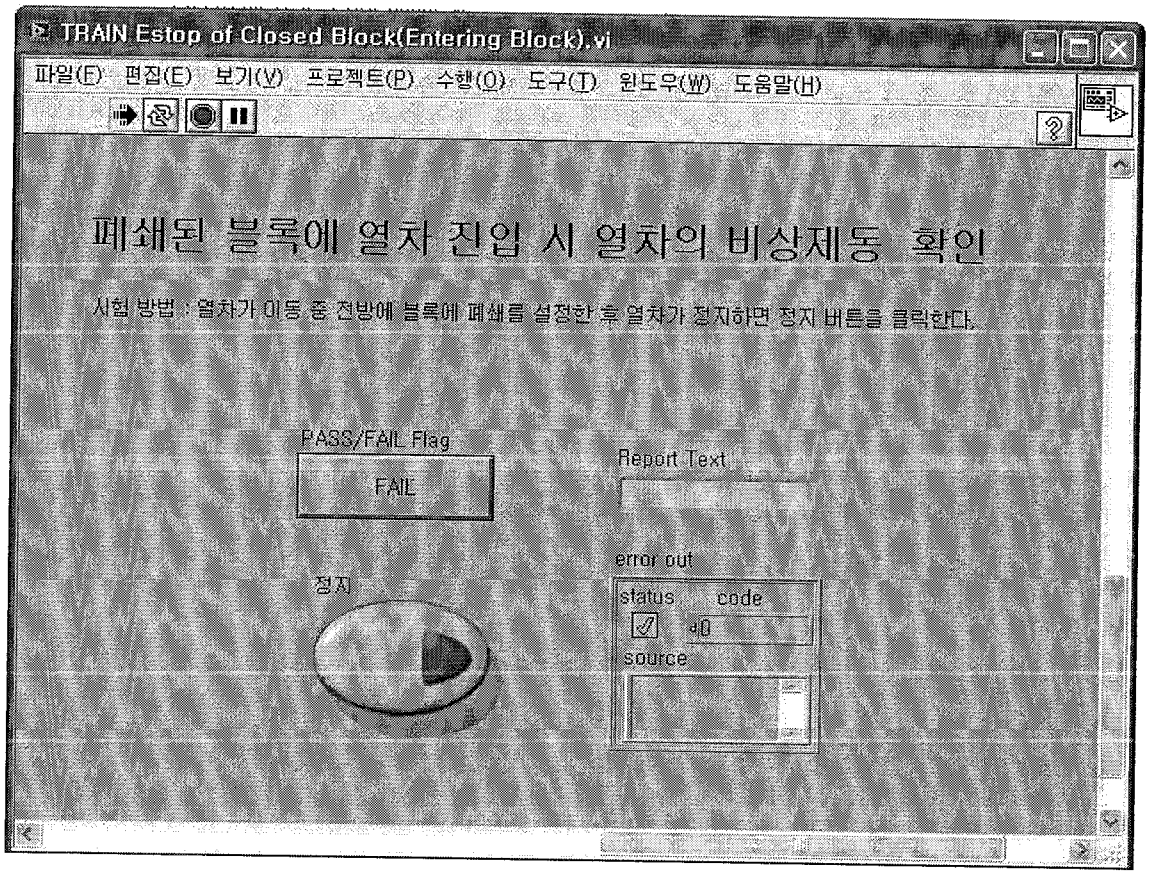
○ SWITCH Locking of Route Control Cancel (케이스 명 : 열차가 통과하지 않고 진로가 취소된 경우 CRD가 취소된 진로상의 선로전환기 전환 명령을 수신한 경우)

- 선로전환기가 포함 된 진로의 해제 시 진로 해제가 완료 된 후 180초 간 선로전환기는 쇄정 상태를 유지함을 시험한다.
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 선로전환기의 방향 : NORMAL (선로전환기의 방향이 동일하게 유지됨)



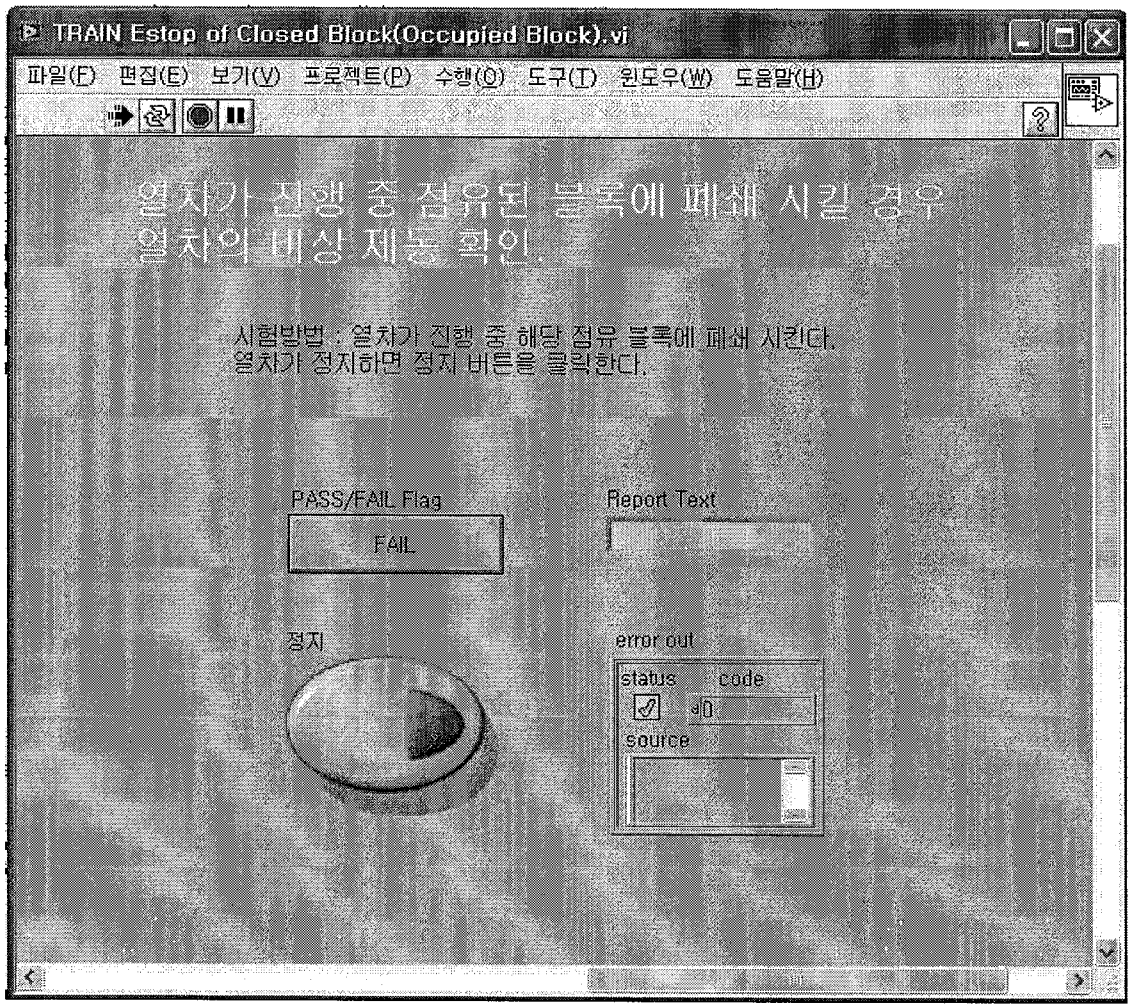
○ TRAIN Estop of Closed Block(Entering Block) (케이스 명 : 폐쇄된 블록에 열차가 진입 한 경우)

- 폐쇄된 블록에 열차가 진입한 경우 열차가 비상제동에 의해 정지해야 함을 시험
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



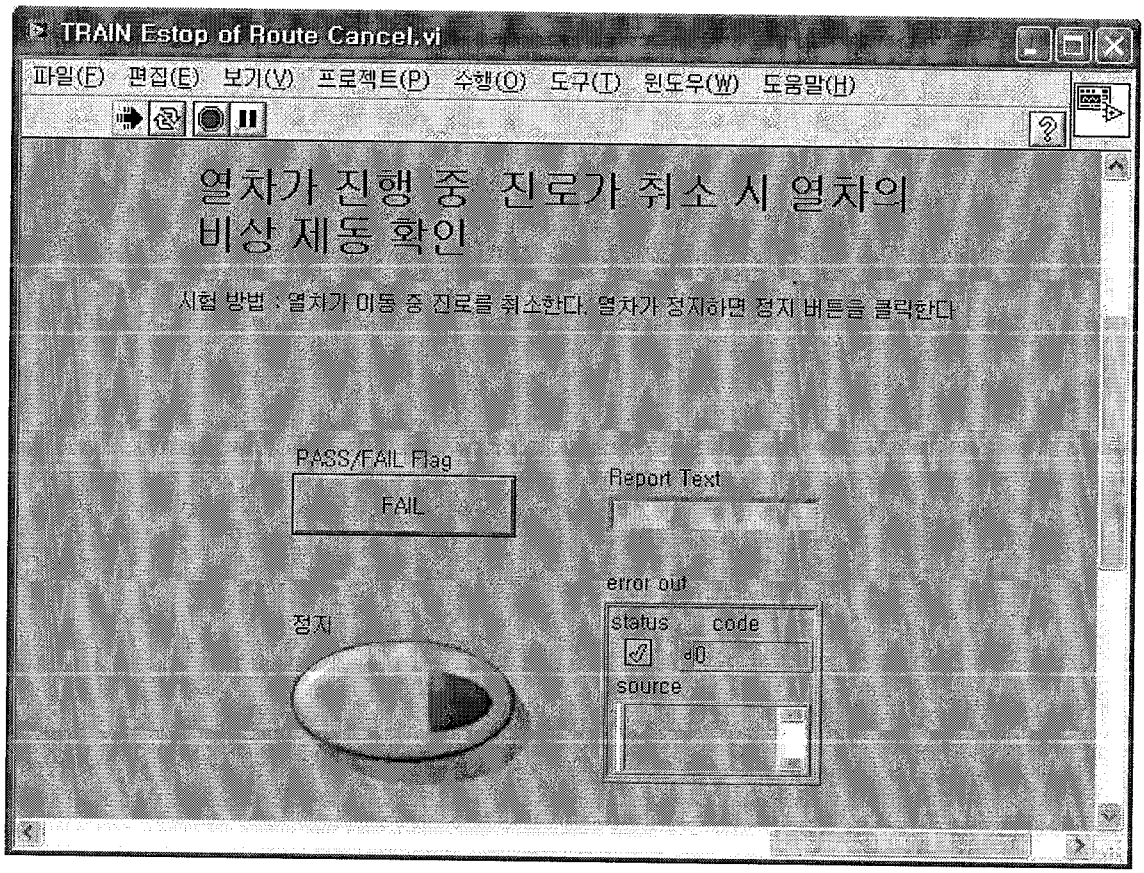
○ TRAIN Estop of Closed Block(Occupied Block) (케이스 명 : 열차가 위치한 블록에 폐쇄 명령이 수행된 경우)

- 열차가 점유 된 블록에 폐쇄한 경우 열차가 비상제동에 의해 정지해야 함을 시험
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



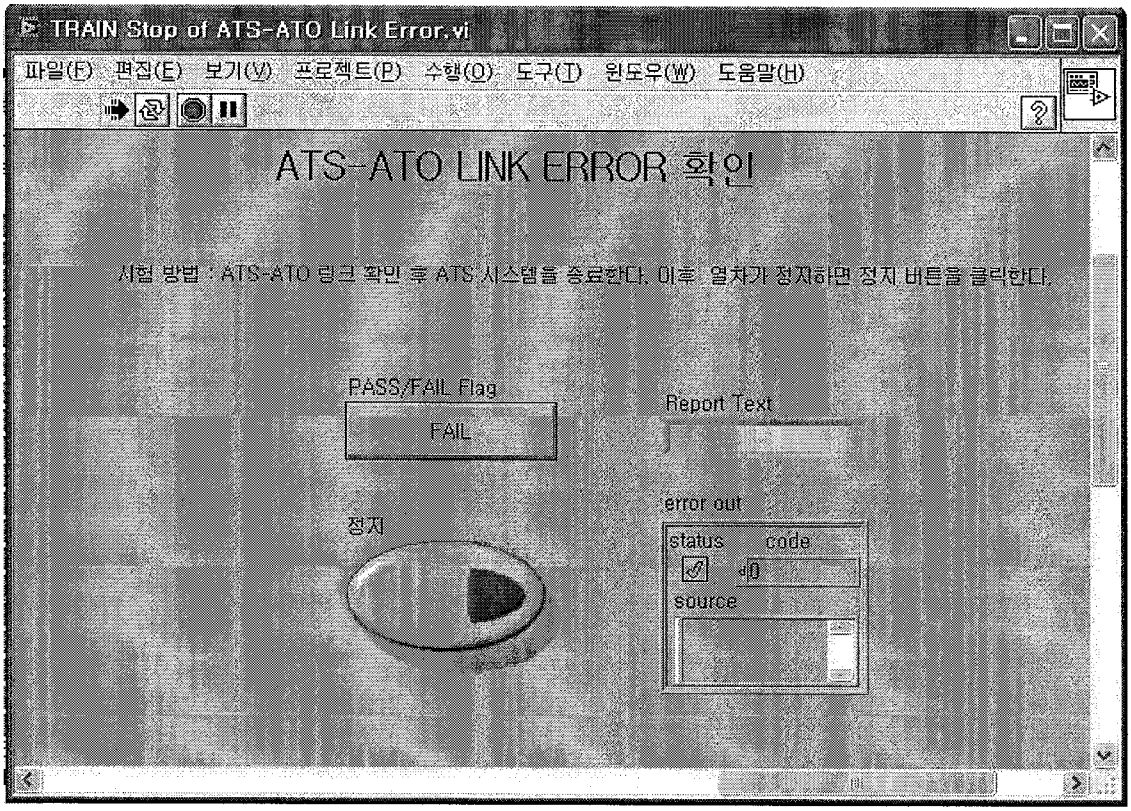
○ TRAIN Estop of Route Cancel (케이스 명 : 이동되는 열차에 대해 진로가 취소되는 경우가 발생하여 허용이동권한이 이동중인 열차에 대해 취소되는 경우)

- 열차가 진로에 의해 진행 중 진로 취소가 수행 되어 진로의 PMA에 의해 열차가 비상제동에 의해 정지해야 함을 시험
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



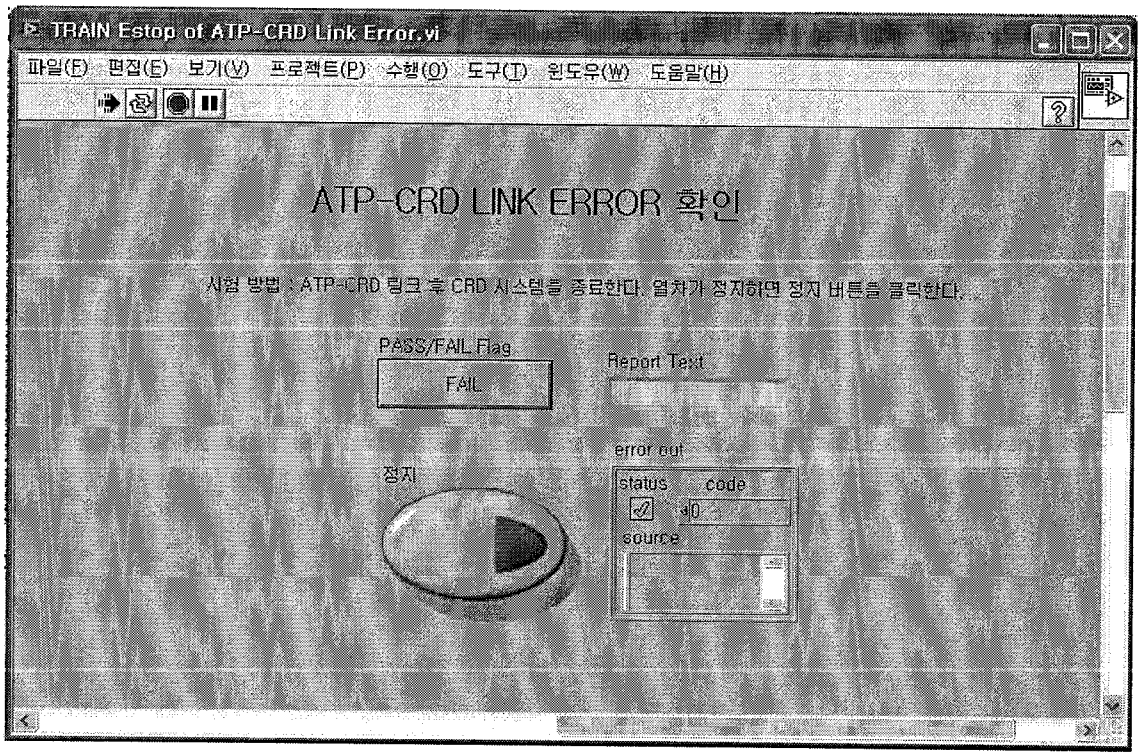
○ TRAIN Stop of ATS-ATO Link Error (케이스 명 : ATS 기능에 장애가 발생하여 차상(ATO)시뮬레이터 사이 통신 장애가 3초이상 발생할 경우)

- ATS-ATO 통신 에러에 의한 열차의 상용 제동에 의해 정지 됨을 시험
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



○ TRAIN Estop of ATP-CRD Link Error (케이스 명 : CRD 기능에 장애가 발생하여 차상 (ATP) 시뮬레이터 사이의 통신 장애가 발생할 경우)

- ATP-CRD(DCM) 통신 에러에 의한 열차의 비상제동 확인
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



○ SWITCH Break Error (케이스 명 : 선로전환기 고장이 발생된 경우)

- 선로전환기 고장이 발생한 경우 고장 처리를 하는지 확인.
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- Measurement : 1 측정 값
- Limits : Low : 1

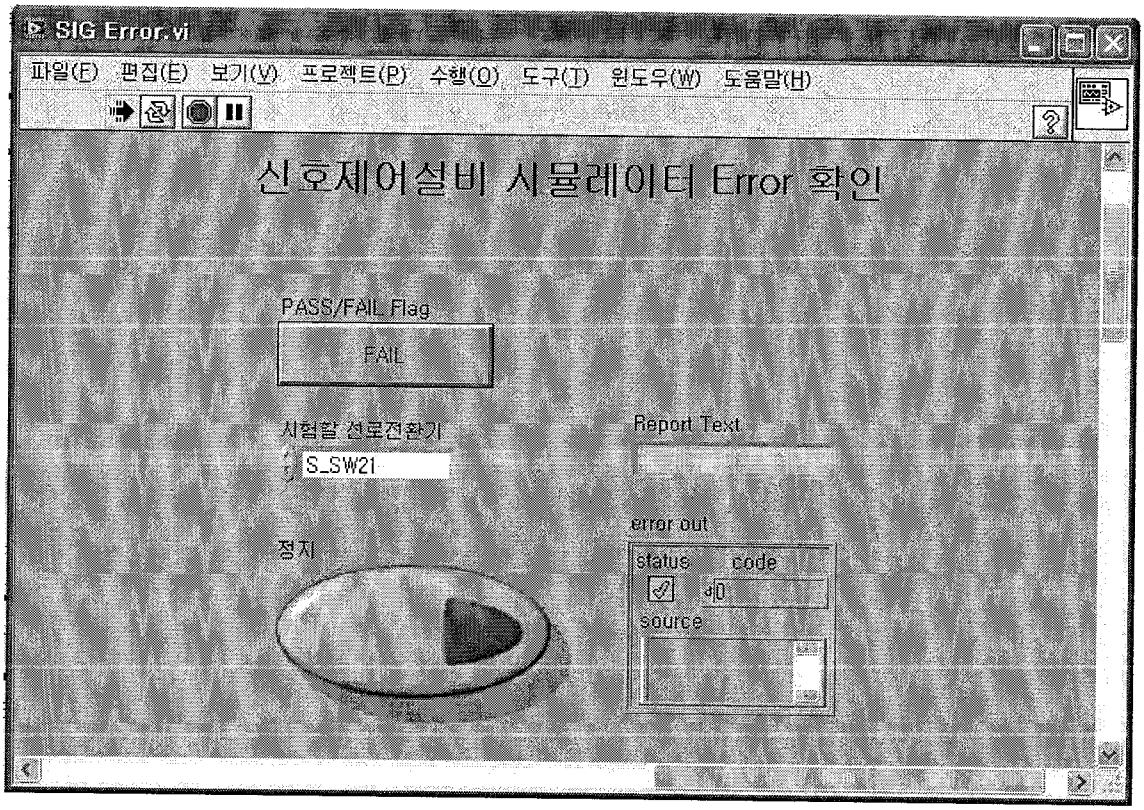
  Comparison Type : EQ(==) 같아야 함

  측정 값 과 기준이 되는 값이 같으므로 Pass가 된다.
- 결과 TEXT : 열차번호 2 (비상제동에 의해 정지된 열차 번호)



○ SIG Error (케이스 명 : 신호제어설비 시뮬레이터 기능에 장애가 발생한 경우)

- 신호제어설비 고장으로 인한 고장 처리 확인
- STATUS : 수행 결과 (PASSED : 성공 , FAILED : 실패)
- 결과 TEXT : 선로전환기 : 0 번 (S_SW21)



(3) 인터페이스

시뮬레이터는 안전성 평가용 대상 열차제어시스템에서 유기적으로 동작되어야 하며 이를 위해 안전성 평가용 대상 열차제어시스템을 구성하는 장치간 신뢰성 있는 인터페이스가 구성되어야 한다. 본 절에서는 시뮬레이터를 포함한 안전성 평가용 대상 열차제어시스템의 기능 및 성능을 구현하기 위해 장치간 인터페이스 되는 메시지와 통신흐름에 대해 설명한다.

(가) 전송 메시지

안전성 평가용 대상 열차제어시스템간 통신은 크게 네트워크 통신과 시리얼 통신으로 분류된다. 네트워크와 시리얼 통신에 사용되는 메시지 구조는 다음과 같다.

① 네트워크 통신 메시지 구조

네트워크를 통한 통신은 다음의 시스템간에 이용되며, 이중 CRD 모듈과 외부 시스템간 접속은 CRD의 EIM 모듈과 외부시스템과의 물리적인 접속이 이루어진다. 즉, EIM은 ICM, DCM으로부터 정보를 수신하여 이 정보를 외부시스템으로 전송시

키고, 외부 시스템으로부터 수신한 정보를 ICM, DCM으로 다시 전송해주는 중간 인터페이스의 역할을 수행한다. 따라서 외부시스템으로의 전송정보 생성과 외부시스템으로부터의 수신정보 처리는 EIM에서 수행되는 것이 아니라 ICM, DCM에서 수행된다.

- CRD(ICM - EIM) ⇔ ATS 시뮬레이터
- CRD(DCM - EIM) ⇔ ATS 시뮬레이터
- CRD(DCM - EIM) ⇔ 차상 시뮬레이터(ATP)
- CRD(ICM - EIM) ⇔ 신호설비제어 시뮬레이터
- ATS 시뮬레이터 ⇔ 차상 시뮬레이터(ATO)

표 3.6.24 네트워크 통신 메시지 구조

영역	필드	바이트 수
HEADER	수신자 클래스	1 Byte
	수신자 ID	1 Byte
	송신자 클래스	1 Byte
	송신자 ID	1 Byte
	수신자 Sequence 번호	2 Byte
	송신자 Sequence 번호	2 Byte
	Data Length	2 Byte
DATA	Data	1 ~ 1024 Byte
CHECK SUM	CRC 16	2 Byte

네트워크 통신 메시지 구조는 표 3.6.24과 같이 헤더 부분과 데이터 부분으로 크게 구성되도록 설계하였으며, CRC-16 코드를 에러검지 코드로 사용하였다. 헤더부분은 송수신자 클래스와 ID, 데이터 필드 길이 그리고 시컨스 번호 필드로 구성되도록 하였다. 이 중 송수신자 클래스는 시스템간 통신 시스템의 식별을 위해 사용된다. 즉, 각각의 시스템은 정보를 수신해서 송신자 또는 수신자 클래스가 자신의 시스템 클래스와 일치하는 경우에만 정보를 처리하고, 그 외의 정보는 처리한지 않는다. 데이터 필드는 실제 전송할 정보의 내용을 포함하는 필드로서, 모든 데이터 영역 내에서 1 바이트 이상으로 구성된 데이터는 처음 전송된 바이트가 최상위 바이트(MSB : Most Significant Byte)이고 마지막으로 전송된 바이트가 최하위

Byte(LSB : Least Significant Byte)다. CRC-16 코드는 '$X^{16} + X^{15} + X^2 + 1$' 코드를 적용하였다.

② 시리얼 통신 메시지 구조

시리얼 접속 또는 VME 버스, PCI 버스를 통한 통신을 위한 메시지 구조를 정의하며 다음의 시스템 간에 이용된다. 다음의 접속 중 ICM과 EIM간, DCM과 EIM간 접속은 ICM이나 DCM에서 EIM을 통해 이루어지는 외부시스템과의 접속이 아닌 ICM, DCM과 EIM간 상호상태정보를 전송하기 위한 접속을 가리킨다.

- ICM ⇔ DCM간(시리얼 통신)
- EIM(1계) ⇔ EIM(2계)간(시리얼 통신, 상태정보 전송 시)
- ICM ⇔ EIM간(VME BUS, 상태정보전송 시)
- DCM ⇔ EIM간(VME BUS, 상태정보전송 시)

표 3.6.25 시리얼 통신 메시지 구조

영역	필드	바이트 수
HEADER	STX	1 Byte
	LENGTH	1 Byte
	SEQUENCE 번호	1 Byte
	TYPE	1 Byte
DATA	DATA	1 ~ 1024 Byte
CHECK SUM	CRC 16	2 Byte

시리얼 통신의 메시지 구조는 표 3.6.25 같으며, 이 전송 프레임도 앞에서와 마찬가지로 헤더 부분과 데이터 필드 부분으로 구성되며 CRC-16 코드를 적용하였다.

③ 메시지 종류

앞 절에서 설명한 프로토콜 기반으로 각 장치들간 전송되는 메시지들의 주요 내용은 다음과 같다.

○ ICM ⇔ ATS시뮬레이터간 메시지

표 3.6.26 ICM ⇔ ATS 시뮬레이터간 메시지 종류

종류	내용	Source	Destination
ICM요구정보	ICM요구정보는 POLL 메시지로서 ATS시뮬레이터가 ICM으로 전송할 Real 메시지(명령)가 없을 경우 ICM에게 ICM정보를 수신하기 위하여 전송하는 메시지	ATS 시뮬레이터	ICM
현장신호설비 제어명령	현장신호설비제어명령은 ATS시뮬레이터가 현장신호설비를 제어하기 위해 ICM으로 전송하는 메시지 - 진로요청/취소 명령 - 선로전환기 전환 명령	ATS 시뮬레이터	ICM
CRD계절체 명령	CRD 계절체명령은 CRD 계절체를 위해 ATS시뮬레이터가 CRD로 전송하는 메시지	ATS 시뮬레이터	ICM(EIM)
ICM정보	ICM정보는 ATS시뮬레이터로부터의 ICM요구정보와 현장신호설비제어명령에 대한 응답메시지로서 ICM이 관리하는 정보를 전송	ICM	ATS 시뮬레이터

○ DCM ⇔ ATS 시뮬레이터간 메시지

표 3.6.27 DCM-ATS시뮬레이터간 메시지 종류

종류	내용	Source	Destination
DCM요구정보	DCM요구정보는 POLL 메시지로서 ATS시뮬레이터가 DCM으로 전송할 Real 메시지(명령)가 없을 경우 DCM에게 DCM정보를 수신하기 위하여 전송하는 메시지	ATS 시뮬레이터	DCM
블록제어명령	특정 또는 모든 블록을 개방/폐쇄하기 위한 메시지	ATS 시뮬레이터	DCM
임시속도제한 명령	특정 또는 모든 블록에 임시속도를 지정/해제 하기 위한 메시지	ATS 시뮬레이터	DCM
DCM정보	DCM정보는 ATS시뮬레이터로부터의 DCM요구정보와 제어명령에 대한 응답메시지로서 DCM이 관리하는 정보를 전송	DCM	ATS 시뮬레이터

○ DCM ⇔ 차상 시뮬레이터(ATP)간 메시지

표 3.6.28 DCM-차상시뮬레이터(ATP)간 메시지 종류

종류	내용	Source	Destination
PMA정보	PMA정보는 POLL 메시지로서 DCM이 차상시뮬레이터(ATP)로 전송하는 메시지	DCM	차상시뮬레이터(ATP)
열차정보	PMA정보에 대한 열차상태 응답메시지	차상시뮬레이터(ATP)	DCM

○ ATS 시뮬레이터 ⇔ 차상 시뮬레이터(ATO)간 메시지

표 3.6.29 ATS시뮬레이터-차상시뮬레이터(ATO)간 메시지 종류

종류	내용	Source	Destination
POLL메시지	ATS시뮬레이터가 차상시뮬레이터(ATO)로 전송할 Real 메시지(명령)가 없을 경우 전송하는 메시지	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차운행제어명령	열차운행 정지명령은 열차를 정지시키기 위해 직접적으로 차상시뮬레이터(ATO)에 상용제동을 가하도록 하는 명령어이며, 열차운행 출발명령은 열차를 다시 진행하게 하는 명령	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차출입문제어명령	열차의 출입문을 개방 또는 폐쇄 하기 위한 메시지	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차비상제동해지명령	비상제동 해지 명령은 열차의 비상제동을 해지하는 명령으로 차상시뮬레이터(ATO)가 차상시뮬레이터(ATP)로 비상제동 해지명령을 요청하도록 하기 위한 명령어	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차운행속도제어명령	열차의 속도제한 범위 내에서 Percent(%) 형태로 열차의 서비스 속도를 제어하기 위한 메시지며, 서비스 속도의 조절은 시스템의 속도 한계치를 초과하지 말아야 함	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차목적지제어명령	열차가 운행방향으로 진행할 수 있도록 열차의 다음 목적지와 최종 목적지를 지시하는 메시지. 차상시뮬레이터(ATO)는 열차가 승강장에 도착하면 다음 목적지와 최종 목적지 정	ATS 시뮬레이터	차상시뮬레이터(ATO)

	보를 Update.		
플랫폼대기명령	승강장에 열차를 대기시키기 위한 명령어	ATS 시뮬레이터	차상시뮬레이터(ATO)
플랫폼정차시간제어명령	현재 설정된 정차시간을 전송하는 메시지며, 열차가 승강장에 도착할 때 단 한번만 열차 정차에 적용. 따라서, 일반적으로 열차가 승강장에 도착할 때 마다 명령이 전송	ATS 시뮬레이터	차상시뮬레이터(ATO)
플랫폼상태제어명령	차상시뮬레이터(ATO)의 내부 승강장 리스트에서 승강장 상태를 변경하게 하는 메시지	ATS 시뮬레이터	차상시뮬레이터(ATO)
열차ATO정보	차상시뮬레이터(ATO) 상태 메시지며, ATS시뮬레이터에서 전송된 Poll 메시지나 다른 제어 메시지에 대한 응답 메시지	차상시뮬레이터(ATO)	ATS 시뮬레이터

○ ICM ⇔ 신호설비제어 시뮬레이터간 메시지

표 3.6.30 ICM-신호설비제어시뮬레이터간 메시지 종류

종류	내용	Source	Destination
POLL 메시지	ICM이 신호설비제어 시뮬레이터로 전송할 Real 메시지(선로전환기 전환명령)가 없을 경우 전송하는 메시지	ICM	신호설비제어 시뮬레이터
선로전환기 전환명령	특정 선로전환기를 전환시키기 위한 메시지	ICM	신호설비제어 시뮬레이터
선로전환기 상태정보	ICM으로부터의 폴링 메시지나 선로전환기 전환명령에 대한 응답메시지로서 신호설비제어 시뮬레이터가 관리하는 선로전환기의 상태를 전송	신호설비제어 시뮬레이터	ICM

(나) 통신흐름

시뮬레이터를 포함한 안전성평가용 대상 열차제어시스템에서 이루어지는 인터페이스를 수행하기 위한 통신흐름에 대해 정의한다.

① 통신 개시

시뮬레이터를 포함한 안전성 평가용 대상 열차제어시스템에서 네트워크를 통한 시스템간 통신의 경우 CMI(Communication Initiator) 시스템에 의해 시작되며

CMR(Communication Receiver) 시스템의 응답에 의해 통신이 유지된다. CMI 시스템은 RFC(Request For Communication) 메시지를 생성하여 CMR 시스템에 전송하고 CMR 시스템은 최초 RFC메시지를 수신하면 CMI 시스템을 폴링함으로써 시스템간 통신이 개시된다. CMI 시스템은 CMR 시스템에 의해 폴링될 때까지 RFC 메시지를 주기적으로 CMR 시스템에 전송한다. 시뮬레이터를 포함한 안전성평가용 대상 열차제어시스템에서의 CMI, CMR 시스템과 RFC 메시지는 다음 표와 같다.

표 3.6.31 시스템간 통신개시에 따른 장치/메시지 구분과 Polling주기

CMI 시스템	CMR 시스템	RFC 메시지	Polling	Polling주기
CRD(ICM)	ATS시뮬레이터	ICM 정보	ICM 요구정보	500ms
CRD(DCM)	ATS시뮬레이터	DCM 정보	DCM 요구정보	500ms
차상(ATP) 시뮬레이터	CRD(DCM)	열차정보	PMA 정보	400ms
차상(ATO) 시뮬레이터	ATS시뮬레이터	열차정보	Polling	500ms
신호설비제어 시뮬레이터	CRD(ICM)	선로전환기 상태정보	선로전환기 상태요구명령	500ms

② 송수신자 시컨스 번호 관리

CMI와 CMR 시스템간의 메시지에는 수신자와 송신자 Sequence 번호를 포함하게 되며, 각자 자신의 송신자 Sequence 번호를 생성하여, 메시지를 전송할 때 마다 자신의 송신자 Sequence 번호를 증가 시켜 전송한다. 수신자 Sequence 번호는 상대 시스템으로부터 수신 받은 메시지 내에 포함된 송신자 Sequence 번호를 의미한다. CMI 와 CMR 시스템 간에 통신이 확립되지 않았을 경우에는 CMI 시스템은 통신 확립을 위한 최초 RFC메시지를 전송하게 되며 이때는 아직 수신자 Sequence 번호를 모르기 때문에, 수신자 Sequence 번호를 "0"(null)으로 하여 전송한다. 이와 같이 CMI와 CMR 시스템 간 통신이 확립되기 전에 CMI가 CMR시스템으로 수신자 Sequence 번호를 null로 하여 전송하는 메시지를 RFC 메시지라고 정의한다. RFC 메시지의 수신자 Sequence 번호는 반드시 null 이어야 하며, null 이 아닌 경우는 Sequence 번호 실패의 경우로 처리된다.

CMR 시스템은 송신자 Sequence 번호가 포함되어 전송된 RFC 메시지에 대한

응답으로 CMI 시스템이 전송한 송신자 Sequence 번호를 수신자 Sequence 번호에 실어서 CMI 시스템으로 전송한다. CMI 시스템은 CMR 시스템으로부터의 폴링 정보에 자신이 전송한 Sequence 번호를 확인하면 통신이 확립된 것으로 간주한다. 이 때 CMI 시스템은 RFC메시지 전송을 중지하고 자신의 Sequence 번호를 증가시키고 CMR로부터 수신한 Sequence 번호를 수신자 Sequence 번호에 실어서 전송한다. CMR 시스템은 CMI 시스템으로부터의 정보에 자신이 전송한 Sequence 번호를 확인하면 통신이 확립된 것으로 간주한다.

이와 같이 CMI 와 CMR 시스템은 메시지를 보낼 때 마다 자신의 송신자 Sequence 번호를 증가시킨다. 시스템 간 통신이 확립되면, 각 시스템은 이전 메시지의 승인 여부에 상관없이 매 전송 시에 자신의 송신자 Sequence 번호를 증가시킨다. 송수신되는 시컴스 번호의 관리는 다음 그림과 같다.

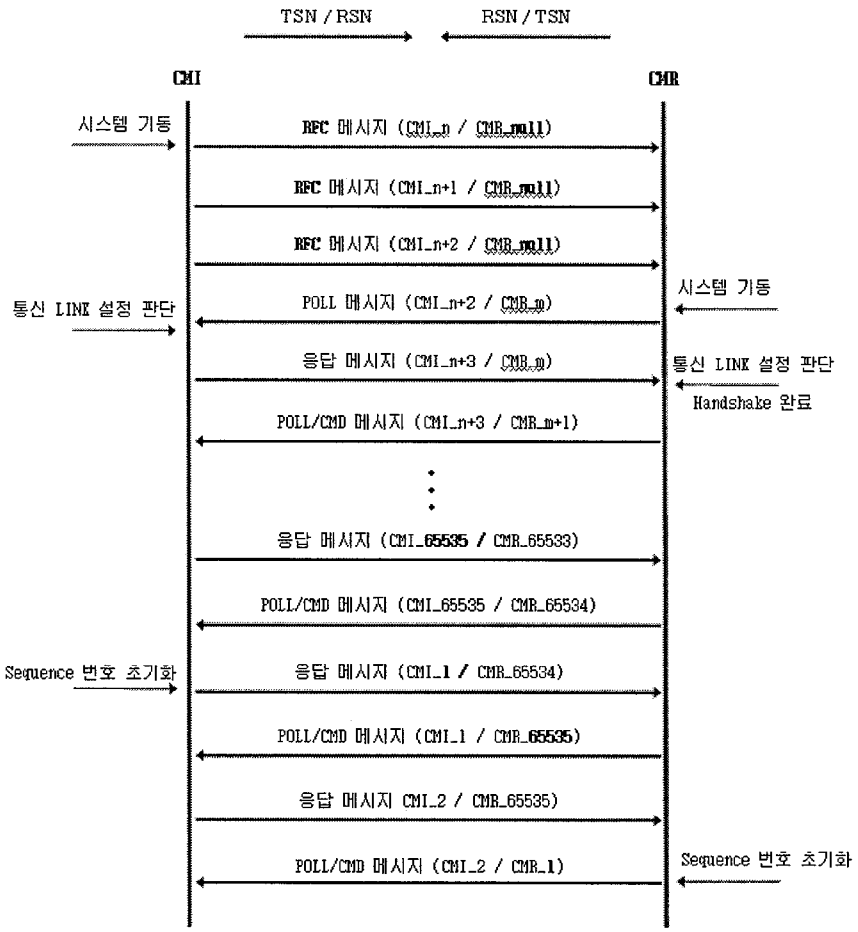


그림 3.6.18 CMI와 CMR 사이의 시컨스 번호 관리

(4) 인터페이스 시험

시뮬레이터를 포함한 안전성 평가용 대상 열차제어시스템의 인터페이스 시험은 작성되어진 시험절차서에 의해 하도록 한다. 인터페이스를 위한 시험절차서에는 다음 항목과 같은 구조로 작성하였다.

- 시험 목적
- 시험 필요사항
- 시험(초기) 조건
- 시험 순서, 시험자 기록 사항
- 시험 범위
- 시나리오별 시험 절차, 예상 결과, 확인
- 시나리오별 시험케이스와 내용, 단계, 결과

본 절에서 설명하는 인터페이스 시험을 위한 시험절차서는 다음과 같은 여러 인부분에 대한 작성되었으며, 본 보고서에는 이 중 "ATS 시뮬레이터 ⇔ CRD(ICM) 인터페이스 시험" 하나만 포함하였다. 나머지 인터페이스 시험도 이와 같은 형태로 시험절차서가 당해 연도 연구를 통해 작성되었다.

- ATS 시뮬레이터 ⇔ CRD(ICM) 인터페이스
- ATS 시뮬레이터 ⇔ CRD(DCM) 인터페이스
- ATS 시뮬레이터 ⇔ 차상 시뮬레이터(ATO) 인터페이스
- 차상 시뮬레이터(ATP) ⇔ CRD(DCM) 인터페이스
- 신호설비제어 시뮬레이터 ⇔ CRD(ICM) 인터페이스

■

시험 목적 :		
ATS ⇔ CRD(ICM)과 통신연결 조건 및 상태를 확인한다.		
시험 필요 사항 :		
- *동작중인 CRD 시스템* - *동작중인 ATS 시뮬레이터*		
초기 조건 :		*확인 √*
01	*시스템은 하드웨어 결함이 전혀 없다.*	

시험 순서 :

ATS 시뮬레이터 실행을 시켜 메시지 수신 대기 상태에서 CRD 시스템이 시작되면 CRD(ICM)에서 RFC메시지를 전송한다. 이후 시퀀스 넘버가 증가하며 핸드쉐이크 하듯 메시지를 주고 받는다.	
시험자 기록 사항 :	
01	이 시험은 모든 시험 케이스의 선행 조건이다.
02	
03	
04	

시험 범위 :

이 절차는 다음의 시험 케이스를 검증한다.

시험 시나리오 :

1) 통신 초기 연결 조건을 확인한다.
2) 통신 초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류 처리를 확인한다.
3) ATS 시뮬레이터 응답 미처리 시 반응을 확인한다.
4) CRD(ICM)의 응답 미처리시 반응을 확인한다.
5) 시퀀스 오류 시 반응을 확인한다.
6) 통신실패 처리를 확인한다.

시나리오 01: 통신 초기 연결 조건을 확인한다.			시험케이스 목록 TestCase 01-12
1.1	ATS 시뮬레이터 프로그램을 실행한다.		이 단계는 관제설비 로그인 절차 단계를 수행한다.
1.2	CRD(ICM) 시스템을 실행한다.	CRD(ICM) 시스템에서 초기 연결 조건의 RFC메시지를 주기적으로 전송한다.	
1.3	ATS 시뮬레이터에서 RFC 메시지 확인 후 시퀀스 넘버 증가 후 Poll 메시지를 전송한다.		
1.4	CRD(ICM)시스템에서 Poll 메시지 수신 후 진로예약정보, 선로전환기 상태정보 등을 전송한다.	주기적으로 폴링 메시지 수신되고, 진로정보 선로전환기정보를 송신한다.	
시나리오 02: 통신 초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류 처리를 확인한다.			
2.1	ATS 시뮬레이터 프로그램을 실행한다.		이 단계는 관제설비 로그인 절차 단계를 수행한다.
2.2	CRD(ICM)시스템에서 RFC	ATS 시뮬레이터는 통신 실	

	메시지를 전송한다.	패로 간주하고,3 초간 연결을 중단한다.	
2.3	CRD(ICM) 시스템에서 RFC메시지를 재전송한다.	ATS 시뮬레이터는 RFC메시지를 확인하고 폴링 메시지를 전송한다.	
2.4	CRD(ICM)시스템에서 Poll 메시지를 수신하면, 진로 정보, 선로전환기 상태 정보를 전송한다.	이후 주기적으로 메시지를 주고 받는다.	
시나리오 03: ATS 시뮬레이터 응답 미처리 시 반응을 확인한다.			
3.1	ATS 시뮬레이터에서 명령메시지를 전송한다.		
3.2	CRD(ICM) 시스템에서 응답메시지를 전송한다.		
3.3	ATS 시뮬레이터에서 응답메시지를 수신되지 않아 처리가 되지 않았다.		
3.4	ATS 시뮬레이터에서 이전 수신자 시퀀스 넘버와 송신자 시퀀스 넘버에 1을 증가시켜 재전송한다.		
시나리오 04: CRD(ICM)의 응답 미처리시 반응을 확인한다.			
4.1	ATS 시뮬레이터에서 명령메시지를 전송한다.		
4.2	CRD(ICM)시스템에서 ATS 시뮬레이터 명령메시지를 수신하지 못하였다.		
4.3	ATS시뮬레이터에서 송신자 시퀀스 넘버를 1증가시켜 재전송한다.		
4.4	CRD(ICM) 시스템에서 메시지를 처리한다.		
시나리오 05: 시퀀스 오류 시 반응을 확인한다.			
5.1	ATS 시뮬레이터에서 명령메시지를 전송한다. (수신자 시퀀스 넘버 오류발생)		
5.2	CRD(ICM) 시스템에서 시퀀스 오류 탐지 후 본래 시퀀스 넘버로 응답한다.	연속 3회 이상 시퀀스 오류를 발견하면, 3초간 통신을 중단한다.	
5.3	CRD(ICM) 시스템에서 RFC메시지를 생성하여 ATS시뮬레이터로 전송한다. (수신자 시퀀스 넘버는 '0'이		

	다)		
5.4	ATS 시뮬레이터에서 RFC 메시지를 확인하여 명령(Poll)메시지를 전송한다.	주기적으로 폴링 전송 후 응답 메시지를 수신하면 재 연결 상태가 된다.	

상세 시험 케이스 목록 : 시험 케이스의 완성된 목록은 실행된 각 단계의 시험 케이스에 작성된 결과표와 함께 상기 절차를 검증한다.

시험 케이스	시험 케이스 내용	단계 x.1	단계 x.2	단계 x.3	단계 x.4	양호/불량		비 고
시나리오 01: 통신초기 연결조건을 확인한다.								성공적으로 수행된 단계의 각각의 항목에 체크마크 (✓)를 표시하고 실패한 단계에는 "X"를 표시한다. 만약 한 시험 케이스의 모든 단계가 통과되었으면, 시험 케이스의 양호/불량란에서 "P"에 원을 그린다. 만약 한 시험 케이스의 하나 이상의 단계가 실패했으면, 시험 케이스의 양호/불량란에서 "F"에 원을 그리고, 여기에 해당하는 SCR 번호를 적는다.
01	ATS-CRD(ICM)	✓	✓	✓	✓	P	F	
시나리오 02: 통신초기 연결 시 RFC 메시지의 시퀀스 넘버의 오류처리를 확인한다.								
04	ATS-CRD(ICM)	✓	✓	✓	✓	P	F	
시나리오 03: ATS 시뮬레이터 응답 미처리 시 반응을 확인한다.								
07	ATS-CRD(ICM)	✓	✓	✓	✓	P	F	
시나리오 04: CRD(ICM)의 응답 미처리 시 반응을 확인한다.								
10	ATS-CRD(ICM)	✓	✓	✓	✓	P	F	
시나리오 05: 시퀀스 오류 시 반응을 확인한다.								
13	ATS-CRD(ICM)	✓	✓	✓	✓	P	F	

■

제7절 고안전성 연산제어 시스템 개발

	검증계획서 (Verification Plan)	**ID No :** TC - SR05 - SSR02 - 2010 작성일 : 2010. 05. 14 수정일 :

5. 프로젝트는 열차제어시스템 안전향상 핵심기술을 개발하여야 한다

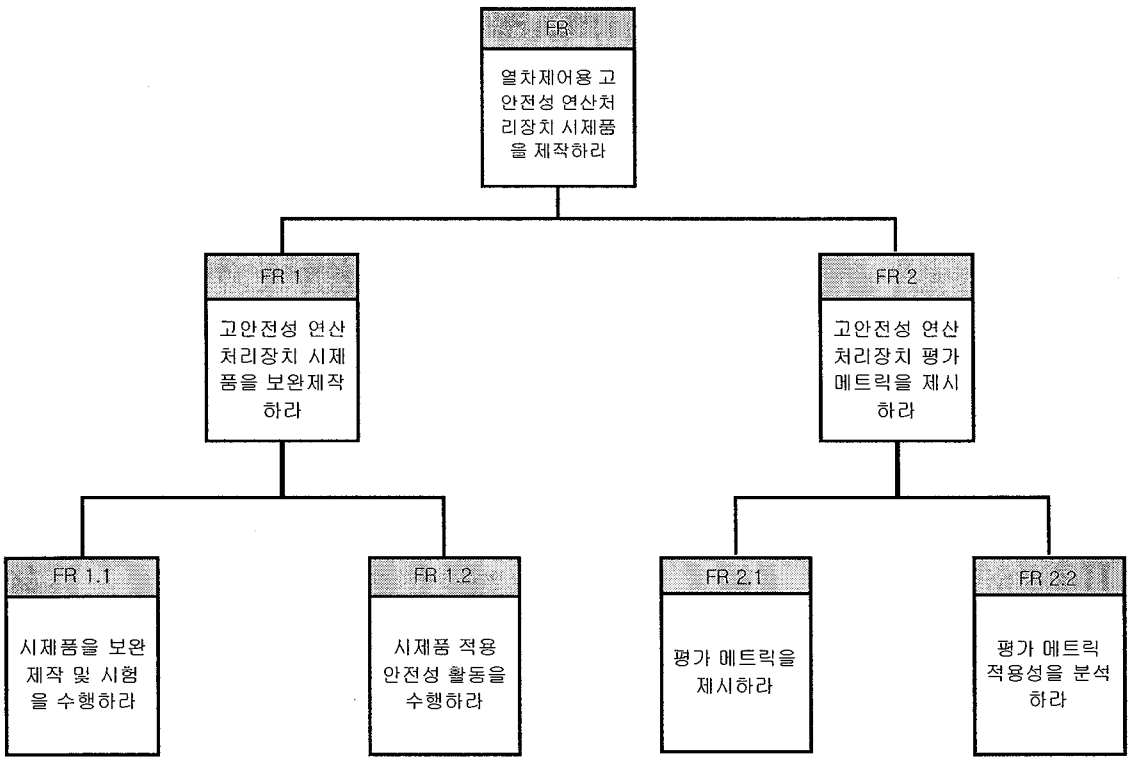
5.2 프로젝트는 열차제어시스템을 위한 고안전성 연산제어 시스템 기술을 개발하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 열차제어용 고안전성 연산제어 시스템 보완 및 제작 - 타사 고안전성 연산제어시스템 조사 - 시스템 평가 메트릭 ☐ **검증 방법** - 1.2 외국자료와 비교, 2.1 단순 상황분석, 2.2 공학적 해석	- SE 검증	- 수정 VRTM - 검증결과표

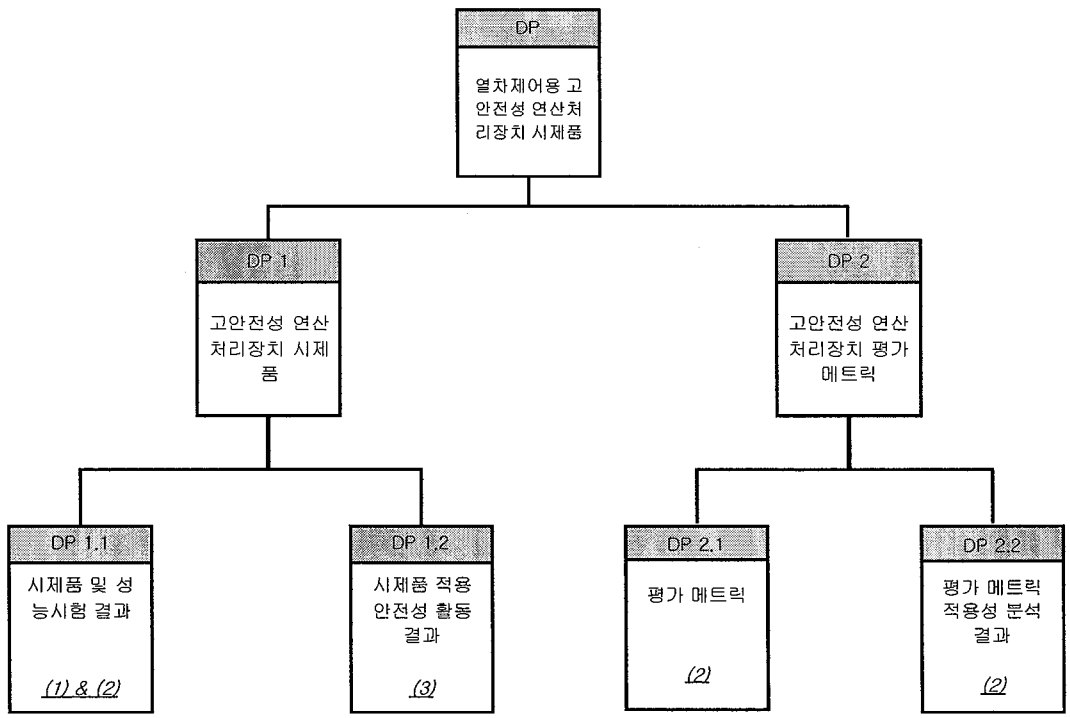
Verification Specification (검증기준) :

1. 고안전성 연산처리장치의 시제품이 보완되었는가?
2. 시제품의 성능시험이 수행되었는가?
3. 열차제어용 고안전성 연산처리장치 평가 메트릭이 제시되었는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

열차제어용 고안전성 연산제어 시스템 구성안 제시 및 설계 문서 작성은 시스템 요구사항 『SR 5. 프로젝트는 열차제어시스템 안전향상 핵심 기술을 개발하여야 한다.』 중 『SSR. 5.2. 프로젝트는 열차제어시스템을 위한 고안전성 연산제어 시스템 기술을 개발하여야 한다.』에 해당하는 내용이다. 당해 연도는 전년도에 개발한 열차제어용 고안전성 연산처리 시스템의 안전성을 높이기 위해서 시스템을 보안 제작하였고, 보완된 시스템의 성능확인을 위해 테스팅 프로그램을 이용하여 성능시험을 진행하였다. 또한 보완된 시스템의 성능시험 결과와 유사한 타 시스템의 분석 등을 통해 고안전성 연산제어 시스템의 평가 메트릭을 도출하였고, 마지막으로 고안전성 연산제어시스템의 안전성 활동의 기본 내용을 수행하였다.

나. 설계기준

- Patrick C. Aremett and Don MaCown, "TMR and Squeeze at Gifabit Areal Densities", IEEE : Transations on Magnetics, (July 1992)
- M.Hassner and J.Mortelmans, "Exponential Series Statistical Modeling of Track Misregistration Noise in Magnetic Storage Channels". IEEE : Transations on Magnetics, (July 1992)
- Jia Di, "A Framework on Mitigating Single Event Upset using Delay-Insensitive Asynchronous Circuits", IEEE : Region 5 Technical Conference, (April 2007)
- Mojtaba Valinataj and Saeed Safari, "Fault Tolerant Arithmetic Operations with Multiple Error Detection and Correction", 22nd IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems
- Fred H. Hardie and Robert J. Suhocki, "Design and Use of Fault Simulation for Saturn Computer Design", IEEE : Transations on Electronic Computers, (August 1967)
- S.J. Bavuso, "Advanced Reliability Modeling of Fault Tolerant Computer

Based Systems", NATO Advanced Study Institute Presentation, (1982)
- J. Lara, "Advanced Information Processing System", AIAA/IEEE 6th Digitel Avionics Conference Proceedings, (December 3, 1984)
- L.A. Bryant and J.J. Stiffler, CARE III Phase II Report User's Manual, NASA LaRc CR-165864 (September 1982)
- J.J. Stiffler and L.A. Bryant, CARE III Phase II Report Mathematical Description NASA CR-3566 (November 1982)
- D.M. Rose, R.E. Altschul, J.W. Manke, and D.L. Nelson, "Review and Verification of CARE III Mathematical Model and Code : Interim Report", NASA Contractor Report 166096 (April 1983)
- Eliezer Gai, "Advanced Information Processing System(AIPS) Methodology Report", The Charles Stark Draper Laboratory, Inc., Cambridge, MA (July 1984)
- J.L. Lala, "interactive Reductions in the Number of States in Markov Reliability Analysis", The Charles Stark Draper Laboratory, Inc., Cambridge, MA (1983)
- Kishor Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Prentice Hall, Englewood Cliffs, NJ (1982)
- Robert Geist and Kishor Tribedi, "Ultrahigh Reliability Prediction for Fault Tolerant Computer Systems", IEEE : Transations on Computers C-32(12) (December 1983)
- Kishor Trivedi and Robert Geist, "A Tutorial on the CARE III Approach to Reliability Modeling", NASA Contractor Report 3488 (December 1981)
- S.J. Bavuso and P.L. Petersen, CARE III Model Overview and User's Guide (first revision), NASA TM-86404 (April 1985)
- Ying W. Ng and A. Avizienis, "A Unified Reliability Model for Fault Tolerant Computers", IEEE : Transactions on Computers C-29(11) (November, 1980)
- S. Makam, A. Avizienis, and G. Grusas, ARIES 82 User's Guide, University of California at Los Angeles, Los Angeles (August 1982)

다. 검증 방법에 따른 증거 자료

당해 연도에는 전년도에서 시제품으로 제작된 열차제어용 고안전성 연산처리 시스템의 안정성을 높이기 위하여 시스템의 보완 제작 작업을 진행하였다. 보완된 시제품의 성능확인을 위해 테스팅 프로그램을 이용하여 평가 메트릭에 따른 확인 시험이 수행되었다. 그리고 보안된 제품에 대한 국제 규격에 준하는 안전계획서, 위험원 도출 등 안전성 활동을 수행하였다.

라. 성과물의 내용 및 결과

본 절에서는 당해 연도에 수행한 고안전성 연산제어 시스템의 보완 제작, 평가 메트릭에 따른 성능시험 결과 및 수행한 안전성 활동에 대해 설명한다. 안전성 활동은 안전 계획서 작성과 위험원이 도출되었고, 이러한 안전성 활동에 기반을 두어 고안전성 연산제어 시스템을 보완하다. 보완된 시스템의 평가 메트릭의 제시 및 시험을 수행하였다.

(1) 고안전성 연산제어 시스템의 보완 제작

본 연구과제에서 전년도에 개발된 열차제어용 고안전성 연산처리 시스템의 안전성을 높이기 위하여 기존에 입력과 출력을 위해 사용하던 DI(Digital Input), DO(Digital Output)보드를 VDI(Vital Digital Input), VDO(Vital Digital Output) 보드로 대체하였다. 기존 시스템에서 사용된 DI, DO보드는 입, 출력 단에 하드웨어 이상이 발생될 경우 이를 감지할 수 없다는 단점을 가지고 있다. 이러한 단점을 극복하고 안정성을 높이기 위하여 전년도에 개발된 열차제어용 고안전성 연산처리 시스템의 I/O보드를 VDI, VDO 보드로 대체하는 보안작업을 수행하였다. VDI 보드는 이중화된 입력 채널을 비교하여 입력을 수신하기 때문에 입력단의 하드웨어적 이상을 감지할 수 있다. 또한 VDO보드는 출력을 피드백하여 확인하기 때문에 출력단의 하드웨어적 이상을 감지할 수 있게 된다. 건널목 침입검지 어플리케이션을 개발하여 고안전성 연산제어 시스템에서 동작시킴으로써 시스템의 안정성 및 적합성을 실험하였다. 건널목 침입 검지를 VDI 입력으로 받고, VDO 출력으로 건널목 신호기를 점등하여 열차의 진입을 막았다. 제어 및 현재 상태 표시화면은 델파이를 이용하여 제작하였다.

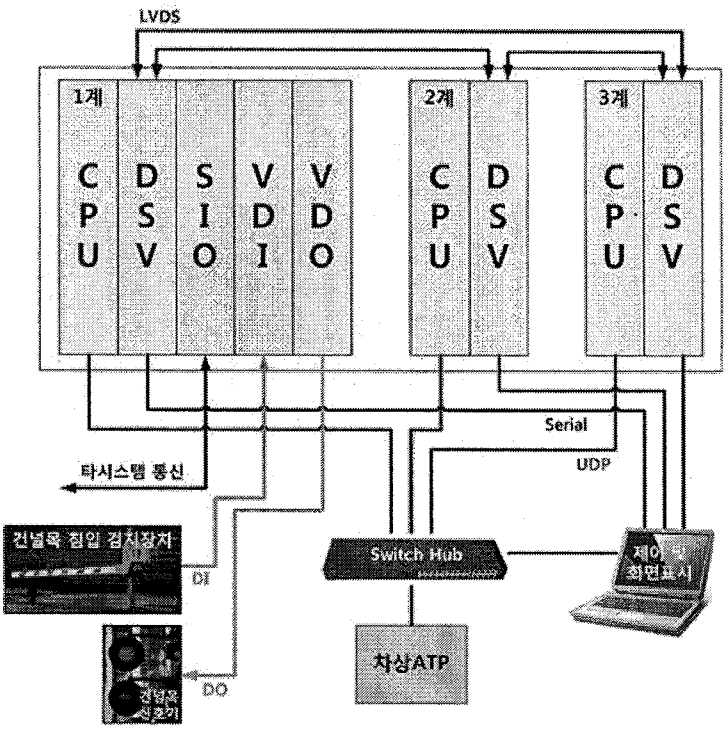


그림 3.7.1 시제품의 전체 구성

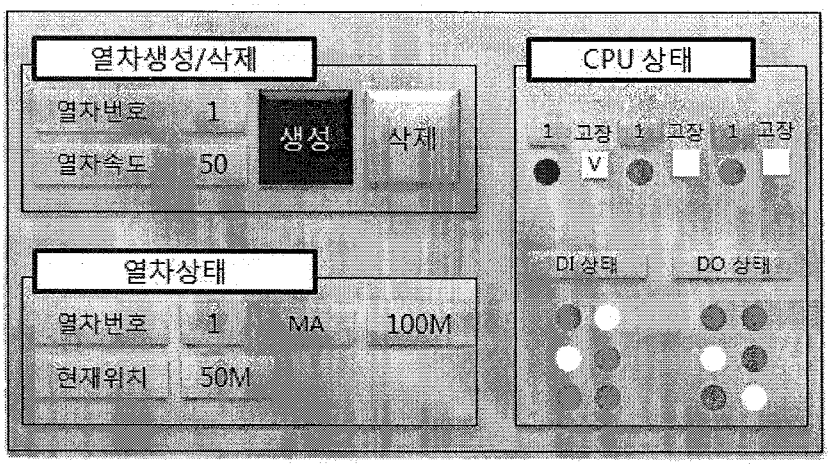


그림 3.7.2 시제품 시험을 위한 화면 구성 예시

① 고안전성 연산제어 시스템

보안 제작된 고안전성 연산제어장치 시스템은 다음 그림과 같이 3계로 구성되어 있다. 1계는 CPU, DSV(Data Share & Voter), SIO(Serial Input Output), VDI, VDO로 구성되어 있고, 2와 3계는 CPU, DSV로 구성되어 있다. 고안전성 연산제어 시스템의 특징은 다음과 같다.

- 3중계 2-out-of-3 연산
- 입출력 동기화
- 고속통신에 의한 입출력 공유
- 안전관련 입출력을 Vital I/O 처리(VDI, VDO)

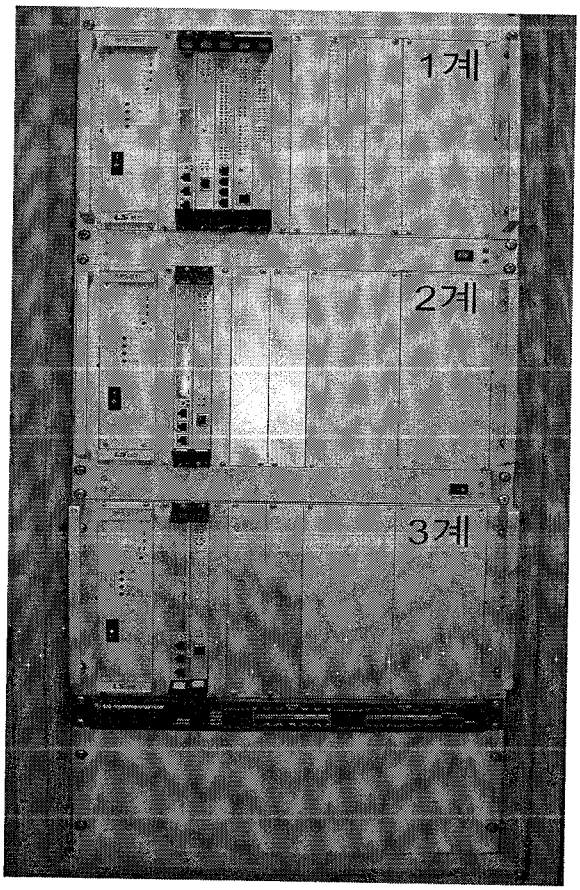


그림 3.7.3 고안전성 연산제어 장치 시제품

각 보드들의 사양은 다음과 같다.

- CPU 보드
  - MPC 7410 500MHz
  - 2xGb Ethernet
  - 2x COMs
  - -40 to +85°C
  - MTBF: 220,017h(IEC/TR62380)
- VDI 보드

- 이중화된 입력 채널 비교하여 입력 수신
- 전압 check 기능 (1/0이 아닌 값이 들어올 경우 에러 판정)

● VDO 보드
- 출력을 Feedback 하여 확인
- 포트별 Fail Safe 설정 가능

● DSV 보드
- TMS320C6713-300Hz
- VME Master/Slave 기능
- System Controller 기능
- 2MB 공유 메모리
- 최대 256MB 보팅 가능

● SIO 보드
- 외부 Serial 통신 기능

고안전성 연산제어 시스템은 3중화 방식인 TMR(Tripple Modular Redundancy)를 사용하고 있다. TMR 시스템은 크게 연산처리를 담당하는 CPU 보드, 데이터 공유 및 보팅을 담당하는 DSV 보드, 그리고 입출력 부분을 담당하는 VDI, VDO 보드로 구성되어 있다. VDI 보드로 입력된 동일한 입력에 대하여 3중화로 구성된 세 개의 CPU 보드가 연산한 결과를 2 out of 3 보팅하여 출력한다. 입력 및 출력에 대한 동기 수행, 입력 및 출력데이터 공유, 2 out of 3 보팅 수행 등을 위한 하드웨어 장치 및 소프트웨어에 대하여 기술한다.

다음 그림은 본 연구를 통해 개발된 열차제어용 고안전성 연사제어 시스템의 구조를 나타내고 있다. 시스템은 크게 두 부분으로 나누어 볼 수 있는데, 첫 번째 부분은 3중계로 구성되어있는 CPU 연산부이다. CPU의 연산은 입력받은 값을 이용하여 내부의 제어 연산을 수행하고 해당 연산의 결과를 Voter역할을 담당하는 DSV로 출력한다. DSV는 CPU와 마찬가지로 3중으로 구성되어 있으며 독립된 3중의 Voting을 수행한다. LVDS는 각 Voter간의 값들을 공유하기 위해서 고속의 통신으로 구성된다. 두 번째 부분인 입출력 부분은 I/O 블록으로써 VDI, VDO 보드로 구성되어 잇다. I/O는 1계만 장착되어 있으며 1계 CPU는 수신한 I/O 데이터를 DSV를 통해 2계, 3계에 공유한다. 1계, 2계, 3계의 출력은 서로 모두 공유되며 최종 보

팅은 1계에서 수행된다.

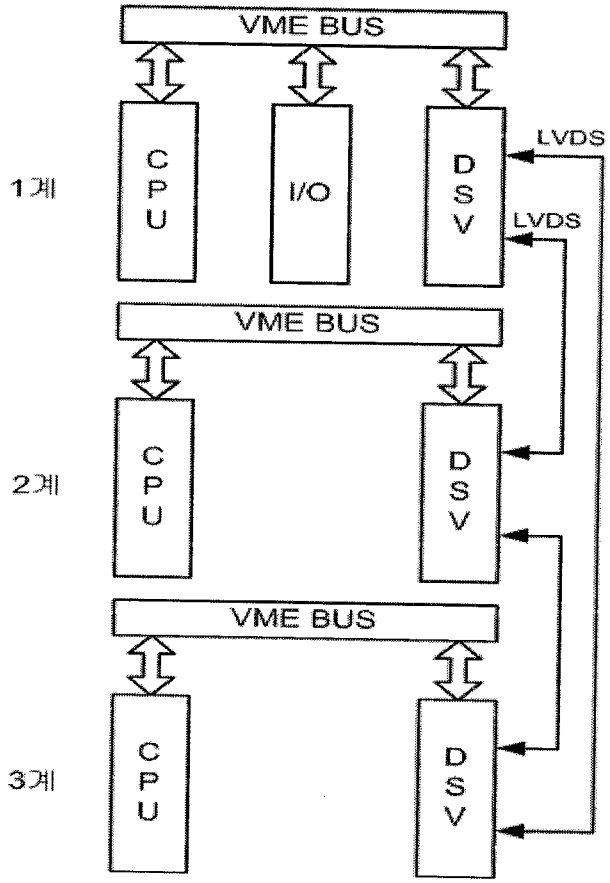


그림 3.7.4 고안전성 연산제어 시스템의 구조

② DSV 보드

DSV 보드는 고안전성 연산제어 시스템의 핵심 기능인 삼중화용 메모리 공유 보드로써 TMR 기능을 수행하기 위한 핵심적인 보드이다.

● 주요 사양

- System Bus

DSV 보드는 VME Master/Slave 기능을 가진 보드로서 A32/A24/A16 및 D32/D16을 지원한다. 또한, DSV 보드 단독으로 동작하는 것을 고려하여System Controller 기능 및 Interrupt Handler 기능도 지원한다.

- 공유 메모리(Shared Memory)

공유 메모리는 DSV 보드가 속해 있는 System의 Data 및 다른 두 System의 Data를 공유하고 Voting된 값을 저장하는 공간으로 사용된다. VME Bus 상에

구현되며 DSV 보드의 DSP 및 다른 VME Master에 의해 읽거나 쓸 수 있다. VME Bus 상의 공유 메모리의 크기는2Mbytes(Standard Addressing Mode)로 되어 있다.

- Console 포트

DSV 보드는 전면으로 사용자가 Interface할 수 있는 UART 1포트를 제공한다. 이 포트는 보드 디버깅용으로 사용할 수 있다. 통신 속도는 9,600bps에서 115,200bps 까지 지원 가능하다.

- LVDS 통신

DSV 보드는 그림 1의 3중화 구성도와 같이 LVDS(Low Voltage Differential Signals)를 이용하여 P2 커넥터에서 다른 시스템과 서로 데이터를 주고 받을 수 있다. 이 데이터는 DSP 칩에서 Interrupt로 받을 수도 있고, Polling 방식으로 받을 수도 있다.

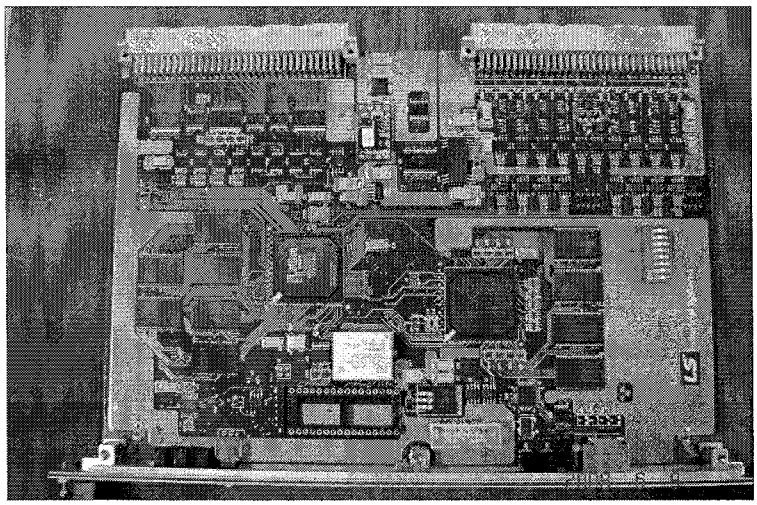


그림 3.7.5 DSV 보드

- 하드웨어 구조

  - 프로세서 : TI사 TMS320C6713B-300MHz Commercial

  - 메모리

  SRAM 2MBytes

  FRAM 1MBytes

  EPROM 512kBytes

NVRAM(RTC 포함) 32kBytes

Shared Memory 2MBytes

- Serial 통신

Isolated LVDS Tx/Rx 통신 2 Ports

UART 1 Port

Sync. Input(RS-485) 1 Port

- VME System Controller/Slave

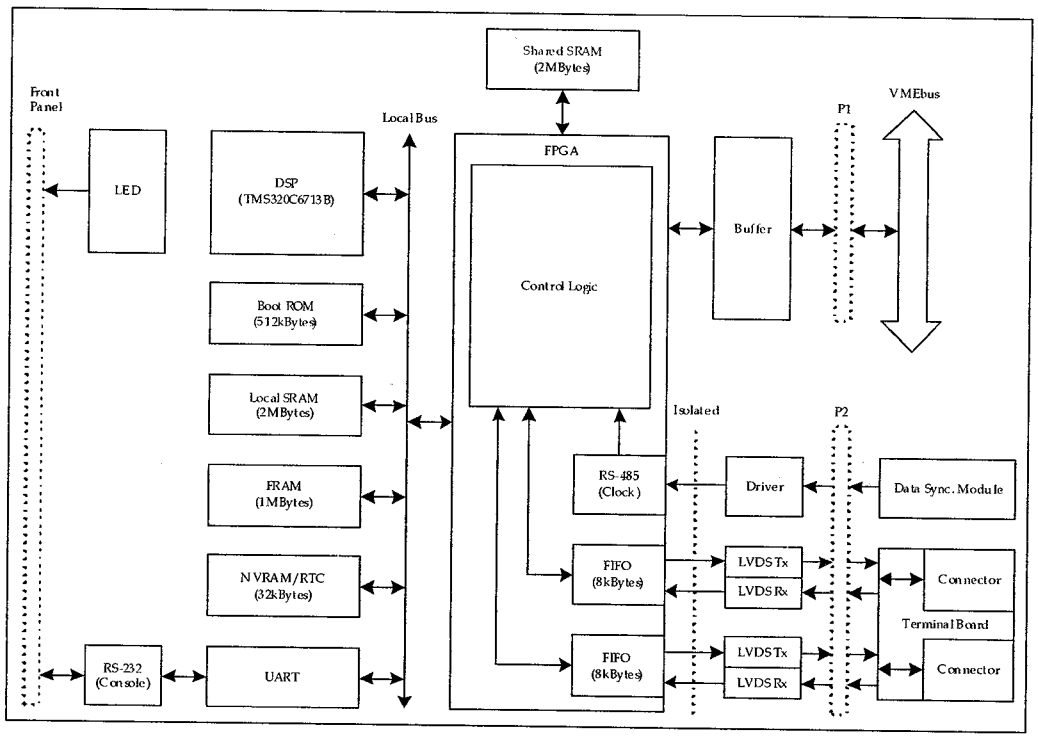


그림 3.7.6 DSV 보드의 하드웨어 구조

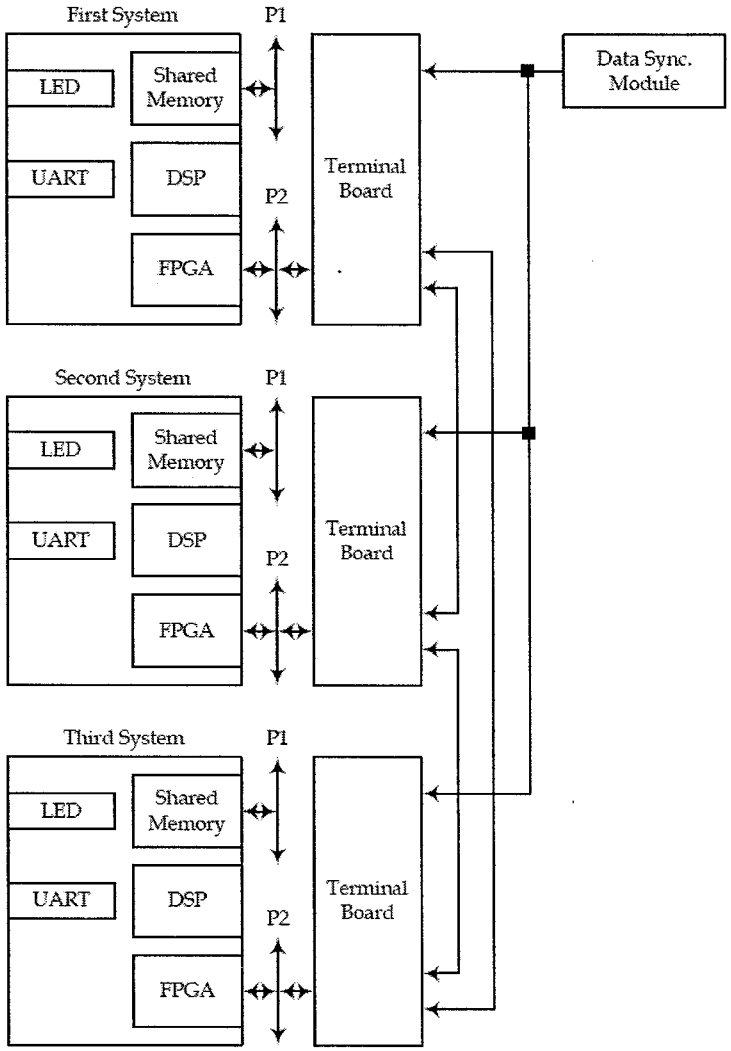


그림 3.7.7 3중화 구성도

③ VDI 보드

VDI보드는 VME BUS를 지원하는 VME Slave 보드로써, P1 Connector는 VME BUS용이고 P2는 IO 영역이다. VDI 보드는 현장의 디지털 입력을 받아서 CPU에 전달하는 기능을 한다. 입력은 12 Channel이며 입력 전압은 24V 전용이며 입력 전압의 Level이 측정 되는 VME Slave보드 이다. 입력의 Common은 12점으로 되어 있으며 - Common(N Common)이다. 입력 회로는 이중화로 구성이 되어 있으며 두 개의 입력이 일치 하는 경우에 이것을 입력으로 사용하고 다를 경우에는 Error를 표시한다. Point Error는 전면의 Console을 이용하거나 Point Error 정보를 보면 알 수 있다. VDI 보드의 입력은 VME BUS의 P2 Connector로 받도록 되어 있다. VDI

보드의 특징은 다음과 같다.

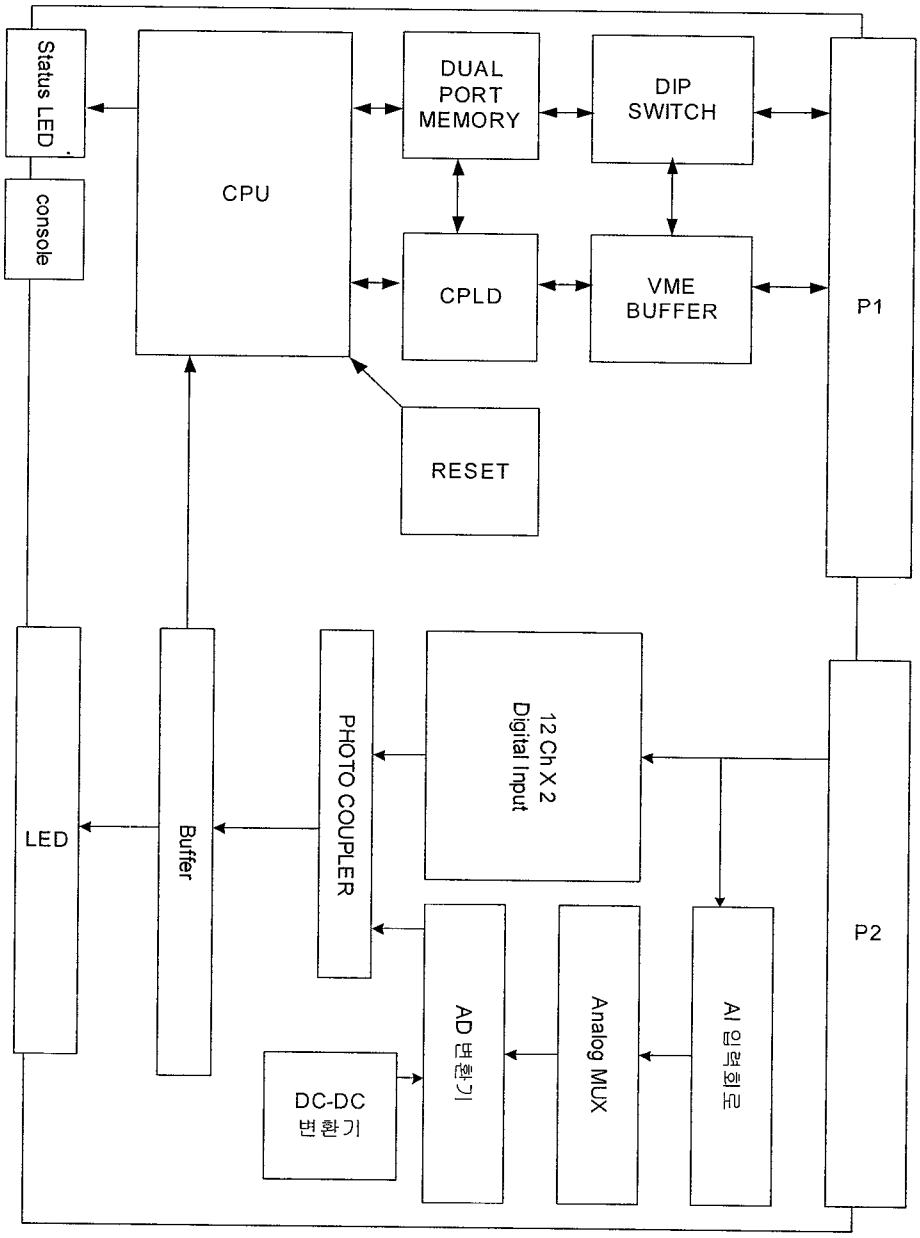


그림 3.7.8 VDI 보드 블록 다이어그램

- 주요사항
  - 24V 입력 회로 12 Channel 이상
  - 입력 포트 검사 기능 (내부에서 두 개로 나누어 받아 비교하는 기능)
  - VME bus 인터페이스 (A16, DPRAM 사용, VME address 변경 가능함)
  - 포트 scan 주기 1ms 이하 (변경 가능하여야 함)

- 전압 check 기능 (1/0이 아닌 값이 들어올 경우 에러 판정, 가능할 경우)
- LED 상태 표시 (VME, 포트 별 ON/OFF)
- 동작온도 -30 ~ 70 °C

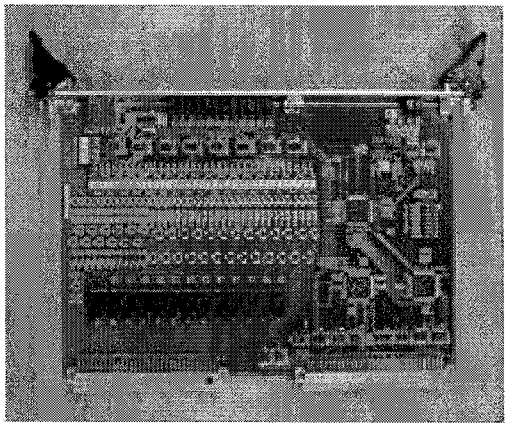


그림 3.7.9 VDI

④ VDO 보드

VDO보드는 VME BUS를 지원하는 VME Slave 보드이다. P1 Connector는 VME BUS용이고 P2는 IO 영역이다. VDO 보드는 VME CPU가 주는 출력을 내보내는 보드이다. 출력은 8 Channel이며 NPN Transistor출력이며 출력은 Feedback 되어 확인이 되어야 한다. 최종 출력은 이중화를 하기 위해 Relay로 연결이 된다. 보드가 RUN 이면서 정상 동작을 하면 이 Relay를 붙인다. 출력 전압은 24V 전용이다. VDO보드의 출력은 VME BUS의 P2 Connector로 연결된다. VDO 보드의 특징은 다음과 같다.

- 주요사항
  - NPN Transistor 출력 8port
  - 출력 포트 검사 기능 (출력이 1로 나갈 때 이를 짧은 시간 중단 시켜 실제로 중단 되는지 확인하는 기능, 또는 이에 해당하는 기능이 있어야 함)
  - VME bus 인터페이스 (A16, DPRAM 사용, VME address 변경 가능하여야 함)
  - 포트 별 fail safe 값 설정 기능 (변경 가능하여야 함)
  - VME scan 주기 10ms 이하 (변경 가능하여야 함)
  - Feedback 기능(출력 값을 feedback 회로로 받아 내부 값과 비교가 가능해야 함)

- LED 상태 표시 (VME, 포트 별 ON/OFF)
- 동작온도 -30 ~ 70 °C

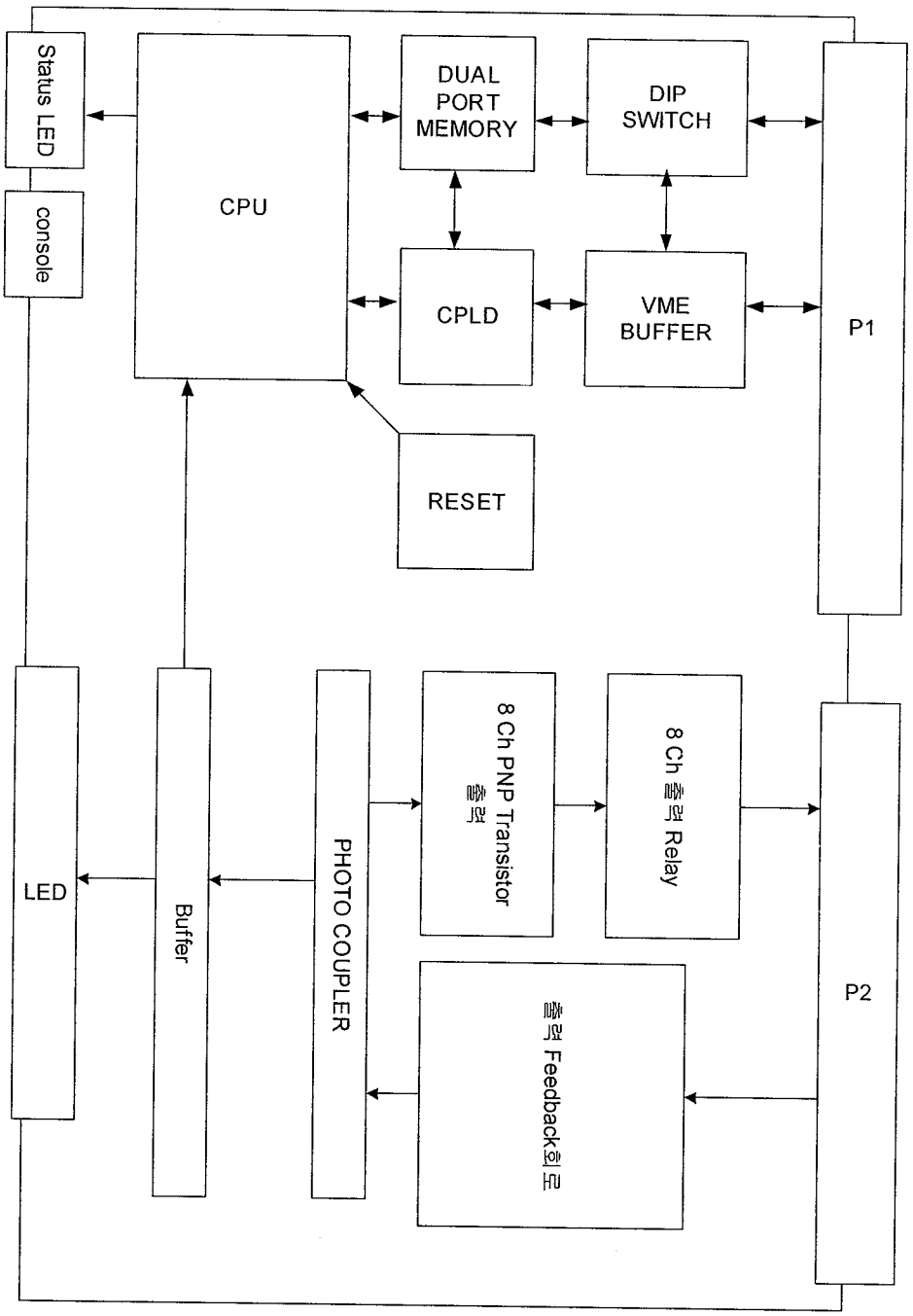


그림 3.7.10 VDO 블록 다이어그램

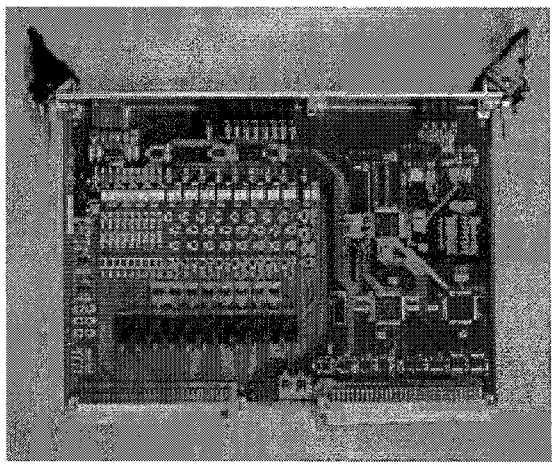


그림 3.7.11 VDO

⑤ CPU 보드

CPU 보드로 구현된 어플리케이션이 구동되는 부분으로써 VID로 입력된 특정 외부 신호를 처리하여 결과를 DSV 보드에게 전송 후 2 out of 3 보팅 과정 후 출력이 나갈 수 있게 하는 기능을 한다. CPU 보드의 특징은 다음과 같다.

- 주요사항
  - MPC7410 500MHz
  - 512MB ECC SDRAM
  - 17MB Flash
  - 2MB L2 cache
  - Two sites for 32/64-bit PMC expansion cards
  - 32 KB NVRAM
  - Two 10/100 Mbit/s Fast Ethernet interfaces
  - VME Bus(Tundra Universe)

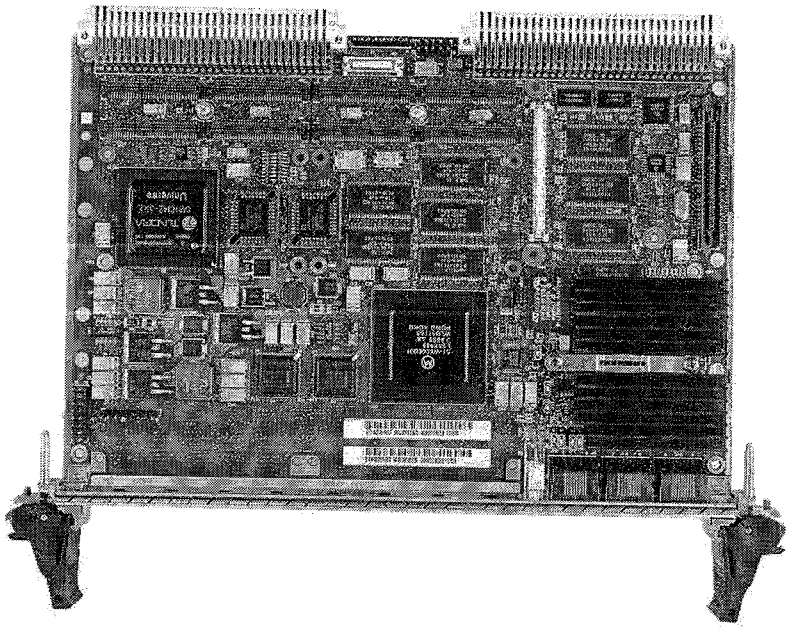


그림 3.7.12 CPU

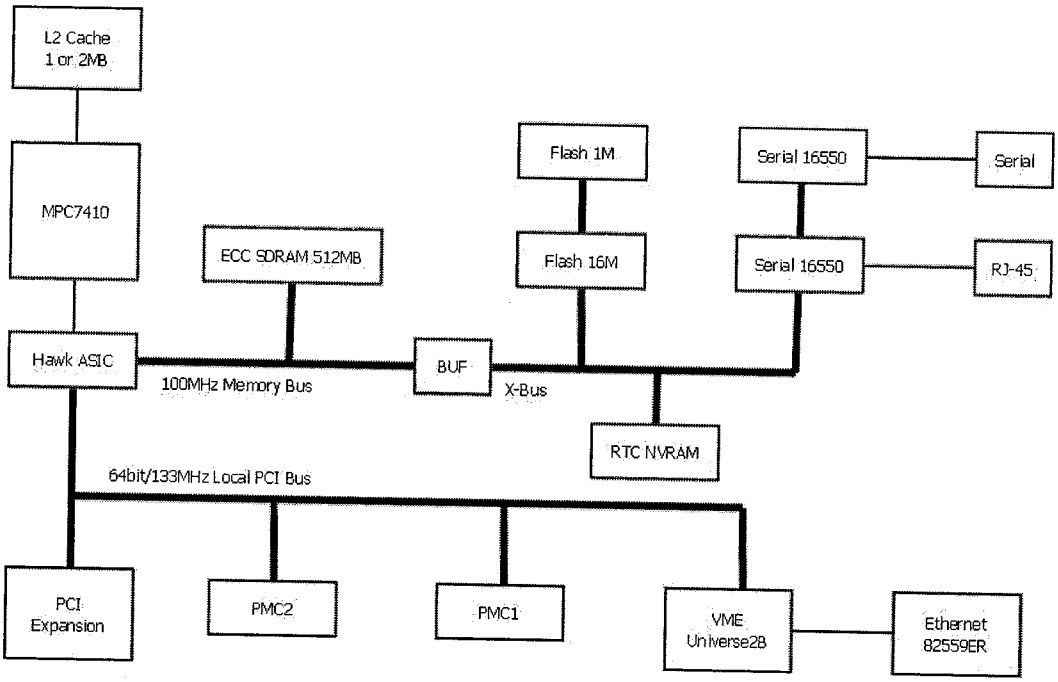


그림 3.7.13 CPU 블록 다이어그램

⑥ SIO 보드

SIO 보드는 16 channel serial port Input/Output TM 보드로써 RS232/485 통신을 제고하고 있다. SIO 보드의 특징은 다음과 같다.

● 주요사항

- 6 channel 의 RJ45 port를 통해 RS232/485 통신을 제공한다.
- 고속의 Serial data 전송 속도(최대 115.2Kbps)를 제공한다.
- Jumper에 의해 RS232 와 RS485 통신 방식을 간단히 변경할 수 있다.
- Power의 ON/OFF를 전면부에 있는 Power LED를 통해 확인 할 수 있다.

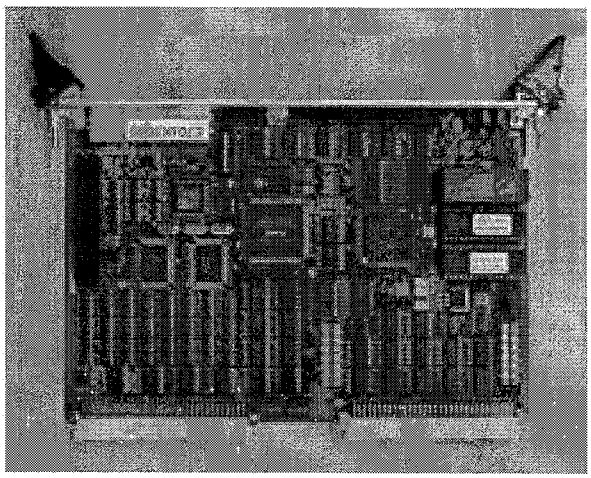


그림 3.7.14 SIO 보드

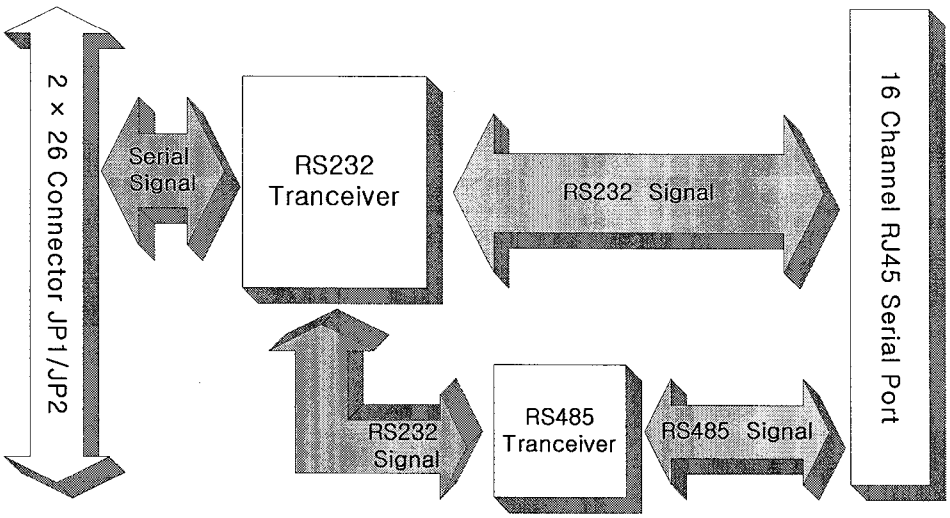


그림 3.7.15 SIO 보드 블록 다이어그램

(2) 고안전성 연산제어 시스템 평가 Metric

시스템 평가 Metric 에서는 보완된 고안전성 연산제어 시스템의 평가 항목을 제시하고 실험적인 방법으로 평가 결과를 확인한다. 이를 통하여 보완된 고안전성 연산제어 시스템의 성능을 평가하고 실제 열차제어시스템에 적용 가능 여부를 타진하게 된다.

① 평가 Metric 항목 및 시험

항 목	세부 항목
DSV보드 LVDS 전송 성능	전송 지연 시간 측정
	전송 속도 측정
DSV 메모리 공유 및 보팅 성능	1KB 공유 시간 측정
	1KB 공유 보팅 시간 측정
최대 입력 처리 성능	최대 처리 개수 측정
보팅성공률	보팅 성공률
Vital 입력 처리 가능	Vital 입력 처리 성공률 측정
Vital 출력 처리 가능	Vital 출력 처리 성공률 측정

- DSV보드 LVDS 전송 성능

  - 전송 지연 시간 측정

  그림 3.7.16은 순수하게 송신 측 Digital Isolator 입력단과 수신 측 Digital Isolator 출력단을 오실로스코프로 측정한 파형으로 하드웨어 간 전송지연 시간은 약 52n초 정도가 걸리는 것을 알 수 있다. 또한, 그림 3.7.17은 Tx 시의 CLK를 측정한 파형으로 자세한 통신 타이밍은 그림 3.7.18에 나와 있다. 그림 3.7.18를 보면 앞의 2비트는 통신 Marker로 사용되고, 송신되는 CLK 신호 및 Tx Enable 신호를 이용하여 동기 Serial 통신이 되도록 구성되어 있다. 수신측에서는 Tx Enable이 Assert 되었을 시에 Shift Register를 이용하여 Data를 수신하고, Rx Acknowledge 신호를 Assert 한다.

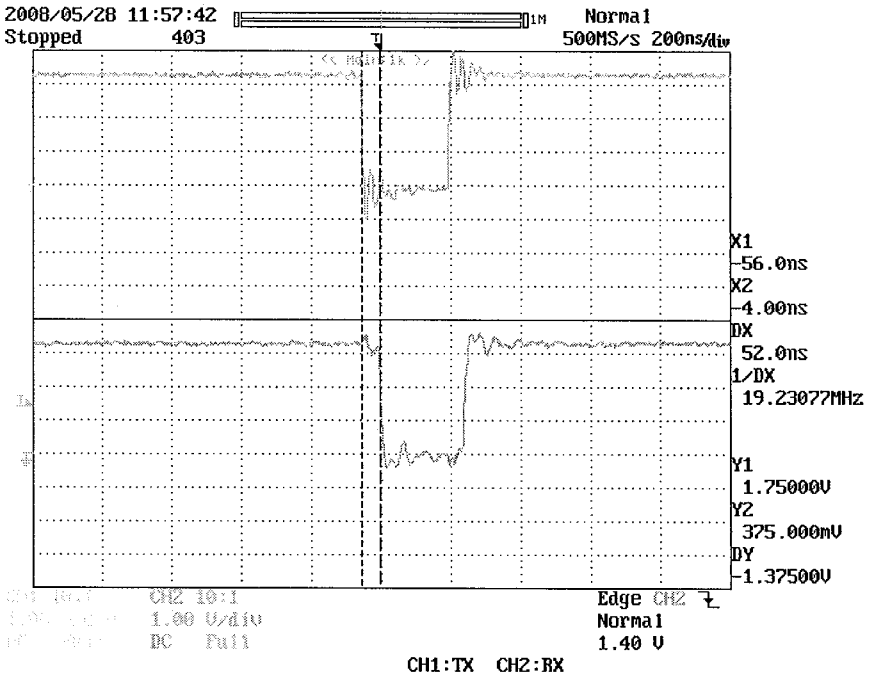


그림 3.7.16 LVDS 신호 전송 지연 시간

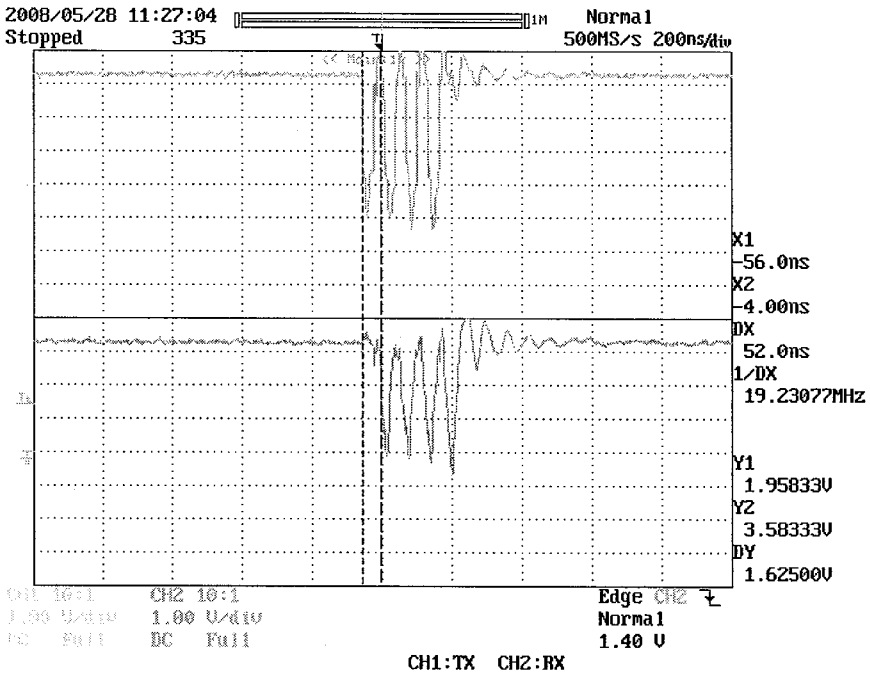


그림 3.7.17 LVDS 신호 전송 지연 시간

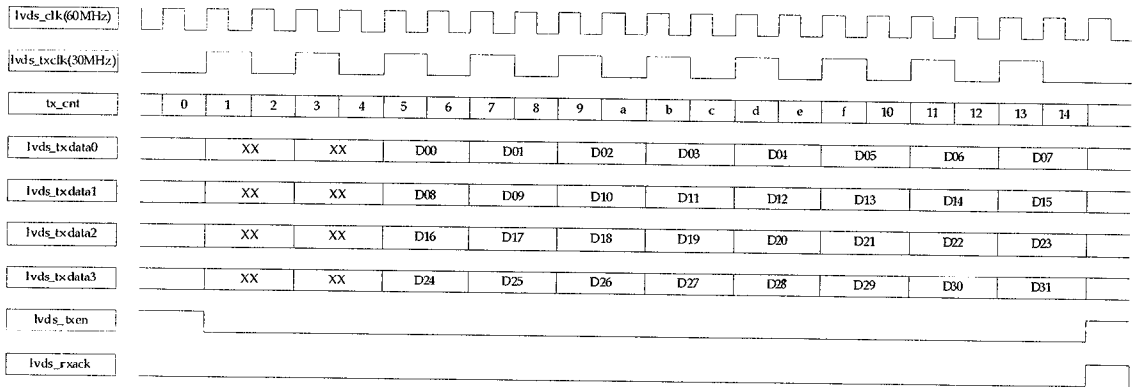


그림 3.7.18 LVDS Link Port Serial 통신 Timing Diagram

-전송 속도 측정

이론적으로 LVDS 통신은 90Mbps 이나 케이블 길이나 통신 환경에 따라 영향을 받는다. 아래 그림은 소프트웨어를 이용하여 송신 시점에서 LED를 On하고, 수신 시점에서 LED를 Off한 파형을 측정한 그림이다. 실질적으로 DSP에서 프로그램이 돌아가는 시간도 있으므로, 전송속도는 약 42.5Mbps 정도가 나오는 것으로 알 수 있습니다.

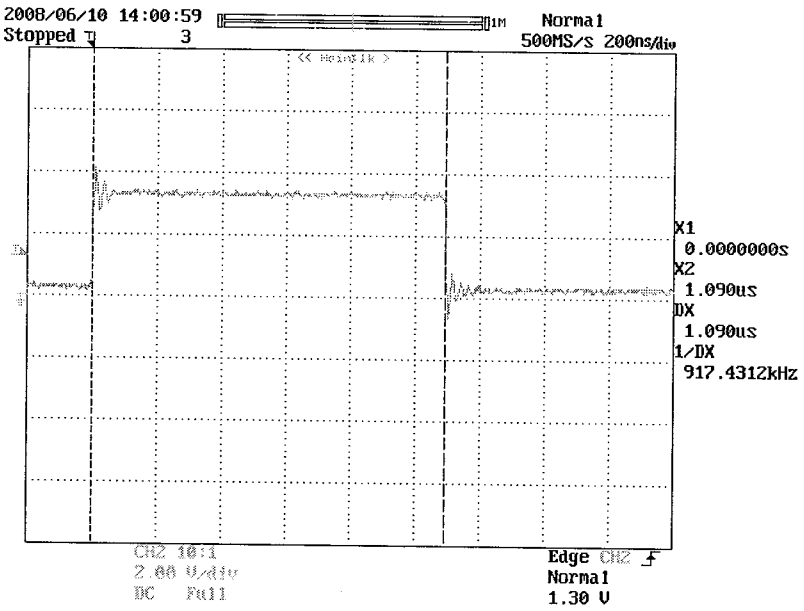


그림 3.7.19 LVDS 전송속도

- 1Kbytes 공유 시간 측정

메모리 공유 시간은 보팅 링크 성능과 관련이 있다. 각 DSV 보드에서 보팅 링크 시험 결과는 아래와 같다.

```
DSV:₩>lvds 10000000
**********************************************
*            LVDS LOOPBACK TEST              *
**********************************************

LVDS Port 1 --> LVDS Port 2
.....................................................................
.....................................................................OK!!
LVDS Port 2 --> LVDS Port 1
.....................................................................
.....................................................................OK!!
```

테스트는 2 가지 형태로 구성되어 있다.

1) DSV 보드 #1 Vote link 1 송신 후 수신 DSV 보드 #2 Vote link 2 수신 후 송신

```
DSV:₩>lvds 1000000 2 1
**********************************************
*            LVDS LOOPBACK TEST              *
**********************************************

DSV #1's LVDS Port 1 <--> DSV #2 LVDS Port 2
AAAAAAAAAAAAAAAaaaaaaaaaaaaaaa. OK!!
DSV #1's LVDS Port 2 <--> DSV #2 LVDS Port 1
BBBBBBBBBBBBBBBbbbbbbbbbbbbbbb. OK!!
```

2) DSV 보드 #1 Vote link 2 송신 후 수신 DSV 보드 #2 Vote link 1 수신 후 송신

```
DSV:₩>lvds 1000000 2 2
**********************************************
*            LVDS LOOPBACK TEST              *
**********************************************

DSV #1's LVDS Port 1 <--> DSV #2 LVDS Port 2
ccccccccccccccCCCCCCCCCCCCCCC. OK!!
DSV #1's LVDS Port 2 <--> DSV #2 LVDS Port 1
ddddddddddddddddDDDDDDDDDDDDDDD. OK!!
```

아래 그림은 각 DSV간에 데이터 공유 및 보팅을 시험하기 위한 시험용 시스템 구성이다.

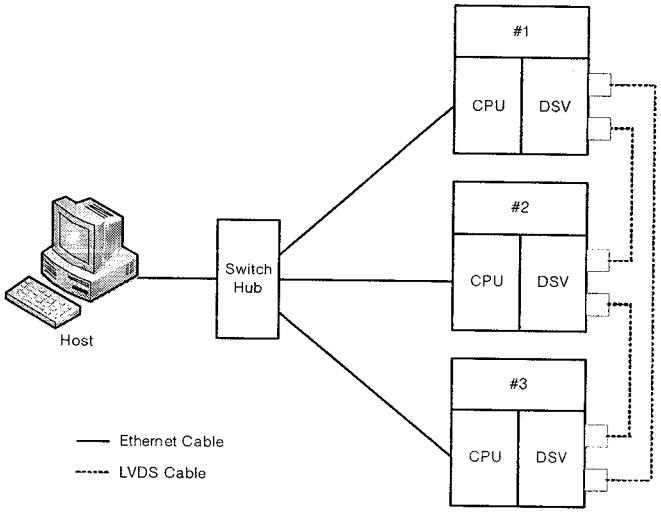


그림 3.7.20 보팅기능 테스트 환경

- 1Kbytes 의 데이터를 1계, 2계, 3계 DSV 보드가 모두 공유하는데 소요되는 시간을 측정한다. 이는 LVDS 통신 속도에 좌우된다. 측정값은 4ms가 된다.

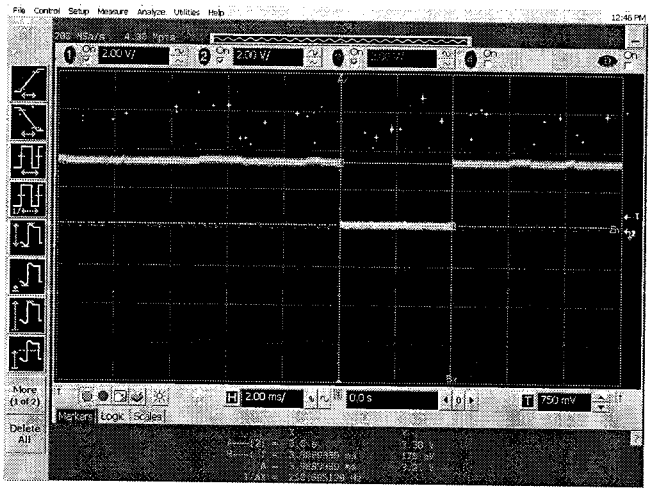


그림 3.7.21 1Kbytes 공유시간

- 1Kbytes 공유 보팅 시간 측정

1Kbytes 의 데이터를 1계, 2계, 3계 DSV가 모두 공유하고 보팅하는데 까지 소요되는 시간을 측정한다. 이는 LVDS 통신 속도와 DSV 보드의 메모리 접근 시간에 좌우된다. 이 측정값은 DSV에서 소요된 총 시간이다. 측정값은 26ms가 된다.



그림 3.7.22 공유 보팅 시험

- 최대 처리 개수 측정
  - 1대 당 평균 300ms 마다 통신한다고 가정
  - 10대 동시 통신 시에 평균 30ms 마다 통신
  - 1회 최대 패킷크기는 1Kbytes
  - 데이터 공유 및 보팅 지연 시간 26ms
  - 입력 큐를(1024Kbytes) 설정하면 놓치는 패킷 없이 모두 처리 가능함

- 보팅 성공률
  - DSV 보드의 보팅 성공률을 측정한다.
  - 하드웨어 고장이 없을 때 성공률을 측정한다.
  - 1Kbytes 데이터를 10,000회 보팅 수행시 100% 성공

- Vital 입력 처리 가능
  - VDI 보드의 입력 처리 가능을 측정한다.
  - 하드웨어 고장이 없을 때 입력 처리 성공률을 측정한다.

- 외부에 스위치를 이용하여 디지털 값을 10,000회 입력하였을 때 100% 처리 가능

- Vital 입력 처리 가능
  - VDO 보드의 입력 처리 가능을 측정한다.
  - 하드웨어 고장이 없을 때 입력 처리 성공률을 측정한다.
  - 오실로스코프를 이용하여 출력되는 디지털 값을 10,000회 감지하였을 때 100% 출력 가능

② 결과

표 3.7.1 평가 Metric 시험 결과

항목	결과	비고
DSV 보드 전송 지연 시간	52ns	
DSV 보드 전송 속도	42.5Mpbs	
1Kbytes 데이터 공유 시간	4ms	
1Kbytes 데이터 공유-보팅 시간	26ms	
최대 처리 가능한 입력 개수	제한 없음	
보팅 성공률	100%	
Vital 입력 처리 가능	100%	
Vital 출력 처리 가능	100%	

③ DSV 보드 챔버 테스트(Test Chamber)

DSV 보드의 온도 신뢰성 테스트를 위하여 챔버 테스트를 진행한다. 아래 표는 가 부품별 지원 온도 사항이다.

표 3.7.2 챔버 테스트

부품명	지원 온도
TI TMS320C6713B 300MHz DSP	0℃~90℃
LVDS Cable - 3M	0℃~60℃
Power Module	Unknown
Others	0℃~60℃
* 부품의 지원 온도 제한으로 인해서 -30℃~75℃ 테스트는 수행하기 어려움으로,일반적인 commercial test에 적용하는 0℃~60℃ 테스트를 적용했음	

테스트 방법은 첫 번째 60℃에서 20시간 동안 테스트를 진행하였고, 두 번째로 60℃에서 4시간, 0℃에서 4시간 반복 테스트를 진행하였다. 테스트 부품은 아래와 같고 무한으로 반복하며 에러 발생 시에 발생된 에러 부분에서 테스트를 멈추도록 테스트 코드를 구현하여 수행하였다.

- 자체 메모리(NVRAM, FRAM, SRAM, Shared Memory) read/write 테스트
- LVDS 포트 loopback 테스트
- Sync 포트 테스트
- RTC 테스트
- LED 테스트

첫 번째 60℃에서 20시간 동안 테스트 방법의 상세 설명은 아래와 같다.

표 3.7.3 시간별대 온도 설정

0~1시간(1시간 동안)	상온(27℃) 60℃로 온도 상승
1~21시간(20시간 동안)	60℃로 온도 유지
21~22시간(1시간 동안)	60℃ 상온(27℃)로 온도 하강

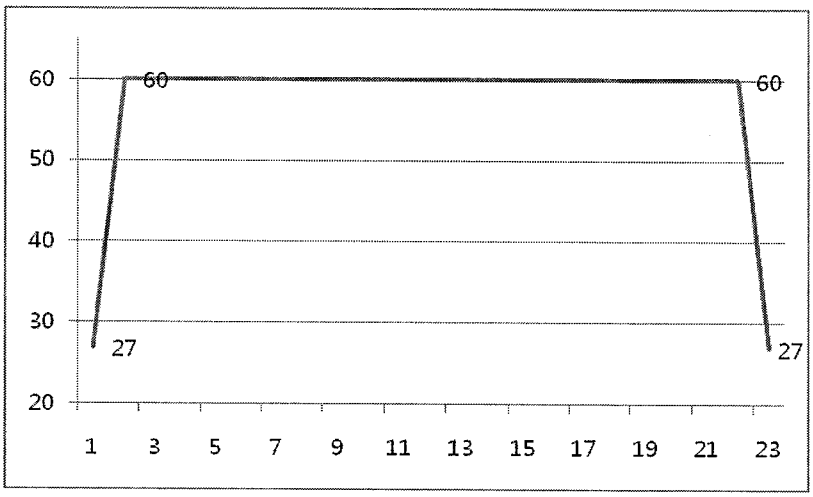


그림 3.7.23 시간별도 온도 설정 그래프

두 번째 60℃에서 4시간, 0℃에서 4시간 반보 테스트 방법의 상세 설명은 아래와 같다.

표 3.7.4 시간별 온도 설정

0 ~ 1시간(1시간 동안)	상온(27℃) 60℃로 온도 상승
1 ~ 5시간(4시간 동안)	60℃로 온도 유지
5 ~ 6시간(1시간 동안)	60℃ 0℃로 온도 하강
6 ~ 10시간(4시간 동안)	0℃로 온도 유지
10 ~ 11시간(1시간 동안)	0℃ 60℃로 온도 상승
11 ~ 15시간(4시간 동안)	60℃로 온도 유지
15 ~ 16시간(1시간 동안)	60℃ 0℃로 온도 하강
16 ~ 20시간(4시간 동안)	0℃로 온도 유지
20 ~ 21시간(1시간 동안)	0℃ 상온(27℃)로 온도 상승
21 ~ 24시간(3시간 동안)	상온(27℃)로 온도 유지

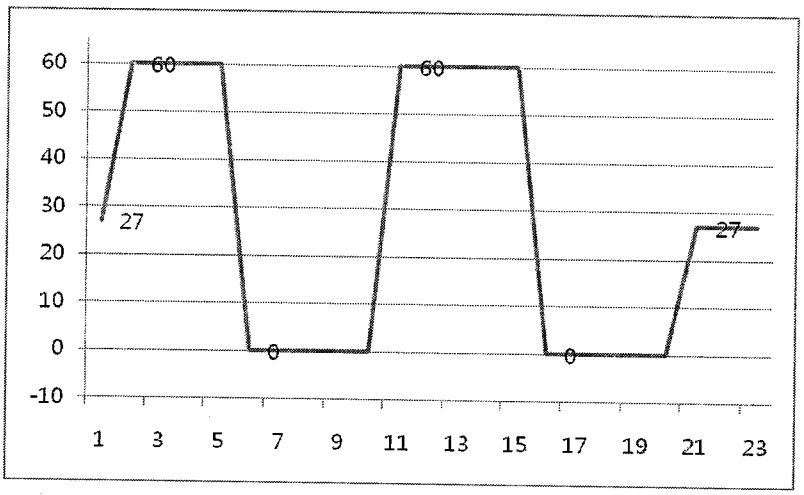


그림 3.7.24 시간별도 온도 설정 그래프

④ DSV 보드 Voting 테스트

● 삼중화 시스템 개요

삼중화 시스템(TMR, Triple Modular Redundant)을 구축하기 위해서는 최소한 다음과 같은 기능이 제공되어야 한다.

가. 현재 필드에서 입력되는 데이터를 동일하게 삼중화 시스템의 IO 보드에 전달하는 기능.

나. 삼중화 시스템의 IO 보드가 필드로 출력되는 데이터를 현장에서 어떻게 보팅할 것인가의 기능.

다. 삼중화 시스템의 IO 보드에 입력된 데이터의 공유 기능 및 보팅 기능.

라. 삼중화 시스템의 CPU 보드상에 운용되는 로직 소프트웨어의 주기 및 동기 일치 기능.

마. 어떤 이벤트에 따라 로직 수행이 영향을 미친다면 과거 발생한 이벤트 및 내부 데이타의 유지 관리 기능 및 이의 공유 기능.

바. 하나의 모듈(CPU 보드 또는 DSP 보드)이 고장이 발생하였을 경우 이의 인지 및 복구시 내외부 데이터 일치 기능.

- 데이터 입력 절차
  - 외부 입력이 I/O 보드를 통해 수신된다.
  - 하나의 입력이 처리되기 전에 수신된 입력은 큐에 저장된다.
  - 1계 CPU 는 해당 입력을 수신한 후 고유의 입력 ID 부여한다.
  - 1계 CPU 보드가 1계 DSV 보드에 고유 입력 ID를 부여한 입력 데이터를 메모리영역의 입력영역에 Write 한다.
  - 1계 DSV 보드는 새로운 입력 ID 수신 시 2계, 3계 DSV 보드로 해당 입력을 공유시킨다.
  - 1계, 2계, 3계 CPU 보드는 각각 입력영역으로부터 데이터를 읽어들여 연산을 수행한다.

- 보팅 및 출력 절차
  - 1계, 2계, 3계 CPU 보드는 연산 결과를 자신의 DSV 출력 영역에 써넣음 (1계 CPU는 CPU1 출력영역, 2계 CPU는 CPU2 출력영역, 3계 CPU는 CPU3 출력영역)
  - 1계, 2계, 3계 DSV 보드는 각기 자신의 영역의 데이터를 다른 DSV에 공유시킨다. (이로써 각 DSV의 CPU 출력영역에 모두 데이터가 저장됨)
  - 각 DSV는 CPU1, CPU2, CPU3 출력영역의 데이터에 대하여 2 out of 3 보팅을 수행한다.

- 각 DSV 보드는 보팅 결과를 보팅영역에 저장한다.
- CPU 보드는 보팅영역에 새로운 입력 ID의 데이터가 저장되었을 경우 이를 I/O 보드를 통해 출력한다.

● 자체 기능 시험

아래 그림은 DSV(Data Shared Voting) 보드를 테스트하기 위한 기본 구성도를 나타낸다. DSV 보드는 1개의 콘솔 포트와 2개의 LVDS 포트를 가지고 있다. LVDS 포트에 대한 기본적인 테스트는 포트1과 포트2를 loopback 케이블로 연결해서 테스트한다. 이 환경에서는 DSV 보드의 VME Master 기능 테스트도 수행할 수 있다.

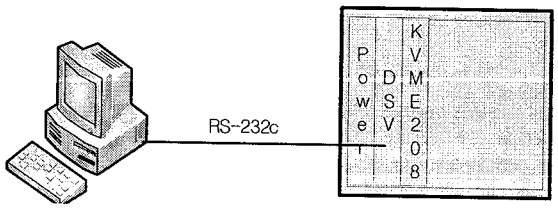


그림 3.7.25 DSV 보드 시험 환경

- Vote 기능 테스트

아래의 그림은 DSV 보드가 가진 Vote 기능을 테스트하기 위한 구성도를 나타낸다. 이 기능은 VME Slave 기능과 LVDS 포트 테스트 기능을 같이 테스트하면서 내부에 구현된 Vote 알고리즘을 테스트하기 위함이다.

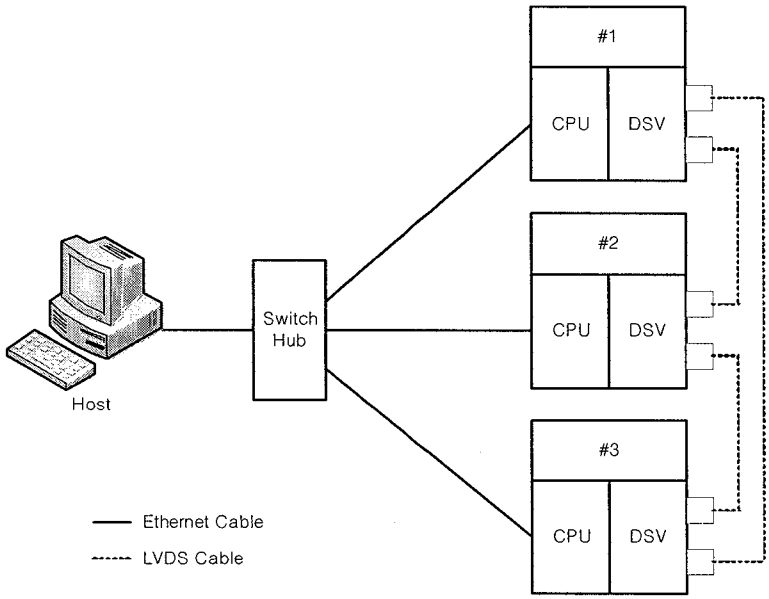


그림 3.7.26 보팅기능 테스트 환경

- 테스트 명령어 리스트

DSV 보드는 자체적으로 내부 하드웨어 및 소프트웨어 기능을 확인하기 위한 명령어를 제공한다.

표 3.7.5 테스트 명령어 리스트

명령	설 명
logo	DSV 보드 logo를 화면에 표시
nvram	NVRAM을 Test (테스트 주소: 0x90080000 ~ 90087ff7)
sram	SRAM을 Test (테스트 주소: 0x80000000 ~ 0x801fffff)
fram	FRAM을 Test (테스트 주소: 0xa0200000 ~ 0xa02fffff)
vme_master	VME Master Extended 모드 테스트
vme_std	VME Master Standard 모드 테스트
vme_sht	VME Master Short 모드 테스트
vme_syscon	VME System Controller 모드 테스트
shmem	Shared Memory Test (테스트 주소: 0xa0000000~ 0xa01fffff)
dip	DIP Switch의 상태값을 읽어 들임
led	LED 0과 1에 대해서 ON/OFF Test
rtc	RTC(Real-Time Clock) 테스트
vote	Voting 테스트
date	DATE 테스트
lvds	LVDS 포트 테스트

sync	Sync 포트 테스트
vsbar	VME Slave Base Address Register 설정
watchdog	Watchdog 테스트
reboot	Reboot 테스트
fill	특정 메모리 영역에 데이터 채우기 명령
dump	특정 메모리 영역의 데이터 읽기 명령
mem_all	NVRAM, SRAM, FRAM, Shared Memory 테스트
vme_slave	VME Slave 모드 테스트 (VME Master 보드와 연동해서 테스트)
vme_interrupt	VME Interrupt 테스트
vme_set_mode	보드별 VME Slave 모드 관련 레지스터 설정
clear	특정 메모리의 내용을 모두 지운다.
test_all	내부의 모든 메모리, LED, RTC, LVDS & Sync 포트 테스트
help	명령들에 대한 Help 기능

● 구현 및 시험

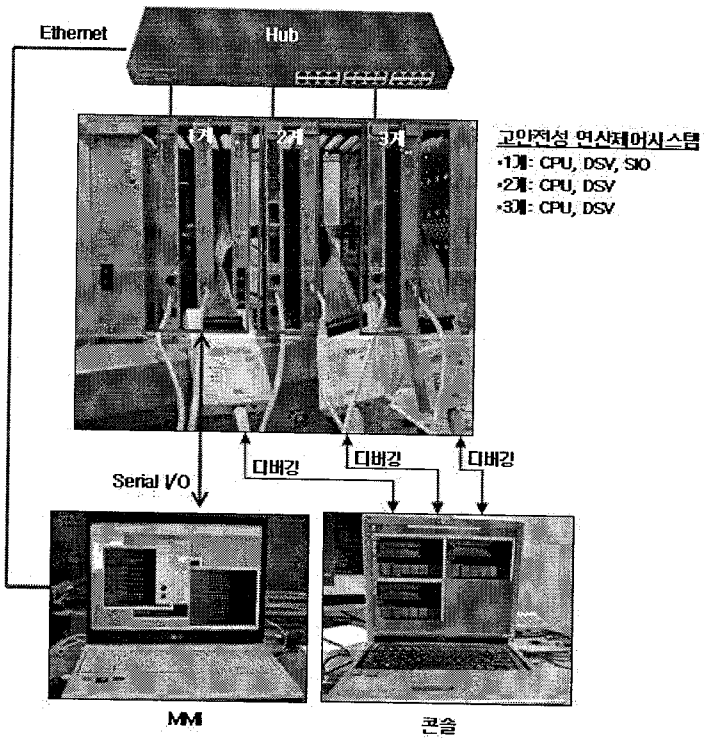


그림 3.7.27 시험용 시스템 구성

● 시험용 시스템 주요 특징

- CPU, DSV 모듈의 3중화 (TMR)

- 시리얼 단일 입출력
- 입출력의 동기화
- MMI를 통한 시험 수행 및 결과 확인
- 콘솔 화면을 통한 DSV 디버깅 및 동작 확인
- Ethernet 을 통한 CPU의 디버깅 및 동작 확인

● 시험 수행 순서

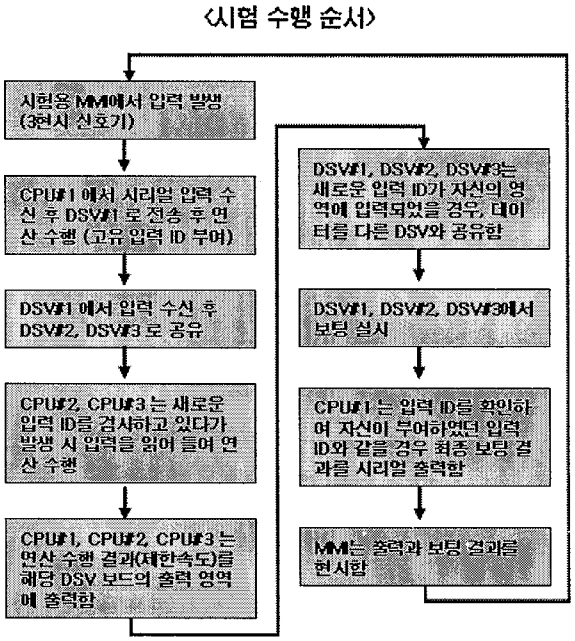


그림 3.7.28 시험 수행 순서

- STEP1: 시험용 MMI에서 입력 발생 (3현시 신호기)
- STEP2: CPU#1 에서 시리얼 입력 수신 후 DSV#1 로 전송 후 연산 수행 (고유 입력 ID 부여)
- STEP3: DSV#1 에서 입력 수신 후 DSV#2, DSV#3 로 공유
- STEP4: CPU#2, CPU#3 는 새로운 입력 ID를 검사하고 있다가 발생 시 입력을 읽어 들여 연산 수행
- STEP5: CPU#1, CPU#2, CPU#3 는 연산 수행 결과(제한속도)를 해당 DSV 보드의 출력 영역에 출력함
- STEP6: DSV#1, DSV#2, DSV#3는 새로운 입력 ID가 자신의 영역에 입력되었을 경우, 데이터를 다른 DSV와 공유함

- STEP7: DSV#1, DSV#2, DSV#3에서 보팅 실시
- STEP8: CPU#1 는 입력 ID를 확인하여 자신이 부여하였던 입력 ID와 같을 경우 최종 보팅 결과를 시리얼 출력함
- STEP10: MMI는 출력과 보팅 결과를 현시함
- STEP1부터 다시 시작함

● 시험 수행

시험용 프로그램은 신호기 Y, R, G 에 해당하는 시리얼 정보를 생성하여 1계의 SIO 보드로 전송한다. 연속 전송 버튼은 정해진 주기에 따라 정해진 회수만큼 연속적으로 동일한 데이터를 전송한다. 결과 확인 창에서는 제한 속도 수신과 1계, 2계, 3계의 보팅 결과를 확인 가능하다.

<시험용 프로그램 설명>

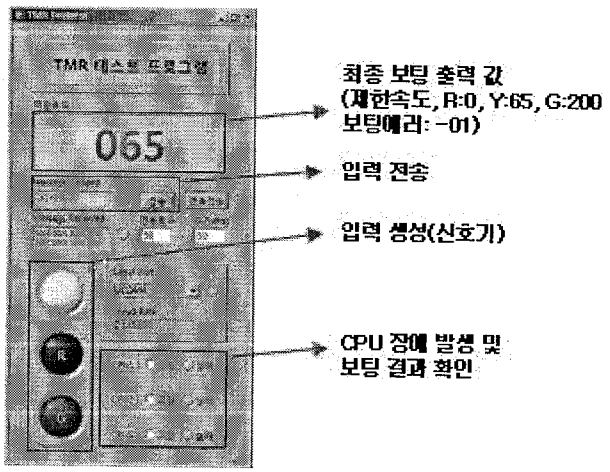


그림 3.7.29 시험용 프로그램

아래 그림은 3회의 시험 시(R, Y, G), 세 개의 CPU 가 모두 동일한 출력을 발생한 경우를 보인다. 보팅 결과 정상을 확인할 수 있다.

<시험결과1 - 세 개의 CPU 보드 정상 시 정상 보팅 >

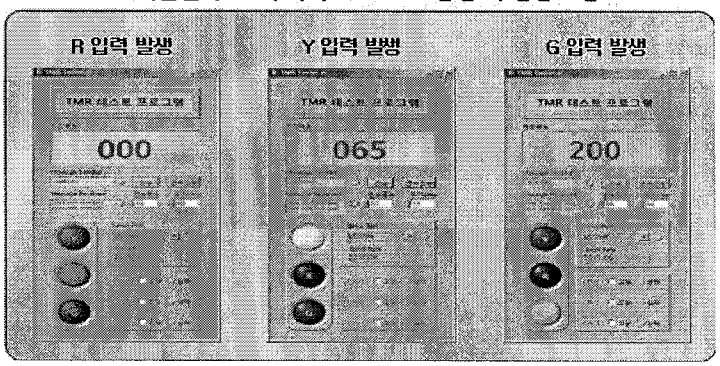


그림 3.7.30 세 개의 CPU 정상 시 결과

아래 그림은 임의로 하나의 CPU에 오류를 발생시켜서 다른 출력을 발생한 경우를 보인다. 2 out of 3 보팅에 따라 두 개의 CPU 결과가 같으면 정상 출력을 발생한다.

<시험결과2 - 하나의 CPU 보드 고장 시 정상 보팅 >

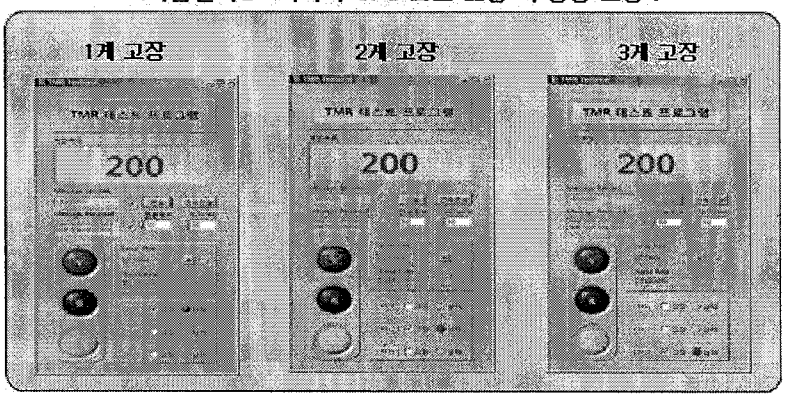


그림 3.7.31 하나의 CPU 고장 시

아래 그림은 임의로 두개의 CPU에 오류를 발생시켜서 다른 출력을 발생한 경우를 보인다. 2 out of 3 보팅에 따라 출력 오류가 발생되었다.

<시험결과3 - 2개 이상의 CPU보드 고장 발생 시 보팅 에러 >

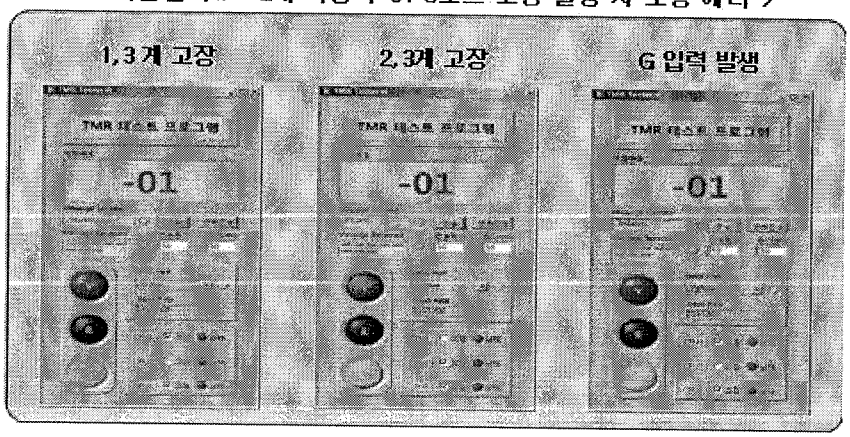


그림 3.7.32 2개 이상의 CPU 보드 고장 발생시

● 통합 시험

TMR 시스템 상에서 DSV 보드가 정상적으로 동작하는 가의 시험은 다음과 같다.

가. KVME080 보드가 VME 공유 메모리 영역에 데이터를 저장할 수 있는가?

나. KVME080 보드가 공유메모리에 저장한 데이터를 DSV 보드가 읽을 수 있는가?

다. DSV 보드가 읽은 데이터를 각 DSV 보드가 LVDS 통신라인을 통해 공유할 수 있는가?

라. DSV 보드가 공유한 데이터를 2 out of 3 voting 알고리즘을 이용 정상적으로 보팅을 하는가?

마. DSV 보드가 보팅한 결과를 VME 공유 메모리에 저장할 수 있는가?

바. KVME080 보드가 보팅한 결과를 VME 공유 메모리에서 읽을 수 있는가?

이를 시험하기 위해 다음과 같은 절차로 정상 여부를 결정한다.

단계	내용	결과
1.	PC에서 통신 프로그램을 이용 CPU#1에 telnet으로 로그인한다.	CPU 보드에 로그인이 가능하다
2.	PC에서 통신 프로그램을 이용 CPU#2에 telnet으로 로그인한다.	CPU 보드에 로그인이 가능하다
3.	PC에서 통신 프로그램을 이용 CPU#3에 telnet으로 로그인한다.	CPU 보드에 로그인이 가능하다
4.	CPU#1 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	FALSE(=0)가 저장되어 있다.
5.	CPU#2 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	FALSE(=0) 가 저장되어 있다.
6.	CPU#3 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	FALSE(=0) 가 저장되어 있다.
7.	CPU#1 에서 시험용 프로그램을 이용 공유영역의 특정영역에 데이터를 TRUE(=1) 로 저장한다.	
8.	CPU#1 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	TRUE(=1) 로 설정되어 있다.
9.	CPU#1 에서 시험용 프로그램을 이용 공유영역상의 CPU#2, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#2과 CPU#3의 값이 FALSE(=0) 로 설정되어 있다. CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), FALSE(=0), FALSE(=0) 이므로 Voting 결과 값은 FALSE(=0) 이다.
10.	CPU#2 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#1에서 변경된 TRUE(=1) 값은 통신 라인을 통해 수신한다. 따라서 CPU#1의 값은 TRUE(=1), CPU#3의 값은 FLASE(=1) 이다.

		CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), FALSE(=0), FALSE(=0) 이므로 Voting 결과 값은 FALSE(=0) 이다.
11.	CPU#3 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#2 및 Voting 영역의 값을 읽는다.	CPU#1에서 변경된 TRUE값은 통신 라인을 통해 수신한다. 따라서 CPU#1의 값은 TRUE(=1), CPU#2의 값은 FLASE(=0) 이다. CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), FALSE(=0), FALSE(=0) 이므로 Voting 결과 값은 FALSE(=0) 이다.
12.	CPU#2 에서 시험용 프로그램을 이용 공유영역의 특정영역에 데이터를 TRUE(=1) 로 저장한다.	
13.	CPU#2 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	TRUE(=1) 로 설정되어 있다.
14.	CPU#2 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#1은 TRUE(=1), CPU#3은 FALSE(=0) 이다. CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), TRUE(=1), FALSE(=0) 이므로

		Voting 결과 값은 TRUE이다.
15.	CPU#1 에서 시험용 프로그램을 이용 공유영역상의 CPU#2, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#2에서 변경된 TRUE(=1) 값은 통신 라인을 통해 수신한다. 따라서 CPU#2의 값은 TRUE(=1), CPU#3의 값은 FLASE(=0) 이다. CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), TRUE(=1), FALSE(=0) 이므로 Voting 결과 값은 TRUE(=1) 이다.
16.	CPU#3 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#2 및 Voting 영역의 값을 읽는다.	CPU#2에서 변경된 TRUE(=1) 값은 통신 라인을 통해 수신한다. 따라서 CPU#2의 값은 TRUE(=1), CPU#1의 값은 TRUE(=1) 이다. CPU#1, CPU#2, CPU#3의 값이 각각 TRUE(=1), TRUE(=1), FALSE(=0) 이므로 Voting 결과 값은 TRUE(=1) 이다.
17.	CPU#3 에서 시험용 프로그램을 이용 공유영역의 특정영역에 데이터를 TRUE(=1) 로 저장한다.	
18.	CPU#3 에서 시험용 프로그램을 이용 공유영역의 특정영역에 저장되어 있는 데이터를 확인한다.	TRUE(=1) 로 설정되어 있다.

19.	CPU#3 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#2 및 Voting 영역의 값을 읽는다.	CPU#1 및 CPU#2 값이 모두 TRUE(=1) 이다. CPU#1, CPU#2, CPU#3의 값이 모두 TRUE(=1) 이므로 Voting 결과 값은 TRUE (=1)이다.
20.	CPU#1 에서 시험용 프로그램을 이용 공유영역상의 CPU#2, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#3에서 변경된 TRUE(=1) 값은 통신 라인을 통해 수신한다. 따라서 CPU#1 및 CPU#2 값이 모두 TRUE(=1) 이다. CPU#1, CPU#2, CPU#3의 값이 모두 TRUE(=1) 이므로 Voting 결과 값은 TRUE(=1) 이다.
21.	CPU#2 에서 시험용 프로그램을 이용 공유영역상의 CPU#1, CPU#3 및 Voting 영역의 값을 읽는다.	CPU#3에서 변경된 TRUE(=1) 값은 통신 라인을 통해 수신한다. 따라서 CPU#1 및 CPU#2 값이 모두 TRUE(=1) 이다. CPU#1, CPU#2, CPU#3의 값이 모두 TRUE 이므로 Voting 결과 값은 TRUE(=1) 이다.
22.	앞의 시험 결과를 반복적으로 수행한다.	CPU#1, CPU#2, CPU#3에서 변경한 값이 서로 공유되고, 2 out of 3 voting 알고리즘에 따라 보팅 결과가 결정된다.

(3) 보안된 고안전성 연산제어 시스템의 안전성 활동

안전성 활동이란 열차제어시스템으로 인한 위험 원을 도출하고 도출된 위험원으로부터 허용할 수 있는 리스크레벨을 설정하여 위험원으로 인한 리스크가 허용할 수 있는 수준으로 제어되었음을 입증하는 활동을 의미한다. 이러한 활동을 위해 국제규격 IEC(International Engineering Consortium)과 미국방부 규격 MIL(Military Specifications and Standard)에서는 열차제어시스템의 RAMS(Reliability, Availability, Maintainability, Safety)의 목표설정, 예측, 평가를 포함한 관리방안을 제시하고 있다. IEC에서 제안하고 있는 적용규격과 문서화 기준은 다음과 같다.

표 3.7.6 적용규격과 문서화 기준

규격	목표	적용활동
IEC 61508	전기전자프로그래머블 제어기의 안정성	수명주기 전체
IEC 62278 (EN 50126)	철도신호시스템의 안전성요구사항	수명주기 전체
IEC 62279 (EN 50128)	철도신호시스템 소프트웨어 안전성	소프트웨어 위험원도출 및 안전요구사항 확인
IEC 62425 (EN 50129)	철도신호시스템 안전필수 요구사항	시스템 위험원도출 및 안전요구사항 확인
IEC 62280 (EN 50159)	철도신호시스템통신안전성	통신 위험원도출 및 안전요구사항 확인
IEC 61882	HAZOP Application	예비위험원분석, 위험원도출 및 분석
IEC 60812	고장모드영향분석	예비위험원분석, 위험원도출 및 분석
IEC 61025	결함트리분석(FTA)	위험원발생빈도 분석

보완된 열차제어용 고안정성 연산제어 시스템은 안정성 활동 기술체계에 따라

시스템의 설계 및 개발에 따른 안전성 활동을 진행하였다. 철도시스템 RAMS관련 규격인 IEC 62278을 근거로 하여 안정성 활동 시작단계에서 안전계획을 수립하였다. 당해 연도에는 보완된 고안정성 연사제어 시스템의 핵심 부분인 TMR 시스템을 중심으로 예비 위험원 분석(PHA)과 FTA를 통해 시스템에 존재하는 잠재적 위험원을 정량적으로 산출하였고 이를 바탕으로 위험원을 도출하였다.

① 안정성 활동 조직

표 3.7.7 안전성 활동 조직

조직	역할	책임
Project Manager	시스템 개발과 관련된 모든 사항에 대해 관리한다.	안전성활동의 계획 및 수행에 대한 책임
Designer/ Implementer	시스템 설계와 개발을 담당한다.	안전요구사양에 적합한 시스템 설계 및 개발
Verifier/ Validator	독립적인 팀으로써 Lifecycle 의 각 단계에 대한 verification과 validation을 수행한다.	verification계획과 결과, validation계획과 결과
Safety Manager	안전성 수명주기에 따른 안전성 활동을 수행하며, 시스템의 안전성 확보에 주력한다.	안전성 활동

열차제어시스템 안전향상 핵심기술 부분에서 요구하는 인력은 조직의 독립성 확보에 기반을 둔다. 그러나, 연구과제의 특성상 평가그룹은 안전성 보증팀에서 독립적인 인원으로 구성하여 수행한다. 철도종합안전개발사업의 대상 시스템을 위한 연구의 품질이나 제품의 중요성을 고려할 때 중, 고급 개발 인력이 투입되어야 한다. 외부와의 연결 창구 역할은 프로젝트 리더가 맡도록 한다. 본 문서에서 안전성 보증팀이라 함은 안전성 활동 업무를 담당하는 인원을 가리키며, 설계/개발팀은 제품 설계 및 개발 업무를 담당하는 인원을 가리키며 팀장은 각 팀의 리더를 지칭한다.

본 과제는 열차제어시스템의 안전향상 핵심기술 확보를 위한 연구개발 과제로서, 안전성 평가 및 적용성 연구를 위한 대상 열차제어시스템 및 시뮬레이터 개

발을 병행 수행하는 장기간의 과제이며, 투입인력의 역할 분담 및 협조를 위한 분산형 팀으로 구성한다. 또한, 투입되는 인력이 제한되어 있으므로 각 단계의 역할이 순환되도록 한다.

대상시스템의 설계/개발과 관련된 활동은 설계/개발팀에서 수행하며, 안전성 활동은 안전성 보증팀에서 수행함을 원칙으로 한다. 통합시험 단계에서는 독립된 팀을 구성하여 수행함이 원칙이나 본 과제에서는 안전성 보증팀의 주관하에 설계/개발팀에서 수행하는 것으로 한다.

② 시스템 설명

안정성 활동을 위한 대상시스템은 본 과제에서 개발한 열차제어용 고안전성 연산제어 시스템이다. 고안전성 연산제어 시스템은 시스템의 안정성을 확보하기 위하여 TMR(Triple Modular Redundancy)시스템으로 구성되어있다. 총 3계의 시스템으로 구성되어 있고 1계는 CPU 보드, DSV, 보드, SIO 보드, VDI/VDO 보드로 구성되어 있고 2계와 3계는 CPU 보드, DSV 보드로 구성되어 있다. 3개의 DSV 보드에는 각 보드별로 공유하는 공유 메모리가 있는데 자기 영역 이외에 다른 2개의 보드로 보내는 데이터가 여기 위치하게 된다. 1계 시스템은 VDI 보드로부터 데이터를 입력받아서 입력된 데이터를 DSV 보드를 통해 다른 2,3계의 시스템과 공유하게 된다. DSV 보드들은 공유된 데이터를 처리하여 다신 1계의 시스템에게 보내준다. 1계 시스템은 2 out of 3 알고리즘을 이용하여 처리된 데이터를 VDO 보드를 통해 출력하는 구조로 되어있다. 3중화와 2 out of 3 알고리즘을 이용함으로써 1개의 시스템이 오동작을 하더라도 전체 시스템에 영향을 미치지 않음으로써 시스템을 안정성을 향상 시켰다. 또한 VDI/VDO 보드를 사용함으로써 DI/DO 보드를 사용하였을 때 입력단의 오류나 출력이 제대로 나가는지를 확인 할 수 없다는 문제점을 극복하였다.

③ 예비위험원분석 (PHA)

예비 위험원 분석(PHA)기법은 시스템의 관련 정보가 적은 상태에서도 비교적 쉽게 수행할 수 있는 방법이며, 여러 가지 분석방법 중 가장 우선적으로 수행되는 방법이다. 대상시스템의 도출된 위험원에 대한 분석을 수행하며, 이에 대한 증거자료로 예비위험원 분석 보고서를 작성하였다. PHA(Preliminary Hazard

Analyzer)는 도출된 위험원의 사고 위험 정도를 평가하여, 위험원의 영향과 심각도 등을 분석하여야 한다. 또한 도출된 위험원을 제거하거나 경감시키기 위해 수립되어야 할 설계 및 안전 요구사항을 포함한다. 본 연구에서는 EN 50129 Application Guideline에서 권장하고 있는 HAZOP을 적용하였다. 평가대상 시스템인 고안전성 연산제어시스템에 적용 예정인 열차제어시스템의 안전성을 확보하기 위해 열차제어시스템으로부터 발생할 수 있는 기본 위험원을 다음과 같이 도출하였다.

- 정의된 최소 열차간격 이하로 열차간 접근: 이 위험원은 열차제어시스템의 열차 간격제어 기능의 실패로 인해 발생할 수 있는 상황으로 열차간 충돌의 가능성이 높다.
- 열차의 안전속도를 초과하는 열차: 이 위험원은 열차제어시스템의 간격제어와 관련하여 제어시스템의 열차 속도제어 실패 시, 열차간 충돌의 가능성이 높다.

PHA는 위에서 정의한 위험원에 대해 그 원인을 파악하고 그에 대한 대책을 수립하는 분석기법으로 시스템 구상 단계에서 수행되었다. 열차제어시스템의 핵심 기능을 담당하는 CPU 모듈과 연관된 고안전성 연산제어시스템의 열차간격제어와 같은 연차 방호기능을 담당한다. 본 연구에서는 철도시스템의 위험원 분석에 효과적으로 적용할 수 있도록 Parameter와 Guide word를 수정하여 적용하였다. HAZOP Study에서의 Parameter와 Guide word를 적용할 수 있는 물리적, 시간적, 운영적인 변수들을 의미하며 다음과 같이 특정변수와 일반 변수로 구분하여 적용하고 있다.

- HAZOP Guide word 정의

본 연구에서 제안한 철도시스템에 적용하기 위한 HAZOP에서의 Guide word는 다음과 같이 정의되었다.

Guide word	Description	관련 Parameter
No, Not, None	정의된 Parameter가 없음	Interface, Time, Action, Limit, Procedure, Data
Pard of	일부만 수행되거나 고려됨	Action, Procedure, Outside, Data
early	정의된 시간보다 일찍 수행됨	Time, Action, Data
Late	정의된 시간보다 늦게 수행됨	Time, Action, Data
More	변수의 초과 및 증가	Limit, Data
Less	변수의 미달 및 감소	Limit
Other than	비정상적인 Parameter	Interface, Action, Limit, Procedure, Outside, Data

- 고안전성 연산제어시스템의 HAZOP Study
- 고안전성 연산제어 시스템 적용가능성이 있는 열차제어시스템의 HAZOP Study는 위험원별로 구분하여 수행하였으며, 각 위험원에 적합한 Parameter와 Guide word를 적용하여 수행하였다.

Hazard-1 정의된 최소 열차간격 이하로 열차간 접근						
Parameter	Guide word	Deviation	Causes	Description	Consequences	Mitigation
Interface	No	Interface 불가	열차의 위치 확인 실패	열차의 위치확인 불가로 열차간 접근을 확인할 수 없음.	열차충돌	열차와의 인터페이스 불가 시 열차 비상정지
			열차 속도정보 확인 실패	열차와의 인터페이스 불가로 열차의 속도를 확인할 수 없음.	열차충돌	열차와의 인터페이스 불가 시 열차 비상정지
			열차 고장정보 확인 실패	열차의 고장정보 확인불가로 열차의 고장유무를 확인할 수 없음	열차충돌	열차와의 인터페이스 불가 시 열차 비상정지
			열차 이동권한 전송 실패	열차이동권한 차상으로 전달하지 못함	열차충돌	열차와의 인터페이스 불가 시 열차 비상정지
Action	No		열차 위치보고 실패	전방의 열차 위치 보고가 부정확하거나 잘못 계산되어 충돌사고	열차충돌	열차 절대 위치 확인
	Other	비정상적인 동작	제어기 이상동작 및 확인 실패	제어기의 이상동작에 대한 사전 감시장치 이상으로 제어 기능이 무결성하지 않음	열차충돌	제어기 상시 감시 장 치 동작 이상 유무 확인
Limit	More	한계 초과	열차 안전속도 초과	열차 과속으로 인한 안전 제동 실패	열차충돌	열차 속도 초과 시 열차 운행속도 제어
Data	No	Dara 없음	열차 이동권한 설정 실패	안전하지 못한 열차이동권한 설정으로 열차간 접근	열차충돌	열차제어시스템 다중계 설계
	Other	비정상적인 Data	열차 속도 표시 오류	열차의 속도 표시장치 오류 정보처리로 전방열차와의 근접	열차충돌	열차제어시스템 다중계 설계
			수동 및 자동정지 장치 제어 인터페이스 오류	과주에 대한 수동 및 자동정지 장치 제어 인터페이스 오류	열차충돌	열차제어시스템 다중계 설계

④ FTA

FTA는 시스템에 존재하는 잠재적 위험원을 정량적으로 산출하는 방법으로 FTA에 대한 자료를 충분히 제시하여야 하며, 대상시스템에 적용한 증거자료를 작성한다. 아래 그림은 기본적인 열차제어시스템에서의 고장분류를 표시한다.

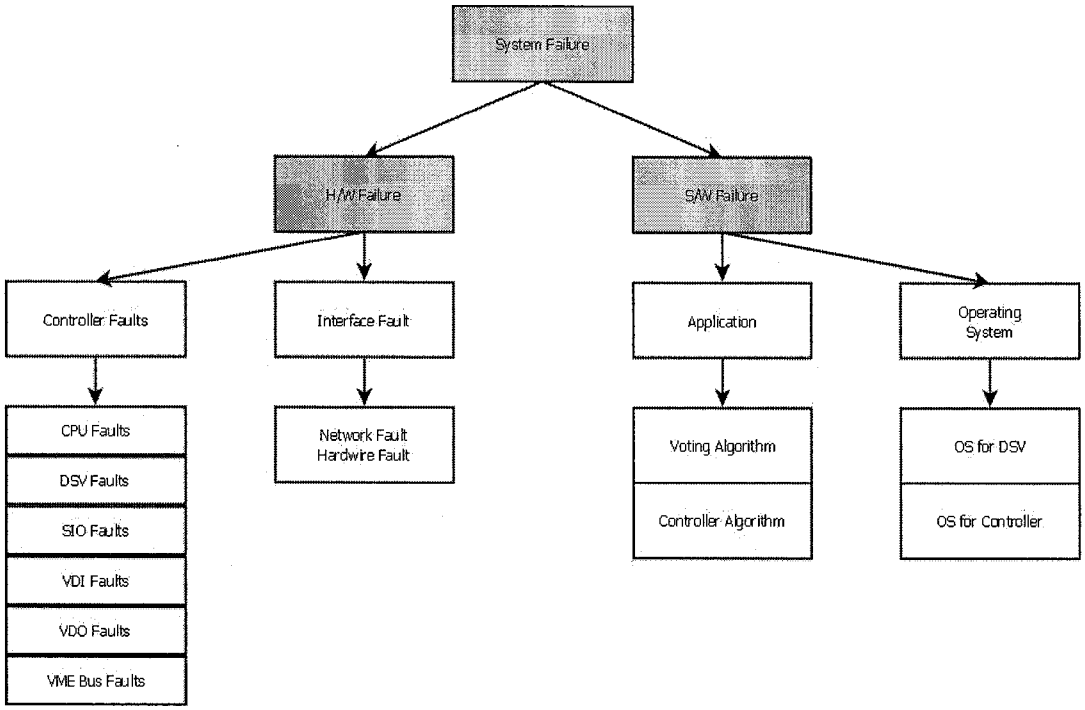


그림 3.7.33 기본 열차제어시스템 고장 분류

위의 시스템 모델은 2가지 종류의 레벨로 구성된 계층적 모델로 설명되고 있다. 상위 레벨의 모델은 고장 트리 모델이고 각각의 고장 요소들은 Markov 체인을 포함하고 있다.

- 상위 레벨 고장 트리 모델

  아래의 그림 전체 시스템은 2개의 controller subsystem과 한 개의 VDI/VDO subsystem을 포함하고 있는 상위 레벨 고장 트리 모델을 보여준다. controller subsystem은 CPU, DSV, SIO가 하나로 묶여진 시스템을 의미하며 VDI/VDO는 입출력을 담당하는 VDI, VDO를 의미한다. controller subsystem은 3중화와 2 out of 3로 구성되어 있기 때문에 3개의 시스템 중 2개 이상의 시스템 이상이 생길 경우만 오류가 발생한다. 그래서 두 개의 시

스템을 AND 게이트로 연결하여 2개다 이상이 발생할 경우만 전체 시스템 결함이 발생되도록 하였다.

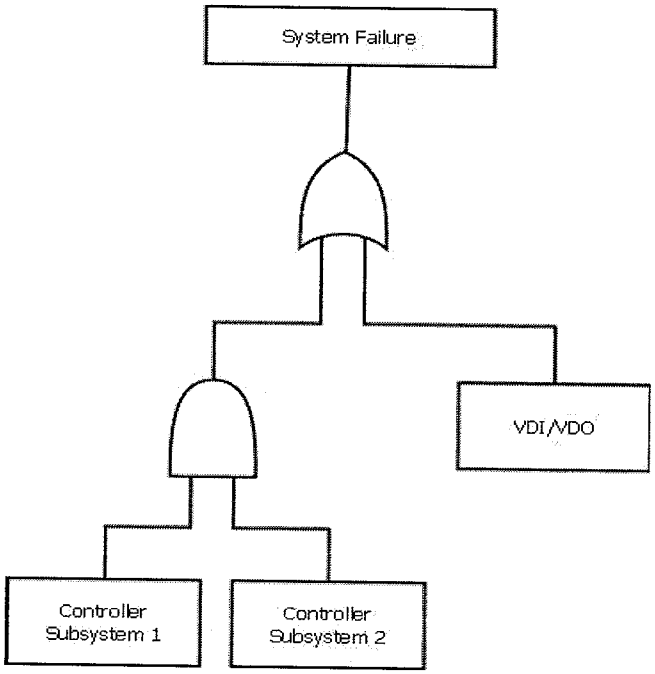


그림 3.7.34. 시스템 고장에 대한 책임 트리

controller subsystem은 또한 하나의 상위 레벨이 될 수 있으면, 제어용 하드웨어 고장, OS의 고장, S/W의 고장을 포함할 수 있다. 그림 3.4.35는 controller subsystem의 고장 트리를 보여준다.

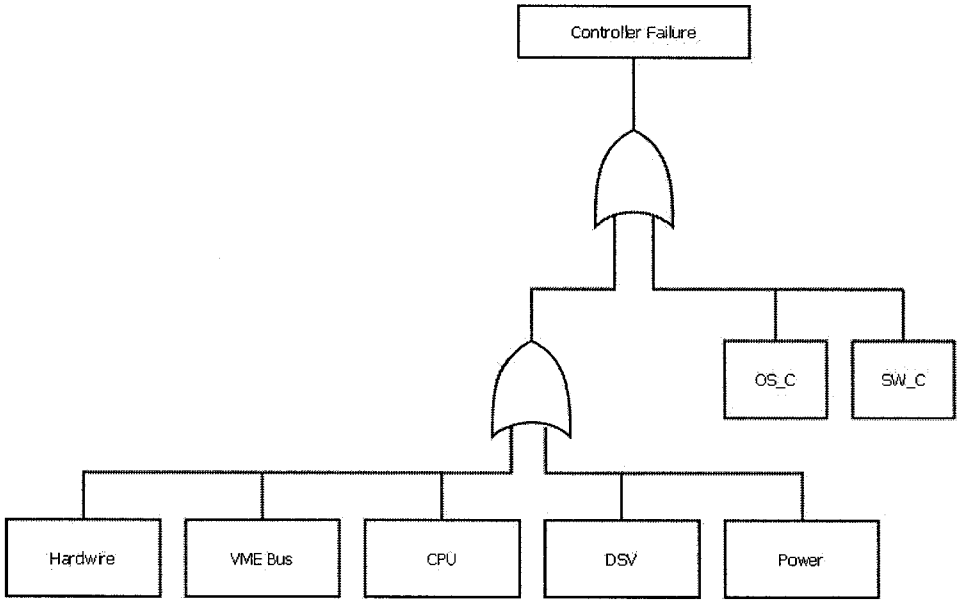


그림 3.7.35 Controller subsystem의 고장 트리

아래 그림 3.7.36은 VDI/VDO의 고장 트리를 보여준다. VDI/VDO는 운영체제(OS)를 가지고 있지 않은 시스템이기 때문에 소프트웨어 부분에서는 소프트웨어(SW)에 의한 고장만을 고려하였다.

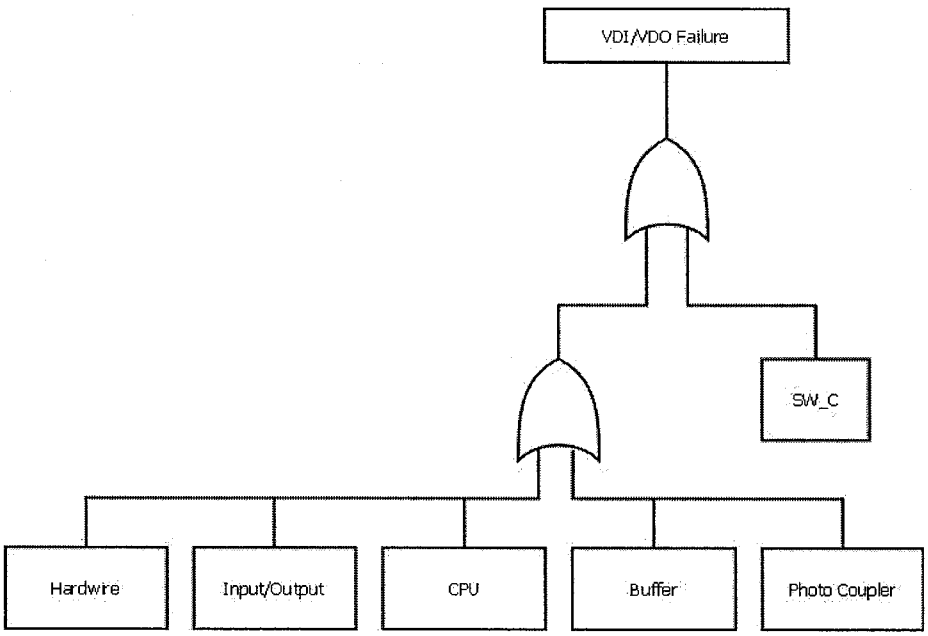


그림 3.7.36 VDI/VOD의 고장 트리

• 하위 CPU 레벨 Markov 체인 모델

상태는 ST에서 시작되어서 G로 이동하게 된다. ST상태는 부트 시퀀스가 시작되기 전 자가 진단을 하는 셀프 테스트 상태를 의미한다. G상태는 동작과 제어가 준비가 상태인 동작 상태를 의미한다. FE 상태는 고장이나 에러가 발생하였을 때를 나타내는 상태로써 coverage 가능성에 따라 평균 감지 시간이후 SF나 혹은 UF 상태로 이동하게 된다. 또한 ST 상태는 SF나 UF 상태에게 γ_{CPU}를 전송한다. ST는 일반적으로 sojourn 시간을 배포한다. ST에서 G 상태로 이동은 파라미터3과 3/T를 포함하여 Erlang distribution의 세 단계 상태를 거치게 된다.

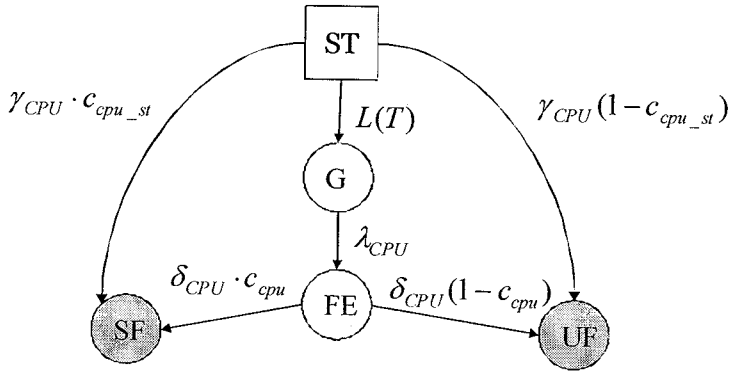


그림 3.7.37 CPU를 위한 Semi-Markov 모델

• SIO 서브 모델

아래의 그림은 SIO(Serial Input Output)를 위한 신뢰성과 안정성 모델을 보여준다. TCN 서브모델과 비슷하게, G 상태가 초기 상태이고 $1/\lambda_{SIO}$는 평균 고장시간을 의미한다. C_{SIO} 의 확률로 평균 고장 감지 시간이 $1/\lambda_{SIO}$와 고장은 SF 상태로 이동되게 된다. UF상태의 MTTF는 위의 서브모델에 의해 유도되어진다.

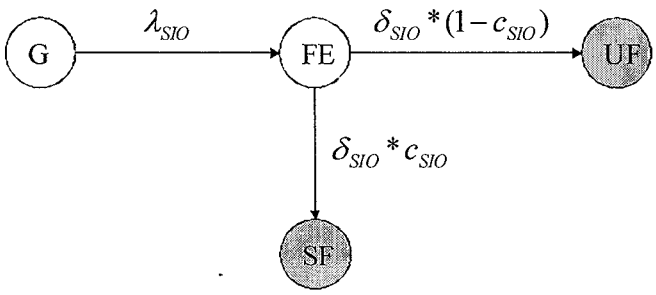


그림 3.7.38 SIO을 위한 신뢰성, 안정성 모델

$$MTTF = \frac{1}{\lambda_{SIO}} + \frac{1}{\delta_{SIO}}$$

$$CMTTF_{|UF} = \frac{1}{1 - c_{SIO}} \left(\frac{1}{\lambda_{SIO}} + \frac{1}{\delta_{SIO}} \right)$$

- VDI 서브 모델

아래의 그림은 VDI(Digital Input)를 위한 신뢰성과 안정성 모델을 보여준다. VDI는 $1/\lambda_{DI}$의 평균 시간에 의해 고장이 발생되고, C_{DI}의 확률로 복원되게 된다.

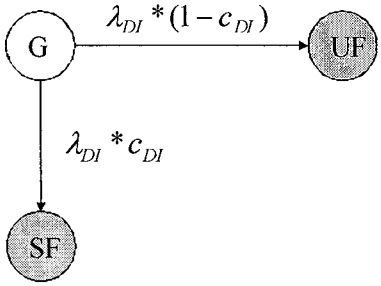


그림 3.7.39 VDI을 위한
신뢰성, 안정성 모델

$$MTTF = \frac{1}{\lambda_{DI}}$$

$$CMTTF_{|UF} = \frac{1}{\lambda_{DI}(1 - c_{DI})}$$

• VDO 서브 모델

아래의 그림은 VDO(Vital Digital Output)를 위한 신뢰성과 안정성 모델을 보여준다. G 상태는 초기화 상태이고 $1/\lambda_{DO}$와 $1/\delta_{DO}$에 의해 고장이 발생된다. 고장은 C_{DO}의 확률로 복원된다. MTTF는 위의 서브모델에 의해 유도되어진다.

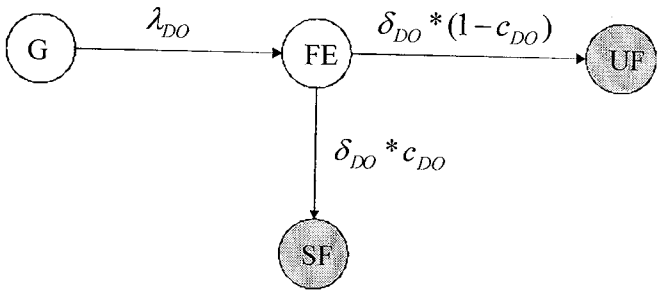


그림 3.7.40 VDO을 위한 신뢰성, 안정성 모델

$$MTTF = \frac{1}{\lambda_{DO}} + \frac{1}{\delta_{DO}}$$

$$CMTTF_{|UF} = \frac{1}{1-c_{DO}}\left(\frac{1}{\lambda_{DO}} + \frac{1}{\delta_{DO}}\right)$$

⑤ 위험원 도출

열차제어시스템 위험원 도출에 대한 내용을 정리하면 다음과 같다.

(가) 주요 열차제어시스템의 위험원 종류

- 철도차량의 충돌
- 철도차량의 탈선
- 선로설비에 의한 충돌
- 선로설비에 의한 탈선
- 선로설비에 의한 건널목 사고
- 신호취급원에 의한 충돌
- 신호취급원에 의한 탈선

- 신호취급원에 의한 건널목 사고
- 외부요인에 의한 충돌
- 외부요인에 의한 탈선

(나) 철도차량의 충돌

1) 차상설비에서 열차의 속도정보 오류로 인한 열차 이상으로 충돌

- 위험원 설명 : 열차에 대한 속도정보의 오류로 인해 열차속도의 차상현시 오류, 열차 퇴행 등의 열차 이상 발생
- 위험원 요인

  차상속도계측 장치의 고장

  차상 통신장치의 고장

  차상속도정보 송신의 오류

  차상속도정보 수신의 오류
- 사고 시나리오

  차상속도계측 장치에서 현재 열차속도보다 낮은 속도로 정보 발생

  차상 통신장치의 정보 오류교정기능 결함,외란 등으로 속도정보의 왜곡 발생

  차상 신호설비의 과속 검지 불가 및 과속 차단 제어 불가

  안전한 운행간격 제어 불가 및 열차 제동거리 부족 상태 유지
- 안전대책(안)

  차상속도계측 장치의 신뢰성 확보

  차상 통신장치의 정보 오류교정기능 하드웨어화 및 신뢰성 확보

  차상속도계측 장치의 속도정보를 운행장치 속도정보와 비교 재확인

2) 차상설비에서 열차의 상태정보 오류로 인한 열차 이상으로 충돌

- 위험원 설명 : 열차에 대한 상태정보의 오류로 인해 열차속도의 차상현시 오류, 열차 퇴행, 편성 분리 등의 열차 이상 발생
- 위험원 요인

  차상 인터페이스 결함

  차상속도계측 장치의 고장

  차상 통신장치의 고장

차상 정보송신의 오류

차상 정보수신의 오류

- 사고 시나리오

차상속도계측 장치에서 현재 열차속도보다 낮은 속도로 정보 발생

차상 통신장치의 오류 교정기능 결함, 외란 등의 고장으로 속도정보의 왜곡 발생

차상 신호설비의 과속 검지 불가 및 과속 차단 제어 불가

열차의 안전한 운행간격 제어 불가 및 열차 제동거리 부족 상태 유지

- 안전대책(안)

차상속도계측 장치의 속도정보를 운행장치 속도정보와 비교 확인

3) 차상설비에서 열차의 속도정보 오류로 인한 운전취급 결함으로 충돌

- 위험원 설명 : 열차에 대한 속도정보 오류로 인하여 상황 오판, 신호위반, 비상제동 취급 등과 같은 운전취급 결함 발생

- 위험원 요인

차상속도계측 장치의 고장

차상 통신장치의 고장

차상속도정보 송신의 오류

차상속도정보 수신의 오류

차상속도정보 현시의 오류

- 사고 시나리오

차상속도계측 장치에서 현재 열차속도보다 낮은 속도로 정보 발생

차상 통신장치의 정보 오류교정기능 결함, 외란 등으로 속도정보의 왜곡 발생

차상의 속도정보표시기에 잘못된 열차속도를 현시

과속 상태에 대한 오판, 신호 위반 등의 규정 위반 발생

차상 신호설비의 과속 검지 불가 및 과속 차단 제어

열차의 안전한 운행간격 제어 불가 및 열차 제동거리 부족 상태 유지

- 안전대책(안)

차상속도계측 장치의 속도정보를 운행장치 속도정보와 비교하여 불일치가 발

생할 경우 청각적, 시각적 경보를 발생

4) 차상설비에서 열차의 상태정보 오류로 인한 운전취급 결함으로 충돌
- 위험원 설명 : 열차에 대한 상태정보 오류로 인하여 상황 오판, 속도제어, 신호위반, 비상제동취급, 열차방호 오류 등과 같은 운전취급 결함 발생

5) 차상설비에서 열차속도의 제어 오류로 인한 운전취급 결함으로 충돌
- 위험원 설명 : 열차에 대한 속도의 제어 오류로 인하여 상황 오판, 신호위반, 비상제동취급, 열차방호 오류 등과 같은 운전취급 결함 발생

6) 차상설비에서 열차이동권한의 제어 오류로 인한 운전취급 결함으로 충돌
- 위험원 설명 : 열차에 대한 이동권한의 제어 오류로 인하여 상황 오판, 속도제어 오류, 신호위반, 비상제동취급, 열차방호 오류 등과 같은 운전취급 결함 발생

7) 차상설비에서 열차의 속도정보 오류로 인한 차단구간 오진입으로 충돌
- 위험원 설명 : 열차에 대한 속도정보 오류로 인하여 파손된 선로구간 운행, 무허가 구간 운행, 작업 및 공사 구간 운행, 분기기 파손 등과 같은 차단구간 오진입 발생

8) 차상설비에서 열차의 상태정보 오류로 인한 차단구간 오진입으로 충돌
- 위험원 설명 : 열차에 대한 상태정보 오류로 인하여 파손된 선로구간 운행, 무허가 구간 운행, 작업 및 공사 구간 운행, 분기기 파손 등과 같은 차단구간 오진입 발생

9) 차상설비에서 열차속도의 제어 오류로 인한 차단구간 오진입으로 충돌
- 위험원 설명 : 열차에 대한 속도의 제어 오류로 인하여 파손된 선로구간 운행, 무허가 구간 운행, 작업 및 공사 구간 운행, 분기기 파손 등과 같은 차단구간 오진입 발생

10) 차상설비에서 열차이동권한의 제어 오류로 인한 차단구간 오진입으로 충돌

- 위험원 설명 : 열차에 대한 이동권한의 제어 오류로 인하여 파손된 선로구간 운행, 무허가 구간 운행, 작업 및 공사 구간 운행, 분기기 파손 등과 같은 차단구간 오진입 발생

- 고안전성 연산제어시스템 위험원 도출 1단계에 대한 내용을 정리하면 다음과 같다.

  " 위험원 도출의 가장 우선적인 단계는 최상위 위험원을 선정하는 작업이다. 최상위 위험원이라 함은 개발되는 시스템에서 발생할 수 있는 최악의 사고 또는 최종적인 사고의 결과이다. 안전성 관련 국제규격에서 사고 피해 심각도에 대한 정의가 인명에 대한 피해정도와 재산상의 피해정도로 분류되어 있기에 최상위 위험원의 결정도 이와 마찬가지로 시스템이 인명에 대한 피해정도와 재산상의 피해 정도를 고려하여 결정하여야 한다."

표 3.7.8 위험원 도출 1단계

위험원	설명	비고
잘못된 보팅결과 출력	2 out of 3 알고리즘에 위배되는 결과 출력	DSV
동작 불능	출력이 안 나오거나, 고정 값 출력	DSV
입력 불능	외부 변화에 따른 입력이 변하지 않음	VDI
출력 불능	보팅 후 올바른 값이 출력되지 않은	VDO

최상위 위험원을 발생시킬 수 있는 위험원을 도출하는 단계이다. 위험원이란 용어는 매우 광범위하고 모호함을 지니고 있기에 이러한 오류를 줄이기 위해 시스템 기능, 인터페이스, 특성, 관련 설비 범주를 선정한다.

범주는 위험원에 쉽게 접근할 수 있도록 회의에서 전문가 및 엔지니어의 의견으로 결정된다. 위험원을 도출한다는 것은 매우 광범위한 작업이다. 개발하려는 시스템이 어떠한 잠재 위험원을 내재하고 있는지 예상하기란 쉬운 일이 아니다. 위험원의 모호성이란 위험원의 정답은 없다는 뜻을 내포하고 있다. 정답은 없으나 도출된 위험원을 벗어나 발생되는 사고에 대해서는 책임을 져야 하기에 시스템에서 발생

가능한 모든 사고를 만족시키는 위험원을 도출해야 한다. 따라서 위험원 도출 단계에서는 모든 사고를 만족시키는 결과를 얻어야 하지만, 세분화된 위험원을 무작정 도출한다면 안전성 활동 및 관리대상이 방대해져 개발 라이프사이클동안 안전성 활동이 이루어지기 어려울 것이며, 미쳐 고려되지 않은 잠재위험원이 존재할 수 있는 오류를 범할 수 있다. 고안전성 연산제어시스템 위험원 도출 2단계에 대한 내용을 정리하면 다음과 같다

표 3.7.9 대상시스템 위험원 도출 Sheet

	보팅결과 이상	동작 불능		하드웨어 불능			소프트웨어 불능	
	마이너 리포트	고정된 출력	출력 무	메모리 오류	CPU 오류	입,출력 오류	알고리즘 오류	통신 오류
	A1	B1	B2	a	b	c	a	b
TMR	•						A1-d	A1-e
		•				B1-c	B1-d	
			•	B2-a	B2-b	B2-c		
VDI		•					C1-c	
			•		C1-a	C1-b		
VDO		•					D1-c	
			•		D1-a	D1-b		

위에서 제시된 표를 기반으로 위험원을 도출하면 다음의 표와 같다.

표 3.7.10. 도출된 위험원

사고	No.	ID	상위 위험원
잘못된 voting 결과 출력	1	A1-d	TMR시스템의 알고리즘 오류로 인한 minority report
	2	A1-e	TMR시스템의 통신 오류로 인한 minority report
동작 불능	3	B1-c	TMR시스템의 입출력부 오류로 인한 고정된 출력
	4	B1-d	TMR시스템의 알고리즘 오류로 인한 고정된 출력
	5	B2-a	TMR시스템의 메모리 오류로 인한 출력 無
	6	B2-b	TMR시스템의 CPU 오류로 인한 출력 無
	7	B2-c	TMR시스템의 입출력부 오류로 인한 출력 無
	8	C1-a	VDI 보드 CPU 오류로 인한 출력 無
	9	C1-b	VDI 보드 입출력부 오류로 인한 출력 無
	10	C1-c	VDI 보드 알고리즘 오류로 인한 고정된 출력
	11	D1-a	VDO 보드 CPU 오류로 인한 출력 無
	12	D1-b	VDO 보드 입출력부 오류로 인한 출력 無
	13	D1-c	VDO 보드 알고리즘 오류로 인한 고정된 출력

(4) 고안전성 연산제어 시스템의 특징 및 장점

여기에서는 앞에서 설명한 개발 시제품의 주요한 특징 및 장점에 대해 간략하게 정리하였다. 또한 개발 시제품의 실용화 추진을 위해 당해연도에는 작성한 개발 시제품을 기준으로 한 고안전성 연산제어시스템 설치 및 확인 지침서 초안을 설명하고 있다. 이 지침서 초안은 본 개발 시제품의 실증시험을 거친 후 보완되어 실용화를 위한 기반 문서로 활용될 예정이다.

개발한 고안정성 연산제어 시스템은 I/O보드로부터 입력된 신호를 3중으로 동일한 프로세스를 처리함으로써 불특정 하나의 시스템에서 문제가 발생되어도 지속적인 기능을 제공할 수 있다. 또한 3중화로 인하여 시스템에서 연산한 결과를 3중으로 비교함으로써 출력에 대한 높은 신뢰성을 제공하고 있다. I/O 보드들은 VDI, VDO를 이용함으로써 I/O 보드들의 입출력 부분의 오류에 의한 오동작을 방지함으로써 안정성을 더욱 향상 시켰다. 보안된 고안정성 연산제어 시스템에 사용되는 보

드들은 크게 CPU 보드, DSV 보드, VDI/VDO 보드로 분류할 수 있다.

DSV 보드는 300MHz 급의 고성능 DSP, 256Kbytes(최대 512Kbytes)의 내부 보팅용 메모리 영역, 시리얼 통신, 이더넷 통신 제공하므로 써 데이터 공유 및 보팅에 뛰어난 성능을 제공한다. 한편, VME System Controller와 Slave 를 모두 사용 가능하기 때문에 별도의 CPU 보드 없이 DSV 보드만으로도 열차제어시스템 구성이 가능한 장점이 있다. 본 고안전성 연산제어 시스템의 주요 장점은 아래와 같다.

- 하나의 연산제어 시스템 결함이 발생하여도 지속적 기능 제공 : 고안전성 연산제어 시스템은 2 out of 3 보팅에 따라 출력 결과를 선택한다. 즉 3개 시스템 출력을 검사하여 2개 이상의 출력이 같을 경우만 해당 출력을 사용한다. 따라서 3개 중 하나의 시스템에 결함이 발생하더라도 나머지 2 시스템으로 지속적으로 시스템 기능을 제공할 수 있다.
- 소프트웨어적인 완벽한 입출력 동기화 제공 : 입력이 발생시 마스터 CPU에서 해당 입력을 동기화시켜 나머지 2개의 CPU로 전송하므로써 세 개의 CPU는 항상 같은 입력에 대한 연산을 수행한다. 세 개의 CPU 가 출력한 출력도 동일한 입력에 대한 출력이 확인 될 경우만 보팅함으로 항상 동기화 할 수 있다.
- 출력 결과의 높은 신뢰성 : 단일 시스템의 출력만 사용하는 것이 아니라 세 개의 시스템이 동일한 입력에 대하여 출력한 결과를 사용하므로 출력 결과의 높은 신뢰성을 보장한다.
- 기존 시스템을 손쉽고 저비용으로 고안전성 연산제어 시스템으로 구축 가능 : 고안전성 연산제어 시스템을 구축하기 위해 DSV 외에 별도의 장비가 필요 없고, VME 버스를 통해 주 CPU 보드와 통신하므로 설치 또한 매우 용이하다. 따라서 구축 및 유지 보수시의 비용 절감 효과가 있다.
- 최소의 설치 공간 차지 : VME 표준 보드로 고안전성 연산제어 시스템을 구축하므로써 별도의 설치 공간 및 공사를 필요로 하지 않는다.
- 고성능 DSP CPU 사용으로 데이터 공유 및 보팅 성능 향상 : 데이터 처리 성능이 매우 뛰어난 300MHz 급의 DSP를 사용 하므로써 데이터 공유 및 보팅 시의 지연시간을 최소화한다.
- CPU 보드 없이 DSV 보드만으로 연산제어 시스템 구축 가능 : DSV 보드가

System Controller 기능을 지원하므로 별도의 CPU 없이 DSV 보드 3장만으로도 고안전성 연산제어 시스템 구축이 가능하다.

- 하드웨어 오류에 의한 입력부분 오작동 감지 : VDI 보드의 이중화된 입력 채널을 비교하여 입력을 수신하는 기능과 전압 체크 기능에 의해 입력부분의 하드웨어 오류를 감지할 수 있다.
- 하드웨어 오류에 의한 출력부분 오작동 감지 : VDO 보드의 출력을 피드백 하여 확인하는 기능과 포트별 Fail Safe 설정 기능에 의해 출력단의 하드웨어 오류에 의한 오작동을 감지 할 수 있다.

■ *고안전성 연산제어 시스템 설치 및 확인 지침서 초안(High Reliable Logic Control System Guide for Installation and Check)*

1. 개 요

1.1. 지침서의 목적

1.1.1. 본 지침서에서는 고안전성 연산제어 시스템을 열차제어를 위해 사용하기 위한 설치와 운영 관련 지침을 제공함을 목적으로 한다.

1.1.2. 본 지침서는 열차제어에 고안전성 연산제어 시스템의 사용을 원하는 사용자를 위하여 시스템을 설치 및 초기 상태를 점검하고 고안정성을 유지하기 위해 작성되었다.

1.1.3. 본 지침서는 열차제어용 고안전성 연산제어 시스템 사용에 대한 기술 지침을 제공하여, 열차 사고 시 발생할 수 있는 인적, 물적 피해의 최소화에 기여 하고자 한다.

1.2. 지침서의 범위

1.2.1. 본 지침서는 사용 대상은 고안전성 연산제어 시스템을 이용하여 열차제어에 사용하는 열차로 한정한다. 고안전성 연산제어 시스템이 사용되지 않은 열차에 대해서는 대상에서 제외한다.

1.2.2. 본 지침서는 열차 시스템에서 안정성을 높이기 위하여 고안전성 연산제어 시스템을 사용하여 열차 신호시스템을 제어하는 차량에 대하여 사용자가 고안전성 연산제어 시스템의 초기화 과정에 적용할 수 있다.

1.2.3. 본 지침서는 열차제어용 고안전성 연산제어 시스템을 설치 와 초기화 과정 이후 전

면부의 LED 등을 통해 시스템이 안정적인 동작여부를 판단하고 열차제어 시스템을 운영할 수 있도록 하는 지침을 제고한다. 이외의 다른 특수 상황이나 기술적인 분야의 구현 알고리즘에 관한 내용은 수록하지 않는다.

2. 설치절차

2.1.1. 열차제어용 고안전성 연산제어 시스템의 외형적 구성은 총 3개의 렉(Rack, 6U)과 2개의 팬(FAN, 1U), 그리고 1개의 허브(Hub, 1U)로 구성되어 있다. 첫 번째 렉인 1계는 1장의 전원보드(12HP)와 5장의 보드(4HP)로 구성되어있다. 두 번째와 세 번째인 2,3계는 1장의 전원보드와 3장의 보드로 구성되어있다. 시스템의 후면에는 각 렉당 1장의 보드들이 터미널 보드를 통해 통신포트가 연결되어 있다.

2.2.2 본 지침서에 의한 제시된 열차제어용 고안전성 연산제어 시스템의 안정화 설치과정 절차는 다음과 같다.

(1) 캐비닛에 렉, 팬, 허브등이 모두 취부 되었는지 확인

(2) 캐비넷에 렉, 팬, 허브등이 제대로 삽입됐는지 확인

(3) 해당 렉별 보드들이 보드 취부 되어있는지 확인

(4) 각 보드들이 렉에 제대로 삽입됐는지 확인

(5) 렉 후면부에 터미널 보드들에 통신 포트가 제대로 연결되었는지 확인

3. 시스템 초기화 이후 안정성 점검

3.1.1. 열차제어용 고안정성 연산제어 시스템에 1계는 CPU 보드, DSV 보드, VDI 보드, VDO 보드, SIO 보드로 구성되어있다. 각 보드들의 전면부 LED를 통해 현재 상태를 표시하고 있다. 이 LED들을 통해 사용자는 현재 시스템이 안정적으로 초기화 되어서 동작되고 있는지를 육안을 통해 확인할 수 있다.

3.1.2. 본 지침서에 의한 제시된 열차제어용 고안전성 연산제어 시스템의 초기화 이후 시스템의 안정화 여부 확인은 각 보드들의 전면부 LED의 상태를 점검함으로써 판단할 수 있다. 다음은 각 보드별 LED들과 역할을 나타내고 있다.

(1) 파워 보드 : 3개의 LED
- *+5V : 녹색 LED, 점등되면 5V 입력이 안정적으로 공급되고 있음을 나타냄.*
- *+12V : 녹색 LED, 점등되면 12V입력이 안정적으로 공급되고 있음을 나타냄.*
- *-12V : 녹색 LED, 점등되면 -12V입력이 안정적으로 공급되고 있음을 나타냄.*

(2) CPU 보드 : 2개의 LED
- *DS1 : 황색 LED, 보드의 이상 유무를 나타냄. 이상이 있을 경우 LED가 점등됨.*
- *DS2 : 녹색 LED, CPU가 현재 안정적으로 동작될 경우 LED가 점등됨.*

(3) DSV 보드 : 10개의 ELD
- *RUN : 녹색 LED, 정상적으로 동작할 경우 LED가 점등됨*
- *VME : 녹색 LED, VME 버스를 통해 데이터를 접근하면 LED가 점등됨*
- *S1 : 황색 LED, 사용하지 않음.*
- *S2 : 황색 LED, 사용하지 않음.*
- *FAIL : 적색 LED, 보드의 이상 유무를 나타냄. 이상이 있을 경우 LED가 점등됨.*
- *SCON : 녹색 LED, 사용하지 않음.*
- *L1Tx : 녹색 LED, 후면부 터미널 보드에서 1번 통신포트를 통해 데이터를 송신할 때 점등됨.*
- *L1Rx : 녹색 LED, 후면부 터미널 보드에서 1번 통신포트를 통해 데이터를 수신할 때 점등됨.*
- *L2Tx : 녹색 LED, 후면부 터미널 보드에서 2번 통신포트를 통해 데이터를 송신할 때 점등됨.*
- *L2Rx : 녹색 LED, 후면부 터미널 보드에서 2번 통신포트를 통해 데이터를 수신할 때 점등됨.*

(4) VDI 보드 : 16개의 LED
- *RUN : 녹색 LED, 정상적으로 동작할 경우 LED가 점등됨*
- *VME : 녹색 LED, VME 버스를 통해 데이터를 접근하면 LED가 점등됨*

- ER : 적색 LED, 보드의 이상 유무를 나타냄. 이상이 있을 경우 LED가 점등됨.
- 1 ~ 12 : 녹색 LED, 각 채널별 동작여부. 동작중인 채널의 해당 LED가 점등됨

(5) VDO 보드 : 12개의 LED
- RUN : 녹색 LED, 정상적으로 동작할 경우 LED가 점등됨
- VME : 녹색 LED, VME 버스를 통해 데이터를 접근하면 LED가 점등됨
- ER : 적색 LED, 보드의 이상 유무를 나타냄. 이상이 있을 경우 LED가 점등됨.
- FS : 황색 LED, Fail Safe 동작 시 LED가 점등됨.
- 1 ~ 8 : 적색 LED, 각 채널별 동작여부. 동작중인 채널의 해당 LED가 점등됨

(6) SIO 보드 : 46개의 LED
- RUN : 녹색 LED, 정상적으로 동작할 경우 LED가 점등됨
- VME : 녹색 LED, VME 버스를 통해 데이터를 접근하면 LED가 점등됨
- DIAG0 : 황색 LED, 사용하지 않음.
- DIAG1 : 황색 LED, 사용하지 않음.
- FAIL : 적색 LED, 보드의 이상 유무를 나타냄. 이상이 있을 경우 LED가 점등됨.
- SCON : 녹색 LED, 사용하지 않음.
- RX 0 ~ 15 : RX 데이터가 0일 때 해당 채널의 LED가 점등됨
- TX 0 ~ 15 : TX 데이터가 0일 때 해당 채널의 LED가 점등됨
- RX P0 ~ P3 : RS232 직렬 포트의 RX 데이터가 0일 때 해당 채널의 LED가 점등됨
- TX P0 ~ P3 : RS232 직렬 포트의 TX 데이터가 0일 때 해당 채널의 LED가 점등됨

3.1.3 파워 보드의 LED들 중 한 개의 LED라도 점등되지 않으면 전원이 안정적으로 공급되지 못하여 시스템이 안정성을 보장할 수 없다.

3.1.4. 각 보드별 LED중 ER, FAIL, DS1의 LED가 점등되면 해당 보드별 소프트웨어 혹은 하드웨어적 문제가 발생한 것을 의미하면, 전체 시스템이 안정성을 보장할 수 없다.

4. 안정화 목적과 목표

4.1. 목적 (Goals)

4.1.1. 본 지침서에서 제시된 절차에 의한 열차제어용 고안전성 연산제어 시스템의 설치 와 초기 안정화 확인 절차의 최종적인 목적은 열차가 실제 운행을 시작하기 전 사전에 안정성을 확인 및 검토함으로써 열차 사고에 의한 피해를 최소화하는데 있다.

4.1.2 본 지침서의 목적은 기관사 등의 시스템 사용자가 육안을 통해 시스템의 이상 유무와 안정성을 검토 및 확인 할 수 있도록 함에 있다.

4.2. 목표 (Objectives)

4.2.1. 본 지침서에 의해 제시된 절차는 다음의 목표를 만족시켜야 한다.

(1) 사용자가 육안을 통해 전체 시스템의 이상 유무를 파악함.
(2) 열차제어용 고안전성 연산제어 시스템에 의한 사고를 미연에 방지.
(3) 시스템에 이상이 발견되었을 경우 사전에 미리 조치할 수 있게 함. ■

제8절 열차제어시스템을 위한 정형기법 적용기술 개발

	검증계획서 (Verification Plan)	**ID No :** TC - SR05 - SSR04 - 2009 작성일 : 2010. 05. 14 수정일 :

5. 프로젝트는 열차제어시스템 안전향상 핵심기술을 개발하여야 한다.

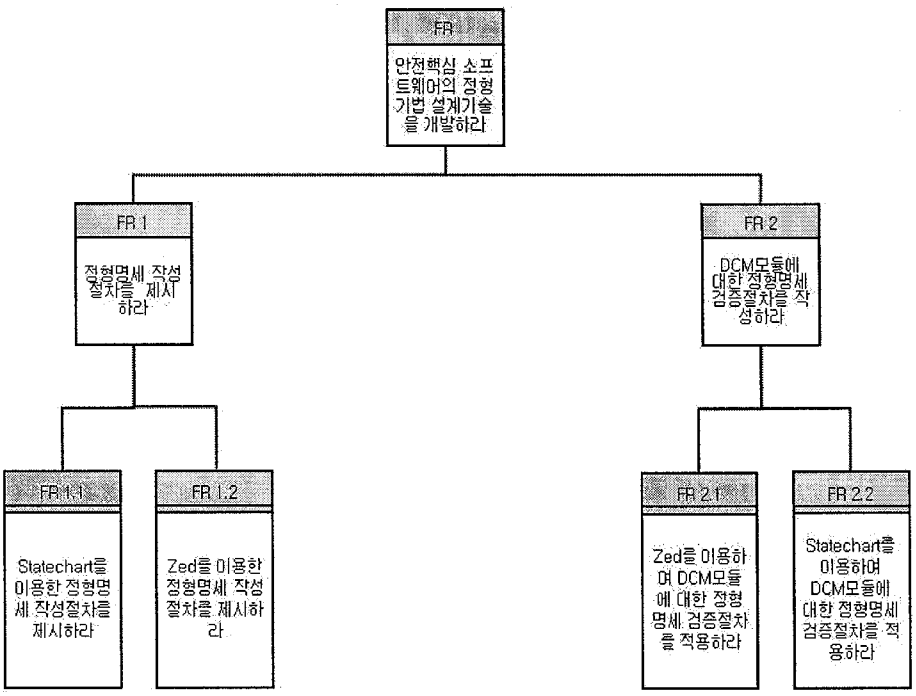
5.4 프로젝트는 열차제어시스템 안전핵심 소프트웨어의 정형기법에 의한 설계기술을 개발하여야 한다.

입력물 :	**업무 :**	**출력물 :**
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 보완된 DCM모듈 정형명세(Z & Statechart) 작성절차 및 검증절차 - 기능 아키텍처 - 물리 아키텍처 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 2.1 단순 상황분석, 3.3 전문가 검토	- SE 검증	- 수정 VRTM - 검증결과표

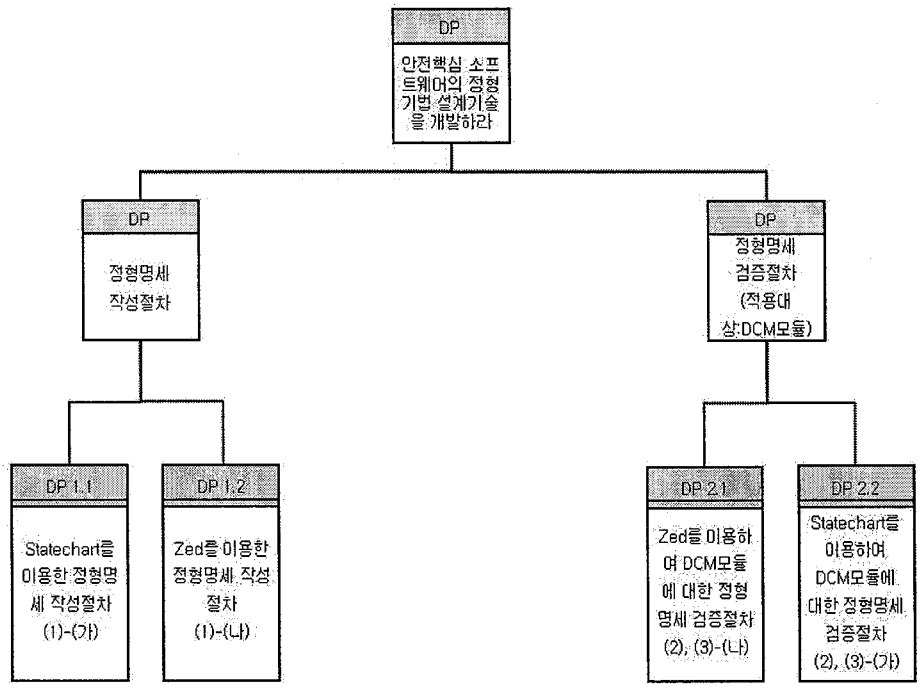
Verification Specification (검증기준) :

1. 열차제어시스템에 적합한 정형명세 작성절차가 제시되었는가?
2. 열차제어시스템에 적합한 정형명세 검증절차가 제시되었는가?
3. Z & Statechart를 예제에 적용하여 제안한 정형명세 작성절차 및 검증절차에 대한 타당성이 충분히 확보되었는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

정형기법 도구를 이용한 열차제어 바이탈 S/W를 위한 정형기법 적용기술의 개발은 시스템 요구사항 『SR 5. 프로젝트는 열차제어시스템 안전향상 핵심 기술을 개발하여야 한다.』 중 **『SSR. 5.4. 안전핵심 소프트웨어의 정형기법 설계기술을 개발하여야 한다.』**에 해당하는 내용이다. 열차제어시스템에 내장되는 안전핵심 소프트웨어의 개발에 정형기법 설계기술을 적용하기 위하여 정형기법도구(Zed, Statemate)를 선정하여 Mock-up시스템의 DCM의 안전핵심소프트웨어 사양서를 대상으로 열차제어시스템 S/W에 적합한 정형명세 작성절차 및 검증절차를 제시하였다.

나. 설계기준

- IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems"
- IEC 62278, "Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)"
- IEC 62279, "Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems"
- IEEE Std 830-1998, "IEEE Recommended Practice for Software Requirements Specification"
- IEEE/EIA 12207, "Standard for Information Technology-Software Life Cycle Processes"
- IEEE1233, "IEEE Guide for Developing System Requirements Specifications"
- Euro-Interlocking Project, 'Defines a strategy and programme to introduce formal methods into EURO-INTERLOCKING Projects2', Forma Methods Strategy Study Report, 2000
- 철도종합안전기술개발사업 , '열차제어시스템 안전성능 평가 및 사고방지기술 개발', 3차년도 연구보고서, 2008.

다. 검증 방법에 따른 증거 자료

본 절에서는 전년도에 요구사양에 따라 정형기법을 적용하여 안전핵심 소프트웨어 사양서에 대해 작성한 정형명세서를 보완하고, 열차제어시스템 안전핵심 소프트웨어의 정형명세 작성절차와 정형명세 검증절차를 제시하였다. 한 후 DCM모듈을 대상으로 그 적용성을 검토하였다. 우선 국내 정형기법 전문가와의 기술협의, 관련 자료의 분석 및 국내 지원환경을 고려하여 적용할 정형기법을 Zed와 Statemate로 정의하였으며, 본 과제에서 제작하고 있는 Mock-up 시스템의 DCM을 대상으로 하여 각 정형기법 도구를 적용하여 정형명세 작성절차와 검증절차의 타당성을 검토하였다.

라. 성과물의 내용 및 결과

(1) 열차제어시스템의 정형명세 작성 절차 연구

열차제어시스템은 안전 필수 시스템으로서 고신뢰성과 고품질이 요구된다. 신뢰성과 품질을 높이기 위해 관련 업계의 다수의 국제 표준에서는 정형기법을 이용한 시스템 개발을 요구하고 있다. 정형기법은 수학적 기반의 개념과 언어를 도입해서 시스템을 명세하고 검증하는 기법과 도구를 가리키는 것으로, 시스템 개발 생명주기 상에서 요구사항 분석과 상위수준의 설계단계에서 주로 사용되고 있다. 정형명세 언어를 사용하여 작성한 요구 명세는 정형명세 언어를 사용하여 자연어 요구사항을 기술하며, 정형요구명세에 대해 정형 검증을 수행하여 요구 사항에 대한 검증 속성의 만족 여부를 검사함으로써 일관성과 완전성을 검사할 수 있다.

정형기법이 수학적 기반의 개념과 언어를 사용하기 때문에, 시스템의 요구 분석이나 설계 단계와 같이, 정형기법을 적용하는 개발 단계에서 설계자나 개발자가 곧바로 정형요구명세를 생성하기 어려운 점이 있다.

본 연구에서는 안전 필수 시스템인 열차제어시스템의 정형요구명세 개발에 관계되어 있는 관계자(발주자, 개발자, 평가자)가 보다 쉽게 접근하기 위해, 정형요구명세의 설계 패턴을 사용하는 명세 작성과 절차와 명세 언어를 사용하여 명세를 작성하는 절차를 제안한다. 본 연구에서 사용한 정형기법 언어와 도구는 상태차트와 Z명세언어이다.

(가) Statechart를 이용한 정형명세 작성절차

상태차트는 대표적인 준정형(semi-formal) 명세언어에 속하며, 이벤트에 의해 시스템의 상태가 전이되고, 기능이 수행되는 내장형 또는 반응형 시스템의 행위를 기술하는데 적합하다.

본 연구에서는 정형요구명세와 검증을 거쳐 제시된 설계 사항들을 하나의 설계 패턴으로 정의하고, 시스템 개발 주기를 고려하여 안전 필수 시스템의 설계 단계에서 활용될 수 있는 패턴을 이용한 정형명세 개발 프레임워크를 제안한다.

디자인 패턴의 정의는 기존 환경에서 반복적으로 발생하는 문제들을 설명하고, 문제해법의 핵심을 설명하는 것으로, 나중에 재사용되는 것을 목적으로 하고 있다.

Gamma가 소프트웨어 공학에 도입했던 디자인 패턴은 객체지향 소프트웨어의 개발에 적합하게 정의되어 있다. 반응형 시스템은 객체지향 소프트웨어와는 다른 특성을 가진다. 예를 들어, 시스템의 실행 도중에 클래스로부터 인스턴스 객체를 생성시키고, 객체 단위로 시스템의 기능을 수행하고 행위를 정의하는 형태의 설계는, 반응형 시스템, 특히 안전 필수 시스템의 경우에는 적합하지 않다. 본 연구에서는 내장형 반응형 시스템의 개발에 적합한 디자인 패턴을 제안한다. 기본적으로 4가지 구성요소를 갖추고 있고 객체지향적인 특성의 항목들을 제외한 나머지 항목들 중에서 6개 항목을 선택하였다. 디자인 패턴의 항목과 기술 내용은 표 3.8.1과 같다: 패턴의 이름, 의도, 활용성, 구조, 결과, 사용 예제.

표 3.8.1 제안하는 디자인 패턴 항목과 기술 내용

항목	기술 내용
1) 패턴의 이름(name)	특정 패턴의 명칭
2) 의도(intent)	해결하고자 하는 문제와 이슈 또는 목적
3) 활용성(applicability)	적용가능한 상황에 대한 기술
4) 구조(structure)	추상화된 패턴의 시각적 표현
5) 결과(consequence)	패턴을 사용한 결과가 갖는 장점과 단점
6) 사용 예제(example)	패턴을 가지고 실제 상태차트를 작성할 때, 작성 단계를 보여주는 사례.

(나) Zed를 이용한 정형명세 작성절차

Z명세 작성 절차는 크게 5단계로 나눌 수 있고, 시스템 구성요소(component)를

명세하기 위해 다시 5단계로 나누어진다.

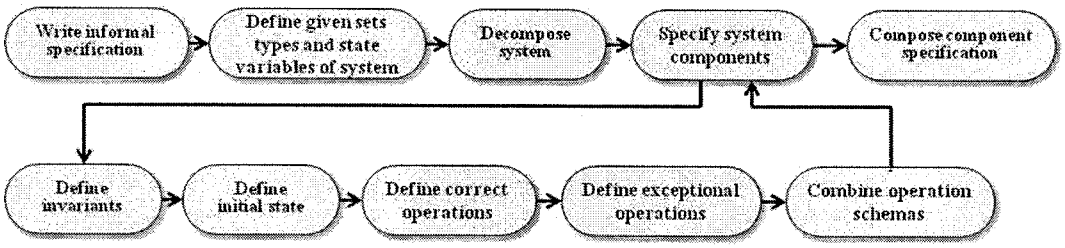


그림 3.8.1 Z 명세 작성 프로세스

각 단계별로 수행되는 작업은 다음과 같다:

- Write informal specification

  시스템의 자연어 기능 명세서를 기술한다.

- Define given sets, types, and state variables of system

  자연어 기능 명세서 분석을 토대로 시스템의 전체 상태 변수들을 식별 및 정의한다.

  또한 상태 변수들을 선언하기 위해 필요한 타입들을 정의한다.

- Decompose system

  정의한 시스템의 상태 변수들을 토대로 관련있는 변수들끼리 묶어 서브 시스템들로 나눈다.

- Specify system components

  각각의 서브 시스템들을 정의한다.

  ① Define invariants

  서브 시스템의 상태변수들이 항상 만족하여야 할 관계들을 정의한다.

  ② Define initial state

  서브 시스템의 초기 상태를 정의한다.

  ③ Define correct operations

  서브 시스템의 올바른 오퍼레이션들을 정의한다.

  ④ Define exceptional operations

서브 시스템의 예외적인 상황(올바른 경우를 제외한 모든 경우)의 오퍼레이션들을 정의한다.

⑤ ③과 ④에 정의된 오퍼레이션들을 하나의 오퍼레이션으로 묶는다.

- 명세된 서브 시스템들을 조합하여 전체의 시스템을 나타낸다. 조합하면서 조합된 서브 시스템 변수들간의 관계(invariants), 조합된 시스템의 초기상태 및 오퍼레이션을 정의한다.

(2) 열차제어시스템의 정형 검증 절차 연구

본 과제에서 사용된 2가지 정형명세 언어, statechart와 Z가 가지는 특성 때문에 정형 검증의 방식이 다르고, 검증 속성이 다를 수 있다. Statechart는 제어 중심의 관점에서 상태 기반으로 시스템을 기술하기 때문에, 시스템의 구성요소 각각의 행위와 구성 요소 사이의 실행 순서에 따른 시스템 전체의 행위를 분석하고 검증하는데 유용하다.

Statechart 명세 도구인 STATEMATE에서 Model checker 라는 모델 체킹 도구를 제공하고 있고, Model checker에서 지원하는 검증 속성은 다음과 같다:

- 비결정성(non-determinism) : 만약 어떤 상태에서 2개 이상의 서로 다른 상태로의 상태전이가 발생가능한 경우라면, 상태 전이에 대한 실행 순서가 정의되지 않았기 때문에 실행 순서에 충돌이 생긴다. 상태 전이들 사이에 우선 실행 순위를 지정함으로써 비결정성 문제를 해결할수 있다.
- 쓰기-쓰기 경쟁(write-write race) : 만약 어떤 한 실행 시점에서 동일한 변수에 대해 2개 이상의 변수값 지정(assignment)이 발생하는 경우, 바로 다음 스텝에서는 그 변수의 값은 지정되지 않는 오류가 발생한다.
- 읽기-쓰기 경쟁(read-write race) : 만약 어떤 한 실행 시점에서 동일한 변수에 대해 읽기와 쓰기를 위한 접근이 수행되면, 읽기와 쓰기 오퍼레이션의 결과가 비결정적일 수 있다.
- 범위 위반(range violation) : 만약 데이터 항목의 값의 범위가 변수값 설정 실행 도중에 underflow/overflow 로 인해 동적으로 값의 범위를 벗어나게 되면, 위반 여부를 알려준다. 현재까지 bounded integer, enumeration 항목이 검사 가능하며, 한도가 없는(unbounded) 데이터 항목은 지원되지 않고 있다.

Z 명세는 데이터와 오퍼레이션(operation) 중심에서 시스템을 기술하기 때문에, 동시성(concurrency) 대신에 시스템의 구성요소 각각에서 처리하는 데이터와 오퍼레이션의 일치성(consistency)과 완전성(completeness)을 검사하여 명세의 정확성(correctness)을 높인다.

Z 명세 언어의 정리증명 도구인 Z/EVES에서 지원하는 자동화 증명 기능은 다음과 같다:

- 단순화(simplification) : 논리식(formula)의 하위논리식(subformula)들에 대해 적용하는 것으로 간략화시키는 것이다.
  - 동일성(equality) : 하위논리식에 대한 대입(substitution) 연산의 결과에 대해서도 동일성을 검사한다.
  - 산술(arithmetic) : 산술 연산과 선형 산술 연산(상수가 포함된 산술 연산)의 결과에 대해서도 진위값을 계산한다.
  - 가정 규칙(assumption rule) : 가정 규칙으로 정의한 정리들에 한해서, 가정 조건이 만족하는 규칙의 정리 논리식이 적용될 수 있다.
  - 전방 규칙(forward rule) : 가정 규칙의 형태가 가정문 논리식 P⇒Q 형태로 되어 있는 정리들을 말한다.
- 재규정(rewriting) : 정리의 형태가 조건식⇒문자패턴=대치식 형태로 되어 있는 정리들을 말한다.
- 축소(reduction) : 단순화와 재규정 둘다 실행하는 것을 말한다.

(3) 예제 시스템 정형명세와 정형 검증 절차서 적용 예 제시

정형명세 언어는 만들어진 목적과 바탕을 두고 있는 논리체계에 따라서 표현력과 복잡성이 달라지기 때문에 전문가가 아닌 설계자나 개발자가 접근하여 사용하기에는 실용성이 떨어진다. 정형기법을 시스템 설계 단계에서 보다 쉽게 적용하고자 하는 목적으로 본 과제에서 표현력과 장점이 다른 두 언어를 이용하여 두 가지 관점으로 시스템의 요구 사항을 정형명세할 수 있도록 정형명세 작성 절차서를 개발하였다.

본 과제에서는 다음 그림 3.8.2과 같이 Statechart와 Z라는 두 가지 정형명세 언어를 사용하여 DCM에 대해 기술한 정형명세를 얻을 수 있도록 도와주는 패턴을

이용한 상태차트 작성 절차와 Z 명세 작성 절차를 제시하였다.

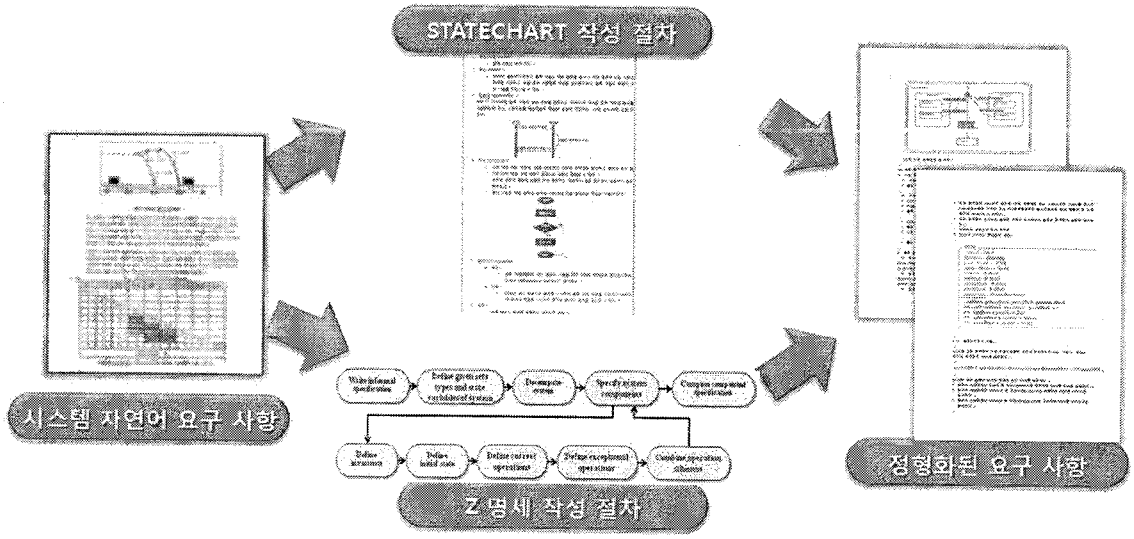


그림 3.8.2 패턴을 이용한 DCM의 statechart 및 Z명세 작성절차

(가) Statechart를 이용한 정형명세와 검증

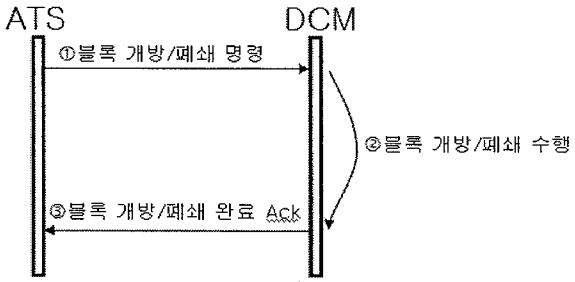
DCM의 5가지 기능에 대한 설계 패턴을 정의하였고, 시스템의 기능적 설계를 위해 기능을 분할하는 구조를 반영하는 한가지 설계 패턴을 정의하였다.

(a) 패턴 예 : 블록 개방과 패쇄

1. 패턴 이름 (name)
블록 개방과 폐쇄 패턴.

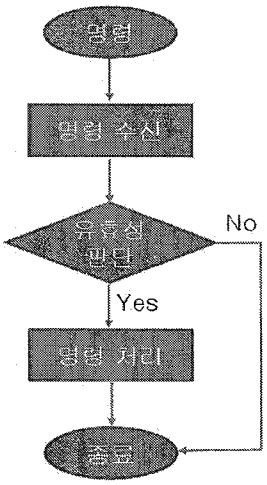
2. 의도 (intent)
DCM이 외부(ATS)로부터 블록 개방과 폐쇄 명령을 받아서, 해당 블록에 대한 개방과 폐쇄를 수행하고, 수행 후에 수행완료 사실을 알려줌으로써, 블록 개방과 폐쇄에 대한 기능을 전담시킬 수 있다.

3. 적용성 (applicability)
ATS 가 DCM에게 블록 개방과 폐쇄 명령을 전달하고, DCM으로 하여금 블록 개방과 폐쇄를 수행하도록 하고, 수행완료를 통보하도록 만드는 상황에 적합하다. (아래 순서 차트 그림 참조.)



4. 구조 (structure)

- 수행 명령 처리 이전에, (명령 이행/처리 가능)의 유효성을 확인하고, 유효성 확인 결과에 따라, 명령 수행 여부가 결정되는 상황에 적용될 수 있다.
- 유효할 경우에 명령을 실행한 후에 종료하고, 유효하지 않은 경우에는 실행하지 않고 종료한다.
- 명령 수행은, 해당 블록의 상태의 개방/폐쇄 값을 설정하는 것으로 이루어 진다.



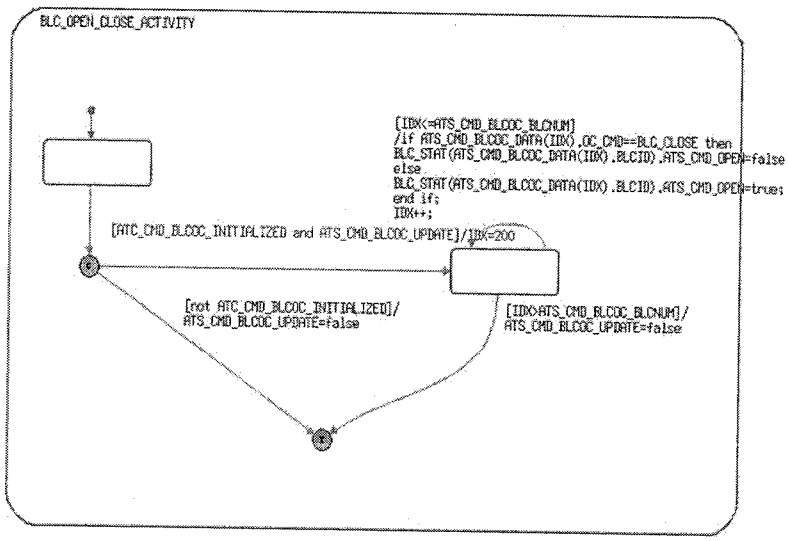
5. 결과 (consequence)

- 블록 개방/폐쇄에 대한 결정과 수행을 각각 ATS와 DCM으로 분리함으로써, DCM의 computational overload가 줄어든다.
- DCM은 ATS로부터의 명령을 수신하여 블록 개방 폐쇄를 수행하기 때문에, ATS로부터 명령을 수신하지 못하는 경우에, 문제를 일으킬 수 있다.

6. 예제 (Example)

ATS(Automatic Train Supervision: 열차 시스템 총괄)는 궤도 유지보수와 같은 작업을 위하여 선로의 일정 구간에 대하여 작업 구간 보호 구역 및 제한된 진로 보호를 위해 블록 폐쇄명령이 DCM으로 전달되면 DCM은 해당블록을 폐쇄하고 인접한 블록도 이에 준하여 이동권한을 설정한 후 해당정보를 ATS로 전송한다.

블록 개방은 반드시 ATS에서 전송된 명령에 따라 이루어지며, 이러한 블록개방 명령이 DCM으로 전송되면, DCM은 해당 블록 상태를 확인한 후 블록을 개방하고 인접한 블록도 이에 준하여 이동권한을 설정한 후 해당정보를 ATS로 전송한다.



블록 개방 및 폐쇄명령이 들어오면, 가상블록의 초기화 상태와 업데이트 가능여부를 판단한다.

- 가상블록이 초기화 되어있지 않으면, 블록 업데이트 가능여부를 'false'로 설정하고 종료한다.
- 가상블록이 초기화 되어있고 블록 업데이트가 가능하면, 인덱스 값을 200으로 (200=첫 블록) 설정한다.
- 가상 블록에 설정된 블록의 개방 및 폐쇄상태에 따라 모든 실제블록에 대해 동일하게 설정한다.
- 설정이 완료되면, 블록 업데이트 가능여부를 'false'로 설정하고 종료한다.

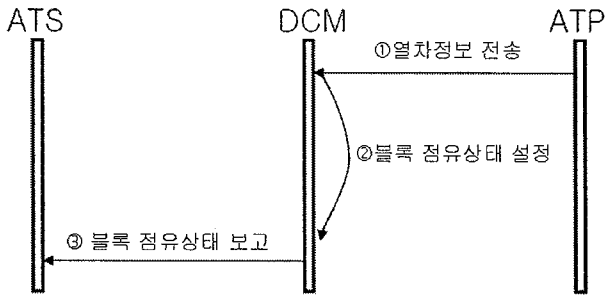
(b) 패턴 예 : 열차위치 확인 및 감시

1. 패턴 이름 (name)
열차 위치 확인 감시 패턴.

2. 의도 (intent)
DCM이 열차(ATP)로부터 열차정보를 수신하여 열차의 위치를 확인한다.

3. 적용성 (applicability)

ATP가 DCM에게 주기적으로 열차정보를 보낼때 마다, DCM은 열차가 현재 위치한 블록을 점유상태로 설정한 뒤, 블록의 점유상태를 ATS에게 보고하도록 하는 상황에 적합하다.(아래 순서 차트 그림 참조.)

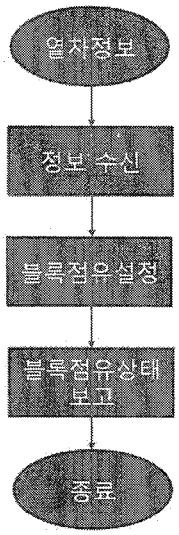


4. 구조 (structure)

-수신한 열차 정보로부터 열차의 위치정보를 확인한다.

-열차가 현재 위치한 블록에 대해 점유상태로 설정한다.

-ATS에게 블록점유상태를 보고한다.

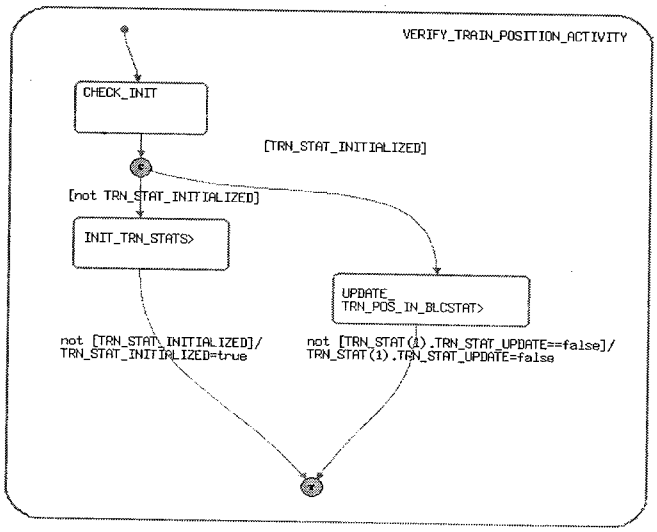


5. 결과 (consequence)

- 열차의 블록점유정보를 즉각적으로 반영할 수 있다.
- 블록 설정과 블록점유상태보고 단계 사이의 연관성을 고려해야 한다.
- ATP로부터 올바른 열차정보 수신에 대한 확인을 고려해야 한다.
- ATS에게 올바른 블록점유정보 전송에 대한 확인을 고려해야 한다.
- DCM이 ATS에게 정보를 올바르게 전송하지 못하는 경우에, 문제를 일으킬 수 있다.

6. 예제

열차 위치 확인을 실행하는 상태차트 예제.



- ATP로부터 열차정보가 수신되면, 열차가 위치한 블록을 점유상태로 설정하고 ATS에게 보고한 뒤 종료한다.
- 열차정보가 초기화 되어있지않으면, 열차정보 업데이트를 가능하도록 열차와의 연결상태를 'true'로 설정하고, 열차정보 초기화 상태도 'true'로 설정하고 종료한다.
- 열차정보가 초기화 되어있으면, 열차가 위치한 블록에 점유상태를 설정하고, ATS에게 보고한 뒤, 종료한다.

조건(Condition)의 데이터타입을 갖는 TRN_STAT_INITIALIZED의 True/False여부에 따라서 수행

열차정보 초기화 안됨

[not TRN_STAT_INITIALIZED]

열차정보 초기화

INIT_TRN_STATS

열차정보 초기화가 완료되면, 초기화가 완료된 상태로 조건 값을 변경

/TRN_STAT_INITIALIZED=true

열차의 위치를 블록정보에 업데이트

UPDATE_TRN_POS_IN_BLCSTAT>

(c) 패턴 예 : 임시속도제한 설정

1. 패턴 이름 (name)

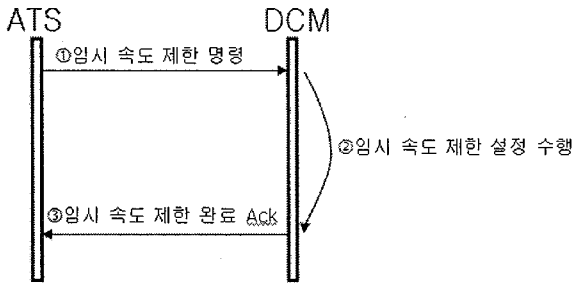
임시 속도 제한 설정 패턴.

2. 의도 (intent)

DCM이 외부(ATS)로부터 임시 속도제한명령을 받아서, 해당 블록에 대한 임시 속도제한을 설정하고, 설정 한 후에 수행완료 사실을 알려준다.

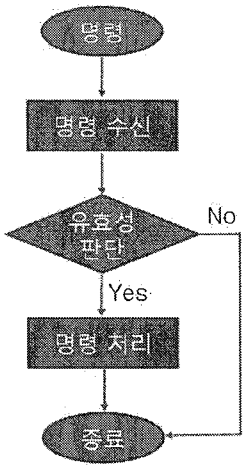
3. 적용성 (applicability)

ATS 가 DCM에게 임시 속도제한명령을 전달하고, DCM으로 하여금 임시 속도 제한 설정을 수행하도록 하고, 수행완료를 통보하도록 만드는 상황에 적합하다. (아래 순서 차트 그림 참조.)



4. 구조 (structure)

- 수행 명령 처리 이전에, (명령 이행/처리 가능)의 유효성을 확인하고, 유효성 확인 결과에 따라, 명령 수행 여부가 결정되는 상황에 적용될 수 있다.
- 유효할 경우에 명령을 실행한 후에 종료하고, 유효하지 않은 경우에는 실행하지 않고 종료한다.
- 명령 수행은, 해당 블록의 상태의 임시 속도 제한 값을 설정하는 것으로 이루어진다.

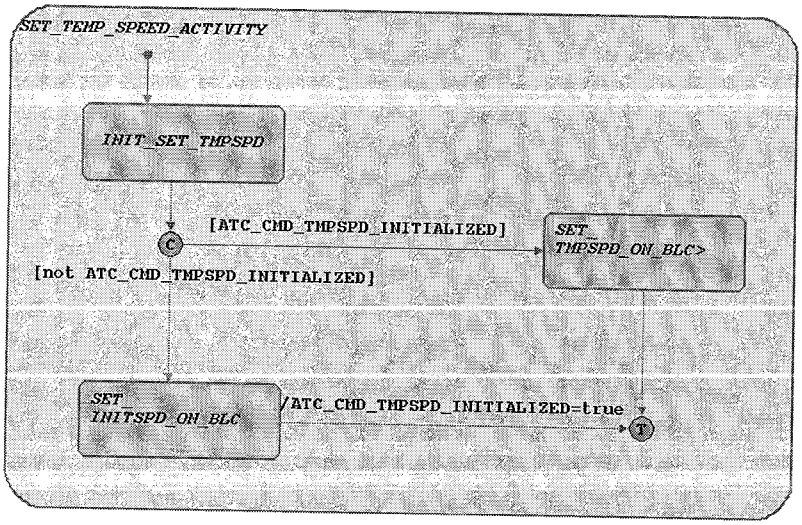


5. 결과 (consequence)

- 임시 속도 제한에 대한 결정과 수행을 각각 ATS와 DCM으로 분리함으로써, DCM의 computational overload가 줄어든다.
- DCM은 ATS 로부터의 명령을 수신하여 임시 속도 제한 명령을 수행하기 때문에, ATS 로부터 명령을 수신하지 못하는 경우에, 문제를 일으킬 수 있다.

6. 예제

임시 속도 제한 설정을 수행하는 상태차트 예제



- 블록 개방 및 폐쇄 기능과 임시속도 제한명령 처리 기능은 열차의 진입 유무와 관계 없이 DCM이 관리하는 블록정보에 업데이트 되므로, 주기적으로 수행된다. 이에 반해, 열차와 관련되어 수행되는 기능인 열차위치확인, 이동방향감시, 간격제어 기능들은 열차가 DCM이 관리하는 블록 내에 있을 때에만 수행이 된다.
- DCM이 관리하는 블록들의 초기화 여부에 따라서, 초기화가 이루어지지 않았으면, 초기화 작업을 수행한다.

조건(Condition)의 데이터타입을 갖는 ATC_CMD_TMPSPD_INITIALIZED의 True/False여부에 따라서 수행

초기화 안됨

[not ATC_CMD_TMPSPD_INITIALIZED]

초기화가 완료되면, 초기화가 완료된 상태로 조건 값을 변경

/ATC_CMD_TMPSPD_INITIALIZED=true

- 초기화가 이미 이루어졌으면, 임시속도 제한 정보에 따라 블록정보를 업데이트 한다

초기화가 안된 상태

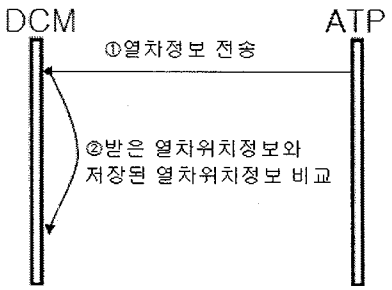
[ATC_CMD_TMPSPD_INITIALIZED]

(d) 패턴 예 : 열차이동방향 감시

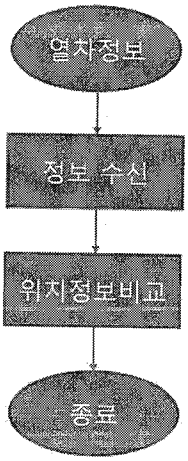
1. 패턴 이름 (name)
열차 이동방향 감시 패턴.

2. 의도 (intent)
DCM이 열차(ATP)로부터 열차정보를 수신하여 열차의 이동방향을 감시한다.

3. 적용성 (applicability)
ATP가 DCM에게 주기적으로 열차정보를 보낼때 마다, DCM은 열차의 현재 위치정보와 저장하고 있는 해당 열차의 위치정보를 비교하여 열차의 이동방향을 감시하는 상황에 적합하다.
(아래 순서 차트 그림 참조.)



4. 구조 (structure)
- 수신한 열차 정보로부터 열차의 위치정보를 확인한다.
- 열차가 현재 위치한 블록이 저장된 (마지막으로 알려진 위치정보) 위치정보를 기준으로 올바른 이동인지 감시한다.

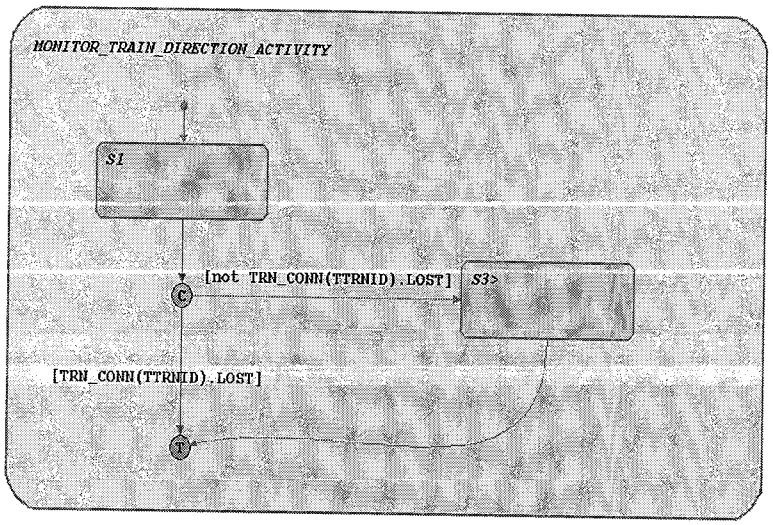


5. 결과 (consequence)

- ATP로부터 올바른 열차정보 수신에 대한 확인을 고려해야 한다.

6. 예제

열차 이동방향 감시를 수행하는 상태차트 예제.



- 열차의 이동방향 감시기능은 열차의 통신 상태를 우선적으로 확인하고, 통신상태가 올바르지 않은 경우, 열차 분실 처리를 한다.

조건(Condition)의 데이터타입을 갖는[TRN_CONN(TRNID).LOST]의 True/False 여부에 따라서 수행

[TRN_CONN(TRNID).LOST] → 통신상태비정상

- 열차와의 통신상태가 올바를 때에는, 열차의 이동방향을 확인하는 작업을 수행한다.

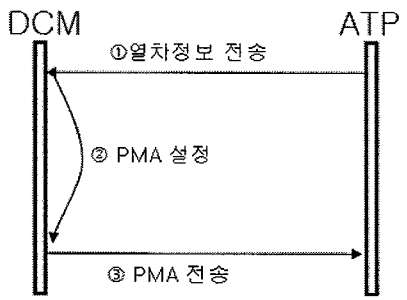
이는, 열차가 현재 갖고 있는 스케줄을 기반으로 하여, 열차의 현재위치와 이전 위치를 확인하여, 열차의 이동방향이 스케줄대로 이루어지고 있는지를 확인한다.

(e) 패턴 예 : 열차간격제어설정

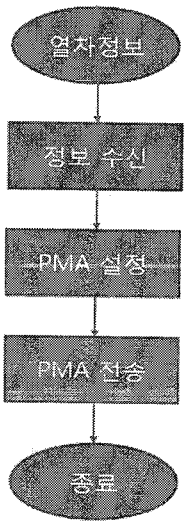
1. 패턴 이름 (name)
열차 간격 제어 설정 패턴.

2. 의도 (intent)
DCM이 열차(ATP)로부터 열차정보를 수신하여, 해당 열차정보를 기초로 블록의 조건과 상태를 고려하여 PMA를 설정한다.

3. 적용성 (applicability)
ATP가 DCM에게 열차정보를 보낼때 마다, DCM은 열차의 현재 위치정보를 기초로 하여 PMA를 설정한 뒤, 열차에게 PMA를 전송한다. (아래 순서 차트 그림 참조.)



4. 구조 (structure)
- 열차로부터 열차정보를 수신한다.
- 열차가 현재 위치한 블록을 기초로 전방 네 개의 블록에 대한 PMA를 설정한다.
- PMA를 열차에게 전송한다.

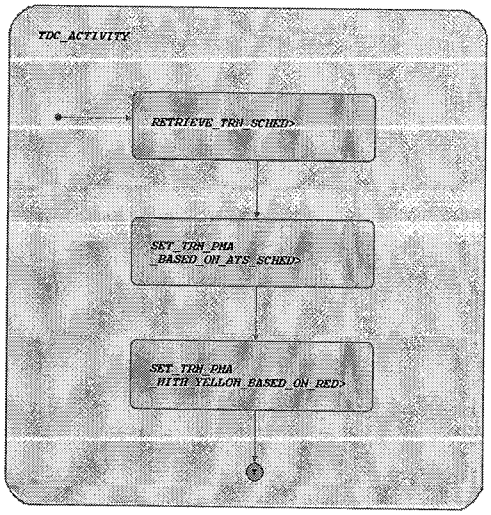


5. 결과 (consequence)

- 열차정보에 포함된 열차의 위치정보를 기준으로 PMA를 설정하지 않는다.
- DCM이 가지고 있는 블록정보에 대해서 열차의 위치정보를 업데이트 하고, 이것을 기초로 PMA를 설정한다.

6.예제

열차 간격 제어를 수행하는 상태차트 예제.



- 열차의 이동과 관련하여 해당 열차의 예약진로에 대한 PMA를 설정하기 위해, 진로정보를 확인

RETRIEVE_TRN_SCHED

- 열차정보를 기초로 DCM이 관리하는 블록에 절대PMA를 업데이트
SET_TRN_PMA_BASED_ON_ATS_SCHED

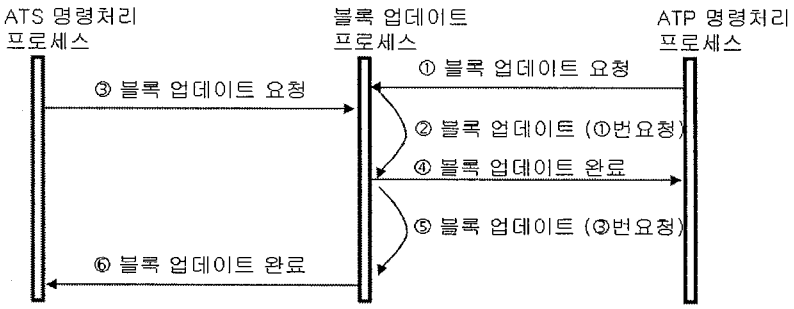
- 열차정보를 기초로 DCM이 관리하는 블록에 상대PMA를 업데이트
SET_TRN_PMA_WITH_YELLOW_BASED_ON_RED

(f) 패턴 예 : 블록 업데이트관련 명령처리

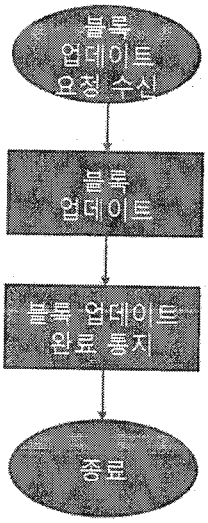
1. 패턴 이름 (name)
블록 업데이트 관련 명령 처리 패턴.

2. 의도 (intent)
DCM이 관리하는 블록에 대해 업데이트에 필요한 정보를 생성하는 과정과 실제로 정보를 업데이트를 수행하는 과정을 분리한다.

3. 적용성 (applicability)
ATP, ATS관련 처리 프로세스가 블록 업데이트 프로세스에게 블록 업데이트를 요청하면 블록 업데이트 프로세스는 순차적으로 블록 업데이트를 수행하고, 업데이트 완료 사실을 보고한다. (아래 순서 차트 그림 참조.)



4. 구조 (structure)
- ATS, ATP관련 처리 프로세스로부터 블록 업데이트 요청을 수신한다.
- 수신한 모든 요청에 대해서 순차적으로 블록 업데이트를 수행한다.
- 블록 업데이트 완료 사실을 통지한다.

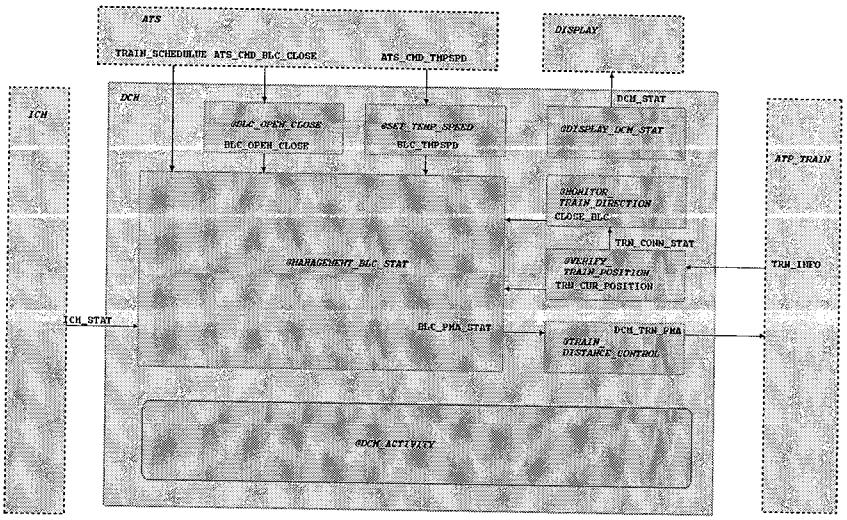


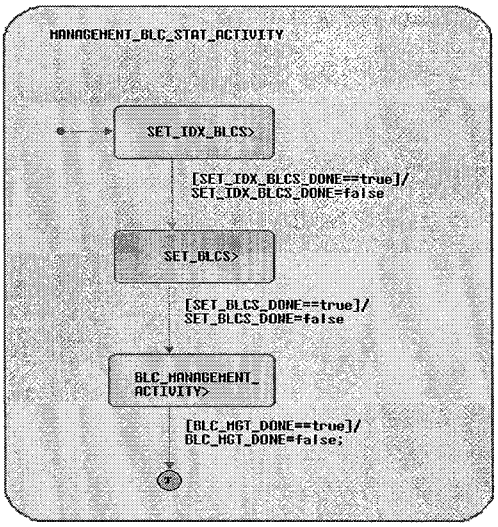
5. 결과 (consequence)

- 공유자원에 접근하는 블록 업데이트 프로세스는 Race Condition을 유발시킬 수 있는데, 이것을 해결하기 위해 모든 블록 업데이트 요청을 순차적으로 처리한다.
- 시스템 성능의 전체적인 측면에서 병목현상이 발생할 수도 있다.

6. 예제

블록 업데이트 관련 명령처리 예제





- 블록 정보를 업데이트 하기 위한 인덱스 값을 블록 별로 설정함
SET_IDX_BLCS>
- 인덱스 설정 완료
SET_IDX_BLCS_DONE

- 절대 블록에 대한 블록 정보를 해당블록에 업데이트함
SET_BLCS>
- 해당 블록정보 업데이트 완료
SET_BLCS_DONE

- 업데이트 된 블록정보를 기초로 관련 블록에 대한 절대 PMA를 설정함
BLC_MANAGEMENT_ACTIVITY>
- 절대 PMA 업데이트 완료
BLC_MGT_DONE

(나) Z를 이용한 정형명세와 검증

Z명세 작성 절차는 크게 5단계로 나눌 수 있고, 시스템 구성요소(component)를 명세하기 위해 다시 5단계로 나누어진다.

- Write informal specification
- Define given sets, types, and state variables of system
- Decompose system
- Specify system components

① Define invariants

② Define initial state

③ Define correct operations

④ Define exceptional operations

⑤ ③과 ④에 정의된 오퍼레이션들을 하나의 오퍼레이션으로 묶는다.

- 명세된 서브 시스템들을 조합하여 전체의 시스템을 나타낸다.

변수들간의 관계, 조합된 시스템의 초기상태 및 오퍼레이션 정의

(a) Write informal specification

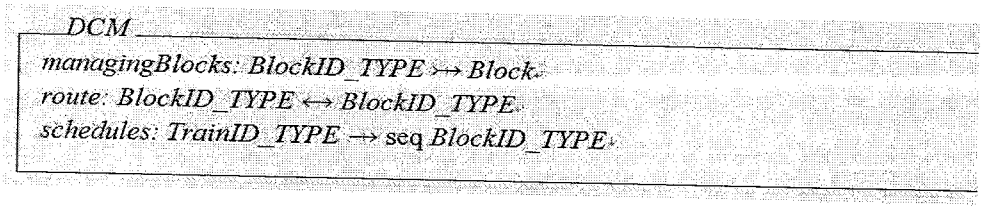
생략

(b) Define given sets, types, and state variables of system

DCM은 제어 영역 내에서 논리적 블록 단위로 나누어 각 블록들을 관리한다. 따라서 각 블록들의 정보들이 필요하다. 각 블록들의 정보를 저장하는 managingBlocks를 정의한다. 각 블록들을 BlockID에 매핑한 이유는 후에 블록의 정보를 읽거나 업데이트 하기 위하여 해당 블록의 접근을 용이하게 하기 위함이다. Block은 우선 추상적 데이터 타입으로 정의하고 BlockID의 타입은 정수로 정의한다.

DCM은 각 블록의 정보들 뿐 아니라 열차가 올바로 이동하는 지를 파악하거나 다른 기능들을 수행하기 위해 제어 영역 내의 선로와 열차들의 스케쥴 정보를 저장하고 있어야 한다.

제어 영역 내의 선로를 나타내기 위해 route를 정의한다. route는 한 블록에서 1개 이상의 블록과 연결될 수 있으므로 관계(relation)으로 타입을 정의한다. schedules는 블록들의 나열(sequence)로 각 열차가 이동할 블록들을 나타낸다.



위와 같이 DCM을 정의하고 DCM의 각 블록들을 관리하기 위해서는 각 블록들의 정보들이 필요하다. 그 정보들을 나타내기 위해 추성적으로 정의된 Block을 상세화한다. 우선 각 블록에는 열차의 안전한 이동을 위해 PMA를 설정한다. 따라서 블록마다 PMA 정보를 가지고 있어야 한다. red/yellow/green으로 구성되며 이를 나타내기 위해 PMA_TYPE을 정의한다.

$$PMA_TYPE ::= red \mid yellow \mid green$$

Block

$id: BlockID_TYPE$

$pma: PMA_TYPE$

이 중 하나의 상태를 저장하기 위해 Block에 상태변수 pma를 선언한다. 또한 각 블록을 식별하기 위한 ID를 선언한다. 또한 블록을 점유한 열차들과 점유하기 위해 예약한 열차들의 정보를 나타낸다.

syntax *optional pregen optional*

$(optional_)X == \{ x : \mathbb{F} X \mid \#x \leqslant 1 \}$

$TrainID_TYPE == \mathbb{Z}$

Block

$id: BlockID_TYPE$

$pma: PMA_TYPE$

$occ: \mathbb{P}\ TrainID_TYPE$

$reservedTrain: optional\ TrainID_TYPE$

열차들을 식별하기 위해 열차ID를 나타내는 TrainID타입을 정의한 후 점유한 열차를 나타내기 위해 occ 상태변수를 정의한다. 한 블록에 0개 또는 1개 이상의 열차들이 점유할 수 있으므로 occ 상태변수를 TrainID의 멱집합(power set)으로 선언한다. (추후 오퍼레이션으로써 2개 이상의 열차가 한 블록에 진입하지 못하도록 오퍼레이션 정의를 하여야 한다.) 예약한 열차를 나타내기 위해 reservedTrain 상태 변수를 정의한다. 각 블록에는 예약한 열차가 존재할 수도 있으며 존재하지 않을 수도 있다. 따라서 이를 나

타내기 위해 optional이라는 구문를 정의하고(예약어가 아니기 때문에 신택스에 추가) reservedTrain을 optional TrainID_TYPE로 선언한다. 즉, 하나의 열차ID를 가지거나 열차ID가 존재하지 않도록 한다.

각 블록에는 PMA, 열차정보 뿐 아니라 개방/폐쇄된 블록 및 임시속도명령설정/미설정 명령 수행을 위해 이에 대한 정보도 저장을 하여야 한다. 따라서 이를 나타내는 상태변수를 정의한다.

설정 또는 미설정을 나타내기 위해 SetStatus_TYPE을 정의한다. obs 상태변수를 두어 블록개방/폐쇄의 상태를 나타내며 tempSpeedLimitStatus를 두어 임시속도설정상태를 나타낸다. 설정상태와 설정된 속도를 나타내기 위해 TempSpeedLimit_TYPE을 tempSpeedLimitSettingStatus, tempSpeed을 가지는 스키마 타입으로 정의한다.

SetStatus_TYPE ::= set | unset

TempSpeedLimit_TYPE

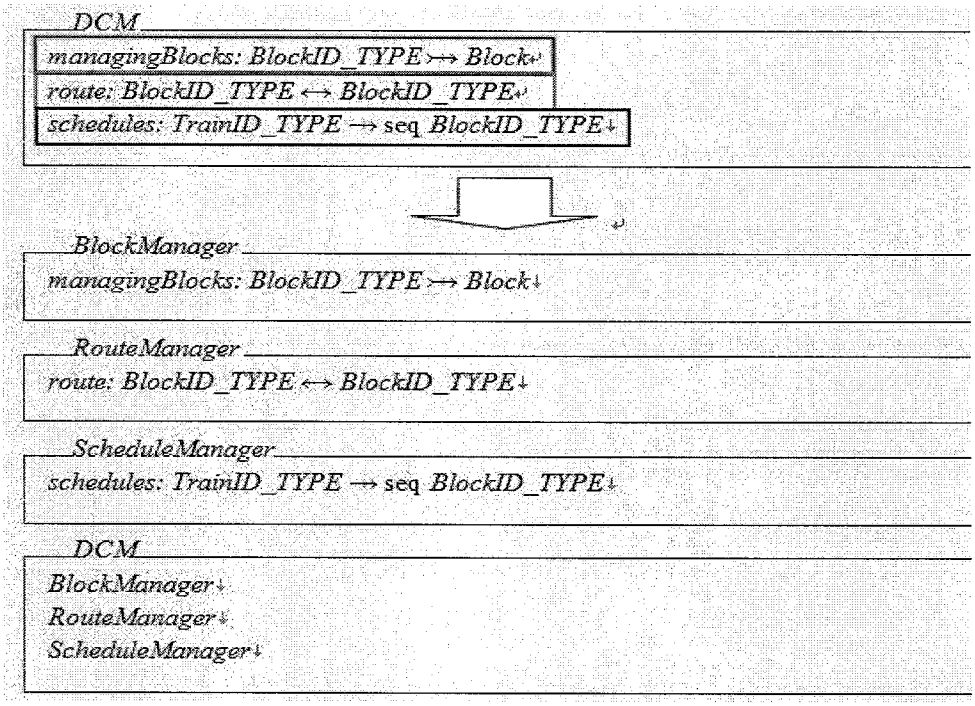
tempSpeedLimitSettingStatus: SetStatus_TYPE
tempSpeed: ℤ

Block

id: BlockID_TYPE
pma: PMA_TYPE
occ: ℙ TrainID_TYPE
reservedTrain: optional TrainID_TYPE
obs: SetStatus_TYPE
tempSpeedLimitStatus: TempSpeedLimit_TYPE

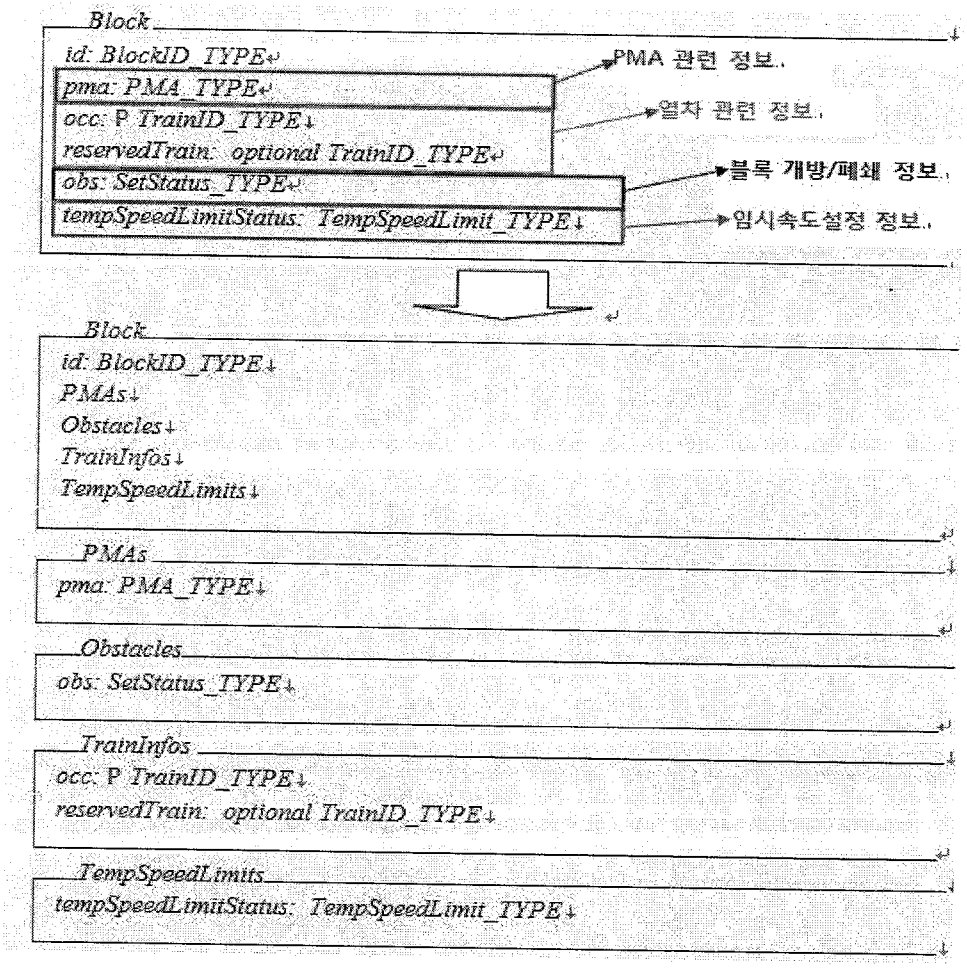
(c) Decompose system

현재까지 정의한 시스템의 상태들을 연관있는 변수들끼리 묶는다.



DCM에 정의된 3변수들(managingBlocks, route, schedules)을 각각의 서브시스템(BlockManager, RouteManager, ScheduleManager)로 나눈 후 각각 정의한다. DCM에는 각각 나뉜 서브시스템들을 포함토록 한다.

블록 역시 PMA관련 정보, 열차관련 정보, 블록 개방/폐쇄 정보, 임시속도설정 정보로 묶어 PMAs, Obstacles TrainInfos, TempSpeedLimits로 정보들을 나눈다.



(d) Specify system components

각각 나눈 서브 시스템들의 초기상태 및 오퍼레이션을 정의한다.

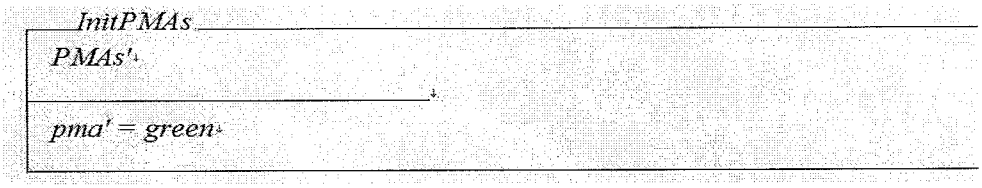
① PMAs

- Define invariants

생략 (변수들간에 만족해야할 관계가 존재하지 않는다.)

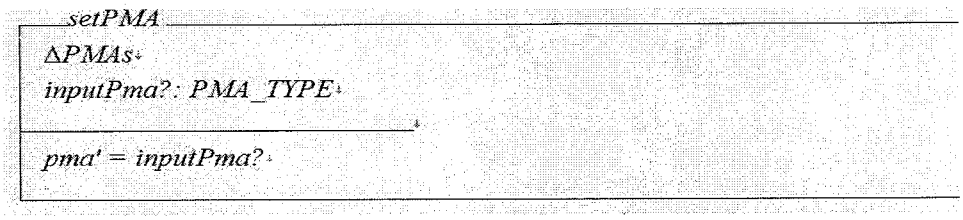
- Define initial state

pma의 초기 값은 green이다.



- Define correct operations

pma를 설정하는 오퍼레이션을 정의한다. DPMAs는 PMAS의 전,후 상태가 달라진다는 것을 의미한다. inputPma?는 상위 시스템로부터의 입력을 의미하며 이 오퍼레이션에서는 입력대로 PMA를 설정한다.



- Define exceptional operations

생략 (예외적인 오퍼레이션이 존재하지 않는다.)

- Combine operation schemas

생략 (정의된 오퍼레이션이 하나이므로 결합할 필요가 없다.)

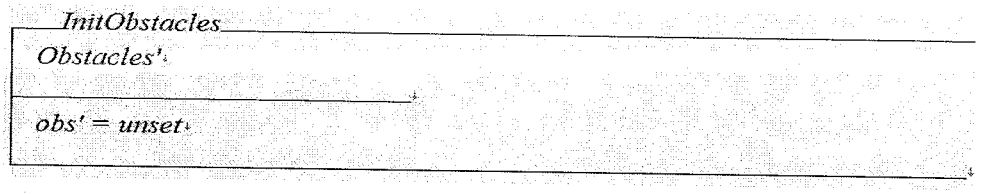
② Obstacles

- Define invariants

생략 (변수들간에 만족하여야 할 관계가 존재하지 않는다.)

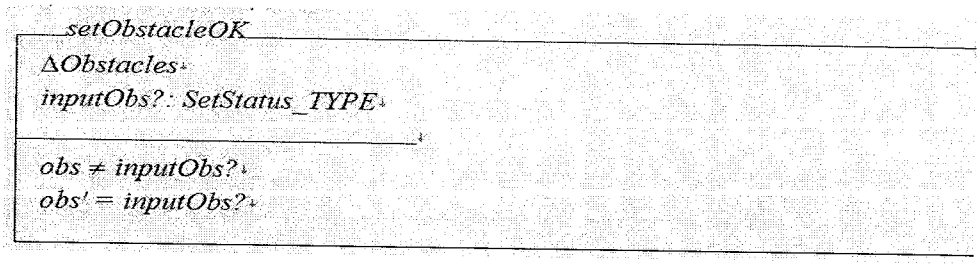
- Define initial state

obs의 초기 값은 green이다.



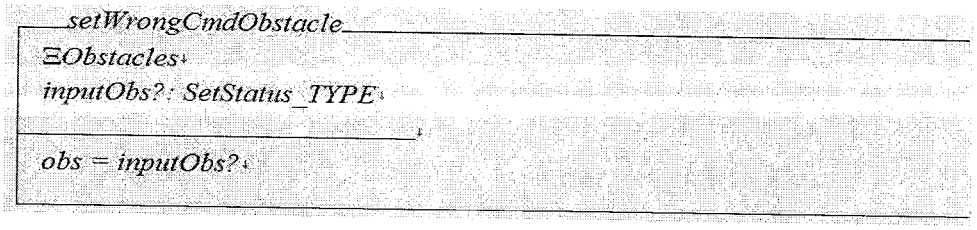
- Define correct operations

obs를 설정하는 오퍼레이션을 정의한다. inputObs?는 상위 시스템로부터의 입력을 의미하며 이 오퍼레이션에서는 기존의 설정상태와 입력상태가 상이할 시에 입력값으로 obs를 설정한다.



- Define exceptional operations

obs의 기존 설정상태와 입력 상태가 동일 시에는 obs를 동일한 상태로 둔다.



- Combine operation schemas

세 번째 및 네 번째에서 정의된 오퍼레이션들을 결합한다.

$$setObstacle \cong setObstacleOK \vee setWrongCmdObstacle$$

③ TrainInfos

- Define invariants

생략 (변수들간에 만족하여야 할·관계가 존재하지 않는다.)

- Define initial state

occ와 reservedTrain의 초기 값은 공집합이다.

$$nil[X] == \varnothing[X]$$

InitTrainInfos

$$TrainInfos'$$

$$occ' = nil$$
$$reservedTrain' = nil$$

- Define correct operations

블록에 예약된 새로운 열차(newTrain?)가 진입시에 occ를 업데이트 하고 예약 정보에서 삭제한다.

entryTrainOK

$$\Delta TrainInfos$$
$$newTrain? : TrainID_TYPE$$

$$occ = nil$$
$$reservedTrain = \{newTrain?\}$$
$$occ' = \{newTrain?\}$$
$$reservedTrain' = nil$$

블록에서 열차가 벗어날 시에 occ정보에서 삭제한다.

exitTrainWithoutDeleteReservationOK

$\Delta TrainInfos$

$newTrain? : TrainID_TYPE$

$newTrain? \in occ$

$newTrain? \notin reservedTrain$

$occ' = occ \setminus \{newTrain?\}$

$reservedTrain' = reservedTrain$

- Define exceptional operations

블록에 예약되지 않은 새로운 열차(newTrain?)가 진입시에도 occ를 업데이트 하고 예약 정보를 그대로 둔다.

entryNotExpectedTrain

$\Delta TrainInfos$

$newTrain? : TrainID_TYPE$

$occ = nil$

$reservedTrain \neq \{newTrain?\}$

$occ' = \{newTrain?\}$

$reservedTrain' = reservedTrain$

이미 열차가 점유한 블록에 새로운 열차가 점유 시에 새로운 열차를 occ에 추가하고 예약정보를 그대로 둔다. (이 경우에는 상위 시스템에서 비상 상황의 처리를 수행하도록 한다.)

entryOverlapTrain

$\Delta TrainInfos$

$newTrain? : TrainID_TYPE$

$occ \neq nil$

$occ' = occ \cup \{newTrain?\}$

$reservedTrain' = reservedTrain$

블록에서 열차가 벗어날 시에 occ정보에서 삭제하며 예약정보에 아직 남아있는 상태이면 이를 삭제한다.

exitTrainWithDeleteReservationOK

$\Delta TrainInfos$

$newTrain? : TrainID_TYPE$

$newTrain? \in occ$

$newTrain? \in reservedTrain$

$occ' = occ \setminus \{newTrain?\}$

$reservedTrain' = reservedTrain \setminus [0 .. 1000] \{newTrain?\}$

- Combine operation schemas

세 번째 및 네 번째에서 정의된 오퍼레이션들을 결합한다.

$entryTrain \triangleq entryTrainOK \lor entryNotExpectedTrain \lor entryOverlapTrain$

$exitTrainOK \triangleq$

$exitTrainWithoutDeleteReservationOK \lor exitTrainWithDeleteReservationOK$

$exitTrain \triangleq exitTrainOK \lor exitNotExistTrain$

④ TempSpeedLimits

- Define invariants

임시속도는 0과 80사이의 값을 가져야 하며 임시속도제한명령이 설정되었을 경우에는 1과 80사이의 임시속도가 설정되어야 하고 임시속도제한명령이 설정되지 않았을 경우에는 임시속도가 0으로 설정되어야 한다.

TempSpeedLimits

$tempSpeedLimitStatus : TempSpeedLimit_TYPE$

$tempSpeedLimitStatus.tempSpeed \in 0 .. 80$

$tempSpeedLimitStatus.tempSpeedLimitSettingStatus = set$

$\Rightarrow tempSpeedLimitStatus.tempSpeed \in 1 .. 80$

$tempSpeedLimitStatus.tempSpeedLimitSettingStatus = unset$

$\Rightarrow tempSpeedLimitStatus.tempSpeed = 0$

- Define initial state

임시속도설정과 임시속도의 초기 값은 각각 unset과 0이다.

InitTempSpeedLimits

TempSpeedLimits'

---

tempSpeedLimitStatus' . *tempSpeedLimitSettingStatus* = *unset*
tempSpeedLimitStatus' . *tempSpeed* = 0

- Define correct operations

임시속도 명령에 대한 입력값이 올바르면(0~80사이의 임시 속도 값을 가지며 설정 명령일 시에는 1~80사이, 미설정 명령일 시에는 0의 값을 가져야 한다.) 입력값으로 임시 속도 상태와 속도를 각각 설정한다.

setTempSpeedOK

ΔTempSpeedLimits
inputTempSpeed?: *TempSpeedLimit_TYPE*

---

inputTempSpeed? . *tempSpeed* ∈ 0 .. 80
inputTempSpeed? . *tempSpeedLimitSettingStatus* = *set*
⇒ *inputTempSpeed?* . *tempSpeed* ∈ 1 .. 80
inputTempSpeed? . *tempSpeedLimitSettingStatus* = *unset*
⇒ *inputTempSpeed?* . *tempSpeed* = 0
tempSpeedLimitStatus' = *inputTempSpeed?*

- Define exceptional operations

임시속도 명령에 대한 입력값이 올바르지 않을 시에는 명령을 수행하지 않고 상태를 그대로 둔다.

setWrongCmdTempSpeed

ΞTempSpeedLimits
inputTempSpeed?: *TempSpeedLimit_TYPE*

---

inputTempSpeed? . *tempSpeed* ∉ 0 .. 80
∨ (*inputTempSpeed?* . *tempSpeedLimitSettingStatus* = *set*
⇒ *inputTempSpeed?* . *tempSpeed* ∉ 1 .. 80)
∨ (*inputTempSpeed?* . *tempSpeedLimitSettingStatus* = *unset*
⇒ *inputTempSpeed?* . *tempSpeed* ≠ 0)

- Combine operation schemas

세 번째와 네 번째에서 정의된 오퍼레이션들을 결합한다.

e) Compose component specifications

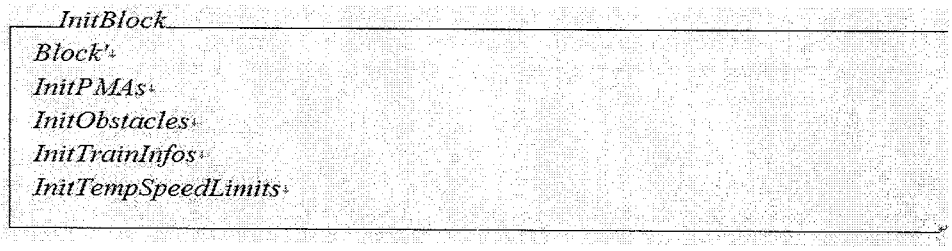
① Block

- invariants 정의

생략 (서브 시스템들의 변수들간의 관계가 존재하지 않음)

- 초기상태 정의

기존에 정의한 각 서브시스템의 초기상태들을 조합하여 상위시스템의 초기상태를 정의한다.



- 오퍼레이션 정의

생략 (Block은 최상위 시스템에서 타입으로 사용되기 때문에 오퍼레이션이 존재하지 않는다.)

② RouteManager

- invariants 정의

생략 (변수들간의 관계가 존재하지 않음)

- 초기상태 정의

DCM 내의 선로 정보는 ATS에서 전송받은 선로 정보를 토대로 초기화된다. receiveInitialInfoFromATS의 inputRoute는 전송받는 선로 정보를 나타낸다. RouteManager 초기 상태에서는 inputRoute를 전송받

아서 route를 업데이트한다.

receiveInitialInfoFromATS

$inputRoute : BlockID_TYPE \leftrightarrow BlockID_TYPE$

InitRouteManager

$RouteManager'$

$receiveInitialInfoFromATS?$

$route' = inputRoute?$

- 오퍼레이션 정의

DCM 운영 중에도 선로 정보는 ATS에서 전송받아 기존의 선로 정보와 상이할 시 업데이트 한다.

updateRouteOK

$\Delta RouteManager$

$receiveInitialInfoFromATS?$

$route \neq inputRoute?$

$route' = inputRoute?$

ATS로부터 전송받은 선로 정보와 기존의 DCM의 선로 정보가 동일할 시에는 상태를 그대로 유지한다.

updateSameRoute

$\Xi RouteManager$

$receiveInitialInfoFromATS?$

$route = inputRoute?$

$updateRoute \triangleq updateRouteOK \vee updateSameRoute$

③ BlockManager

- invariants 정의

DCM 제어 영역 내에 관리하는 블록들은 유한하여야 한다.

BlockManager

$managingBlocks: BlockID_TYPE \rightarrowtail Block$

$managingBlocks \in BlockID_TYPE \rightarrowtail Block$

- 초기상태 정의

DCM 제어 영역 내의 블록들은 ATS에서 전송받은 선로 정보를 통해 식별하며 각각의 초기화는 이전에 정의한 InitBlock을 이용하여 전체 블록을 초기화한다.

InitBlockManager

$BlockManager'$

$receiveInitialInfoFromATS?$

$allBlockID: \mathbb{P}\, BlockID_TYPE$

$allBlockID = \mathrm{dom}\ inputRoute? \cup \mathrm{ran}\ inputRoute?$

$\mathrm{dom}\ managingBlocks' = allBlockID$

$\forall blockID: allBlockID$

$\bullet\ managingBlocks'\ blockID$

$= (\mu Block' \mid blockID = (managingBlocks'\ blockID).id \wedge InitBlock)$

- 오퍼레이션 정의

생략 (BlockManager의 managingBlocks의 상태를 변경시키는 오퍼레이션은 최상위 시스템인 DCM에서 정의된다.)

④ ScheduleManager

- invariants 정의

생략 (변수들간의 관계가 존재하지 않음)

- 초기상태 정의

스케줄 정보의 초기값은 공집합이다.

InitScheduleManager

$ScheduleManager'$

$schedules' = nil$

- 오퍼레이션 정의

ATS로부터 열차의 스케쥴을 입력받으면 이를 업데이트 시킨다. 이 때에 입력받은 열차는 기존에 존재하지 않는 즉 새로 진입한 열차이어야 한다. 새로 진입한 열차에 대한 식별 및 스케쥴 업데이트 프로세스는 추후 전체 시스템 상에서 정의한다.

receiveScheduleInfoFromATS

$inputTrainID: TrainID_TYPE$

$inputSchedule: \text{seq}\ BlockID_TYPE$

getScheduleOK

$\Delta ScheduleManager$

$receiveScheduleInfoFromATS?$

$inputTrain? \in \text{dom}\ schedules$

$schedules' = schedules \cup \{(inputTrainID? \rightarrow inputSchedule?)\}$

ATS로부터 스케쥴 정보를 입력받았을 때 열차가 기존에 존재하는 열차이면 업데이트 하지 않고 상태를 그대로 유지한다.

getWrongSchedule

$\Xi ScheduleManager$

$receiveScheduleInfoFromATS?$

$inputTrainID? \in \text{dom}\ schedules$

$getSchedule \triangleq getScheduleOK \vee getWrongSchedule$

열차의 스케쥴은 입력받은 열차에 대해서 스케쥴이 존재할 시에 이를 삭제한다.

deleteScheduleOK

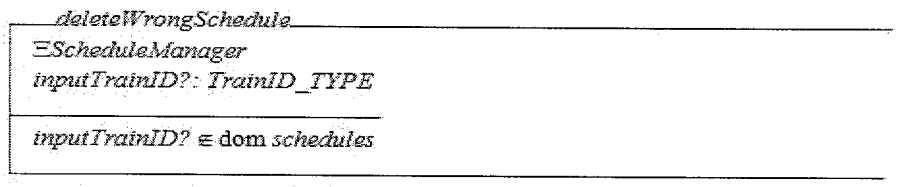
$\Delta ScheduleManager$

$inputTrainID?: TrainID_TYPE$

$inputTrainID? \in \text{dom}\ schedules$

$schedules' = \{inputTrainID?\} \lhd schedules$

입력받은 열차에 대한 스케쥴이 존재하지 않을 경우 상태를 그대로 유지한다.

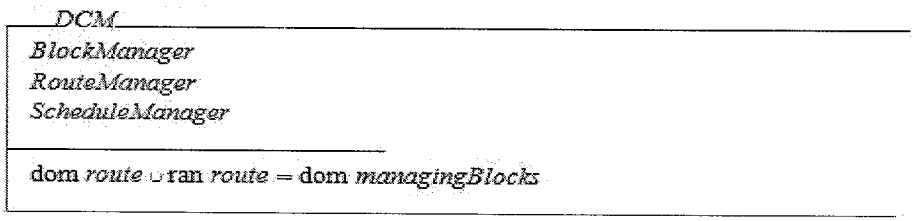


$getSchedule \triangleq getScheduleOK \vee getWrongSchedule$

⑤ DCM

- invariants 정의

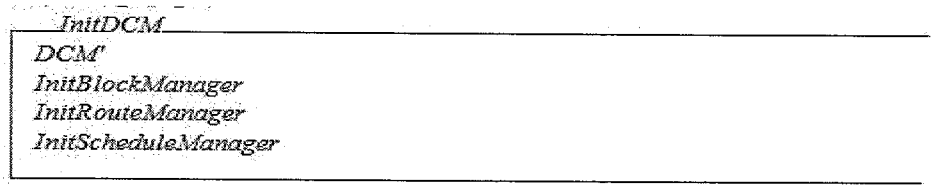
RouteManager에서 관리하는 선로를 구성하는 블록들은 BlockManager에서 관리하는 블록들과 동일해야 한다.



- 초기상태 정의

정의된 각 서브시스템들(BlockManager, RouteManager, ScheduleManager)의 초기 상태을 이용하여 DCM의 초기 상태를 정의한다.

- 오퍼레이션 정의



· PMA 관련 오퍼레이션

PMA 설정 시 BlockManager를 제외한 나머지 서브시스템의 상태는 변경되지 않는다.

또한 BlockManager가 관리하는 Block들의 ID 역시 변경되지 않는다.

securePMASetting

$\Delta BlockManager$

$\Xi RouteManager$

$\Xi ScheduleManager$

$\text{dom}\ managingBlocks = \text{dom}\ managingBlocks'$

우선 모든 블록들의 PMA상태를 green으로 설정한다.

greenPMASetting

ΔDCM

---

securePMASetting

$\forall b: \text{dom}\ managingBlocks$

- $\exists_1 \Delta Block$
  - $\theta Block = managingBlocks\ b \wedge setPMA[green/inputPma?]$
    $\Rightarrow managingBlocks' = managingBlocks \oplus \{(b \mapsto \theta Block')\}$

폐쇄된 블록과 주변의 블록들의 PMA를 red로 설정한다.

redPMASettingByObstacle

ΔDCM

---

securePMASetting

$\forall b$: dom *managingBlocks*

- **let** *nextBlocks* == *route* ({*b*}); *beforeBlocks* == *route* ({*b*})
  - $\forall$ *nextBlock*: *nextBlocks*; *beforeBlock*: *beforeBlocks*
    - (*managingBlocks b*) . *obs* = *set*
      $\vee$ (*managingBlocks nextBlock*) . *obs* = *set*
      $\vee$ (*managingBlocks beforeBlock*) . *obs* = *set*
      $\Rightarrow$ ($\exists_1 \Delta Block$
      - θ *Block* = *managingBlocks b*
        $\wedge$ Ξ*Obstacles*
        $\wedge$ Ξ*TrainInfos*
        $\wedge$ Ξ*TempSpeedLimits*
        $\wedge$ *BlockInvariant*
        $\wedge$ *setPMA*[*red!inputPma?*]
        $\Rightarrow$ *managingBlocks'* = *managingBlocks* $\oplus$ {(*b* $\mapsto$ θ *Block'*)})

열차에 의해 점유된 블록에서 열차의 진행 반대 방향의 블록들의 PMA를 red로 설정한다.

redPMASettingByTrain

ΔDCM

---

securePMASetting

$\forall b$: dom *managingBlocks*

- **let** *nextBlocks* == *route* ({*b*}); *beforeBlocks* == *route* ({*b*})
  - $\forall$ *nextBlock*: *nextBlocks*; *beforeBlock*: *beforeBlocks*
    - ($\exists$ *existingTrain*: *Train_TYPE*
      - *existingTrain* . *id* $\in$ (*managingBlocks nextBlock*) . *occ*
        $\wedge$ *existingTrain* . *direction* = *UPWARD*
        $\vee$ *existingTrain* . *id* $\in$ (*managingBlocks beforeBlock*) . *occ*
        $\wedge$ *existingTrain* . *direction* = *DOWNWARD*)
      $\Rightarrow$ ($\exists_1 \Delta Block$
      - θ *Block* = *managingBlocks b*
        $\wedge$ Ξ*Obstacles*
        $\wedge$ Ξ*TrainInfos*
        $\wedge$ Ξ*TempSpeedLimits*
        $\wedge$ *BlockInvariant*
        $\wedge$ *setPMA*[*red!inputPma?*]
        $\Rightarrow$ *managingBlocks'* = *managingBlocks* $\oplus$ {(*b* $\mapsto$ θ *Block'*)})

폐쇄된 블록을 따져 먼저 PMA를 red로 설정한 후 점유된 블록을 확인하여 PMA를 red로 설정한다.

$$redPMASetting \triangleq redPMASettingByObstacle \fatsemi redPMASettingByTrain$$

블록들의 정보들을 따져(폐쇄된 블록들의 2칸 떨어진 양 옆의 블록들 및 점유된 블록으로부터 열차 진행 방향의 반대로 2칸 떨어진 블록) PMA를 yellow로 설정한다.

$$
\begin{array}{l}
\textit{yellowPMASetting} \\
\Delta DCM \\
\hline
\textit{securePMASetting} \\
\forall b : \mathrm{dom}\ managingBlocks \\
\quad \bullet\ \textbf{let}\ nextBlocks == route\,(\{b\});\ beforeBlocks == route\,(\{b\}) \\
\qquad \bullet\ \textbf{let}\ next2Blocks == route\,(nextBlocks); \\
\qquad\quad before2Blocks == route\,(beforeBlocks) \\
\qquad\quad \bullet\ \forall nextBlock : nextBlocks;\ beforeBlock : beforeBlocks; \\
\qquad\qquad next2Block : next2Blocks;\ before2Block : before2Blocks \\
\qquad\qquad \bullet\ (managingBlocks\ nextBlock).pma = red \\
\qquad\qquad\quad \wedge (managingBlocks\ nextBlock).obs = unset \\
\qquad\qquad\quad \wedge (\exists existingTrain : Train_TYPE \\
\qquad\qquad\qquad\quad \bullet\ (existingTrain.id \\
\qquad\qquad\qquad\qquad \in (managingBlocks\ next2Block).occ \\
\qquad\qquad\qquad\qquad \wedge existingTrain.direction = UPWARD)) \\
\qquad\qquad\quad \vee (managingBlocks'\ beforeBlock).pma = red \\
\qquad\qquad\quad\ \wedge (managingBlocks\ beforeBlock).obs = unset \\
\qquad\qquad\quad\ \wedge (\exists existingTrain : Train_TYPE \\
\qquad\qquad\qquad\quad \bullet\ (existingTrain.id \\
\qquad\qquad\qquad\qquad \in (managingBlocks\ before2Block).occ \\
\qquad\qquad\qquad\qquad \wedge existingTrain.direction = \\
DOWNWARD)) \\
\qquad\qquad \Rightarrow (\exists_1 \Delta Block \\
\qquad\qquad\qquad \bullet\ \theta Block = managingBlocks\ b \\
\qquad\qquad\qquad\quad \wedge \Xi Obstacles \\
\qquad\qquad\qquad\quad \wedge \Xi TrainInfos \\
\qquad\qquad\qquad\quad \wedge \Xi TempSpeedLimits \\
\qquad\qquad\qquad\quad \wedge BlockInvariant \\
\qquad\qquad\qquad\quad \wedge setPMA[yellow/inputPma?] \\
\qquad\qquad\qquad\quad \Rightarrow managingBlocks' \\
\qquad\qquad\qquad\qquad = managingBlocks \oplus \{(b \mapsto \theta Block')\})
\end{array}
$$

전에 PMA설정은 우선 모든 블록의 PMA를 green으로 설정한 후에 red조건을 따져 설정하고 마지막으로 yellow조건을 따져 설정한다.

$$wholePMASetting \cong greenPMASetting \fatsemi redPMASetting \fatsemi yellowPMASetting$$

· 열차 관련 오퍼레이션

열차로부터 입력받는 정보는 열차의 아이디, 진행 상태, 속도, 진행 방향 및 현재 점유하고 있는 블록 아이디이다.

Train_TYPE

$$id: TrainID_TYPE$$
$$runningStatus: RunningStatus_TYPE$$
$$speed: \mathbb{N}$$
$$direction: Direction_TYPE$$

$$runningStatus = STOP \Leftrightarrow speed = 0$$
$$runningStatus = RUNNING \Leftrightarrow speed > 0$$

receiveTrainInfo

$$inputTrain: Train_TYPE$$
$$currentBlock: BlockID_TYPE$$

열차가 새로 진입한 열차일 시에는 ATS로 해당 열차의 스케쥴 정보를 요청한다.

DCMOpWithTrain

$$\Delta DCM$$
$$receiveTrainInfo?$$

newTrainEntry

$$ScheduleManager$$
$$receiveTrainInfo?$$
$$getTrainSchedule!: TrainID_TYPE$$

$$inputTrain?.id \in \mathrm{dom}\ schedules$$
$$getTrainSchedule! = inputTrain?.id$$

새로운 열차가 진입할 시에는 스케줄 정보를 ATS로 요청하고 입력받아 업데이트한다.

$$getScheduleProcess \triangleq newTrainEntry \S getSchedule$$

열차로부터 정보를 수신 받았을 때 스케줄에 해당 열차의 정보가 존재하는지를 따져 새로 진입한 열차인지 존재하던 열차인지를 확인한다.

existingTrain

ScheduleManager
receiveTrainInfo?

---

inputTrain? . *id* ∈ dom *schedules*

정보를 수신 받았으며 존재하던 열차로 확인이 되었을 때 DCM 제어 영역 마지막 블록들을 점유한 열차인지를 확인하여 제어 영역 내에서 이동하는 열차인지 제어 영역에서 벗어나는 열차인지를 확인한다.

exitingTrain

DCM
existingTrain

---

let *endBlocks* == ran *route* \ dom *route*
• ∃*endBlock*: *endBlocks* • *inputTrain?* . *id* ∈ (*managingBlocks endBlock*) .
occ

DCM 제어 영역에서 벗어나는 열차로 확인 되었을 시 이 열차에 대한 스케줄 정보를 삭제한다.

deleteScheduleProcess

exitingTrain
Δ*ScheduleManager*
deleteTrainID: *TrainID_TYPE*

---

deleteTrainID = *inputTrain?* . *id*
deleteSchedule[*deleteTrainID*/*inputTrainID?*]

BlockValidity

DCM
receiveTrainInfo?

---

currentBlock? ∈ dom *managingBlocks*

열차로부터 정보를 수신 후 오퍼레이션을 수행 할 경우 반드시 전송받은 블록이 DCM 제어 영역 내의 블록이어야 하며 전송받은 블록외의 다른 블록에는 영향을 끼쳐서는 안된다.

DCMSecureOpWithTrain

DCMOpWithTrain

ΞRouteManager
ΞScheduleManager
{*currentBlock?*} ⩤ *managingBlocks'* = {*currentBlock?*} ⩤ *managingBlocks*

해당 블록에 진입하는 열차에 대한 occ업데이트 오퍼레이션은 기존에 정의한 entryTrainOK 오퍼레이션을 이용하여 정의한다.

updateBlockOccInEntryTrain

DCMSecureOpWithTrain
Block
tid: TrainID_TYPE

BlockValidity[*currentBlock?*/*blockID*]
BlockValidity'[*currentBlock?*/*blockID'*]
tid = *inputTrain?* . *id*
θ *Block*
= (μΔ*Block*
| θ *Block* = *managingBlocks currentBlock?*
∧ *entryTrainOK*[*tid*/*newTrain?*]
∧ Ξ*PMAs*
∧ Ξ*Obstacles*
∧ Ξ*TempSpeedLimits*
∧ *BlockInvariant* - θ *Block'*)
managingBlocks' currentBlock? = θ *Block*

해당 블록을 빠져나가는 열차 중 예약이 삭제되지 않은 열차에 대한 occ업데이트 오퍼레이션은 기존에 정의한 exitTrainWithDelete ReservationOK오퍼레이션을 이용하여 정의한다.

updateBlockOccDeletingRsvInExitingTrain

$DCMSecureOpWithTrain$
$Block$
$tid: TrainID_TYPE$

$BlockValidity[currentBlock?/blockID]$
$BlockValidity'[currentBlock?/blockID']$
$tid = inputTrain?.id$
$\theta Block$
$= (\mu \Delta Block$
$\mid \theta Block = managingBlocks\ currentBlock?$
$\wedge\ exitTrainWithDeleteReservationOK[tid/newTrain?]$
$\wedge\ \Xi PMAs$
$\wedge\ \Xi Obstacles$
$\wedge\ \Xi TempSpeedLimits$
$\wedge\ BlockInvariant \cdot \theta Block')$
$managingBlocks'\ currentBlock? = \theta Block$

해당 블록을 빠져나가는 열차 중 예약이 삭제된 열차에 대한 occ업데이트 오퍼레이션은 기존에 정의한 exitTrainWithoutDeleteReserva tionOK오퍼레이션을 이용하여 정의한다.

updateBlockOccNotDeletingRsvInExitingTrain

$DCMSecureOpWithTrain$
$Block$
$tid: TrainID_TYPE$

$BlockValidity[currentBlock?/blockID]$
$BlockValidity'[currentBlock?/blockID']$
$tid = inputTrain?.id$
$\theta Block$
$= (\mu \Delta Block$
$\mid \theta Block = managingBlocks\ currentBlock?$
$\wedge\ exitTrainWithoutDeleteReservationOK[tid/newTrain?]$
$\wedge\ \Xi PMAs$
$\wedge\ \Xi Obstacles$
$\wedge\ \Xi TempSpeedLimits$
$\wedge\ BlockInvariant \cdot \theta Block')$
$managingBlocks'\ currentBlock? = \theta Block$

해당 블록을 빠져나가는 열차에 대한 occ업데이트 오퍼레이션을 위의 두가지 경우의 오퍼레이션을 조합하여 정의한다.

$$updateBlockOccInExitingTrain \triangleq upateBlockOccNotDeletingRsvInExitingTrain \vee updateBlockOccDeletingRsvInExitingTrain$$

DCM 제어 구역으로 진입하는 열차, 이동하는 열차, 벗어나는 열차에 대한 occ업데이트 오퍼레이션을 조합하여 전체 occ업데이트 오퍼레이션을 정의한다.

$$updateBlockOccInMovingTrain \triangleq updateBlockOccInEntryTrain \S updateBlockOccInExitingTrain$$

$$updateBlockOcc \triangleq updateBlockOccInEntryTrain \vee updateBlockOccInMovingTrain \vee updateBlockOccInExitingTrain$$

열차의 입력에 대한 오퍼레이션 수행이 완료한 후에 열차에게 명령을 전송한다. 명령은 전송받을 열차의 아이디, 임시속도설정 상태 및 속도 및 열차 점유 블록을 포함한 진행방향의 4개 블록의 PMA설정 상태로 이루어진다. 또한 열차가 예약하지 못한 블록에 대해서는 DCM 내의 PMA설정에 관계없이 red를 전송한다.

```
sendingCommand
DCM
receiveTrainInfo?
nextBlock: BlockID_TYPE
next2Block: BlockID_TYPE
next3Block: BlockID_TYPE
cmd!: CMD
---
BlockValidity[currentBlock?/blockID]
BlockValidity[nextBlock/blockID]
BlockValidity[next2Block/blockID]
BlockValidity[next3Block/blockID]
nextBlock = schedules inputTrain? . id currentBlock?
next2Block = schedules inputTrain? . id nextBlock
next3Block = schedules inputTrain? . id next2Block
cmd! . 1 = inputTrain? . id
cmd! . 2 = (managingBlocks currentBlock?) . tempSpeedLimitStatus
cmd! . 3
  = if inputTrain? . id ∈ (managingBlocks next3Block) . reservedTrain
    then ⟨(managingBlocks currentBlock?) . pma,
          (managingBlocks nextBlock) . pma, (managingBlocks next2Block) .
pma,
          (managingBlocks next3Block) . pma⟩
    else if inputTrain? . id ∈ (managingBlocks next2Block) . reservedTrain
         then ⟨(managingBlocks currentBlock?) . pma,
               (managingBlocks nextBlock) . pma, yellow, red⟩
         else if inputTrain? . id ∈ (managingBlocks nextBlock) .
reservedTrain
              then ⟨(managingBlocks currentBlock?) . pma, yellow, red,
red⟩
              else ⟨yellow, red, red, red⟩
```

새로 열차가 진입하면 ATS로부터 해당 열차에 대한 스케쥴을 요청하여 입력받아 진입한 블록의 occ를 업데이트한 후에 전체 블록의 PMA를 설정하고 열차에게 명령을 전송한다.

$$enterNewTrain \triangleq newTrainEntry \S getSchedule \S updateBlockOccInEntryTrain \S wholePMASetting \S sendingCommand$$

열차가 블록을 이동하면 이동한 블록으로 occ를 업데이트하고 전체 블록의 PMA를 설정한 후 열차에게 명령을 전송한다.

$$moveTrain \triangleq movingTrain \S updateBlockOccInMovingTrain \S wholePMASetting \S sendingCommand$$

DCM 제어 구역을 벗어나면 해당 열차의 스케쥴을 삭제하고 occ를 업데이트 한 후에 전체 블록의 PMA를 설정한다.

$$exitLeavingTrain \triangleq exitingTrain \fatsemi deleteSchedule \fatsemi updateBlockOccInExitingTrain \fatsemi wholePMASetting$$

(e) 블록 개방/폐쇄 및 임시속도 설정 관련 오퍼레이션

ATS로부터 블록 개방/폐쇄 및 임시속도 설정 명령을 전송받으며 개방/폐쇄 명령이 활성화일 시(*setOpenCloseCmd* . 1=*set)*임시속도명령은 비활성화이다. (*setTempSpeedLimitCmd* . 1=*unset*)

receiveBlockInfo

$$inputBlock: BlockID_TYPE$$
$$setOpenCloseCmd: SetStatus_TYPE \times SetStatus_TYPE$$
$$setTempSpeedLimitCmd: SetStatus_TYPE \times TempSpeedLimit_TYPE$$

$$setOpenCloseCmd.1 = set \Leftrightarrow setTempSpeedLimitCmd.1 = unset$$

DCMOpWithATS

$$\Delta DCM$$
$$receiveBlockInfo?$$

블록 개방/폐쇄 시에는 해당 블록 이외에 모든 블록의 정보는 바뀌지 않는다.

DCMSecureOpWithATS

$$DCMOpWithATS$$

$$\exists RouteManager$$
$$\{inputBlock?\} \lhd managingBlocks' = \{inputBlock?\} \lhd managingBlocks$$

블록 개방/폐쇄 오퍼레이션은 기존에 정의한 setObstacleOK를 이용하여 정의한다.

blockOpenClose

$DCMSecureOpWithATS$
$Block$

$setOpenCloseCmd?.1 = set$
$\Delta BlockValidity[inputBlock?/blockID, inputBlock?/blockID']$
$\theta Block$
$= (\mu \Delta Block$
$\mid \theta Block = managingBlocks\ inputBlock?$
$\wedge\ \Xi TrainInfos$
$\wedge\ \Xi PMAs$
$\wedge$ (**if** $setOpenCloseCmd?.2 = set$
then $setObstacleOK[set/inputObs?]$
else $setObstacleOK[unset/inputObs?]$)
$\wedge\ \Xi TempSpeedLimits$
$\wedge\ BlockInvariant \cdot \theta Block')$
$managingBlocks'\ inputBlock? = \theta Block$

블록 개방/폐쇄 후 모든 블록들의 PMA를 재설정한다.

$blockOpenCloseProcess \triangleq blockOpenClose \S wholePMASetting$

블록 개방/폐쇄 오퍼레이션은 기존에 정의한 setTempSpeedOK를 이용하여 정의한다.

setTempSpeedLimit

$DCMSecureOpWithATS$
$Block$
$tempSpeedLimit: TempSpeedLimit_TYPE$

$setTempSpeedLimitCmd?.1 = set$
$tempSpeedLimit = setTempSpeedLimitCmd?.2$
$\Delta BlockValidity[inputBlock?/blockID, inputBlock?/blockID']$
$\theta Block$
$= (\mu \Delta Block$
$\mid \theta Block = managingBlocks\ inputBlock?$
$\wedge\ \Xi TrainInfos$
$\wedge\ \Xi PMAs$
$\wedge\ setTempSpeedOK[tempSpeedLimit/inputTempSpeed?]$
$\wedge\ \Xi TempSpeedLimits$
$\wedge\ BlockInvariant \cdot \theta Block')$
$managingBlocks'\ inputBlock? = \theta Block$

제9절 선로전환 결함방지 기술 분석 및 요구사항 제시

검증계획서 **(Verification Plan)**	**ID No :** **TC - SR05 - SSR05 - 2010** 작성일 : 2009. 05. 수정일 :

5. 프로젝트는 열차제어시스템 안전향상 핵심기술을 개발하여야한다

5.5 프로젝트는 열차제어장치에 의한 선로전환 결함방지 기술분석 및 요구사항이 제시되어야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 조사분석 문서 ☐ **검증 방법** - 0 명칭	- SE 검증	- 수정 VRTM - 검증결과표

Verification Specification (검증기준) :

1. 선로전환 결함 결함 사고 사례가 조사되었는가?
2. 선로전환 결함방지을 위한 설비들이 조사되었는가?

1. 설계분석보고서

가. 요구사항과의 적합성

선로전환 결함 방지기술 조사분석은 『SR 5. 프로젝트는 열차제어시스템 안전향상 핵심 기술을 개발하여야 한다.』 중 『SSR. **5.5. 프로젝트는 열차제어장치에 의한 선로전환 결함방지 기술분석 및 요구사항이 제시되어야 한다.**』에 해당하는 내용이다. 본선과 중요한 측선의 분기를 위해 사용되는 선로전환기는 전환장치 및 쇄정장치가 설치되어야 하며, 연동장치역, 원격장치역, 원격제어구간 및 필요한 개소에 설치된다. 당해연도에는 선로전환기는 열차의 진로를 제어하는 철도신호용품으로 선로전환 결함시 열차의 탈선 및 충돌을 발생시킬 수 있는 안전 필수 시스템으로 선로전환 결함을 방지 또는 예방할 수 있는 기술을 조사분석 하였다.

나. 성과물의 내용 및 결과

본 절에는 당해연도에 수행한 선로전환 결함 방지기술 관련한 선로전환 결함 사고 사례 조사분석, 국내에 운용 중인 선로전환 결함 방지 설비의 특징 및 주요 기능, 국내에 운용 중인 주요한 선로전환기의 관련 규격 조사를 통한 요구사항 분석 등을 수행하였다. 이러한 조사분석 결과를 바탕으로 차년도에 선로전환 결함 방지를 위한 요구사항이 제시될 예정이다.

(1) 선로전환 결함 사고사례

선로전환 결함 방지기술 조사분석을 위해 우선적으로 몇 가지의 선로전환 결함 관련 장해사례를 조사하였다.

(가) 선로전환기 고장

ㅇ 주요기능

- 열차의 가고자하는 진로확보 및 방향 변경기능 제공
- 취급자(TTC) → IF_C → 전자연동장치(SICAS) → 분산제어컴퓨터 (STEKOP) → 선로전환기제어모듈(DEWEMO)에 의해 동작

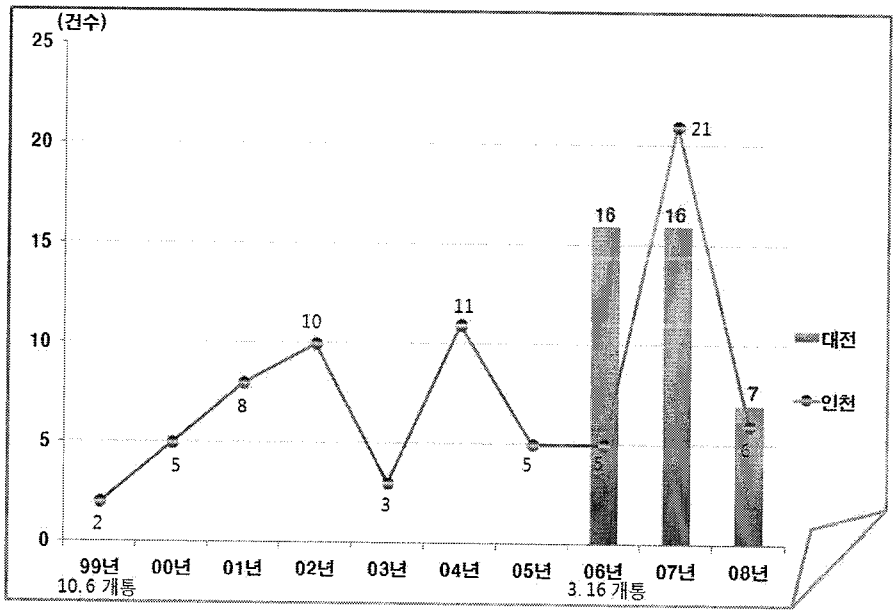


그림 3.9.1 이상현상 발생 현황

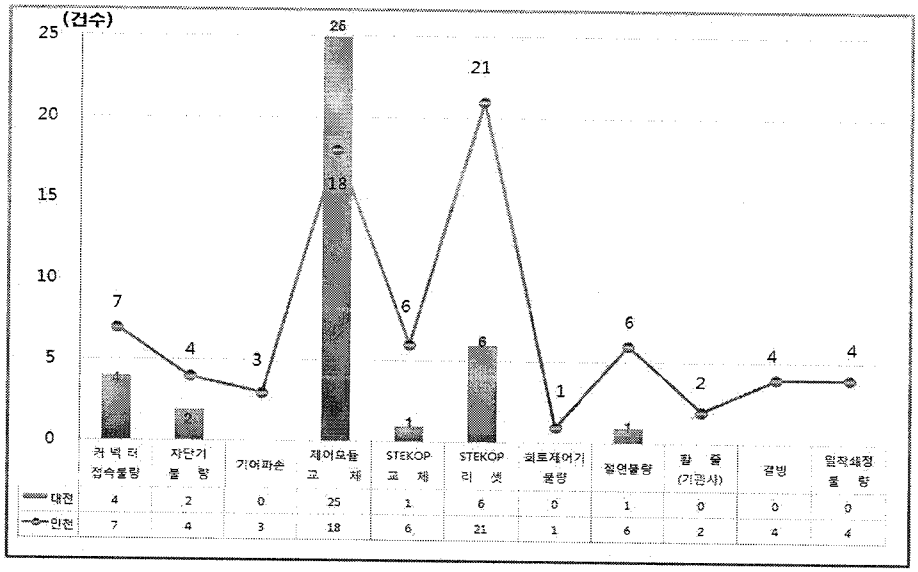


그림 3.9.2 개소별 이상현상 발생 현황

< 인천사례 >

- 안정기 : 개통 후 7년간('99.10 - '06.12) 년 평균 6.2건 이상현상 발생
- 우발적 발생기 : 안정기 이후 2년간 년 평균 13.5건의 이상현상 발생

(계양연장선 개통시 우리와 동일한 전환모듈 사용)

< 대전사례 >

- 정착단계 : 개통 후 2년('06.3 - '06.12) 32건 이상현상 발생
- 안정화 단계 : 정착단계 이후 1년간 년 평균 7건 이상현상 발생

표 3.9.1 이상현상 원인분석 및 조치결과

발생 개소	원인 분석	조치 결과
커 넥 터 (연결장치)	· 모듈을 연결하는 케이블에서 접촉 불량 발생	· 커넥터 교체 및 재접속
차 단 기 (안전장치)	· 단자접촉부 결함으로 인한 접촉불량, 과전류 발생	· 단자접촉부 체결장치 개선
전환장치 (기 어 부)	· 밀착력 과다로 인한 금속피로 현상 발생 (인천사례)	· 기어(치차)교체 및 밀착력 조정
제어모듈 (DEWEMO)	· 모듈내부 계전기 접점불량	· 선로전환기 감시시스템 설치 · 접점불꽃방지장치 설치 · 기능강화 계전기로 교체
STEKOP (분산제어 컴퓨터)	· 메인보드(FEMES)보드 불량	· 분산제어컴퓨터(STEKOP)교체
STEKOP 리 셋	· 선로전환기 장기간(10일) 미사용	· 10일 이전 선로전환기 전환시험
회로제어기	· 불꽃(아크)에 의한 접점 손상	· 회로제어기 교체
절연불량	· 우수침입으로 인한 전선 절연파괴	· 전선 교체, 우수침입 방지작업
활 출 (인천사례)	· 기관사의 신호모진으로 인한 선로 전환기 말착, 쇄정간 손상(만곡)	· 밀착, 쇄정간 교체 · 기관사 교육 실시
선로전환기 결 빙	· 클러치부 우수 유입으로 결빙 · 텅레일부 눈등 이물질유입으로 결빙	· 클러치부 방수(실리콘)작업실시 · 폭설시 주기적 눈 제거실시
밀착쇄정 불 량 (인천사례)	· 밀착력 과다조정으로 반발발생 · 쇄정간격 좌우 상이	· 전환력측정기에 의한 정밀조정 · 쇄정간격 좌우 균등조정

(나) 선로전환기 결빙

○ 발생일시 : 0000. 0. 00(수) 00:00~00:00

○ 발생장소 : 0호선 00기지 (선로전환기)

○ 장애내용 :

- 신호기계실내 궤도회로 전원공급용 휴즈가 소손되어 기지 구내의 신호 제어가 불능되어(1차 장애)
- 휴즈를 교체하여 정상 복구하였으나 선로 전환기 상판의 결빙으로 선로 전환기에 불일치 현상이 발생(2차 장애)
- 선로전환기 해빙조치 및 수신호 취급을 하던 관계로 5개 열차의 출고가 지연된 장애임.

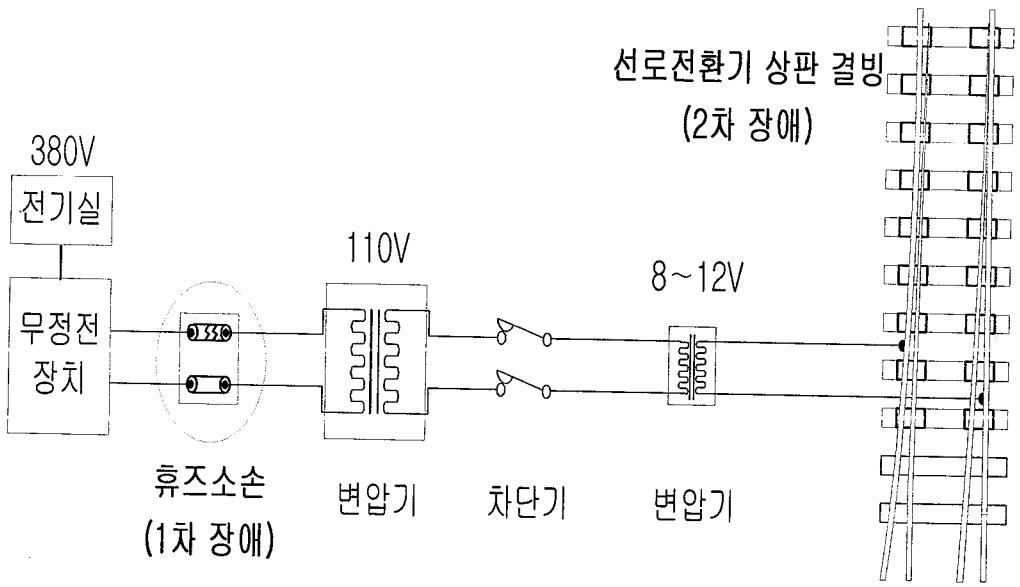


그림 3.9.3 선로전환기 상판결빙 사고

○ 문제점

⇒ 1차 장애 : 휴즈 삽입부 체결볼트 이완으로 접촉불량 발생

- 열차의 점유상태 현시를 위하여 전기적으로 구분된 궤도에 전원을(4~7V) 공급하는 휴즈 삽입부의 체결 볼트가 풀려
- 접촉 불량에 의한 과열 현상으로 동 개소의 열화로 소손 되면서 궤도에 전원 공급이 중단되자 기지구내 궤도가 낙하되어 신호 제어가 불능됨

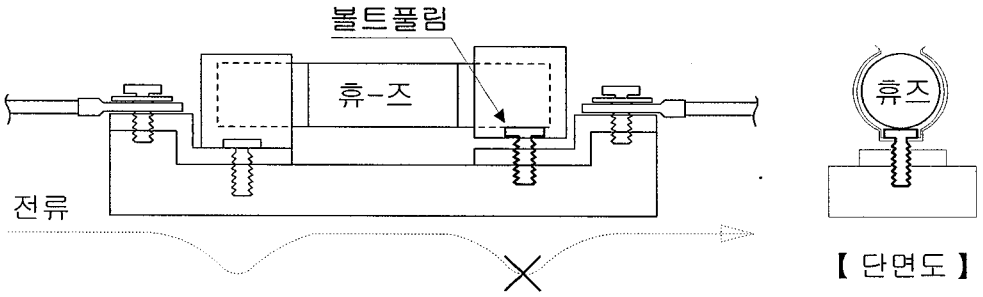


그림 3.9.4 휴즈 삽입부 체결볼트 이완으로 접촉불량

⇒ 2차 장애 : 혹한에 의한 선로 전환기 상판 결빙

- 장애전일 야간에 진눈개비가 내려 청소 및 점검을 시행하였으나 새벽까지 계속된 혹한(영하 13도)에 의하여
- 선로 전환기 상판이 결빙되어 원활하게 작동되지 못하고 불일치 현상이 발생된 것임.

○ 대 책

- 신호기계실내 휴즈홀더 및 기타 주요 접속개소의 접촉 및 체결상태 일제점검
- 각 기지구내 선로전환기 점검 및 관리요령에 대한 특별교육 실시
  (혹한기, 폭설 등 이상 기후시 점검 및 관리요령)
- 기지 주재소에 휴즈류 등 즉시 교체 가능(필요)한 주요 예비품 확보

(다) 선로전환기의 제어 불능

○ 발생일시 : 0000. 00. 00(화). 00:00~00:00

○ 발생장소 : 0호선 000역 구내 (000 선로전환기)

○ 관계열차 : 제0000열차 (000편성, 00발→00행)

○ 장애내용

- 상기 열차가 자동운전으로 강동역 도착후 출발 대기중에 000번 선로전환기에 불일치 현상(신호제어 불능)이 발생되어 선로전환기 수동 및 수신호 취급을 하던 관계로 열차운행이 지연된 장애임.

※ 열차지연 : 제0000열차 외 0개 열차 0~0분 지연

○ 문제점

⇒ 상반된 2개의 명령(정보충돌 현상)으로 불일치현상 발생

- 선로전환기가 정위인 상태에서 마천발 열차가 강동역 상측선에 접근하자
- TTC에서는 선로전환기를 열차가 진행할 방향(반위)으로 전환토록 명령을 송출하여 선로전환기가 전환하려던 중
- 강동역 신호기계실 MLK(전자연동장치)는 전환하려는 선로전환기에 전환 금지 명령을(정위유지) 송출하여
- 상반된 2개의 명령으로 정보충돌(반위명령 실행중 정위유지명령 지시) 이 발생 선로전환기 불일치 현상 발생됨

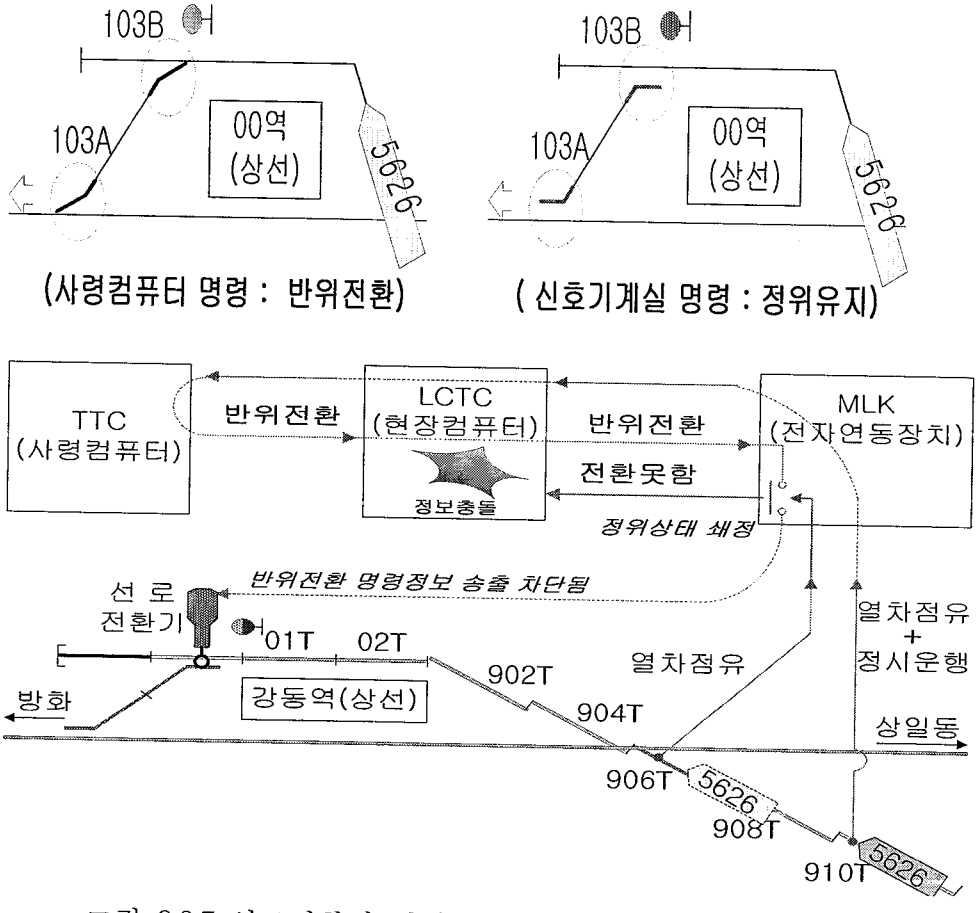


그림 3.9.5 선로전환기 정위 상태에서 명령(정보) 송출 개요

○ 대 책

- 전직원에게 주요 장애 유형별 응급조치 방법에 대하여 이론 교육과 병행하여

실제적인 현장 교육을 주기적으로 실시

- 신호시스템 보완 방안에 대하여 면밀한 검토 및 시스템 보완방안 강구

(2) 선로전환 결함 방지를 위한 설비 조사분석

선로전환 결함 방지기술 조사분석을 위해 선로전환 결함 방지를 위해 국내에서 일부에 운용 중인 선로전환기 레벨감시 장치, 센서형 밀착검지기, 고속분기기용 밀착검지기, 밀봉형 클러치 등의 장치들에 대해 조사분석 하였다. 이러한 각종 설비들의 조사분석을 통해 차년도에 선로전환 결함 방지기술 요구사항이 제시될 예정이다.

(가) 선로전환기 레벨감시 시스템

선로전환기 유지보수 또는 장애발생시 보수요원은 선로전환기의 제어 및 표시정보를 판독하여 고장개소를 실시간으로 계측, 판단하여야 하나 현재의 상태로는 동시에 6개회로의 전압을 수동으로 측정하여 (모터공급전원, 제어전원, 표시전원 입, 출력 전압) 장애개소를 판단, 유지 보수하는 실정으로 작업의 번거로움과 오 측정, 오판단시에는 복구지연 및 안전사고로 이어질 수 있는 요인을 지니고 있다.

이러한 애로사항을 개선하고자 배타적 논리합(XOR)회로와 부정논리합(NOR)회로를 이용하여 실시간으로 회선별 상태를 판단할 수 있도록 하는 감시설비로서, 국내 일부 운영기관에서 운용 중에 있다. 선로전환기 레벨감시 시스템은 선로전환기 각부의 전압을 측정하여 각부의 전압이상 유무를 즉시 판단할 수 있고, 장애 발생 또는 유지보수시 이에 대한 후속 조치를 신속히 할 수 있으며, 1개 연동역의 5대 이상의 전 선로전환기 레벨감시를 위한 논리회로로 제어부는 XOR, 표시부의 표시입력, 표시출력, 제어전압, 모터전압은 NOR회로를 채용하여 선로전환기 상호간 Interlock를 설정하여 오동작으로 인한 혼촉장애를 방지하도록 되어 있다. 이러한 선로전환기 레벨감시 설비의 주요한 특징은 다음과 같다.

- 선로전환 감시시스템 제어부는 안전원칙회로인 부정논리합의 채용으로 측정선로전환기 동작중일 때 타 선로전환기 오동작을 방지하도록 한다.
- 표시부는 제어부와 연계하여 배타적 논리합(NOR) 회로로 설계되어 제어부 회로와 연동하여 계측된 전압값을 디지털 데이터로 표출한다.

- 6회로 동시 자동 레벨 측정이 가능하여 버튼만 누르면 실시간으로 해당 선로전환기의 전압측정이 가능하며 표출부를 Digital Display 채용으로 식별이 용이하도록 한다.
- 측정 포인트를 계속하여 테스터 리드봉 사용시 전선접속재가 탄력이 변형되어 2차 유발장애가 발생할 수 있으나 선로전환 감시스템 적용으로 리드봉을 사용할 필요가 없어 장애요인을 감소시킬 수 있다.
- 장애상태에 따라 단선, 접지 등이 자동검출 계측되어 레벨이 표시되어 유지보수자가 즉시 장애개소를 판단할 수 있다.

현재 국내에서 개발되어 적용되고 있는 선로전환 감시 장치는 다음과 같은 특정한 선로전환기에 적용되고 있다. 현재는 특정한 선로전환기에 적용이 되고 있지만, 인터페이스의 구성을 변경할 경우 다른 형식의 선로전환기에 적용이 가능한 것으로 예상되며, 이러한 설비의 적용을 통해 선로전환 결함 방지 및 유지보수 효율성 향상에 많은 기여가 예상된다.

조사 대상의 감시설비의 선로전환기 제어모듈은 분산제어 컴퓨터와 선로전환기 사이의 인터페이스를 담당하는 모듈이다. 전자연동장치에서 선로전환기 제어에 관련된 명령은 선로전환기 제어모듈을 통하여 현장 선로전환기를 제어한다. 그리고, 분산제어컴퓨터는 선로전환기의 구동을 비롯한 전반적인 제어와 선로전환기 전환상태의 점검 등을 수행하며, 그 정보를 전자연동장치로 보낸다. 하나의 분산제어컴퓨터 보드는 두 개의 선로전환기 즉, 두 개의 선로전환기 제어모듈을 제어한다.

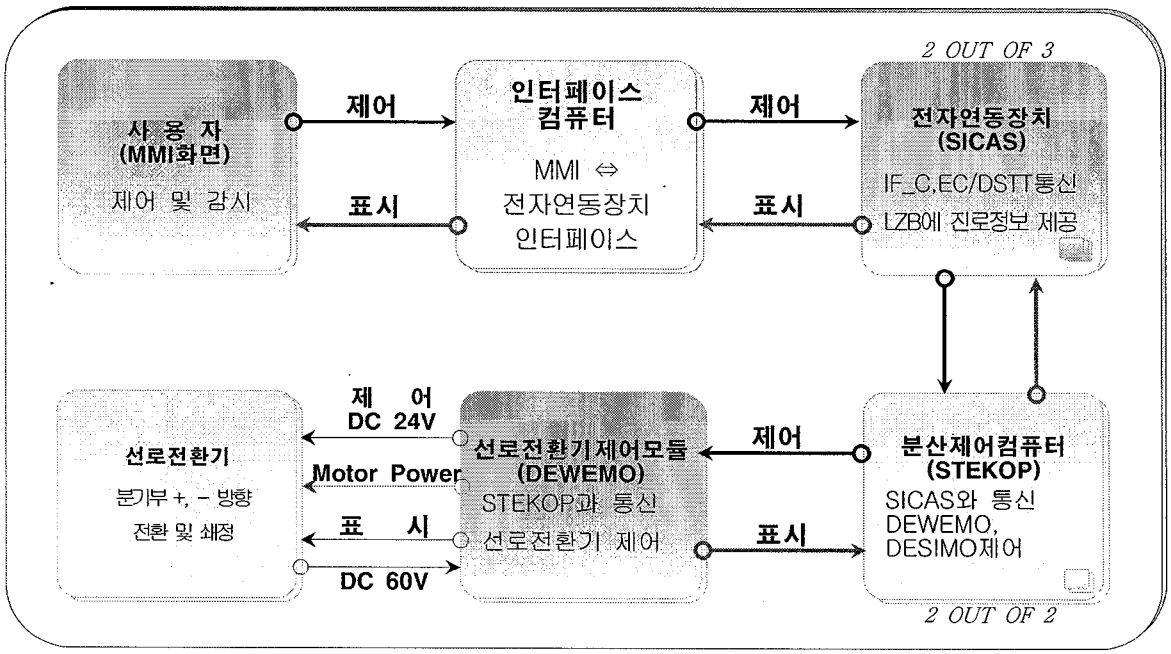


그림 3.9.6 제어 및 표시정보 전송체계도

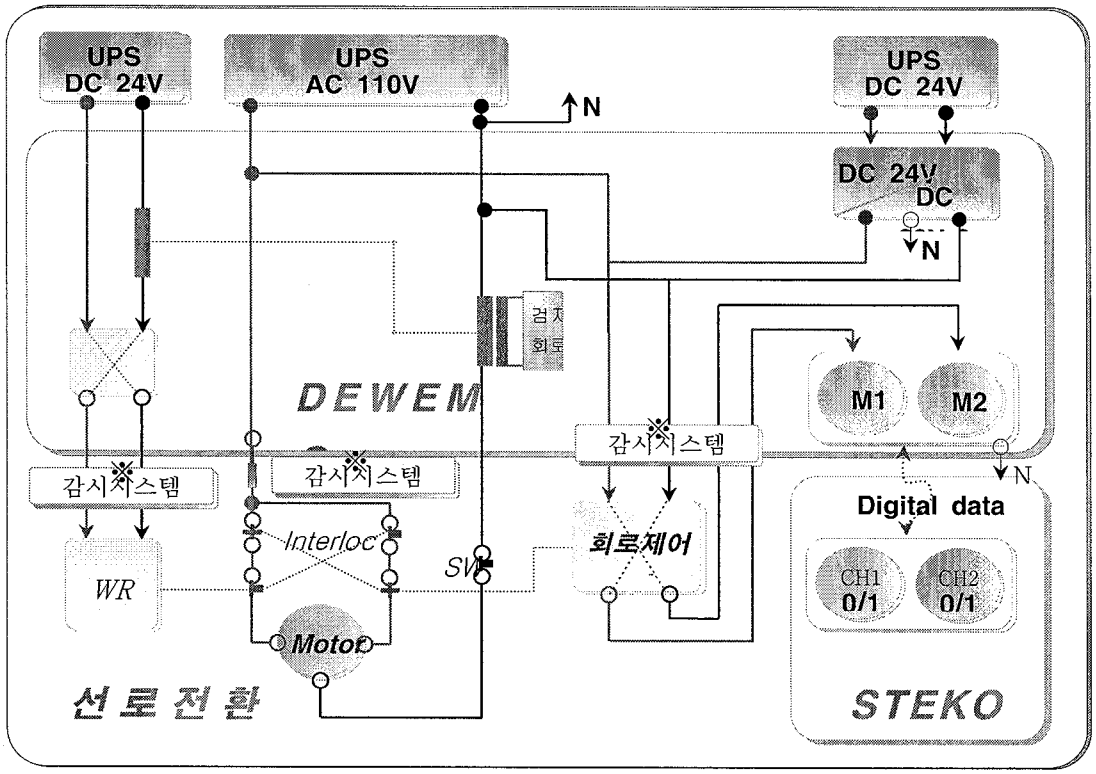


그림 3.9.7 선로전환기 제어모듈 블록도

그림 3.9.7은 선로전환기 제어모듈 블록도를 나타낸 것으로 그림에서 '감시시스

템'으로 표시한 부분의 검지를 통해 선로전환기를 감시하게 된다. 선로전환기 게어 모듈의 전원부는 일종의 DC-DC Converter를 포함하고 있어 DC 24V를 제어모듈 구동용 12V × 2개와 선로전환기 감시에 필요한 DC +60V, −60V생성하여 회로에 공급하는 일종의 SMPS(Switching Mode Power Supply)이다. 선로전환기 표시출력부 감시를 위해 그림 3.9.8 표시출력의 X4-5, X4-6에 측정점을 설치하여 출력되는 전압을 감시하도록 되어 있다.

표시회로는 2개의 표시부로 구성되어 현장 회로제어기의 구성접점에 의해 각각 다른 전압을 입력받게 되어 있다. 회로도에서 살펴보면 OP-Amp U2A, U2B, U3A, U3B로 구성되어 있는 부분이 표시부 1이 되고 OP-Amp U2C, U2D, U3C, U3D로 구성되어 있는 부분이 표시부 2가 된다. Right 방향으로 전환시 회로제어기 접점은 표시부 1로 +60V를 그리고 표시부 2로 -60V를 입력하도록 회로가 구성된다. 그림 3.9.9의 표시부 1은 +60V가 공급이 되면, U2A로 구성된 적분기와 U2B로 구성된 증폭기에 의해 Low를 출력하게 되어 LED 3이 ON되게 된다. 반대로 U3A와 U3B로 구성된 아래 부분은 High를 출력하게 되어, LED 4는 OFF된다. 그림 3.9.10의 표시부2는 −60V가 공급이 되면, U3C와 U3D로 구성된 부분은 Low를 출력하게 되어 LED 2가 ON이 된다. 그리고, U2C와 U2D로 구성된 부분은 High를 출력하게 되어 LED 1이 OFF되게 된다. 만약 좌측 방향으로 전환시에는 표시부1로 60V, 표시부2로 +60V가 입력되게 되어 있어 위의 상황과 반대로 동작하게 된다.

만약 선로전환기가 동작 중에는 U3A, U3C의 적분기 입력은 12V가 입력되고 그 출력이 U3B, U3D의 반전 입력단에 인가된다. U3B, U3D의 비반전 입력단의 분배 전압보다 적게 되어 High를 출력하게 된다. 따라서 LED2과 LED4는 OFF되지만 U2A, U2B, U2C, U2D로 구성된 부분의 LED1, LED3은 ON이 된다. 출력된 +60V와 -60V가 현장 선로전환기의 회로제어기와 제어계전기 접점을 통하여 표시전원이 입력되어 선로전환기의 방향을 결정하게 된다. 입력되는 전압을 측정하기 위하여 아래 그림 3.9.9 입력부 1의 X4-9, X4-10에 측정점을 설치하여 수신전압을 감시한다.

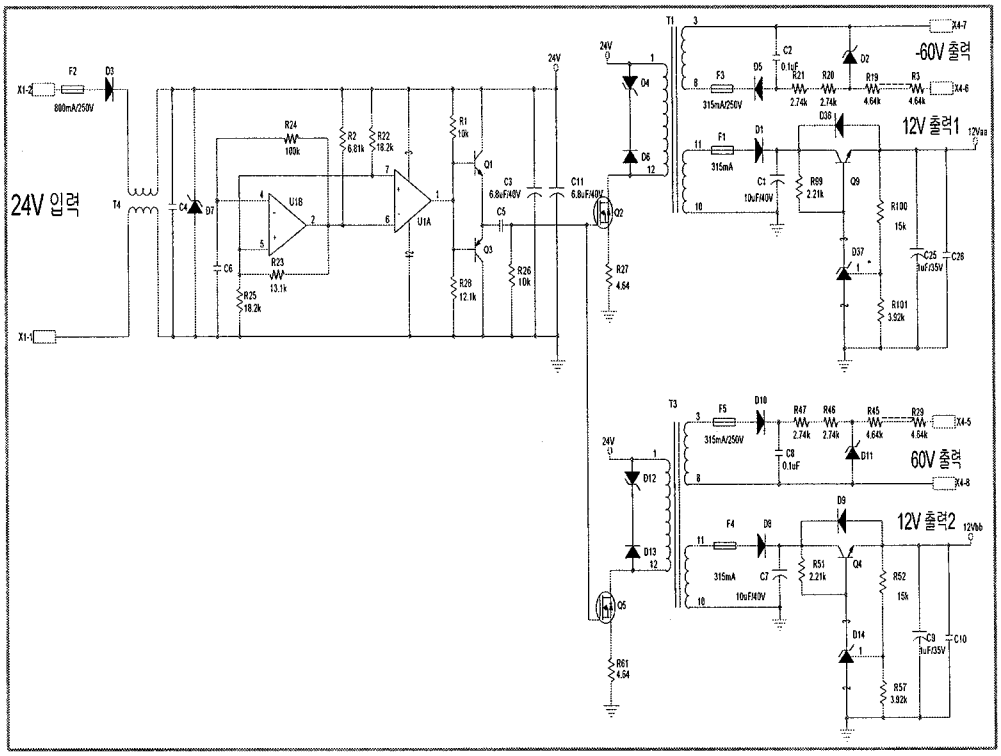


그림 3.9.8 표시출력

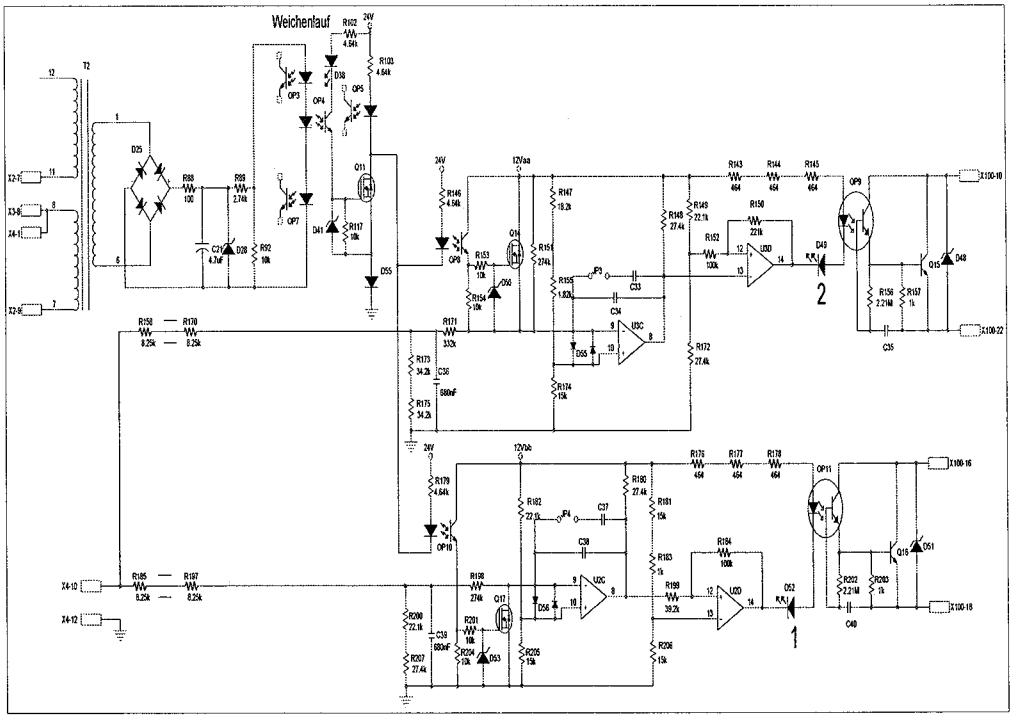


그림 3.9.9 표시 입력부 1

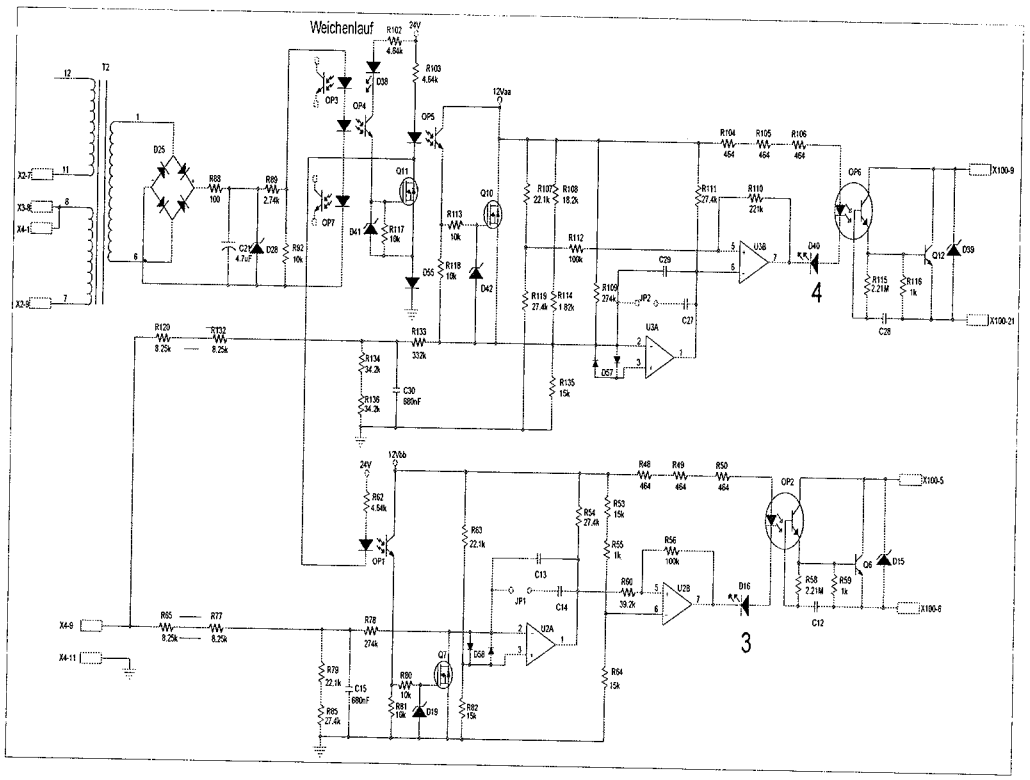


그림 3.9.10 표시 입력부 2

○ 선로전환기 방향 제어부 동작 및 전압측정

분산제어 컴퓨터로부터 '우측 방향으로 전환' 명령이 수신되면 회로도상의 좌측 부분의 K2(R) 계전기가 동작하게 되고, 그에 따라 K1(R2), K8(R1) 계전기가 동작하게 된다. 이때 D23, R LED(이전 상태가 L일 경우)가 동작한다. 즉, 전환명령이 내려지면 D23 LED와 전환명령에 해당하는 각 LED만 동작하게 된다. 이 K1, K8 계전기의 접점을 통하여 현장 선로전환기 내부의 제어계전기를 동작시킨다.

이 제어계전기는 유극계전기로서 선로전환기 전환방향에 따라 인가되는 제어전압 DC24V의 극성이 방향계전기 구동여부에 따라 변하게 된다. 즉, 우측 방향일 경우, K1, K8 계전기가 구동되어 현장 제어계전기로 +24V가 인가되고 Left 방향일 경우는 K3, K5 계전기가 구동되어 우측t 방향일 경우와 반대 극성의 전압이 제어계전기에 인가되게 된다. 제어계전기로 출력되는 전압을 측정하기 위해 그림 3.9.11 제어전압 감시의 X3-3, X3-6단자에 측정점을 설치하여 상시 출력되는 전압을 감시한다.

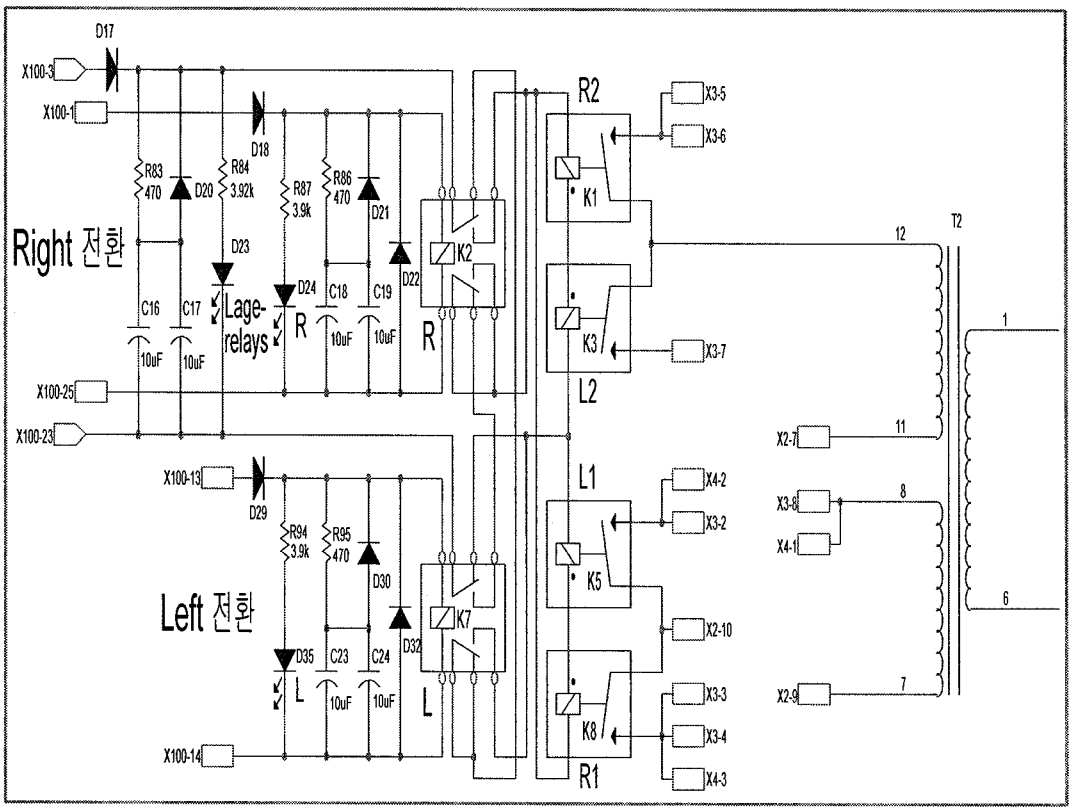


그림 3.9.11 제어전압 감시

○ 모터전원부 측정

분산제어컴퓨터는 제어계전기를 동작시킨 후 회로도 중앙 우측부분의 X100-24 (X100-2단자에는 항상 24V 공급)를 0전위로 만든다. 이 단자를 통해 공급되는 24V는 C20, C31 컨덴서를 충전하는 시간동안은 Q8, Q13을 ON시킴으로써 HS1, HS2 전환보조계전기(K4, K6, K9, K10 계전기)를 동작시키게 된다. 따라서 표시전원 ±60V가 T2 1차측에 흐르지 않아도 HS1, HS2가 동작하게 된다. 이 시간동안 계전기들 접점이 ON상태가 되고 접점을 통해 AC110V가 흐름으로써 이 후 시간동안은 AC110V에 의해 T2 2차측에 전류를 유기하여 OP3, OP4, OP7 Optocoupler를 구동하게 되어 K4, K6, K9, K10 계전기를 구동시킬 수 있다.

위와 같은 절차에 의해 전환 중에는 16초 동안 HS1, HS2 계전기가 동작하게 된다. AC110V의 T2 자화는 회로제어기의 접점이 낙하되어 보조계전기(HS1, HS2)의 접점이 낙하될 때까지 이루어진다. 이러한 방식으로 T2는 AC110V의 감시를 통하여 선로전환기 전환 작업을 수행한다. 그림 3.9.12 모터전원감시의 X3-1, X3-8에

측정점을 설치하여 모터 전원 공급상태를 감시한다.

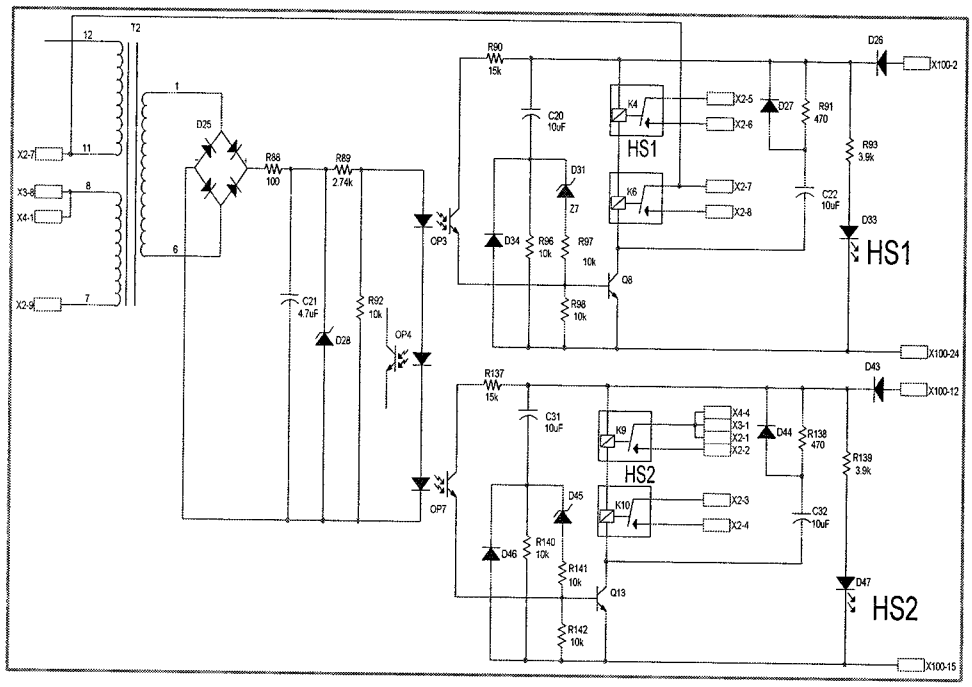


그림 3.9.12 모터전원 감시

○ 출력레벨 감시 장치

보통 연동역은 5대 이상의 선로전환기가 설치되어 운영되고 있으며, 측정 포인트를 설치한 후 일정한 연쇄에 의해 모든 선로전환기 전압측정을 일괄적으로 제어할 수 있다. 또한 1개의 선로전환기 측정 중에는 다른 선로전환기를 측정할 수 없도록 연동장치를 제작하여 전원 혼촉에 의한 장애를 방지하도록 구성한다. 1개 역의 모든 선로전환기 레벨감시를 위한 논리회로로 제어부는 XOR, 표시부의 표시입력, 표시출력, 제어전압, 모터전압은 NOR회로를 채용하여 선로전환기 상호간 Interlock을 설정하여 오동작으로 인한 혼촉장애를 방지하도록 구성하고 있다.

도면과 같이 PB101A를 누르게 되면 101B, 102A, 102B, 103A, 103B, 104계전기의 낙하접점 구성이 되어있는지를 확인하고, 이상이 없을 경우 101A 감시용 계전기가 동작하고, PB101버튼이 복귀되더라도 자기유지회로에 의해 계속 동작된다. 다른 선로전환기 측정을 위해 버튼을 누르더라도 Interlocking에 의해 동작되지 않으며 리셋버튼을 눌러야만 타 선로전환기 측정이 가능하다. (PB101B ~PB104B도

위와 동일한 절차에 의해 동작한다.) 선로전환기 레벨감시는 버튼취급에 의해 동작된 계전기의 여자접점에 의해 7개의 선로전환기 제어, 표시1, 표시2, 모터전압을 실시간으로 감시하게 된다.

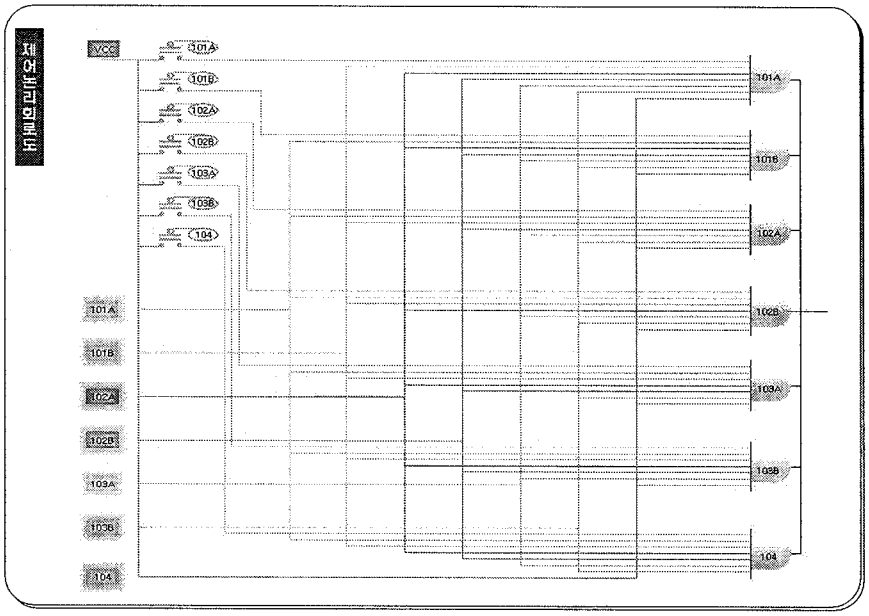


그림 3.9.13 제어부 논리회로

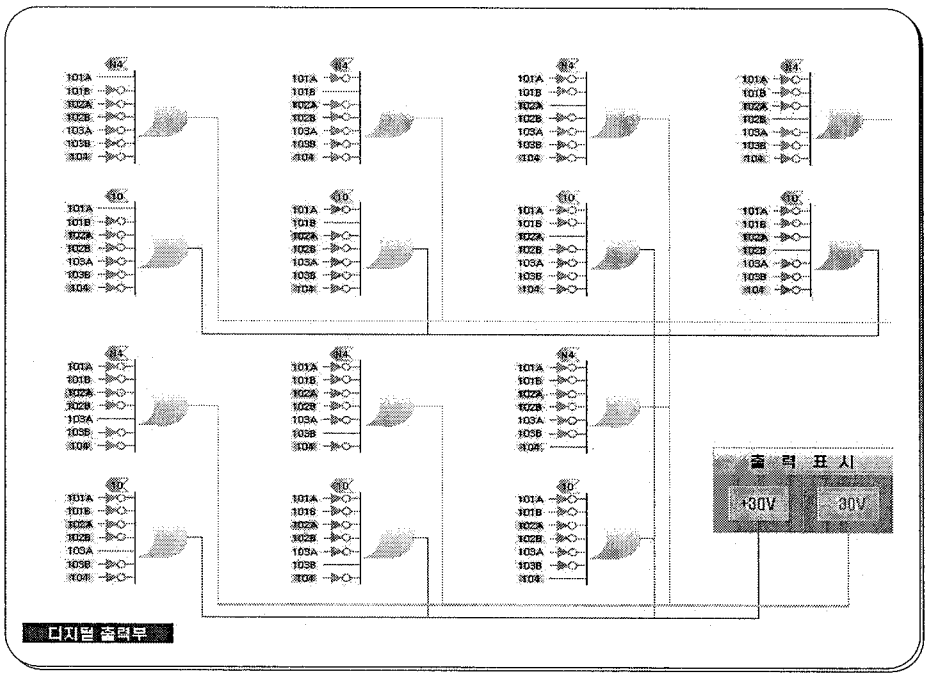


그림 3.9.14 표시부(출력)논리 회로도

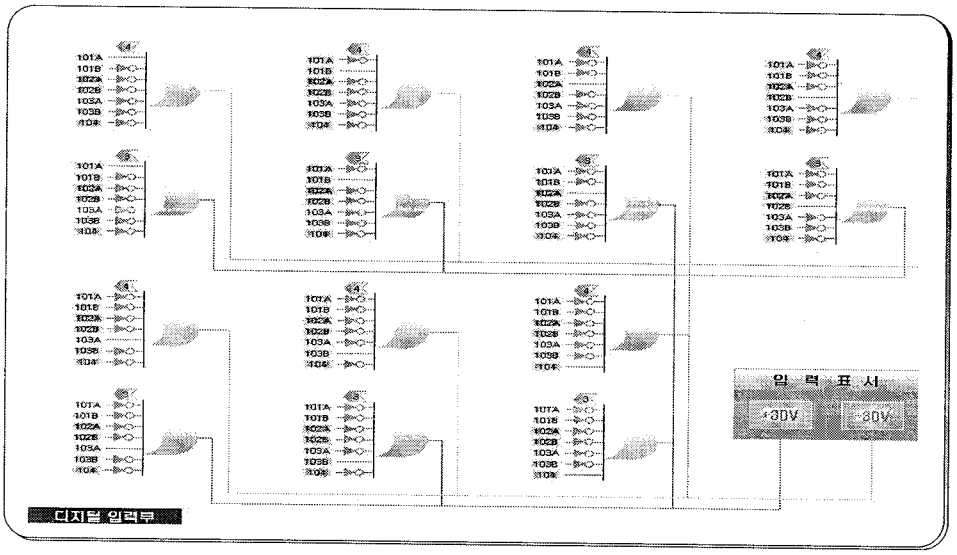
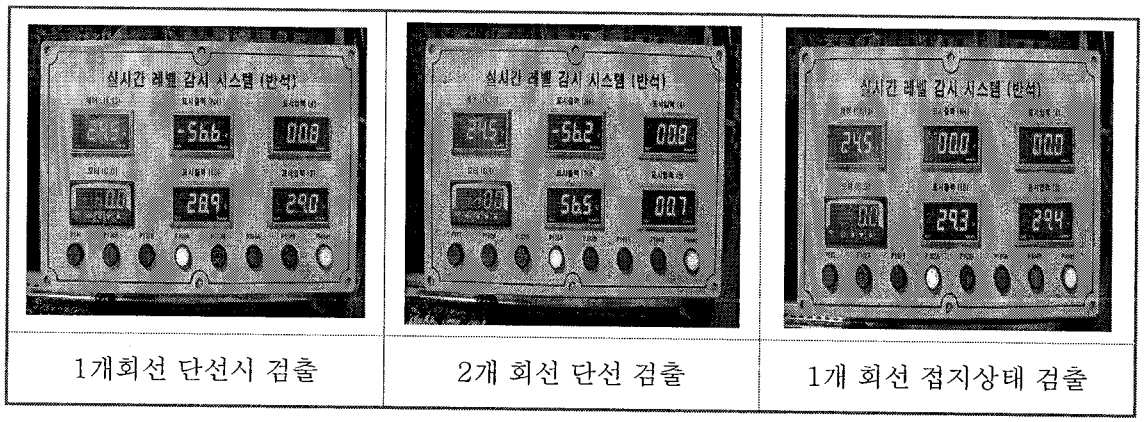


그림 3.9.15 표시부(입력)논리 회로도

그림 3.9.16은 현재 국내에서 운용 중인 감시설비의 전면 패널 사진으로 서, 자동회선 고장 검출 시 다음과 같이 표시되도록 되어 있어 선로전환기의 고장상태를 현장에 가지 않고도 바로 진단할 수 있도록 되어 있다.

- 표시전원 1선 단선 될 경우 60[V], 30[V]를 표출
- 표시전원 2선 단선 될 경우 60[V], 60[V]를 표출
- 표시전원이 접지될 경우 접지된 회선 0[V], 정상회선 30[V]를 표출



1개회선 단선시 검출	2개 회선 단선 검출	1개 회선 접지상태 검출

그림 3.9.16 감시설비 전면 판넬부의 고장상태 표충 현황

(나) 센서형 밀착검지기

열차 운행횟수의 증가에 따라 분기기 부분의 중요성이 강조되어야 하는 실정으로 텅레일과 기본레일간의 이격을 검지하여 열차운행의 안전을 도모하는데 목적을 두고 밀착검지기(근접센서형)가 일부의 분기부에 설치 및 운용되고 있다.

○ 밀착검지기의 구조

밀착 검지기는 마이크로 스위치를 이용한 방식과, 기계적인 접촉부를 없애고 무접촉으로 물체를 검지하는 센서방식 등이 있다. 현재 국철에서는 근접센서방식을 사용하고 있으며 밀착검지기의 구조는 그림 3.9.17과 같다.

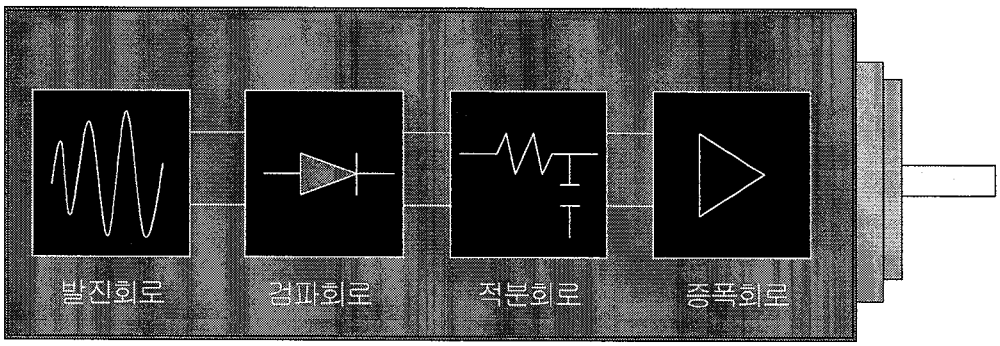


그림 3.9.17 밀착검지기 구조

○ 동작원리

LC로 조합된 고주파 자계 중심에 금속의 물체가 접근하면 전자유도 현상에 의하여 금속에 와전류가 흐르며 이 와전류 I와 고유저항 R에 의하여 I2R의 에너지 손실이 생긴다. 이에 따라 검출부 발진코일의 임피던스 변화로 발진상태를 유지할 수 없게 되어 발진정지 또는 발진폭의 감소가 발생된다. 이 발진부의 발진에너지 변화량을 검출하여 검출체의 유·무를 검출한다. 반복정밀도가 높으며 응답속도가 빠른 특징이 있다.

○ 근접센서 발진파형

근접 센서는 발진회로에서 정파의 고주파를 발진하다가 검출물체가 센서 검출면 근방에 접근을 하면 발진회로의 발진진폭이 서서히 감쇠하고 검출거리에 접근하면 정지한다. 이러한 변화를 전기적 신호로 전환하여 검출체의 유·무를 검출하게 된

다.

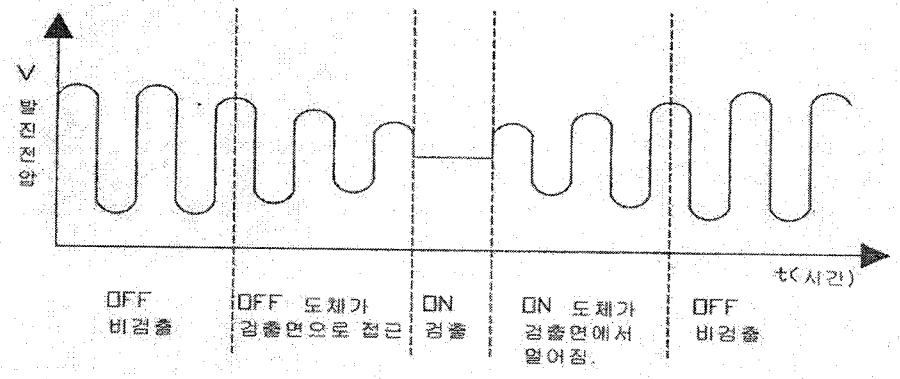


그림 3.9.18 근접센서 발진파형

○ 밀착검지기 특징

- 입력전원은 DC24V 또는 DC60V 공용
- 전철기의 AC모터 전원을 전환 후 차단(동작시간 8~14초)하여 도중전환을 방지하고 모터의 손상을 최소화한다.
- 고장이나 장애 발생시 보수가 용이하도록 밀착검지기 제어부 및 모터 전원 제어부에 직결스위치를 설치하여 신속하게 보수할 수 있다.
- 동작상태의 확인은 제어부에 발광다이오드를 설치하여 좌측 센서 및 검지 우측 센서의 검지상태와 모터전원 공급의 표시를 확인할 수 있다.
- 좌우측 센서에 연결된 전선관에 의하여 궤도회로가 단락되는 문제점이 보완되었다.

○ 설치방법

- 밀착검지기 센서를 텅레일 첨단 끝에서 히루 부분으로 350mm 내의 기본레일에 24mm드릴로 천공하여 좌우에 1조를 설치한다. (천공 후 홀 주위를 매끄럽게 갈아내어 놋치가 생기지 않도록 하여야 한다.) 센서 설치시 텅레일이 붙어있는 쪽을 먼저 배선하고 나머지를 배선한다.
- 근접센서의 간격조절 와샤를 이용하여 간격을 조절하여 센서 보호캡에 삽입한다.(밀착검지 센서는 첨단 텅레일과 기본레일이 5mm이상 불밀착시에 검지)

- 전선관을 침목 모서리 부위에 새들을 이용하여 고정한다.
- 전선관의 길이를 측정하여 자르고 끝부분 보호캡을 씌워 전기선로전환기 내부로 배선한다.

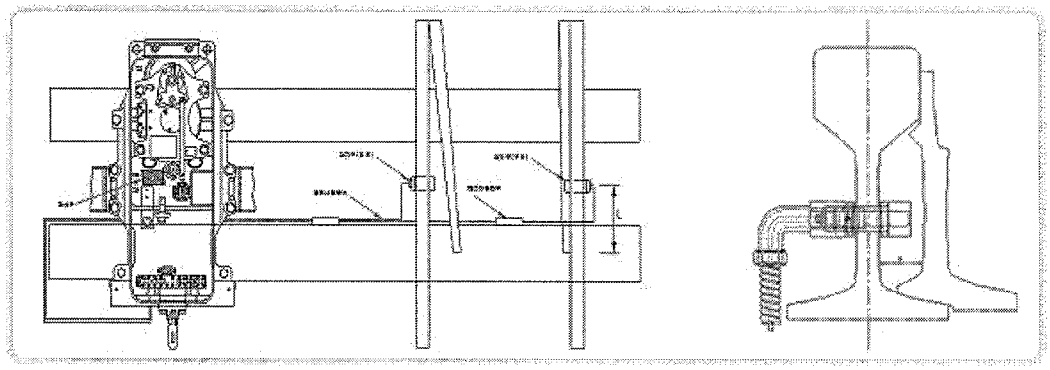


그림 3.9.19 설치도

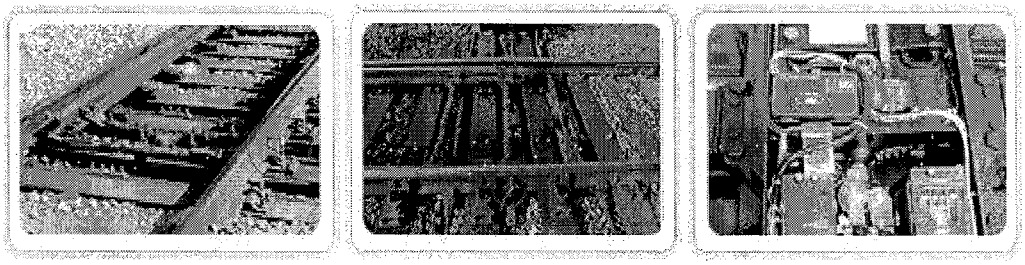


그림 3.9.20 현장 설치도

- 밀착검지 센서케이블 (※ 좌측, 우측의 확인 중요)
  · 갈색(B24), 청색(C24) : 동작전원 DC24V
  · 흑색(N24) : 검지시 제어전원
- 밀착검지부 또는 도중전환 방호부의 고장이나 장애시 카드부의 제어케이블(12C)의 직결 스위치와 모터전원 보조 스위치를 전환하여 직결위치로 한다. 이때 밀착검지 기능과 도중전환 방호기능은 작동하지 않으며 밀착검지기의 설치 이전의 상태로 동작한다.
- 입력전원은 DC24V 또는 DC60V이며, 구형인 경우에는 사용전압에 따라 현장

에서 제어부의 스위치를 전환하여야 하지만 신형인 경우에는 사용전압에 따라 자동으로 전환된다.

○ 결선도

- 정위(N방향)일 때는 표시전원 "+"는 밀착검지 제어부 콘넥터 3번에 연결되어 NS1여자접점, RS1낙하 접점을 거쳐 콘넥터 7번에서 선로전환기 단자 N4에 "+" 표시전원이 인가되고, 표시전원 "-"는 밀착검지 제어부 콘넥터 6번에 연결되어 RS1낙하 접점, NS1여자 접점을 거쳐 콘넥터 10번에서 선로전환기 단자 10에 표시전원이 인가된다.
- 반위(R방향)일 때는 표시전원 "+"는 밀착검지 제어부 콘넥터 4번에 연결되어 NS1낙하 접점, RS1여자 접점을 거쳐 콘넥터 8번에서 선로전환기 단자 R3에 "+" 표시전원이 인가되고, 표시전원 "-"는 밀착검지 제어부 콘넥터 5번에 연결되어 RS1여자 접점, NS1낙하 접점을 거쳐 콘넥터 9번에서 선로전환기 단자 8에 표시전원이 인가된다.

☞ SW1, 2는 밀착검지기 고장 발생시 스위치를 직결하여 밀착검지기를 무시하는 스위치이다.

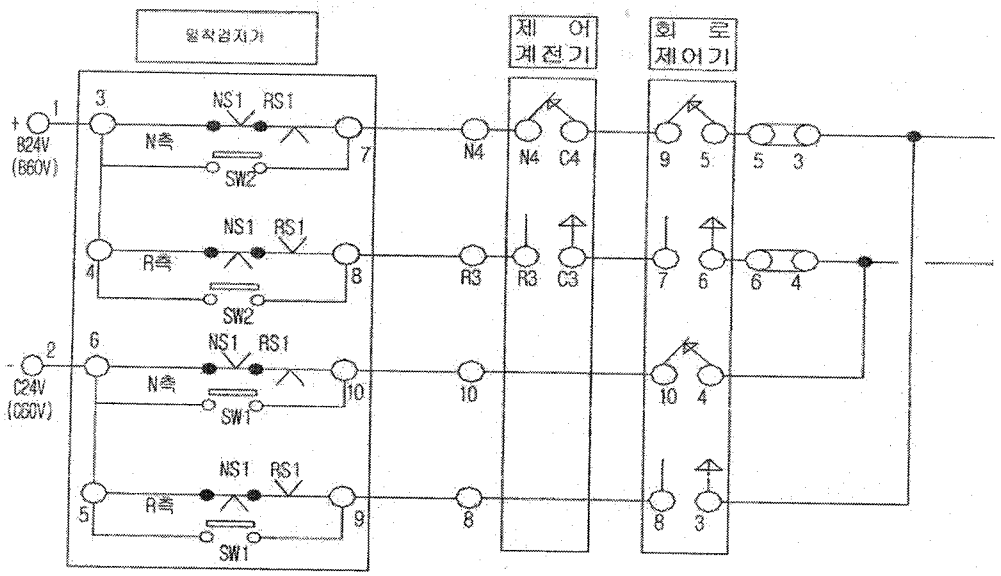


그림 3.9.21 단동기 밀착검지기 결선도

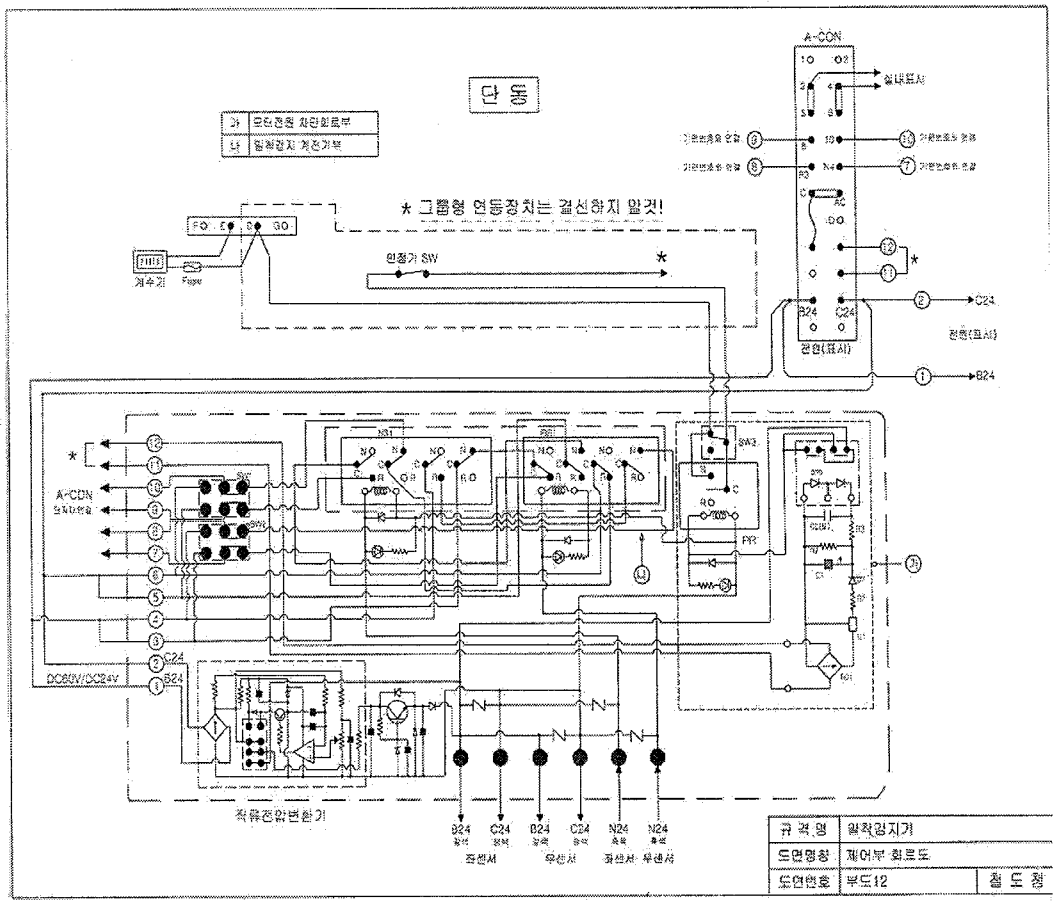
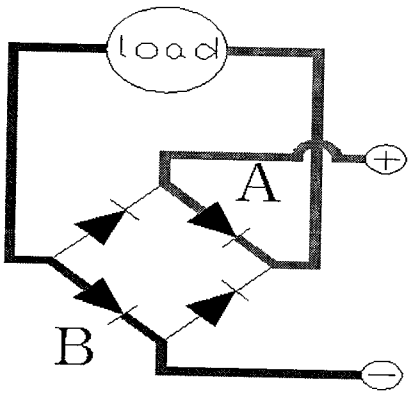


그림 3.9.22 단동 밀착검지기 제어부 회로도

○ 밀착검지기 PR realy전원 변환 원리

현장제어(AS)계전기의 전원 방향은 정, 반위에 따라서 + 와 -가 바뀐다. 그런데 밀착검지기의 모터 AC전원제어부의 PR realy는 전원방향이 바뀌어도 계속 같은 극으로 동작한다. 즉, 그 전원방향이 바뀌어도 BD1이 전원방향을 변환시켜준다.

그림 3.9.22와 같은 방향으로 (+)전원이 투입되면 다이오드(A)가 (+)전원을 부하측에 공급하게 되며, (-)전원이 투입되면 다이오드(B)가 (-)전원을 부하측에 공급하게 된다. 그림 3.9.23과 같은 방향으로 (+)전원이 투입되면 다이오드(C)가 (+)전원을 부하측에 공급하게 되며, (-)전원이 투입되면 다이오드(D)가 (-)전원을 부하측에 공급하게 된다.



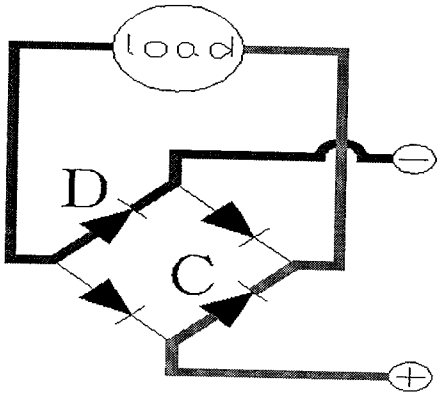


그림 3.9.23 PR realy전원 변환 경우1 그림 3.9.24 PR realy전원 변환 경우2

○ 밀착검지기 요구사항

계전기는 소형계전기를 사용하고 성능은 다음의 표와 같다.

표 3.9.2 제어부의 계전기 성능

항 목	접 점 수	코 일		접 점	
		정격전압	정격전류	정격부하	전압의최대치
표시회로용	4F4B	DC 24V	70mA 이하	AC 220V 3A DC 24V 3A	AC 250V DC 125V
전 동 기 전원차단용	1F	DC 24V	38mA 이하	AC 220V 20A	AC 250V
동작전압	정격의 80%이하				
낙하전압	정격전압의 10%이상				
내 전 압	AC 200V 60Hz 1분간(동극 접점간은 AC1000V)				
절연저항	DC 500V 절연저항계로 100MΩ 이상				

검지부의 검지센서의 성능은 다음의 표와 같다.

표 3.9.2 검지센서의 성능

구 분	성 능	비 고
정 격 전 압	DC 24V	입력전압 DC10~30V에서 검지거리를 일정하게 검지함
동작범위 전압	DC 10 ~ 30V	
검 지 거 리	8±0.5mm	
평 상 시 전류	15mA 이하	검지하지 않았을 때 소비전류
검 지 시 전류	200mA 이하	
온 도 범 위	-30 ~ +85℃	

○ 장애 시 점검사항

표 3.9.3 장애 시 점검 사항

장애현상	점 검 사 항		조 치 사 항
표시상태 불일치시	정,반위 센서LED 소등	밀착된 센서전압측정 (+:갈색,흑색 -:청색)	· SW1이나2 수동전환후 · 갈색,청색 전압측정되고 흑색과 청색 전압미측정시 : 센서 교체. · 갈색,청색 전압미측정시 : 카드교체나 표시전원 점검
	정,반위 센서LED 모두 점등	미밀착 센서전압측정 (+:갈색,흑색 -:청색)	· SW1이나2 수동전환후 · 갈색,청색 전압측정되고 흑색과 청색 전압측정시 : 미밀착된센서 교체
	정,반위 센서LED 정상 점등	카드출력의 7,8,9,10번 출력전압 측정	· 출력전압 미측정시 SW1이나2 수동전환 후 카드 교체
전환 불능시	모터전원 표시LED 소등		· SW3 수동전환후나 AC연결콘넥터 직결
	모터전원 표시LED	WR 전압 인가후 AC 연결콘넥터	· 미 LOOP시 SW3 수동전환후 · AC연결콘넥터 직결

	점등	LOOP 여부 점검	
열차 점유시 불일치시	정,반위 센서LED 점멸 여부 점검	밀착 강도나 센서간격 점검	· 밀착강도 조정 · 센서간격 조정

(다) 고속분기기용 밀착검지기 (센서형)

KTX(고속철도)의 개통으로 기존에 설치되었던 뽈베를 국산화한 제품으로 첨단부, 크로싱부의 밀착상태와 활출상태를 검지하고 궤도절연수지의 강화로 간격간, 첨단간 장애 예방 및 원가절감을 이룩한 장치이다.

○ 특징

- 정전압 회로 구성
- 전기적 절연수지
- 서어지 보호소자 부착
- One Chip Microprocessor 부착으로 고장검지 및 자동 복구 기능 내장
- 스큐류조로 간격간 거리조절

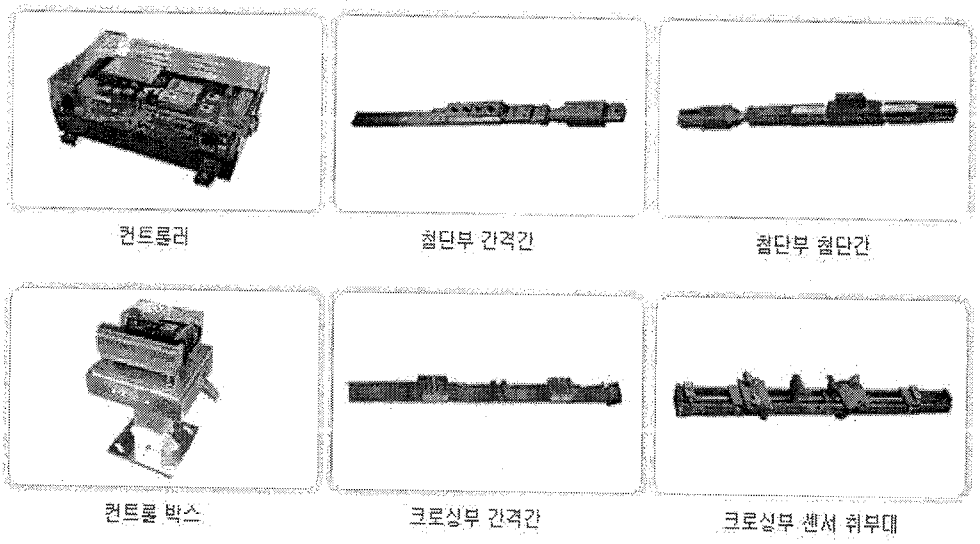


그림 3.9.25 고속분기기용 밀착검지기 구성품

○ 첨단부

- 첨단부 첨단간 : 각 쇄정간에 전달하기 위하여 기계적 쇄정을 위해 전단부에

설치

- 첨단부 간격간 : 각 쇄정간 레일의 유동을 도이하게 하기 위함

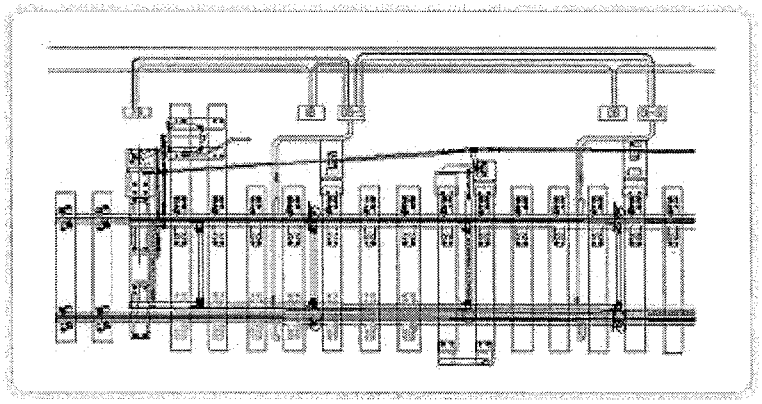


그림 3.9.26 첨단부 설치도

○ 크로싱부

- 크로싱부 센서 취부대 : 크로싱부 센서 고정시켜 레일의 미착 여부를 검지
- 크로싱부 간격간 : 분기기를 구성하는 궤간선에 교차하는 부분의 유동을 동일하게 하기 위함

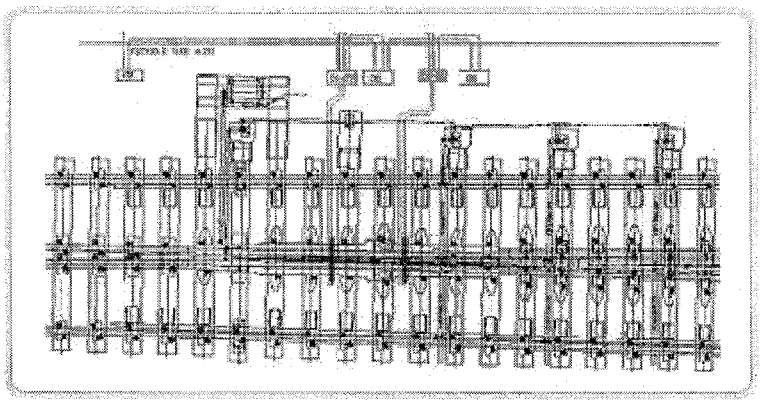


그림 3.9.27 크로싱부 설치도

(라) 밀봉형 클러치 (NS형 선로전환기용)

선로전환기는 모터에 의한 회전운동을 베벨기어와 전환기어에 의하여 직선 왕복운동으로 변환하여 이를 300Kg이상의 하중을 갖고 있는 분기부의 첨단 이동용으로 활용한 장치이다. 이 장치는 궤도변에 설치됨으로써 4계절 취약한 환경에 노출되어 있으며 동력전달체계가 기계적으로 구성됨으로써 정상적으로 첨단을 전환하는데 지장이 되는 장해물이 낄 경우 모터에 과부하가 되며, 이 경우 모터를 보호하기 위

하여 동력전달 중간위치에 클러치를 설치하여 설정된 전환력 이상의 과부하시 동력전달을 차단하고, 모터자체만 공회전(SLIP)하도록 하고 있다.

클러치는 금속의 고정판과 회전판 그리고 마찰판으로 구성되어 있으며 이들은 모터가 공회전하지 않고 300Kg이상의 전환력을 유지할 정도의 적당한 힘을 전달할 수 있는 강도로 스프링을 조정하는 구조로 되어있다. 철도 현장에서는 4계절 온도차에 의한 철의 수축현상을 물리적으로 보상할 수 있도록 클러치내부의 금속마찰판과 회전마찰판간의 밀착정도를 스프링을 조정하여 유지하고 있다.(일명 클러치조정). 클러치는 제작 후 통 안에 윤활유(일반 그리스)를 주입하여 마찰판과 회전판의 동작을 원활히 하고 있다.

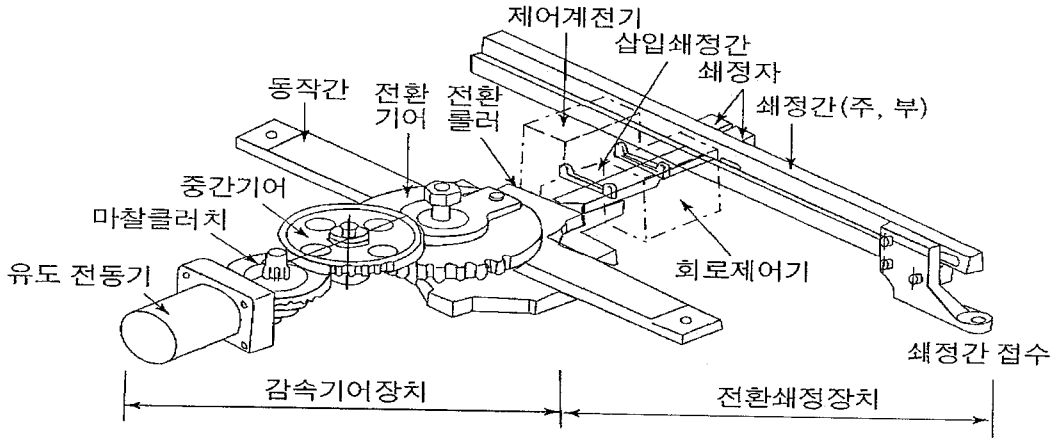


그림 3.9.28 NS형 선로전환기 구조

표 3.9.4 선로전환기 구성부품

부 품	내 용
제어계전기	삽입형으로 유극2위식 자기 유지 계전기이며 정격은 직류24(V), 120(mA)이고 코일저항은 200(Ω)
전동기	콘덴서 기동형 유도전동기로 단상4극이며 정격전압의 80%에서도 동작이 확실
마찰클러치	전동기의 회전력을 전달하고 회전 또는 정지할 때 기어에 충격을 주지 않도록 관성 흡수, 모터 보호
감속기어장치	3개의 기어를 사용하여 강한 회전력을 감속, 전달 1단 베벨, 2-3단 평기어

전환쇄정장치	선로전환기의 해정과 전환 및 쇄정의 세가지 작용을 하는 동작부
회로제어기	전환 쇄정장치의 동작완료 후 전동기 정지, 선로교환기가 위치로 확인하기 위한 제어기
표시회로	선로전환기가 동작 완료 후 계전기실의 표시계전기를 여자시켜 정위, 반위, 전환중 표시
밀착검지기	분기기에 기본레일과 텅레일의 밀착 상태를 검지(근접센서)

○ 밀봉형 클러치 특성

밀봉형 클러치는 통의 구조를 개량함으로써 클러치 통 안의 고품질 윤활유가 20년 이상 보존됨으로써 현장 설치시 1회의 클러치 조정으로 충격 등에 의한 외부의 특별한 변화가 없는 한 클러치를 조정할 필요가 없다. 그러나 기존제품은 적기에 클러치조정을 하지 않을 경우 전환력 부족으로 인한 장애가 유발되는가 하면 반면에 클러치를 과하게 조정할 경우에는 공회전 기능을 잃게 되는 등 문제점을 안고 있는 현실에서 폐사에서 개발한 일체형클러치는 이러한 문제점이 해소되어 보수자들에게 많은 노력을 경감시킬 수 있는 설비이다. 밀봉형 클러치는 기존의 NS형 전철기에서 클러치만을 간단하게 교환할 수 있는 구조로 개발하였으며, 해체공구를 사용 할 경우 40분 정도면 현장에서 간단하게 교환할 수 있다.

○ 기존제품의 문제점

현재 사용 중인 클러치는 통이 상부와 하부로 분리되어 있으며 하부의 중심부에는 회전축(軸)이 외부로 노출되어 있다. 이러한 구조로 인하여 축과 통간에 미세한 공간이 있어 공장에서 조립당시 클러치통에 주입한 윤활유(그리스)가 외부로 유출(流出)됨으로써 마찰에 의한 열로 윤활유의 점도가 낮아져 유출을 가속화 하고 있다. 이러한 문제점은 과부하시 초기에는 공회전을 하나 회전에 의한 마찰열로 인하여 클러치의 회전판과 마찰판이 고정판과 흡착됨으로써 고정판에 의하여 SLIP기능이 상실됨과 동시에 클러치 기능을 잃게 되어 잠시 후 모터는 소손(燒損)된다.

○ 개선 사항

- 클러치 구조개선

통의 상부와 하부를 분리하지 않고 일체형으로 개선하였으며 특히 통 하부에 외

부로 노출된 회전축은 통내부에서 기능을 발휘하도록 베어링을 사용 개량함으로써 회전축 고유의 기능에는 아무런 문제가 없으며 이러한 구조로 인하여 통 안에 주유한 윤활유는 외부로 유출되지 않으며, 또한 통 안에 윤활유 량을 증대하기 위하여 내부공간을 10% 확대하였다.

- 마찰판 구조개선

클러치의 회전판과 마찰판 고정판간에 SLIP현상을 원활히 하기 위하여 별첨 약도와 같이 각 원판에 4개의 홀(Ø:9)과 윤활유 흐름통로(홈)를 만듦으로써 평상시에도 이 공간에 윤활유가 보존되어 SLIP기능을 향상시켰다.

- 윤활유 개선

기존의 윤활유(일반용 그리스)는 열을 받으면 점도가 낮아질 뿐만 아니라 인화성이 있어 윤활유로써의 기능을 잃고 있으나 채택한 고품질의 윤활유는 저온(-30℃) 고온에서 윤활유 본래의 기능을 보존함으로써 오랜 시간 공회전시에도 기능상 문제점이 없다.

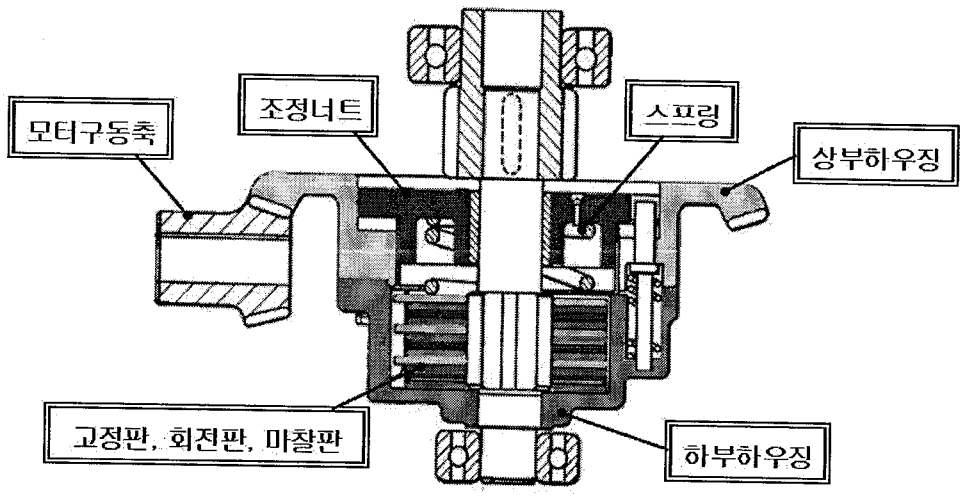


그림 3.9.29 밀봉형 클러치 구조

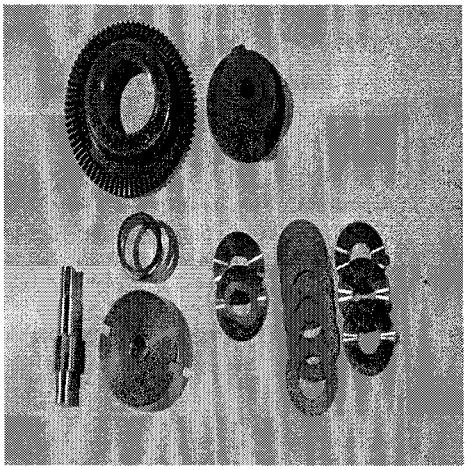


그림 3.9.30 기존 클러치 구성품

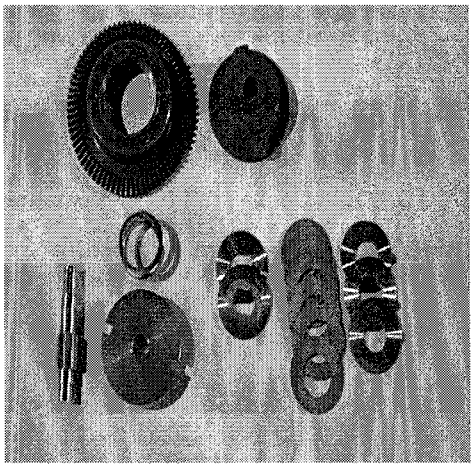


그림 3.9.31 밀봉형 클러치 구성품

(3) 선로전환기 요구사항

선로전환 결함방지를 위해서는 가장 중요한 부분이 선로전환기이다. 국내에서 몇 가지 종류의 선로전환기들이 운용되고 있지만 본 연구에서는 기존선 및 도시철도 구간 대부분에 적용되고 있는 NS형 선로전환기와 고속철도 및 고속선 연결에 적용되고 있는 MJ-81 선로전환기가 만족하여야 할 요구사항들을 국내의 관련 규격들의 조사를 통해 분석하였다.

(가) NS형 선로전환기 요구사항

차량기지용 선로전환기(NS형), 본선용 선로전환기(NS-AM형) 및 간류의 규격은 다음의 표와 같다.

표 3.9.5 NS형 선로전환기

종 류	동 정(MM)		정 격		용 도
	동작간	쇄정간	전 환	제 어	포인트동정 (MM)
교류 NS형(일체형) 및 부속장치	185	130-185	AC105V/220V 단상 60Hz	DC 24V	130-185

표 3.9.6 NS-AM형 선로전환기

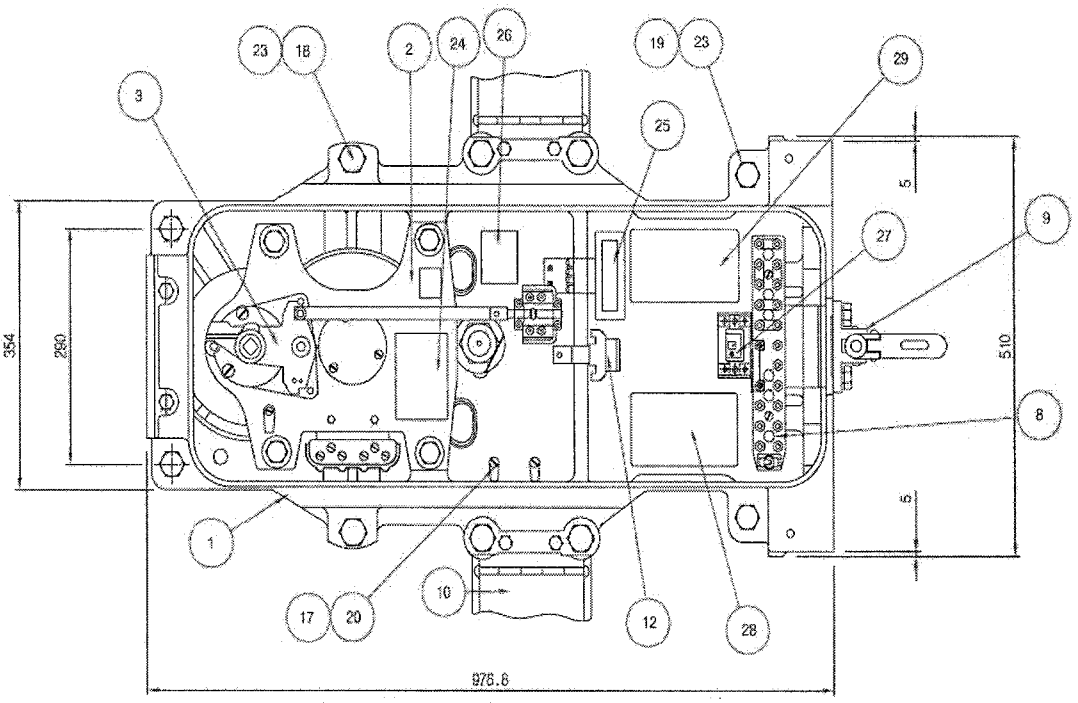
종 류	동 정(MM)		정 격(V)		용 도
	동작간	쇄정간	전 환	제 어	선로전환기 동정(MM)
전자클러치형 및 부속장치	220	185~230	AC 105V/220V 60Hz	DC 24V	185~230

표 3.9.7 NS형 선로전환기 간류

종 별	용 도	비 고
첨단간	텅레일 앞부분 연결	절연체 및 기억쇠 포함 (단조품)
밀착조절간	전기선로전환기 동작간과 연결관 연결	너트풀림방지장치 포함 (단조품)
접속간	첨단간과 선로전환기 쇄정간 연결	절연체 포함 (단조품)
깔판	전기선로전환기를 침목에 고정	
유동방지간	깔판과 기본레일간 연결	깔판(취부판)포함 (단조품)
기억쇠	첨단간과 텅레일간 연결	(단조품)
너트풀림장치	밀착조절간의 너트풀림을 방지	
연결간절연	연결간의 레일 단락을 방지	

o 일반구조

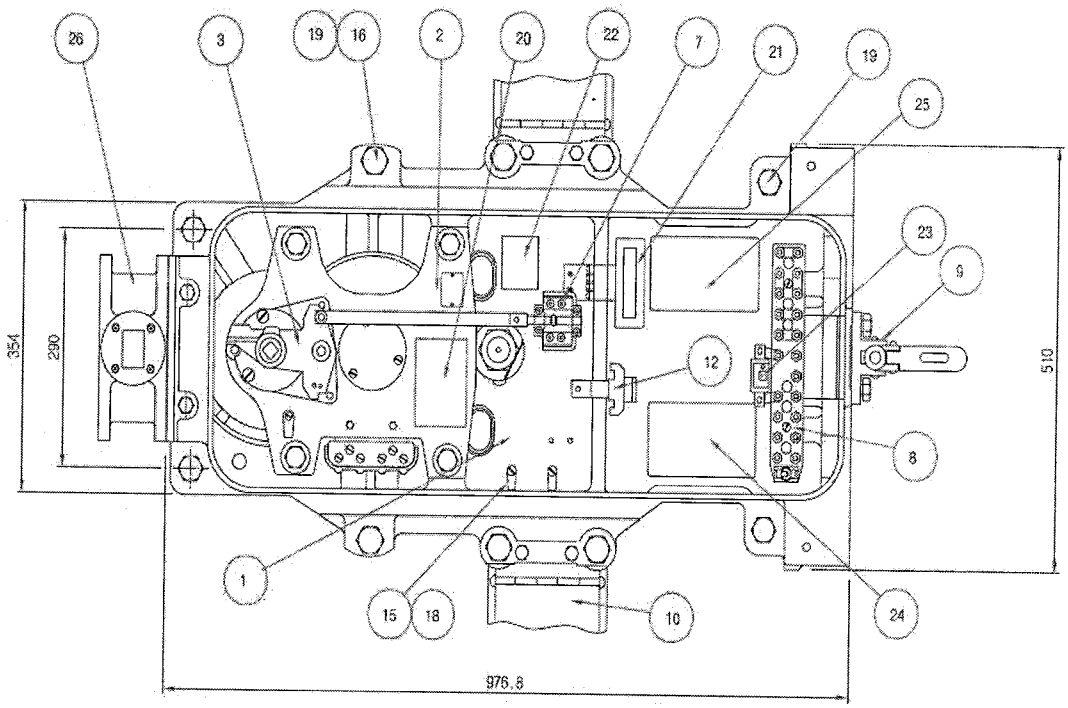
- 전동기, 외함, 전환부, 쇄정부 및 제어장치 등으로 구성한다.
- 단자 등 도체의 노출부분과 다른 금속 부분과의 간격은 5mm 이상이어야 한다.
- 접점 부분에는 기름이 튀어 묻어서는 안된다.



29	제어계전기			1	440-025 참조
28	회로제어기			1	440-059 참조
27	배선용차단기	10A		1	440-118 참조
26	동작 계수기			1	6자리수
25	전열기 앗셈			1	
24	기내배선도			1	
23	스프링 와샤	M20용	SPS3	10	
20	스크류	HB20 X 80	MS/R10	2	
19	상체조임볼트		SS41	4	
18	상체조임볼트		SS41	6	
17	선 신 걸 이		PP유백색	2	
기 호	품 명	품질.형상.치수	재 질	수 량	기 사

12	소 켓 트			1	
10	동작간 덮개			2	
9	걸 이 쇠			1	
8	단자판 앗셈			1	
7	접점대 앗셈			1	
3	안전기후레임앗셈			1	
2	차차지지물 앗셈			1	
1	상 체			1	
기 호	품 명	품질.형상.치수	재 질	수 량	기 사

그림 3.9.32 NS형 선로전환기 구조



26	전자클러치			1	
25	제어계전기			1	
24	회로제어기			1	
23	MCCB	10A		1	
22	등작 계수기			1	6자리수
21	진열기			1	
20	기내배선도			1	
19	스프링 와사	M20용	SPS3	10	
18	스크류	HB20 X 80	MSMR10	2	
17	상체조임볼트		SS41	4	
16	상체조임볼트		SS41	6	
기 호	품 명	품질.형상.치수	재 질	수 량	기 사

15	전 선 걸 이		PP유백색	2	
12	소 켓 트			1	
10	등작간 덮개			2	
9	걸 이 쇠			1	
8	단자판 앗셈			1	
7	집전대 앗셈			1	
3	안전기후레임앗셈			1	
2	차차지지틀 앗셈			1	
1	상 체			1	
기 호	품 명	품질.형상.치수	재 질	수 량	기 사

그림 3.9.33 NS-AM형 선로전환기 구조

○ B. 전환부 및 쇄정부

- 동작간은 전환 종료후에 쇄정간에 의해 쇄정되는 것으로 한다.
- 삽입 쇄정간은 정위 및 반위가 각각 있어야 한다.
- 쇄정자와 쇄정자간의 홈은 직각으로 삽입되게 한다.

○ 급유장치

- 주요한 회전부분 및 습동부분은 용이하게 급유할 수 있는 구조이어야 한다. 다만, 후락숀 클러치 및 볼베아링 부분은 제외한다.
- 급유장치는 전환 회수 2,000회 (매분 5~6회 매일 280회의 어느쪽의 경우라도) 이상의 연속동작에 대하여도 충분히 급유할 수 있으며, 외부에 나타나는 주유구 및 중요한 부분의 주유구는 방진 방수를 할 수 있는 구조라야 한다.

○ 전동기

- 콘덴서 기동형 유도전동기(대칭형 2상 4극)로서 단상전원으로 정·역 양 운전이 될 수 있는 방수 밀폐형으로 한다.
- 전환력, 전환시간 및 동작 전류 (NS형 선로전환기)
  · 전동기의 슬립(Slip) 전류는 AC 8.5A 이하로 되게 한 후 동작간에 100Kg 부하를 가하여 전환하고 전환 종료 전 20mm의 위치로부터 점차 부하를 증가하여 전환종료 시 500kg으로 하였을 때의 전환 시간 및 동작전류는 다음 표와 같아야 한다.

표 3.9.8 전환시간 및 동작전류

전환시간(sec)		운전 전류(A)
정격전압	정격전압×0.8	
6이하	6 이하	7.7 이하

(주) ① 전환시간이란 표시계전기의 접점이 개방되면서부터 선로전환기가 전환하고 표시계전기의 접점이 구성되기까지의 시간을 말한다.

② 운전전류란 전환 중 기동전류를 제외한 최대전류로서 측정은 교류 전류계(가동철편형) 1.0급 20A 및 직류 전류계(가동 코일형) 1.0급

30A로서 시행하여야 한다.

③ 슬립(Slip) 전류의 측정은 전류가 안정된 후에 측정하고, 후락숀 클러치가 동작하기 시작하여 1분 이상 경과한 후에 측정하는 것을 표준으로 한다.

- 정격전압에서 전동기의 슬립(Slip) 전류를 9A 이하로 되게 한 후 동작간에 210Kg의 부하를 가하여 전환하였을 때 전환 시간은 6초 이하라야 한다.
  - 최대 전환력은 정격전압에서 후락숀 클러치를 조였을 때 동작간에 하중 300Kg이상의 부하를 가하여도 전환될 수 있는 것이라야 한다.
- 전환력, 전환시간 및 동작 전류 (NS-AM형 선로전환기)
  - 전동기의 슬립프 전류는 8.5A 이하로 되게 한 후 동작간에 100Kg 부하를 증가하여 전환종료 시 500Kg으로 했을 때의 전환시간 및 운전 전류는 다음 표와 같다.
  - 운전전류의 측정은 교류전류계(가동철편형) 1.0급,20A 및 직류전류계 (가동코일형) 1.0급 30A로서 시행하여야 한다.
  - 슬립 전류의 측정은 전류가 안정된 후에 측정하고, 마그네트클러치가 슬립하기 시작하여 1분이상 경과한후에 측정하는 것을 표준으로 한다.
  - 정격에 있어서 전동기의 슬립프 전류를 교류 NS-AM에서는 9A 이하로 되게 한 후 동작 간에 210Kg의 부하를 가하여 전환하였을 때 전환 시간은 7초 이하라야 한다.
  - 최대전환력은 정격에 있어서 전자클러치를 최대로 조였을 때 동작간에400Kg의 부하를 가하여도 전환될 수 있는 것이라야 한다.

표 3.9.9 전환시간 및 운전전류

종 류	전환시간(S)		운전 전류(A)	슬립전류(A)
	정 격	정격× 0.8		
전자 클러치형	7 이하	8 이하	8.5 이하	15이하

(주) 전환시간 : 표시계전기의 접점이 개방되면서부터 선로전환기가 전환하고 표시계전기의 접점이 구성되기까지의 시간을 말한다.

o 일체형 후락숀 클러치 (NS형 선로전환기)

- 일반구조

  · 동작 종료시 각부에 큰 충격을 주지 않고 또 동작이 방해되었을 때 전동기에 과대한 부하가 걸리지 않도록 하여야 한다.

  · 전마찰판 3매, 고정마찰판 3매, 아스베스트 라이닝(ASPASTE LAINNIG) 6매를 스프링으로 조여 마찰력으로 회전력을 전달할 수 있는 구조로 마찰판 사이에 윤활유(구리스)가 주입되어 제작되어야 한다.

- 외함

  · 클러치 상부와 하부가 일체형인 형태로 각 부품을 수용할 수 있는 구조이여야 한다.

  · 외함 외부로 노출된 회전축을 내부에서 기능을 발휘할 수 있도록 하여 내부에 주유한 윤활유가 하부로의 유출이 없도록 제작 되어야 한다.

- 조정너트

  · 클러치의 회전마찰력(Torque)증감을 위하여 록크플란자를 조정할 수 있는 구멍이 있어야 하며 마찰력 조정시 용이하게 조정할 수 있는 구조이여야 한다.

- 마찰판

  · 회전판과, 마찰판, 고정판간에 Slip을 원활히 하기 위하여 각 원판에 4개의 공간(Φ8mm)을 만들어 윤활유를 보존할 수 있는 구조이여야 한다.

o 전자클러치 (NS-AM형 선로전환기)

- 동작 종료 시 각부에 큰 충격을 주지 않고 또 동작이 방해되었을 때 전동기에 과다한 부하가 걸리지 않도록 하여야 한다.
- 온도에 관계없이 전달 토오크가 일정하여야 한다.
- 전환 종료 시 역회전이 생기지 않아야 한다.
- 공회전시에 전동기를 보호할 수 있도록 비 접촉 형으로 하여야 한다.
- 전자클러치의 토오크 및 공극은 다음 표와 같아야 한다.
- 전자클러치는 차량기지에 납품되는 NS형 선로전환기와 호환되도록 제작하여야 한다.

표 3.9.10 전자클러치 토크 및 공극

항 목	최저슬립토오크 (kg-cm)	정격슬립토크 (kg-cm)	마찰토크 (kg-cm)	공 극 (mm)
기 준 치	21이상	43이상	3이하	0.6~1.2

○ 표시장치

- 표시회로는 부도와 같은 결선이라야 한다.
- 전환도중 단동, 쌍동 또는 3동의 선로전환기 등이 부정한 전환상태일 때는 표시회로 전원을 차단하고 또 표시계전기를 단락하는 것이라야 한다.

○ 접선자

- 접선자 상호간의 간격은 20mm 이상으로 하여야 한다.
- 단자반 및 짹판에 취부하는 접선자는 이완되지 않아야 한다.

○ 수동장치

- 선로전환기는 핸들에 의해 일체형 후락숀 클러치를 거치지 않고 용이 하게 동작하는 것이라야 한다.
- 핸들 삽입에 앞서 전동기회로를 차단하고 또 핸들을 뽑아도 계속하여 회로가 차단되어 있는 것이라야 한다.
- 핸들을 꽂는 구멍에는 뚜껑이 있어야 하며, 전동기 회로를 구성하지 않을 때에는 뚜껑이 완전히 덮이지 않는 구조로 하여야 한다.

○ 제어계전기, 회로제어기

- 형식, 정격 및 접점수는 다음 표와 같아야 한다.
- 제어계전기 및 회로제어기는 용이하게 삽입할 수 있고 또 삽입 후에는 고정을 시켜서 진동, 기타에 의하여 조정된 것이 변화되면 안 된다.

표 3.9.11 제어계전기, 회로제어기 형식

명 칭	형 식	정 격 (20℃ 에서)		비 고 (접점수)
		전압 DC	전류 mA	
제어계전기	자기 유지형	24	120 이하	정반위 4조(NR4)
회로 제어기	삽 입 형	-	-	정위4, 반위 4(N4R4)

- 내부에는 먼지가 들어갈 염려가 없고 또 내부점검이 용이할 것이며, 계전기의 외함에는 통풍 구멍을 뚫어놓아야 한다.
- 제어계전기와 회로제어기의 윗부분에는 정위(N) 및 반위(R) 동작위치를 표시할 수 있는 명판을 부착하여야 한다.
- 정격으로 확실하고 신속하게 동작하는 것으로써 정방향으로 여자되었을 때 정위접점은 접촉, 반위접점은 개방되고 또 역방향으로 여자되었을 때는 정위접점은 개방, 반위접점은 접촉하는 것으로써 전환방향으로 순간 여자되었을 때 정.반위의 중앙점에서 정지하지 않는 것이라야 한다.
- 전류를 통하여 어느 한쪽으로 동작시킨 후 무 여자 되었을 때 그 위치에서 각각 전동기회로는 70g, 표시회로는 50g 이상을 접점 접촉력을 유지하고, 100g (20Hz~40Hz) 이상의 가속도를 어떠한 방향에서 가하여도 접극자는 전환되지 않아야 한다.
- 전환전류의 나눈 값은 정격전류의 0.6 이상, 0.8 이하로 한다. (단, 전환전류란 정격의 2.5배의 전류로 정 또는 역방향으로 여자된 후, 점차 감소하여 전류가 0이 되었을 때 극성을 전극하여 역방향 또는 정방향으로 점차 전류를 증가하여 접극자의 전극이 반위 또는 정위의 접점에 완전히 접촉할 때의 전류를 말한다.)

o 선로전환기 체결장치

- 표준 궤간을 정확히 확보할 수 있어야 한다.
- 60Kg Rail에 적합하며 취부가 용이하여야 한다.
- 선로전환기 전환 시 동력전달이 확실하고, 쇄정이 틀리지 않도록 견고히 체결

할 수 있는 구조라야 한다.

- 보판 취부볼트 부분의 전식방지대책이 있어야 한다.
- 부속장치의 구성은 다음 표에 의한다.

표 3.9.12 체결장치

품 명	재질 명칭	적용 규격
깔 상	GCD450	KSD 4302
프레이트 (와샤, 볼트포함)	GCD450	KSD 4302
롯 트(조인트 포함)	SS41	KSD 3503
하드로크너트	SPS4	KSD 3701
조임쇠 A	아스페스트	
조임쇠 C	SS41	KSD 3503
로드 A, 로드 B	SM45C	KSD 3752

○ 전열기

- 온도 스위치는 바이메탈을 사용하여야 하며 리드선은 KSC 3101 (전기용연동선) ∅0.8mm 상당이상을 사용하여야 한다.
- 발열봉의 열선은 니크롬선을 사용하고 발열봉의 재질은 스테인레스 파이프를 사용하여야 하며, 인출선은 석면피복 절연전선 20/0.18mm 상당이상을 사용하여야 한다.
- 온도스위치는 방수, 방습 되도록 몰딩하여 주위 도체와 절연될 수 있는 구조로 미려하게 제조하여야 한다.
- 발열봉은 열의 분포가 균일하도록 제작하여야 하고 열선과 인출선의 접속부는 단자를 사용 견고하게 제작하여야 한다.
- 발열봉을 취부하는 부라켓트는 두께1.6mm 상당의 철판을 이용 견고 하게 지지할 수 있는 구조로 하여야 한다.
- 전열기는 주위온도 -40℃ ~ +80℃에서도 성능상 변화가 없어야 한다.

- 전열기는 전철제어 계전기 옆의 공간에 설치하여야 한다.

○ 동작계수기

- 동작계수기는 6자리 숫자를 사용하며 표시숫자는 흑색바탕 백색문자로 하며, 40만회 이상이 되면 선로전환기를 교체한다.
- 계수방식은 전자식으로 1펄스 1카운트 {통전(ON)시 1/2, 차단(OFF)시 1/2}로 한다.

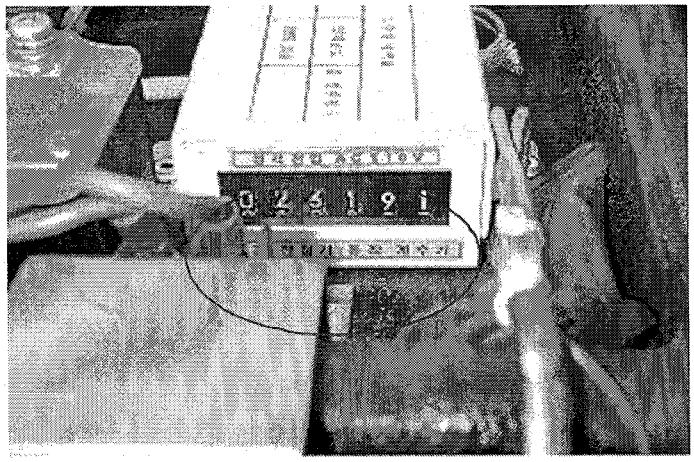


그림 3.9.34 동작계수기

○ 간류

- 간류의 롯드 및 기억쇠는 KSD 3503(일반구조용 압연강재) SS400 또는 동등 이상의 재질로 단조품으로 제작하여야 한다.
- 표준궤간 간격을 정확히 확보할 수 있어야 하며 조정 가능한 구조이어야 한다.
- 50kgN 및 60kg 레일에 적합하고 취부가 용이하여야 한다.
- 전기선로전환기 전환시 동력전달이 확실하고 쇄정이 틀리지 않도록 견고히 체결할 수 있는 구조이어야 한다.
  - 첨단간 : 첨단간은 왼기억쇠와 오른기억쇠로 텅레일의 앞부분에 연결하고 접속간 연결로 전기선로전환기의 전환에 의해 쇄정간을 전환하여야 한다.
  - 밀착조절간 : 밀착조절간은 전기선로전환기의 동작간과 연결간을 연결하여

선로전환기 전화시 텅레일을 전환하고 밀착하여야 한다.

· 접속간 : 접속간은 첨간간과 선로전환기의 쇄정간을 연결하여 주며, 절연형 접속간은 전기선로전환기와 첨단간이 절연되도록 하여야 한다.

· 깔판 : 깔판은 전기선로전환기를 분기기의 침목에 고정시켜야 한다.

· 유동방지간 : 유동방지간은 유동방지용 깔판과 좌,우 기본레일간을 연결하여 기본레일에 유동이 있더라도 쇄정간 걸림 장애 등을 방지할 수 있어야 한다.

· 기억쇠 : 기억쇠는 첨단간과 텅레일의 앞부분을 연결하여야 한다.

· 연결간 절연 및 기타 절연체 : 연결간, 첨단간 및 좌,우 레일간의 단락을 방지하기 위하여 설치한다.

- 각종 간류의 기계적 성질은 KSD 3503 (일반구조용 압연강재)에 적합하여야 하며 연결간 및 첨단간의 절연체 성능은 표 3.9.13과 같고, 접속간 및 유동방지간 절연체의 성능은 다음 표 3.9.14와 같다.

표 3.9.13 연결간 및 첨단간의 절연체 성능

체적저항률 (MΩ.cm)	인장강도 (kg.㎟)	굴곡강도 (kg.㎟)	압축강도 (kg.㎟)	바아콜경도
30이상	70이상	80이상	46이상	70이상

표 3.9.14 접속간 및 유동방지간 절연체의 성능

시험항목	조건 및 처리	단위	성 능		
			절연판	절연원통	유동방지간절연편
흡수율	24시간 침수	%	3이하	1이하	3이하
체적저항율	흡수율시험 후	MΩ.cm	15이상	15이상	15이상
인장강도	상온상습	kg/㎟	5이상	6이상	3이상
	24시간침수 후				
	60℃가열 후				
	-30℃냉각 후				
신장율	상온상습	%	220이상	40이상	220이상

	24시간침수 후		240이상	40이상	240이상
	60℃가열 후		210이상	60이상	210이상
	-30℃냉각 후		150이상	20이상	150이상
압축강도	상온상습	kg/㎟	35이상	35이상	35이상
	24시간침수 후				
	60℃가열 후				
	-30℃냉각 후				
압축율	60℃가열 후	%	50~60	40~60	50~65
	-30℃냉각 후				
경 도	HR M			70~90	
	HR R		60~90		60~90

(나) MJ81 전기선로전환기 요구사항

경부 고속선과 기존선/고속선 연결 구간에 사용되는 분기기는 고속도 및 고밀도 운전에 적합한 노스가동형 분기기가 사용된다. 일반적인 분기기는 첨단부에만 전기선로전환기가 사용되지만 노스가동형은 첨단부와 크로싱부 각각에 전기선로전환기가 사용된다. 노스가동형은 간류의 수가 적어 기계작업 및 유지보수가 용이한 반면 NS형은 년2회 이상 클러치 조정을 해야 하고 간류가 많기 때문에 유지보수와 보선기계작업이 곤란한 단점이 있다. 특히 제어 및 표시회로에서 NS형은 기존연동장치의 변경 없이 사용이 가능하지만 MJ81형은 연동장치의 제어회로를 보완하여야 한다.

표 3.9.15 MJ81 선로전환기 성능

주위온도	사 용 전 원	동 정
-30℃ ~ 70℃	3상 60Hz 220/380V±10%	110-260㎜(조절가능)
	단상 60Hz 220V±10%	

표 3.9.16 MJ81 선로전환기 제원

치 수	하 중 (리버포함)	부 하 (최대동정260㎜)			정격전류 (부하 200kgf시)	내전압
		구 분	정 격	최 대		
길이 : 700㎜ 폭 : 476㎜ 높이 : 215㎜	91kgf ±5%	3상용	200kgf 이상	400kgf 이상	220V시 3.0A이하	2000V 60Hz 1분간
					380V시 2.0A이하	
		단상용	200kgf 이상	360kgf 이상	220V시 7.0A이하	

표 3.9.17 MJ81 선로전환기 최장 전환시간

구 분	시 험 조 건	전환시간
3상용	공급전원 200V, 회선저항 3Ω, 부하 200kgf, 동정 260㎜일 때,	3.8초 이내
	공급전원 200V, 회선저항 3Ω, 부하 400kgf, 동정 260㎜일 때	4.3초 이내
단상용	공급전원 207V, 회선저항 4Ω, 부하 200kgf, 동정 260㎜일 때	3.8초 이내
	공급전원 207V, 회선저항 4Ω, 부하 360kgf, 동정 260㎜일 때	4.3초 이내

표 3.9.18 MJ81 선로전환기 최단 전환시간

구 분	시 험 조 건	전환시간
3 상 용	공급전원 240V, 회선저항 0Ω, 부하 0kgf, 동정 260㎜일 때	3초 이내
단 상 용	공급전원 253V, 회선저항 0Ω, 부하 0kgf, 동정 260㎜일 때	3초 이내

표 3.9.19 MJ81 선로전환기 최대 소비전류

구 분	시 험 조 건	소비전류
3상용	공급전원 240V, 회선저항 0Ω, 400kgf, 동정 260㎜일때	4.8A이하
	공급전원 420V, 회선저항 0Ω, 400kgf, 동정 260㎜일때	2.4A이하
단상용	공급전원 207V, 회선저항 4Ω, 200kgf, 동정 260㎜일때	7.0A이하
	공급전원 207V, 회선저항 4Ω, 360kgf, 동정 260㎜일때	8.0A이하

○ 일반구조

- 전기선로전환기는 철도2250-1061(분기기, 노스가동UIC 60kg레일) 및 철도5620-1062(콘크리트침목, 분기기용)에 적합하게 설치되는 구조로 전기선로전환기는 비상시 수동조작에 의해 전환 가능하다.

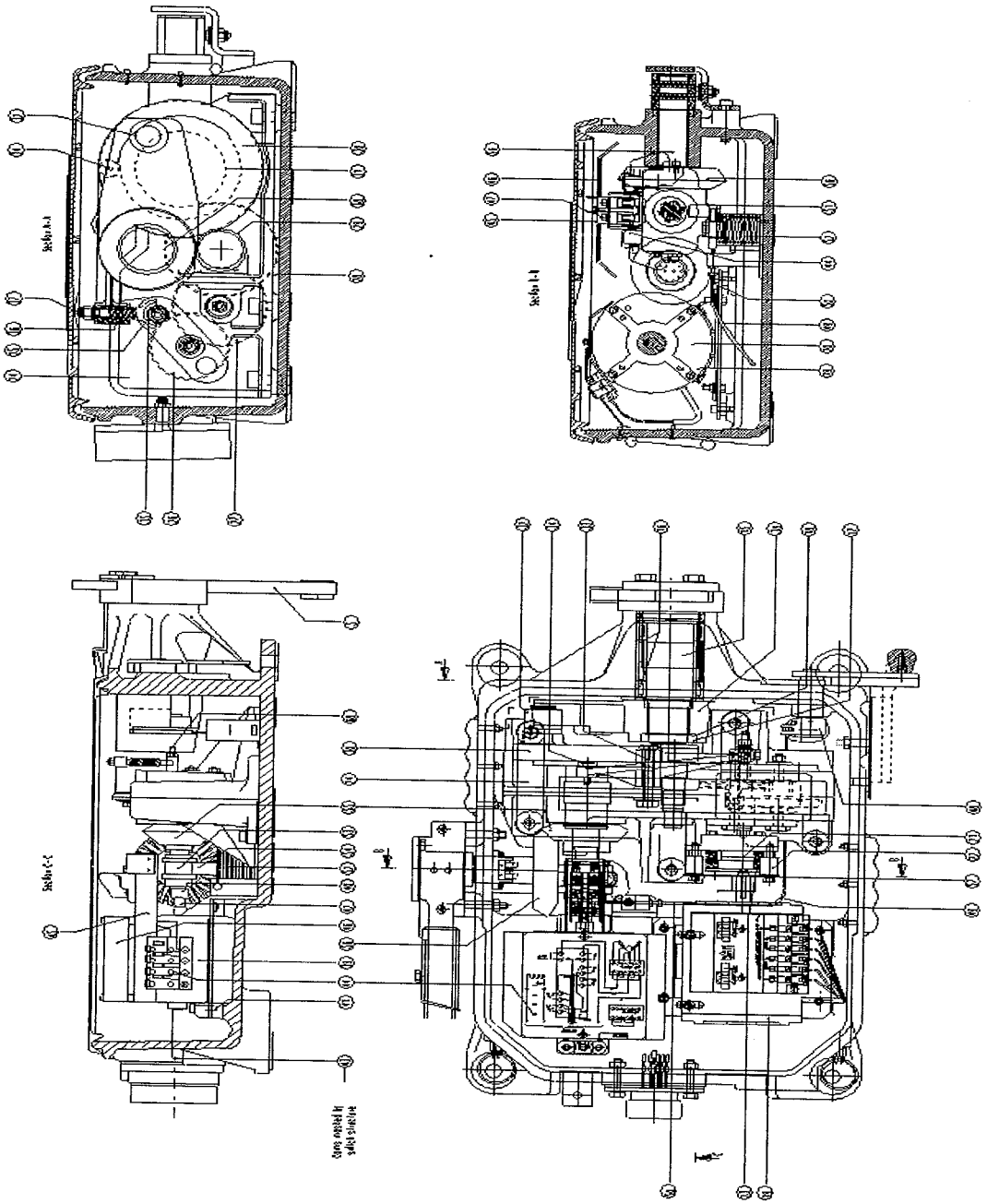


그림 3.9.35 MJ81형 전기선로전환기 내부 상세도

○ 외함

- 전기선로전환기 구성품들은 비, 눈, 먼지로부터 보호될 수 있도록 경합금 주물 덮개와 주철외함 내부에 장착되는 구조이다. 덮개에는 스프링식 잠금장치가 부착되어 쉽게 여닫을 수 있으며, 본체의 외함에는 손잡이가 부착되어 쉽게 들 수 있는 구조로 전기선로전환기 본체 외함은 직경 18㎜의 4개 볼트로 설

치위치에 고정되는 구조이다.

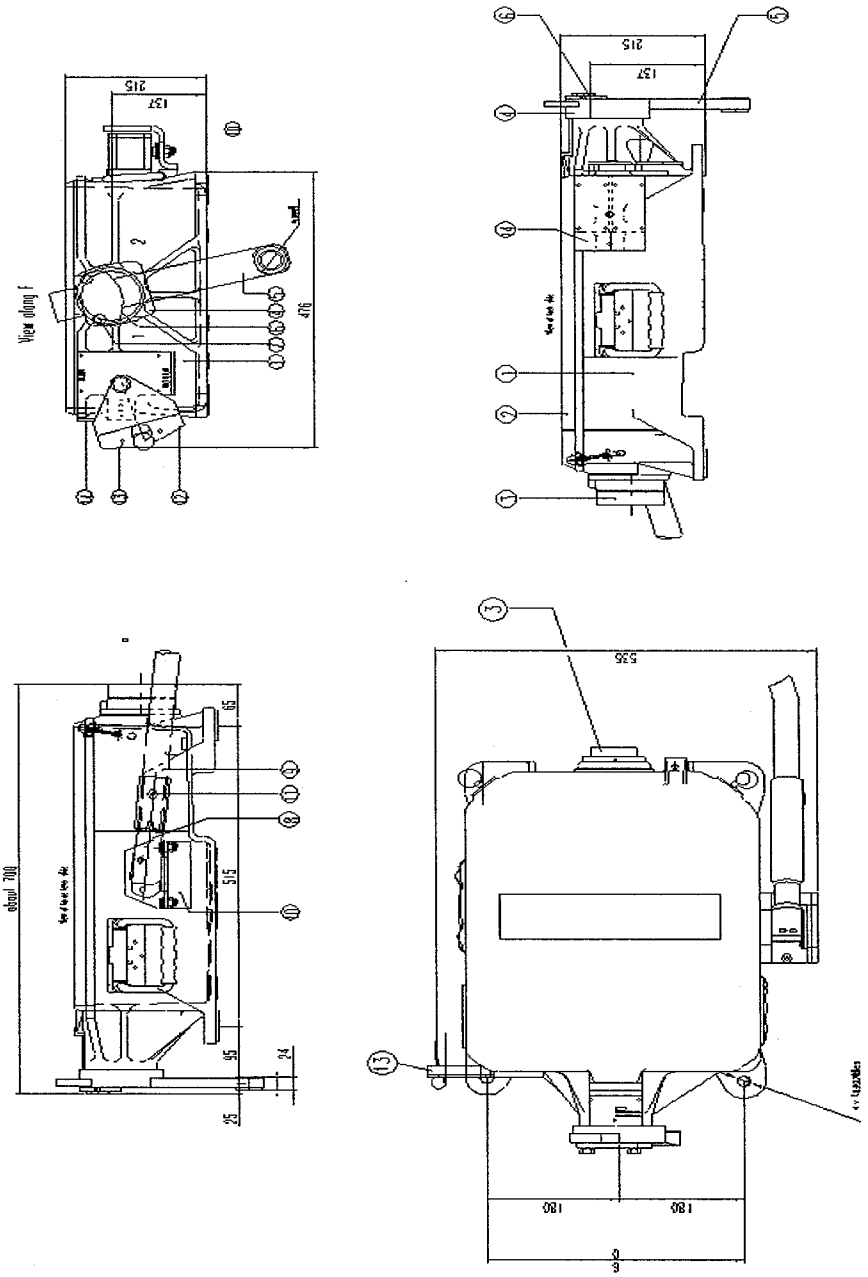


그림 3.9.36 MJ81형 전기선로전환기 외부 상세도

○ 배선

- 전기선로전환기의 전기 회로의 회선들은 제어 암(Arm) 반대편 외함의 수직 면에 부착된 커넥터를 통해 연결되며 전원단자들은 덮개로 보호된다.

○ 전동기

- 3상용의 전동기는 전기제어부 터미널의 결선방법에 따라 3상 교류전원을 입력받아 220V(△결선) 또는 380V(Y결선)로 동작된다. 3상용의 전동기는 3상 전원의 위상을 전환함으로써 역회전되며 동력은 마찰크러치를 통하여 전달된다. 전동기는 KSC 0904(전기기계기구의 방수시험 및 고형물의 침입에 대한 보호등급) 6등급 내수형으로 제작된다. 동기 절연등급은 KSC 4202(일반용 저압3상 유도 전동기) 및 KSC 4004(전기기 절연의 종류)의 F종 절연에 의한다.

○ 감속장치

- 감속기어는 경합금 주물 덮개로 싸여 선로전환기 외함 내부에 장착되고 회전력이 마찰클러치를 통하여 전달되는 구조이다.

○ 제어부

- 제어축(Control Shaft) 끝 부분에는 제어암이 부착되어 롯드를 동작시키는 구조이다.

○ 수동장치

- 전기 선로전환기는 "MANUAL/MOTOR" 선택 스위치가 장착되어 전원으로 제어하는 경우에는 "MOTOR" 위치로, 수동으로 제어하는 경우에는 "MANUAL" 위치로 전환하여 사용할 수 있다. 수동 제어하는 경우는 비상제어 레버로 조작되며, 비상제어 레버는 운반시 편리하도록 분리되는 구조를 갖는다.

제10절 열차제어측면의 사상사고 저감기술개발

	검증계획서 (Verification Plan)	**ID No :** TC - SR10 - SSR01 - 2010 작성일 : 2010. 05. 14 수정일 :

10. 프로젝트는 열차제어측면의 사상사고 방지기술을 개발하여야 한다

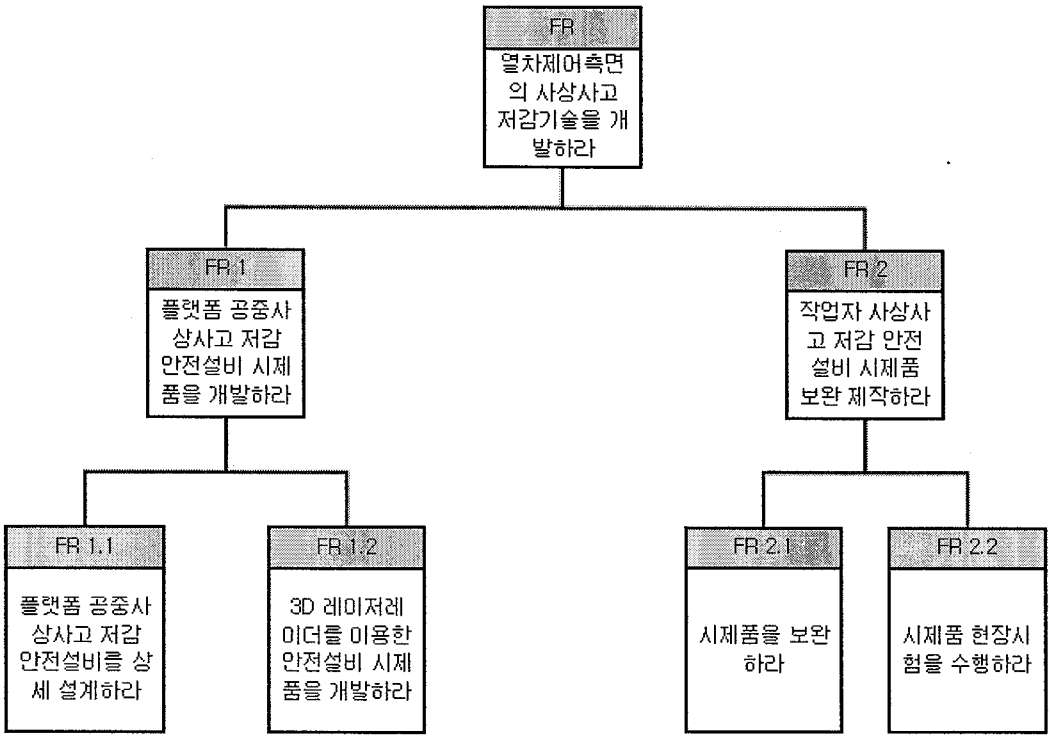
10.1 프로젝트는 열차제어측면의 사상사고 방지기술을 개발하여야 한다.

입력물 :	업무 :	출력물 :
☐ **요구사항 (Requirement)** - 요구사항 문서 - 검증 요구사항 추적 매트릭스 (VRTM) ☐ **기술 개발 계획(Technical Plan)** - 연구계획서 - WBS (Work Breakdown Structure) ☐ **설계정보 및 평가자료** - 성과물 : 플랫폼 공중사상사고 저감 안전설비 상세설계서 및 기본설계서, 작업자 보호 안전설비 시제품 - 설계 분석 보고서 (DARs) ☐ **검증 방법** - 1.2 외국자료와 비교 - 5.3 기능시험	- SE 검증	- 수정 VRTM - 검증결과표

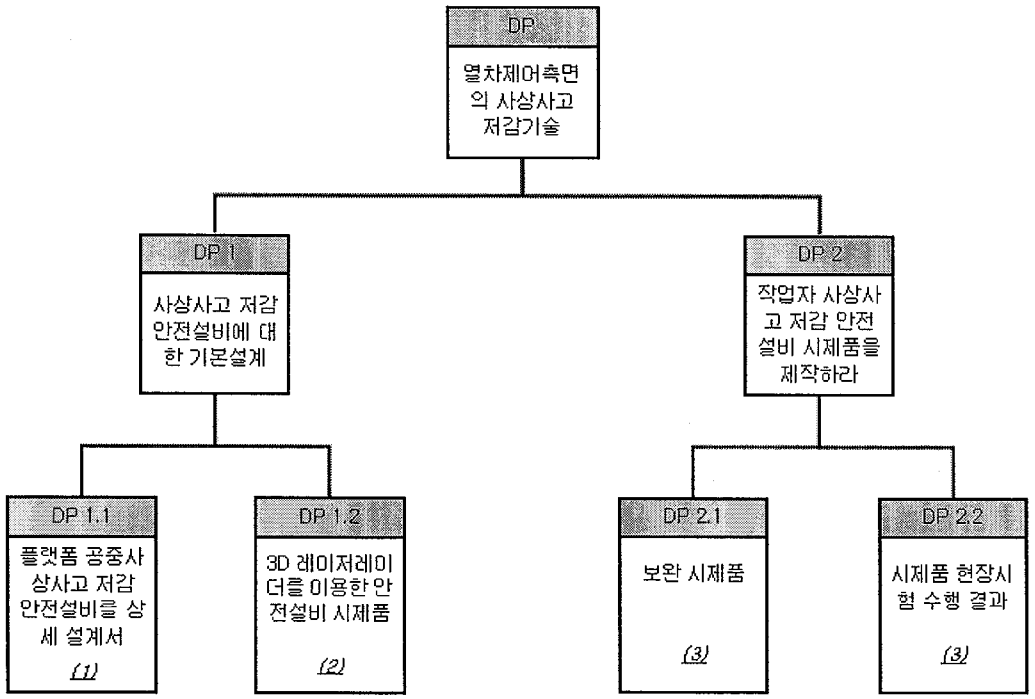
Verification Specification (검증기준) :

1. 3D 레이저레이더 센서를 이용한 플랫폼 사상사고 저감 안전설비의 시제품 개발을 위한 적절한 상세설계를 수행하였는가?
2. 플랫폼 사상사고 저감 안전설비 시제품이 이루어 졌는가?
3. 선로변 유지보수자 사상사고 저감을 위한 안전장치 시제품의 보완제작이 이루어졌는가?
4. 선로변 유지보수자 사상사고 저감을 위한 안전장치 시제품에 대한 현장 시험이 이루어 졌는가?

1. 기능 아키텍처



2. 물리 아키텍처



3. 설계분석보고서

가. 요구사항과의 적합성

열차제어측면의 사상사고 기술개발은 요구사항 『SR 10. 프로젝트는 열차제어측면의 사상사고 방지기술을 개발하여야 한다.』 중 **『SSR. 10.1. 열차제어측면의 사상사고 방지기술을 개발하여야 한다.』**에 해당하는 내용이다. 본 과제에서는 열차제어측면의 사상사고 저감을 위한 안전설비 개발을 위해 전년도에 기본설계한 3D 레이저 레이더를 이용한 플랫폼 공중 사상사고 저감 안전설비에 대한 상세설계와 시제품 제작을 수행하였다. 또한 전년도에 제작한 선로변 작업자 사상사고 저감을 위한 안전설비 시제품을 보완하였으며, 도시철도 운영기관에서의 현장시험을 수행하였다.

나. 설계기준

○ 참고자료

- 국토해양부 보도자료, "2008년 철도사고 2007년도에 비해 4.9 % 감소", 2009. 04. 02
- 정보통신부 보도자료, "지하철 무선영상전송용 주파수 분배 추진", 2007. 03. 19
- 국외 논문 및 관련자료
  - Y. Sasaki, N. Hiura, "Development of Image Processing Type Fallen Passenger Detecting System", JR-EAST Technical Review Special Edition Paper, No. 2, pp. 66-72, 2003.
  - Y. Hisamitsu, K. Sekimoto, K. Nagata, M. Uehara, E. Ota, "3-D Laser Radar Level Crossing Obstacle Detection System", IHI Engineering Review, Vol. 41 No. 2, 2008. 8.
  - "LaserGrab PLS 60 Platform security system for rail roads", Data Sheet, LASER OPTONIX.

○ 출원특허

- "철도 선로변 작업자 안전을 위한 위험 감지 시스템 및 위험 감지 방법",

10-2008-0103434, 2008.10.

- "철도선로변 유지보수 안전 경보시스템 및 방법", 10-2008-0049488, 2008.5.
- "골전도 스피커를 이용한 열차접근 경보 시스템 및 방법", 10-2008-0049496, 2008.5.
- "차량의 접근경보시스템 및 접근경보방법", 10-2009-0105744, 2009.11.

다. 검증방법에 따른 증거 자료

사상사고 저감기술 개발을 위해 본 과제에서는 크게 두 가지의 안전설비를 개발하였다. 하나는 플랫폼 공중 사상사고 저감 안전설비이고, 다른 하나는 선로변 작업사 사상사고 저감을 위한 안전설비이다.

플랫폼 공중사상사고 저감 안전설비는 3D 레이저레이더 센서를 이용한 안전설비로, 전년도까지의 기본설계를 바탕으로 당해연도에는 상세설계와 이에 따른 시제품 제작이 이루어졌다. 선로변 작업사 사상사고 저감 안전설비의 경우 전년도에 1차 시제품이 제작되었고, 당해연도에는 시제품의 보완제작이 수행되었으며 철도 운영현장에서의 현장시험을 통한 개발 시제품의 성능검증이 수행되었다. 또한 개발 시제품의 상용화를 위해 도시철도 운영기관에서의 시연회를 개최하였으며, 현재 개발 시제품을 도시철도 운영기관의 일부 유지보수차량에 시범적용하여 운용 중에 있다. 시범운용 과정에서의 의견 수렴을 통해 차년도에는 본 개발품에 대한 실용화를 추진할 예정이다.

본 연구항목의 검증방법에 따른 증거자료는 플랫폼 공중 사상사고 저감 안전설비의 경우 상세설계 자료와 시제품이며, 선로변 작성자 사상사고 저감 안전설비의 경우 제작된 시제품, 시연회, 현장시험 및 시범설치 사진 등이 있으며, 이러한 자료들은 본 절의 보고서 본문 중에 포함되어 있다.

라. 성과물의 내용 및 결과

열차제어 측면의 사상사고 저감 기술 개발에는 크게 두 가지의 안전설비에 대한 개발이 추진되고 있으며, 플랫폼 공중사상사고 저감을 위한 안전설비와 선로변 작업자 사상사고 저감 안전설비이다.

플랫폼 공중 사상사고 저감 설비의 경우 전년도에 기본설계를 바탕으로 당해연도에는 3D 레이저레이더 센서를 이용한 상세설계와 시제품 제작이 수행되었으며,

차년도에는 당해연도에 제작된 시제품을 기반으로 3D 레이저레이더를 이용한 검지기법, 측정기법, 추적기법 등 안전설비에 적용을 위한 적용성 기술 개발 및 성능검증 시험이 수행될 예정이다. 당해연도의 상세설계를 위한 기초연구로 전년도에 조사분석한 국내외 철도안전설비에 대한 기술과 본 과제에서 개발하고자 하는 안전설비와 유사한 선행기술에 대한 조사분석을 하였으며, 또한 선행기술들과의 본 기술과의 차별점을 분석하였다. 그리고 상세설계를 통해 시제품을 제작하였으며, 현재 제작된 시제품에 대한 성능확인 시험이 진행 중에 있다.

선로변 작업자 사상사고 저감 안전설비의 경우 전년도에 시제품을 제작하였고, 당해연도에는 철도운영기관 대상 시연회를 개최하여 의견을 수렴하였고 이를 반영하여 시제품을 보완제작하였다. 그리고 철도현장에 시범설치하여 현재 시범운영 중에 있으며, 개발 기술의 상용화를 위한 기술이전 협의 중에 있다.

(1) 국내·외 철도안전설비 기술현황 조사

(가) 개요

국내 철도운영은 많은 발전을 이루어 왔으며, 현재 KTX-II 고속철도 및 각 시도의 경량전철사업이 본격적으로 추진되고 있다. 새롭게 건설되는 철도사업에 따라 다양한 열차제어기술이 적용되고 있으며, 기술개발에 대한 많은 관심과 더불어 승객 및 운영인원의 안전과 열차운행에 대한 보다 확실한 안전장치의 필요성이 더욱 강화되고 있는 실정이다. 따라서 현재 개발되어 적용되는 신기술에 대한 안전설비 또는 현재 사용되고 있는 설비에 대한 안전장치의 연구 및 개발이 절실히 필요한 실정이다.

철도사고는 매년 조금씩 줄어들고 있는 추세에 있지만 여전히 인간의 행동적인 측면에 있어서는 사고가 줄어들고 있지 않다. 국토해양부는 "2008년 철도사고는 2007년에 비해 4.9% 감소한 408건 발생하고, 사망자는 159명으로 17% 감소하였다"고 발표하였다. 철도사고 408건 중 열차의 충돌·탈선사고가 7건, 도로와 철도가 교차하는 건널목에서 발생한 사고는 24건, 운행 중인 열차에 치이거나 역·승강장에서 전도·추락한 인명사상사고가 377건이고, 인명피해 410명 중 사망자는 159명, 중상자는 167명, 경상은 84명이며, 전체 인명피해는 '07년(431명) 대비 4.9%(21명)가 감소하였다. 철도사고가 매년 감소하는 것은 철도안전시설을 확충하는 한편, 철도안전

종합계획을 지속적으로 추진하고 철도안전심사 등을 통한 지도감독을 강화한 결과로 볼 수 있다.

철도유형별로는 고속철도의 경우, 열차충돌·탈선사고는 없었으며 인명사상 사고만 13건이 발생하여 전년도(13건)와 동일하며, 일반철도는 231건(열차사고 6건, 건널목 사고 24건, 사상사고 201건)이 발생하여 전년(220건) 대비 5%(11건) 증가하였고, 도시철도는 64건(열차사고 1건, 사상사고 163건)이 발생하여 전년(196건) 대비 16%(32건) 감소하였다. 철도사고 원인별로는 철도시설·차량의 결함으로 인한 사고는 감소추세이나, 표 3.10.1에 보인 것처럼 자살추정·선로 무단횡단 등 공중의 불법행위로 인한 사고는 줄어들지 않고 있다. 열차사고의 경우, 종사자의 규정위반 등 업무소홀로 인한 사고가 사고원인의 71%이고, 건널목사고의 경우 자동차 운전자의 규정위반 등 운전부주의로 인하여 모든 사고가 발생하였으며, 인명사상사고의 경우는 자살시도, 선로 무단통행 등 불법행위에 의한 사고가 56%로 가장 많이 차지하고, 여객이 역·승강장 등에서 전도·추락하거나 작업자의 부주의한 행동 등 인적요인에 의한 사고도 32%나 발생하였다. 특히 지난 2002년~2006년 말까지 자살, 무단출입, 열차접촉 등 승객과 열차의 직접접촉에 의한 사고로 총 412명의 사상자가 발생할 정도로 지하철 승강장의 안전 문제는 심각한 수준에 달하고 있다.

표 3.10.1 국내 철도사상사고 현황 (관련자료: 국토해양부 보도자료, 2009.4)

구분 / 연도		합계	여객						공중			종사자		
			선로무단(근접)통행	승강장 전도추락	승하차시 넘어짐	열차에 뛰어듦	열차내 넘어짐	기타	선로불법통행	열차에 뛰어듦	기타	불안전한 조건	부주의한 행동	기타
'08년		377	15	26	7	81	8	20	79	35	4	9	70	23
		(%)	4.0	6.9	1.9	21.5	2.1	5.3	21.0	9.3	1.1	2.4	18.6	6.1
'07년		399	24	8	6	98	9	14	81	36	8	16	85	14
		(%)	(6.0)	(2.0)	(1.5)	(24.6)	(2.3)	(3.5)	(20.3)	(9.0)	(2.0)	(4.0)	(21.3)	(3.5)
대비	건수	-22	-9	18	1	-17	-1	6	-2	-1	-4	-7	-15	9
	%	-5.5	-37.5	225.0	16.7	-17.3	-11.1	42.9	-2.5	-2.8	-55.0	-43.7	-17.6	64.3

(나) 철도안전설비 기술현황

① 국내

현재 한국철도에서 사용하고 있는 철도시스템 주요 안전설비에 대한 내용은 표 3.10.2와 같다. 경부고속철도 구간에는 차축 및 휠온도검지장치, 지장물검지장치, 끌림검지장치, 기상검지장치, 안전스위치, 열차접근감확인장치, 터널경보장치, 분기기

히터제어장치, 레일온도검지장치, 기계실출입자감시장치, 지진감시장치, 현장장치 기능감시장치 등을 설치하여 운용하고 있고, 일반철도 구간에는 분기기히터제어장치, 기계실출입자감시장치, 승강장 비상정비스위치, 승강장 스크린도어(Platform Screen Door, PSD) 등을 설치하여 운용하고 있다. 광역철도(도시철도 및 지하철) 구간에는 승강장 비상정지버튼, 승강장 스크린도어 등을 설치하여 운용하고 있으며, 용인 경량전철에는 가이드웨이 침범검지시스템(Guideway Intrusion Detection System, GIDS)을 적용하여 공사 중에 있다. 이와 같이 그동안 한국철도는 경부고속철도를 도입함에 따라 보다 진보적인 안전설비가 IT산업과 접목되어 괄목할만한 성장을 이루어 왔다.

표 3.10.2 철도시스템 안전설비 설치현황

구 분	안 전 설 비	
경부 고속철도	• 차축 휠온도검지장치	• 지장물검지장치
	• 끌림검지장치	• 기상검지장치
	• 안전스위치	• 열차접근감확인장치
	• 터널경보장치	• 분기기히터제어장치
	• 레일온도검지장치	• 기계실출입자감시장치
	• 지진감시장치	• 현장장치 기능감시장치
일반철도	• 분기기히터제어장치	• 기계실출입자감시장치
	• 승강장 비상정비스위치	• 승강장 스크린도어
광역철도	• 승강장 비상정지버튼	• 승강장 스크린도어
경량전철	• 승강장 스크린도어	• 가이드웨이 침범검지시스템

② 국외

국외의 경우에는 한국철도에 설치된 안전설비 이외에도 보다 진보된 지능제어시스템을 채택한 안전설비가 사용되고 있다. 미국의 ITS/HRI(Highway Rail Intersection)는 도로상의 차량(roadway vehicle)과 철도와의 인터페이스를 다루는 분야로서, 철도와 차량의 이동을 감시하여 운전자에게 미리 경고함으로써 사고를 감소시키게 하는 역할을 담당하고 있다. 1995년 10월 일리노이주 Fox River Grove에서 발생하였던 통근열차와 스쿨버스 간의 충돌사고로 인해 7명의 학생이 사망하게 되었는데, 이 사고를 계기로 도로와 철도의 안전을 향상시키기 위하여 국가

ITS 계획의 30번째 분야로서 "Highway Rail Intersection"이 채택되게 되었으며. 그림 3.10.1은 ITS/HRI 시스템의 구성도를 보인 것이다.

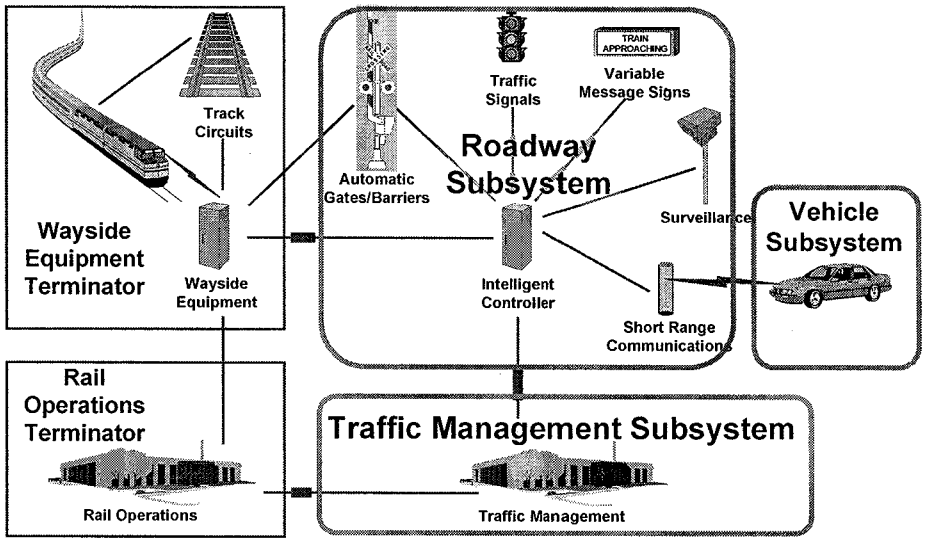


그림 3.10.1 ITS/HRI 시스템 구성도
(자료: Wisconsin Statewide ITS Users Group, 2000.4)

미국의 연방철도국(Federal Railway Administration, FRA)은 연방도로국(Federal HighWay Administration, FHWA)의 협조로 차량근접경고(Vehicle Proximity Alert) 프로젝트를 수행하였으며, 이는 철도건널목을 이용하는 자동차 운전자 및 열차 기관사에게 각각 경고(alert)를 줄 수 있는 SmartStops, EARS(Electronic Accident Reporting System), DVSS(Dynamic Vehicle Safety System) 등 3개의 시스템을 개발하여 시험을 수행하였고, 설계된 대로 동작하는지에 대한 시스템의 능력, 동작의 일관성에 대한 시스템의 능력 그리고 모든 시스템의 결함에 대한 평가를 수행하였다. 평가결과 무선통신을 이용하여 도로 측의 차량과 열차와의 정보를 송수신하는 시스템인 SmartStops 및 DVSS의 효과가 우수한 것으로 나타났다. 또한 미네소타교통부(Minnesota Department of Transportation, MnDOT)에서는 3M 및 DVSS와 공동으로 음향과 시각적인 신호로 스쿨버스 운전자에게 버스가 건널목에 어느 정도 접근했는지와 건널목에 열차의 존재 유무를 알려줄 수 있는 차내경고(In-Vehicle Signing) 시스템을 개발하였다. 주요 구성요소로서 열차검지장치, 건널목 송신기, 차량 수신기, 차내 표시기 등이 있으며, 평가결과 버스 운전

자에게 철도 건널목에서의 열차유무를 경고하는 것이 효과적이라는 결과를 얻었다.

일본의 경우, 철도 안전에 대한 최우선 목표는 승객이 목적지에 안전하게 도착하는 것을 확실히 하는 것이다. 이 목표를 달성하기 위하여 동일본철도회사(JR)는 비상정지 버튼, 열차 비상정지 경보, 점자블록, 안전선(생명선), 승강장계단, 승객 추락(또는 전락) 검지매트 등을 수도권 지역의 주요 역과 곡선으로 인해 역 승강장과 열차 진입 문 사이의 거리가 넓어진 역에 안전설비를 설치하여 운영하고 있다. 그러나 추락하는 승객을 검지하는 매트는 승강대 바로 밑에만 설치되어 있기 때문에 그것은 승강장 선로의 전 부분을 커버할 수가 없다. 이 문제를 해결하기 위하여 동일본철도회사는 ITS 기술에 사용된 입체이미지 처리기술을 사용하여 그림과 같이 승강장 선로의 거의 전 구간에 걸쳐 추락 승객을 검지할 수 있는 지능형 안전장치를 개발하였다.

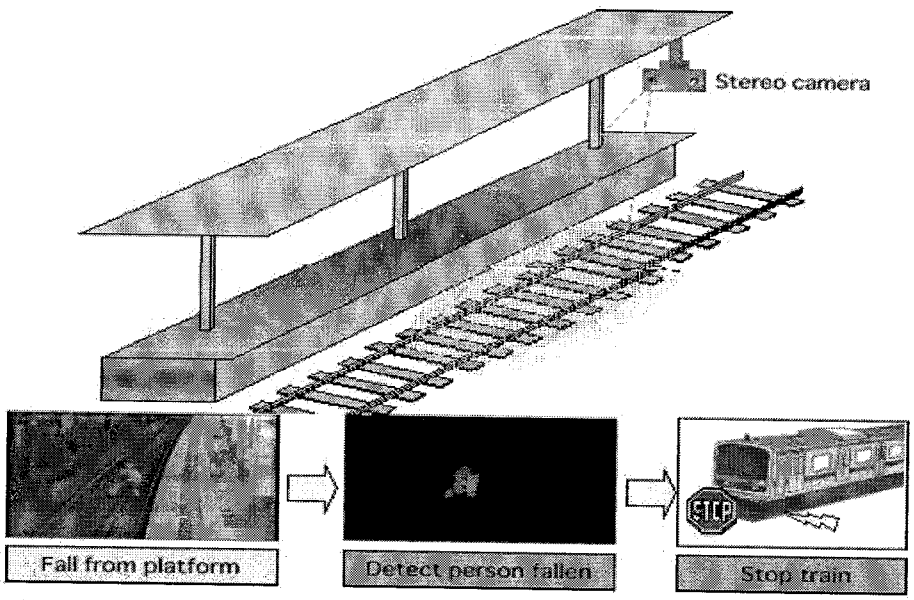


그림 3.10.2 카메라를 이용한 승강장 추락검지 시스템
(자료: JR동일본 안전연구소, 2004)

또한 일본의 IHI사에서는 그림 3.10.3과 같이 3D 레이저 레이더 센서를 이용하여 철도건널목 장애물 검지장치를 개발하여 2006년부터 동일본철도 노선에 500대 이상(건널목 당 1대) 설치하여 운영 중에 있다. 종전의 철도건널목 장애물 검지장치는 레이저 광선 교차방식으로 설계되었기 때문에 한 쌍의 광선을 수신하고 송출하는 장치가 철도의 양쪽에 설치되어야 했다. 만약 건널목 가까이에 분기기나 역 승

강장이 있는 경우에는 장치를 설치할 수 없는 문제점을 가지고 있었다. 이는 지나가는 통행인들에 의해 광선 수신 및 송출장치에 쓸데없는 간섭과 광축의 변위, 비가 오는 때에 광선 수신 및 송출장치의 오작동 등의 문제가 포함된다. 그리고 루프코일 방식으로 설계된 철도건널목 장애물 검지장치는 검지코일이 건널목 안쪽의 철도를 따라서 지하에 매설되어야 하기 때문에 대규모의 설치공사가 필요하다. 그러므로 검지코일이 끊어지거나 이상이 발생하는 경우에는 유지보수작업에 상당한 노력과 인력이 필요하다. 그러나 IHI사가 개발한 장치는 레이저 레이더 헤드가 철도 외측에 세워진 특별한 콘크리트 침목에 설치된다는 것과 건널목의 전 구간(길이 20m 폭 10m까지)이 하나의 장비에 의하여 감시될 수 있다는 것이다. 본 장치는 지표로부터 4m 이상의 높이에 설치되기 때문에 그러한 문제가 없다는 장점이 있다. 또한 전선의 끊어짐이 없으며 유지보수작업이 용이하다는 것이다.

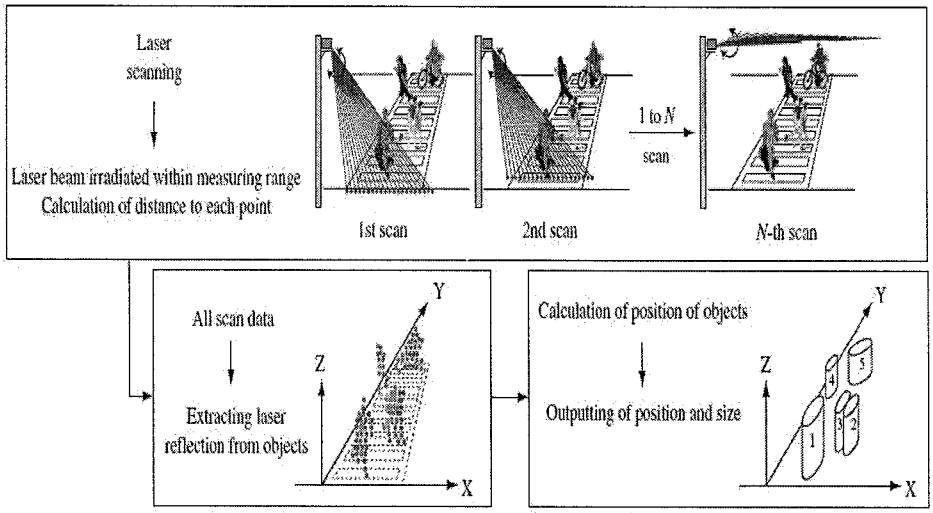


그림 3.10.3 철도건널목 장애물 검지시스템
(자료: 일본 IHI Engineering Review, 2008)

(2) 선행기술조사 및 차별화 방안

6차년도에 본 연구를 수행하기 위한 선행조사로써 영상처리기술에 의한 스크린도어 잔류검지, 영상처리기술에 의한 승강장 낙하물 검지기술, 선로차단 지원시스템, 승강장 안전시스템 등을 검토하였으며, 개략적인 적용방안 및 동작원리는 다음과 같다.

(가) 영상처리기술에 의한 스크린도어 잔류검지

① 개요

· 승강장 곡선이 큰 역에 설치된 스크린도어와 전동차와의 간격이 넓은 곳에서 광센서에 의한 잔류 물체검지 방법은 광센서의 특성상 사각이 발생.

· 이러한 사각을 최소화 할 수 있는 영상처리기술을 응용한 센서 개발이 필요.

② 이미지 센서의 검지방법

표 3.10.3 이미지 센서 검지방법

지 장 검 지	· 스크린도어가 닫힘 동작 개시부터 닫히기까지의 시간 사이에 승강 전동차와 스크린도어 사이의 지장물 검지
잔 류 검 지	· 스크린도어의 개/폐 전/후의 화상을 비교하여 사람이 잔류하는 지를 검지
이미지센서 시험	· 영상에 영향을 주는 요인을 충분히 파악하여 잔류검지를 위한 알고리즘을 개발

③ 주요기능

표 3.10.4 영상처리기술의 주요 기능

항목	지하철 평가 내용	지상역 평가 내용
검지능력	· 3세(신장 70cm) 이상의 사람 검지 · 스크린도어의 선로 측 전체영역 검지	· 3세(신장 70cm) 이상의 인물 검지 · 스크린도어의 선로 측 전체영역 검지
외란배제	· 조명, 인형, 차량 흔들림 및 낙하물체 등의 외란 배제	· 태양광, 눈, 비, 안개 등의 외부환경 배제
동기처리	· 스크린도어의 열림신호 및 모든 닫힘신호와의 동기처리 확인(전기적 인터페이스 필요)	· 스크린도어와 전기적 인터페이스 필요 없음

(나) 영상처리기술에 의한 승강장 낙하물 검지기술

① 개요

· 스크린도어가 설치되어 있지 않는 승강장에서 승객의 부주의로 인하여 발생하는 추락 사고를 방지하기 위함.

· 승강장에 영상처리기술을 이용하여 동작 감시범위를 설정하고 동작 감시범위에 음주승객 또는 아동들의 부주의로 많이 발생하는 추락사고를 빠르게 검지하여 경보 또는 안전조치를 취하여 2차의 사고를 미연에 방지하는 기술.

② 시스템 구축 방안

표 3.10.5 승강장 낙하물 검지범위

승강장 범위	· 현장 감시용 카메라를 설치하여 선로 측 부분을 감시
기계실 범위	· 영상정보를 처리하는 주장치, 인터페이스장치 및 단말장치로 구성
위험경보 대상	· 승강장의 승객 및 역무원

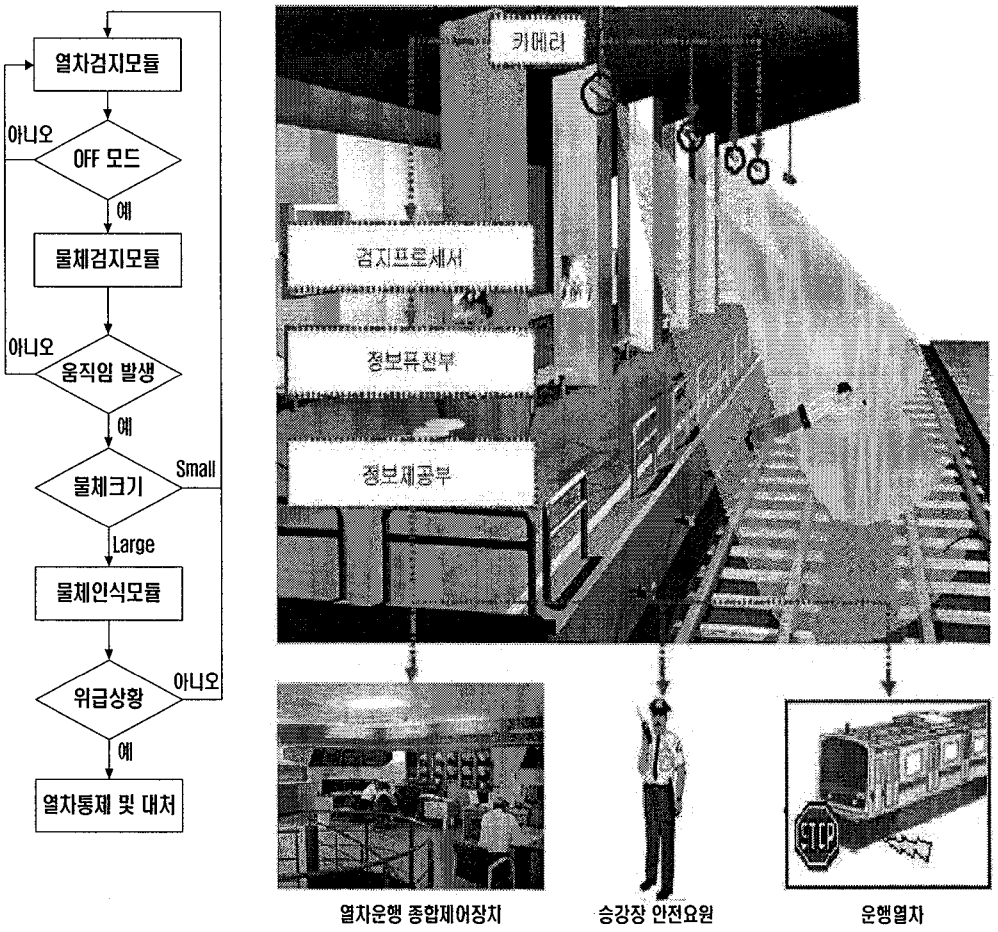


그림 3.10.4 영상기반 승강장 안전시스템 구성 일례

③ 주요기능

표 3.10.6 승강장 낙하물 검지 주요 기능

검 지 기 능	· 선로방향으로 촬영 가능한 카메라를 설치하여 동작하는 물체를 인식
분 석 기 능	· 감시영상 범위의 이동물체를 인식하고 일정 시간의 행위를 분석
경 보 기 능	· 위험범위내의 이동물체감지에 따른 경고 및 알람을 수행

(다) 선로차단 지원 시스템

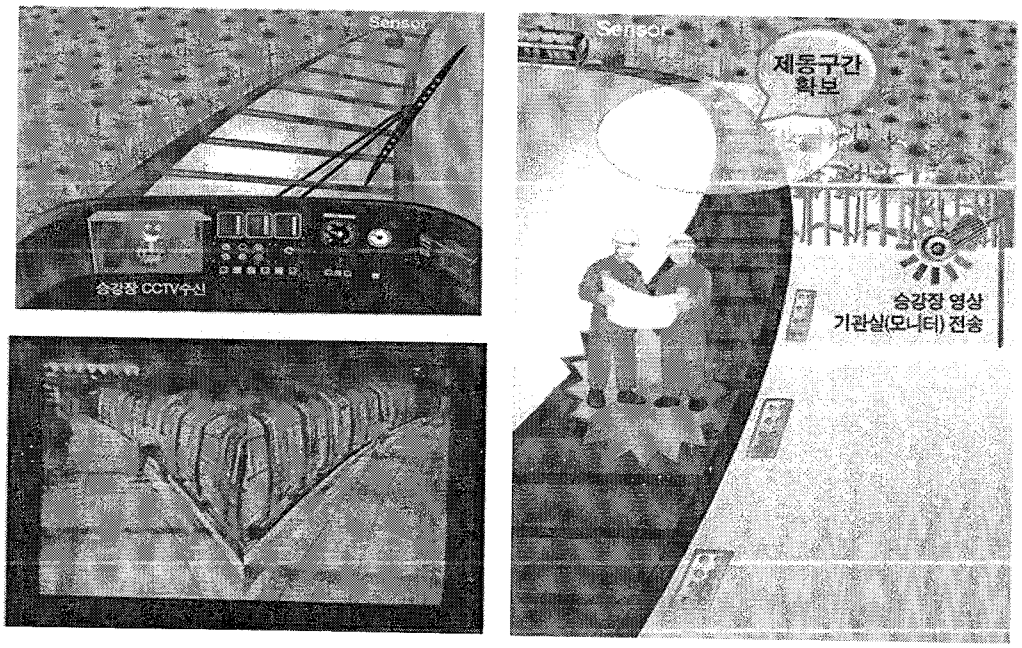


그림 3.10.5 선로차단 지원 시스템 구성 일례

① 개요

· 열차운행 현황의 파악, 선로 차단공사의 착수, 종료수속, 보수용 차량의 진로 요구 등을 이동단말을 이용하여 조작

· 선로차단 책임자가 모바일 단말을 조작하여 교통관제사를 개입시켜 선로차단 공사의 안전성 향상과 간소화 도모

② 시스템 구축 방안

표 3.10.7 선로차단 지원시스템 구축방안

기본사항	· 보수용 제어서버, 작업계획 Dia 서버, Dia 표시장치보수용 단말 · 모바일 단말로 구성, 보수용 제어서버는 교통관제센터와 연계
시스템 기능	· 선로차단 수속 지원 기능, 운행상황 파악 기능 · 착수, 종료보고 통보 기능, 보수용 차량 진로구성 기능
작업계획 입력	· 작업계획은 보수분소의 단말에서 등록 ·
주요 기능	· 열차운행상황 확인:열차번호, 지연, 다음열차 위치 표시 · 관제실 운용 -. 선로차단 착수 종료 -. 선로전환기 전환 · 시스템 작업시간대 운용

(라) 승강장 안전시스템

① 개요

· 지상구간의 저상홈 형태의 승강장에 스크린도어의 설치가 미비

· 저상홈 등 스크린도어 설치가 부적합한 곳에 승강장 안전시스템을 설치하여 승객의 안전을 확보

② 시스템 구축 방안

표 3.10.8 승강장 안전 시스템 구축방안

동작시스템	· 열차가 일정구간을 지나칠 때 동작을 수행하고, 열차가 안전하게 정차하면 작동을 정지 시키는 시스템
검지시스템	· 승강장에서 승객이 선로로 접근 또는 추락하는 것을 감지하는 시스템
열차정지시스템	· 선로에 침입자 및 장애물이 있는 경우 열차를 정지시키는 시스템

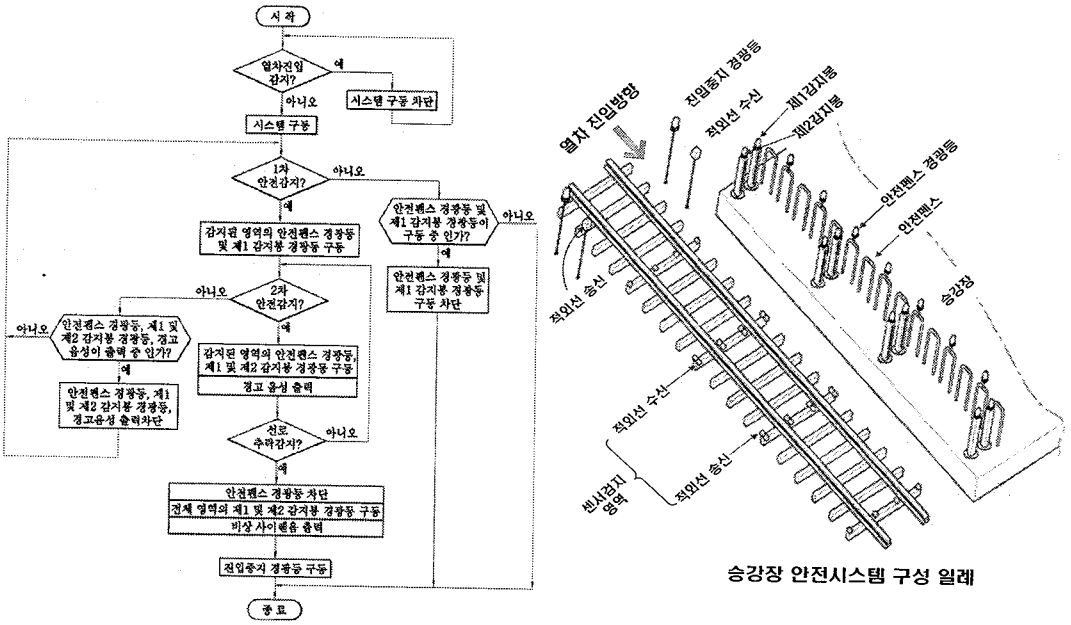


그림 3.10.6 승강장 안전시스템 구성 일례

(마) 비교검토 결과

영상처리 기술의 승강장 접근센서 응용은 최근 신설되는 스크린도어의 자체 검지센서 도입 등과 같은 기술발전으로 기술의 이중투자가 될 요소가 있으며, 영상처리기술의 승강장 낙하물 검지기술은 본 연구내용과 동일하나 철도의 개방된 정거장의 경우 빈번한 조류의 이동으로 적합하지 않고, 선로차단 지원시스템은 대상이 운영보수 요원이므로 본 연구과제의 대상 항목과 맞지 않는다. 따라서 이 중 가장 적용성이 높고 실현가능한 아이템인 승강장 안전시스템이 6차년도 연구과제로 선정되었다.

표 3.10.9 안전시스템의 비교

구 분	설 치 위 치	보 호 대 상	운영비절감내용
영상처리기술의 스크린도어 잔류검지	스크린도어에 설치	승객	출입문사고의 사전예방을 통한 비용 절감
영상처리기술의 승강장 낙하물 검지기술	승강장에 설치	승객 및 운영요원	사고발생에 따른 대처 비용 절감
선로차단 지원 시스템	유지보수자 위주의 유동적 구간	운영보수요원	사고발생에 따른 대처 비용 절감
승강장안전시스템	승강장내 및 인근 선로부 설치	승객 및 운영요원	사고발생에 따른 대처 비용 절감

(바) 타 과제 중복성 검토 및 차별화

① 연구개발과제 중복성 조사

㉮ 화상처리식 검지시스템 기술개발

○ 연구개요

차세대 첨단 도시철도시스템 기술개발사업(주관기관: 한국철도기술연구원)에서 수행 중인 "화상처리식 검지시스템 기술개발 "과제는 승강장에서 승객 선로추락, 승객 끼임 및 화재 등의 위험상황을 새로운 영상처리기술을 이용하여 자동검지하고, 위험도를 판단하여 실시간으로 종합관제실, 역무실 및 진입열차에 전송하는 기술개발과제임.

○ 적용환경

- 빈번한 열차 진출입, 열차 불빛, 반사광, 승객의 이동 및 그림자, 날씨 및 기후의 변화 등과 같은 다양한 철도 승강장 환경조건에도 정확한 검지가 이루어져야 함
- 승강장 열차 진출입 및 승객의 승하차에 지장을 주지 않으면서 정확한 위험상황 검지가 이루어져야함
- 시스템 설계시 최적의 검지 효율을 위한 설계보다는 운영 및 승객의 안전을 우선적으로 고려해야하는 제약이 있음

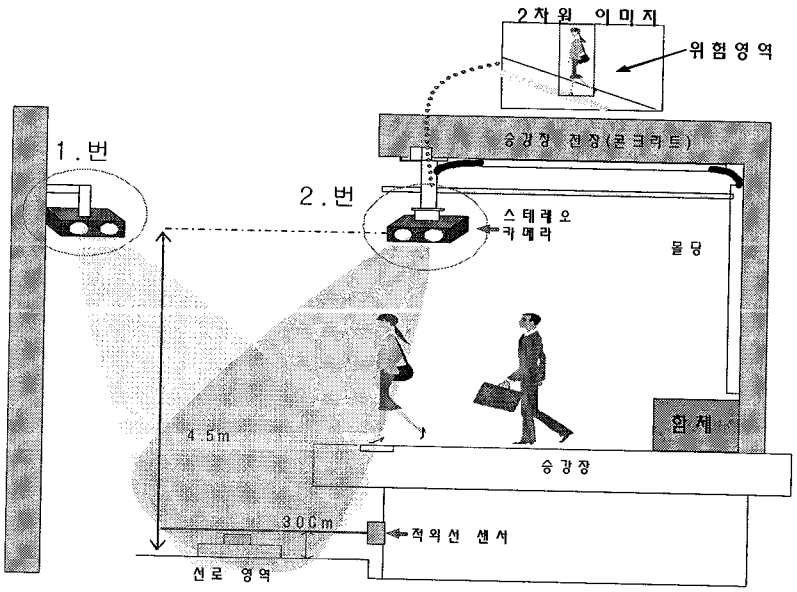


그림 3.10.7 화상처리식 검지시스템 구성 일례

- 그림 3.10.7 에서 1번의 위치는 검지효율 면에서는 최적의 설치 위치이나, 열차 운영 및 유지보수성 등의 면에서는 설치될 수 없는 위치이다. 반면, 2번 위치는 차량한계, 유지보수성, 승객 승하차 등이 종합적으로 검토된 위치이지만, 2차원 영상만으로 분석하면 승객이 위험영역 안에 존재하는 것처럼 오검지 할 가능성이 높다는 문제가 있다. 따라서 이러한 문제를 해결하기 위해서 스테레오카메라 및 스테레오 비전 알고리즘을 적용하여 3차원 물체검지 방식을 적용하여 개발을 진행하고 있다.
- 3차원 기반 물체검지 알고리즘은 물체의 좌표, 높이 등을 계산함으로써, 열차의 불빛 및 그림자(높이가 제로임), 쓰레기 투기(신문지 등)에 의한 오검지를 제거 할 수 있다.

○ 검지대상

- 열차상태 판별 : 진입(IN), 정차(ON), 출발(OUT), 없음(OFF) 상태
- 승객 및 물체의 선로추락 검지(OFF 상태에서 수행)
- 승객의 안전선 침범 및 문틈끼임 상황검지(IN, ON상태에서 수행)
- 검지 영역내 화재 상황 검지 등

○ 주요기능

- 승강장 내 위험상황 검지

- 승강장 추락물체 검지(사람, 위험물체 판단)

  · 승강장 승객 승하차 상황 검지 (안전선 침범 및 문틈 끼임 상황)

  · 승강장 검지영역 내 화재상황 검지

- 검지영상 및 경보 메시지 전송

  · 위험 상황 발생시 사전에 지정된 운영자(진입열차, 종합관제실, 역무실 등)에게 검지된 영상 및 경보메시지 실시간 전송

- 검지된 위험상황 저장 및 검색

  · 검지된 위험상황에 대한 저장 및 검색기능

○ 주요개발내용

- 하드웨어 분야

  · 철도 승강장 선로영역 모니터링을 위해 최적화된 시스템 구성 방안도출 및 설계

  · 철도 승강장 모니터링 환경에 적합한 스테레오카메라 개발

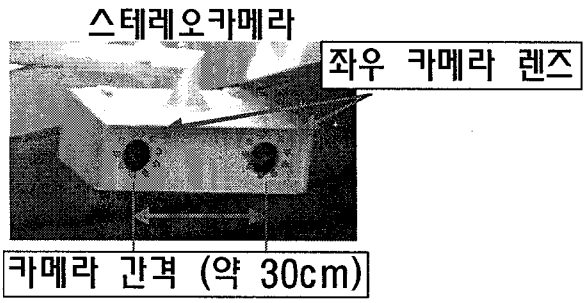


그림 3.10.8 개발된 스테레오 카메라

  · 스테레오카메라, 열상카메라 및 적외선 센서 제어시스템(제어에 필요한 H/W) 개발

- 소프트웨어 분야

  · 정확한 위험상황 판별을 위한 열차상태 검지 알고리즘 개발

  · 철도 승강장 모니터링을 위한 스테레오비전기반 검지 알고리즘(3차원 기반 물체검지) 및 위험상황 검출을 위한 검지 알고리즘 개발

  · 개별 카메라 및 센서로부터 얻어진 검지 결과를 바탕으로 승강장 위험도 판단을 수행하는 위험도 판단 알고리즘 개발

· 스테레오카메라, 열상카메라, 적외선 센서로부터 검지된 결과를 바탕으로 최종 위험상황 판단

· 관제실, 역무실, 역무원 PDA용 및 전동차 사용자별 정보표출, 관리 및 제어 프로그램 개발

○ 시스템 구성

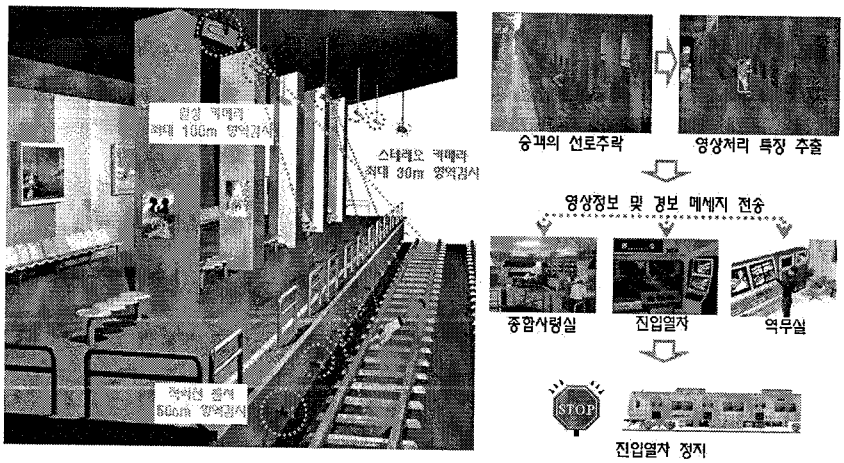


그림 3.10.9 전체적인 시스템 구성도

○ 주요 특징

- 다양한 철도 승강장 환경을 위한 검지 알고리즘 개발

· 다양한 빛의 조건을 고려한 영상처리기술 개발

· 스테레오비전 기반 검지 알고리즘 개발

- 물체까지의 거리 및 높이 판정가능 → 3차원 검지

· 개별 센서 및 카메라(열상, 스테레오)로부터 얻어진 검지정보를 바탕으로 최종 위험도 판단 알고리즘 개발

· 검지결과를 사전에 정의한 운영자(관제실, 역무실, 진입열차 등) 실시간으로 전송

- 운영기관 신호시스템과 연계 시 자동으로 열차정지 가능함.

㉯ 열차제어측면의 사상사고 저감기술 개발

○ 연구개요

본 과제에서 수행 중인 "열차제어측면의 사상사고 저감기술 개발"과제는 국내의 일반 철도가 대부분의 승강장이 개방형의 저상홈으로 구성되어 있으며, 안전설비가 없으므로 공중사상사고 발생 시 사상사고 저감을 위하여 승강장 선로의 승객추락, 선로침입, 장애물검지를 수행하여 경보 및 상황을 실시간으로 종합 관제실, 역무실 및 승강장에 진입하는 열차에 전송.

○ 적용환경

- 철도 선로주변에 사용되는 검지기는 먼지, 비, 안개 및 눈을 처리할 능력이 있어야 하는데 먼지나 비 또는 눈 모두가 수시로 휘날리고 소용돌이 칠 수 있다. 이러한 환경에서도 정확한 장애물 검지가 이루어져야 함. 이러한 이유로 카메라와 음파탐지기와 스캐닝 레이저 등은 잘못된 측정결과를 가져올 수 있음.
- 장애물 검지 센서는 태양광이 들어오게 하거나 그림자에 의한 영향 및 야간의 조명에 의한 영향으로 오작동이 되어서는 안되는 데 3D 레이저 레이더 센서는 이러한 환경에서도 정확하게 동작되도록 되었음.

○ 검지대상

- 일반 철도 개방형 승강장에서 승객 추락 검지
- 일반 철도 개방형 승강장에서 선로 침입자 및 장애물 검지

○ 주요기능

- 승강장 내 위험상황 감시 : 3D 레이저 레이더 및 감시카메라
- 상황분석 및 경보 전송 : 승강장 선로 안전설비 서버
- 검지상황 저장 및 검색 : 승강장 선로 안전설비 서버
- 승강장 상황의 정보수신 : 역무실 제어장치, 차상과 관제실 연계는 타 과제기술 적용

-진입 열차정지 : 타 과제 수행기술 적용

○ 주요개발내용

- 하드웨어 분야

· LaserGrab(Laser Scan Unit): Laser Radar System으로 특정 지역을 Scan하여 물체를 포착/감시하는 기능을 수행하며, LCU와 연동하여 3D 이미지 분석/제어 및 경보를 발생한다.

· LCU (Local area Control Unit): LaserGrab과 영상카메라를 제어하며, SCU

와 연동하여 원격 제어에 따른 명령수행 및 통신 수단과 연동하여 수집 정보를 원거리의 SCU로 전송한다.

· UIU (User Interface Unit): LCU와 SCU의 사이에 구성되는 다양한 통신 매체와의 연동을 담당하며, 사용자 요구에 맞게 구현되는 통신 정합장치이다. 또한 지역상황실(local area) 및 통합감시센터와 망을 구축하여 실시간으로 승강장 상황 을 연계하여 관리할 수 있다.

- 소프트웨어 분야

· Linux Server를 이용한 시스템 통합관리 소프트웨어 개발

· Scan된 장애물의 이미지 분석 및 처리 알고리즘 개발

· 감시 영역 내에 있는 물체의 정확한 식별 및 감시 알고리즘 개발

· 타 보안시스템과의 연동 및 통합 가능한 TCP/IP 기반의 인터페이스 소프트웨어 개발

· 고객 요구사항에 대한 보완 · 수정 · 추가가 용이한 MMI 인터페이스 소프트웨어 알고리즘 개발

○ 시스템 구성

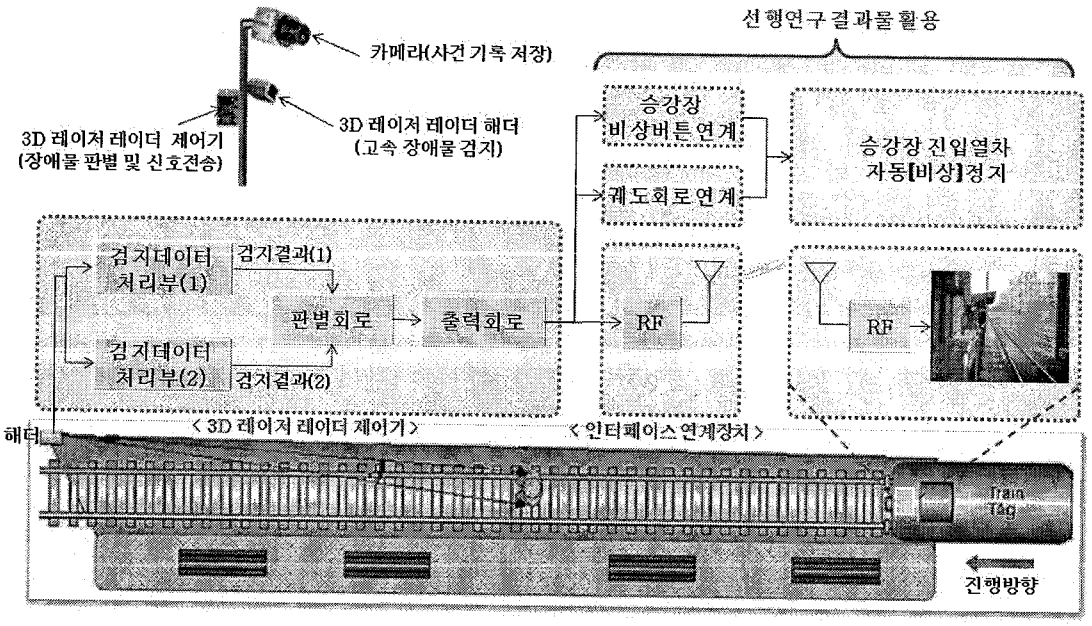


그림 3.10.10 3D 레이저 레이더를 이용한 장애물 검지시스템의 구성도

○ 주요 특징

- 카메라로 검지하는 경우와 비교할 때 정확성이 훨씬 뛰어나며 넓은 검지 영

역의 데이터를 얻을 수 있다. 이미지 센서와 다르게 빛의 양에 관계없이 범위 데이터를 얻을 수 있고 해상도도 초음파 센서보다 더 높다.

- 3D 레이저 레이더 센서를 사용한 장애물 검지 장치는 입체적으로 광범위한 영역을 검지할 수 있으며, 이상 물체를 포착시 경보 신호를 송출하고, 고성능 카메라를 제어하여 검지된 물체의 영상을 상황실로 실시간 전송하여 신속한 상황파악 및 대처가 용이함.
- 장애물 또는 침입자를 검지하여 경보를 보내고 필요에 따라 모니터로 확인하며 대처할 수 있도록 하여 사고를 미연에 방지할 수 있는 양방향성 검지 시스템

② 연구개발의 차별화 방안

- 차세대 첨단 도시철도시스템 기술개발사업(한국철도기술연구원)에서 수행 중인 "화상처리식 검지시스템 기술개발 "과제는 카메라를 사용하여 장애물을 검지하는 방법 및 목적은 동일하지만, 승객의 안전선 침범, 문틈 끼임 상황검지, 화재 등 검지대상에 따른 수많은 알고리즘개발과 시행착오를 거쳐 관련 설계사양 및 제반규정을 정립하는 데 있어서 주어진 시간 및 예산으로 분야별 특성화된 기술개발을 시도하는 것은 매우 바람직하다고 생각된다.
- 아울러, 본 과제에서 다루는 승강장 선로에 침입되는 장애물(우산, 풍선, 비둘기, 개, 고양이, 추락자, 유지보수 요원 등)에 대한 식별 및 조치에 대한 알고리즘개발과 제반규정을 정립하는 것도 최근 선진국에서 추진하고 있는 승강장 선로의 요소기술에 특화된 유형으로 기존 기술개발사업과 중복성에 저촉되지 않는다고 볼 수 있다.
- 본 연구에서 개발하려는 일반철도 개방형 승강장의 선로 지장물 검지설비는 일반철도구간의 승강장의 길이가 길고 개방형의 승강장으로 구성되어진 정거장에 설치를 목적으로 하고 있으므로 다른 개발 사업에서의 중복성은 저촉되지 않는다고 볼 수 있다. 또한 각각의 안전설비의 적용되는 장소 및 환경이 다르므로 개발 사업에서의 중복성은 저촉되지 않는다고 볼 수 있다.

(3) 플랫폼 공중사상사고 저감 안전설비 상세 설계

(가) 지능형 안전설비 구축을 위한 고려사항

① 검지기술

마이크로프로세서가 사람의 두뇌를 대신하고, 복잡한 알고리즘과 프로그램이 의사결정을 대신하고, 액츄에이터가 가속이나 제동 장치의 작동을 위한 발을 대신하고 조종간의 작동을 위한 손을 대신하게 되었다. 불행하게도 사람의 가장 중요한 특성은 모방하기가 가장 어렵다. 사람이 볼 수 있는 능력과 눈으로 많은 사물을 파악하는 것이 해답이다. 눈이 없이는 마이크로프로세서는 복잡한 알고리즘과 프로그램을 장님처럼 처리할 것이다. 따라서 안전설비에 어떤 검지센서를 적용할 것인가를 결정하기 전에 우리는 다음과 같은 설치되는 환경과 제약조건 등에 대한 조사가 선행되어야 한다.

- 기후 : 검지기는 먼지, 비, 안개 및 눈을 처리할 능력이 있어야 하는데 먼지나 비 또는 눈 모두가 수시로 휘날리고 소용돌이 칠 수 있다. 이러한 이유로 카메라와 음파탐지기와 스캐닝 레이저 등은 잘못된 측정결과를 가져올 수 있다.
- 빛과 조명 : 열차운행은 아침 동트기 전에 운행이 시작되고 그 후 낮이 되면서 점차 빛의 강도가 높아지고 정오에 고점에 달한다. 이 시점에서 낮이 저물면서 빛은 줄어들기 시작한다. 그러나 하루 종일 날씨가 변하는 경우에는 빛의 양도 따라서 변할 수 있다. 이것은 우리의 검지센서가 빛의 어떤 조건 하에서도 작동해야 한다는 것을 의미한다. 예를 들면, 태양광이 들어오게 하거나 그림자에 의한 영향 및 야간의 조명에 의한 영향이 계절에 따라서도 변화 하는 지를 평가하여야 한다. 이러한 환경에 대해서는 음파탐지기, 스캐닝 레이저, 밀리미터파 레이저, 3D 레이저 레이더 등은 상대적으로 변화하는 빛의 조건에 의해 영향을 받지 않으며 변화하는 빛의 조건을 다루기 위한 좋은 선택일 것이다.
- 거리의 검지 : 장애물 검지센서는 2~3초 이내에 장애물의 존재를 검지하고, 장애물 회피 알고리즘은 회피 진로를 정확하게 결정하여야 한다. 이것은 검지센서가 회피조치를 안전하게 수행할 수 있을 만큼 빨리 장애물을 검지해야 한다는 것을 의미한다. 이 제한으로 우리는 철도시스템에 사용되는 장애물 검지센서가 최소한 몇 미터의 검지범위를 가져야 하는지를 결정해야 한다. 이것은 장

애물의 파악과 회피진로의 계산을 위해 충분한 시간을 준다. 이 요건에 따라 초음파 센서는 최대 범위가 5미터 정도이고, CCD 카메라와 스캐닝 레이저와 3D 스캐닝 레이저 및 밀리미터파 레이더 모두는 최대 검지범위가 최소 15미터 이상이다.

- 응답시간 : 검지센서가 적절하기 위해서는 장애물을 파악하고 열차에 대응하도록 하는 시간이 매우 중요하다. 3D 스캐닝 레이저의 경우에 차량의 전방에 있는 하나의 이미지를 스캔 하는데 필요한 시간은 80초이며 이것은 명백히 실시간 장치를 위해서는 수락할 수 없는 수준이다. 음파탐지기는 장애물이 존재하는 경우에 신속하게 결정하지만 음파탐지기는 단지 짧은 거리만을 볼 수 있다. 즉, 음파탐지기가 장애물을 검지할 수 있기 전에 열차는 장애물에 이미 너무 근접되어 있을 것이다. CCD 카메라의 응답시간은 이미지 처리속도와 처리능력에 따라 다르다. 속도가 빠른 컴퓨터의 경우에는 이것은 문제가 되지 않으며 카메라의 응답시간은 안전한 거리에서 장애물을 검지하기에 충분히 빠르다. 2차원 스캐닝 레이저는 매우 빠른 응답시간을 가지고 있는데 데이터를 출력하는 해상도와 속도에 따라 1초에 대해 17ms의 정도로 응답한다. 이것은 스캐닝 레이저로 하여금 안전한 거리에서 장애물을 검지하도록 허용하고 장애물의 적절한 검지와 회피를 가능케 한다. 밀리미터파 레이더도 충분히 빠른 응답시간을 갖고 있다. 카메라에서와 마찬가지로 좀 더 빠른 컴퓨터의 경우에는 레이더 신호를 좀 더 빠르게 계산할 수 있도록 한다. 3D 레이저 레이더는 장애물을 안전한 거리에서 검지할 수 있다.
- 검지기의 비교 : 일반적으로 안전설비의 장애물에 대한 식별 방법은 적외선 센서, 레이더 센서, 초음파 센서, CCD 또는 IR 카메라 등과 같은 센서를 이용하고 있다. 그러나 이들 센서들은 전기장, 자기장, 빛 등과 같은 외부환경에 민감하게 반응한다는 문제점을 가지고 있다. 즉, 적외선 센서는 거리 성능이 떨어지고, 레이더 센서는 거리 성능은 우수하나 외부환경에 민감하여 거리에 대한 신뢰도가 떨어지며, 초음파 센서는 거리 성능 및 거리 분해능이 떨어진다는 문제점이 있다. 이로 인하여 측정된 데이터가 왜곡되어 측정 데이터가 달라지므로 장애물 검지 센서의 선택은 매우 중요하다.

승강장 선로의 안전설비에는 3D 레이저 레이더 센서가 모든 기후조건에서 잘 작

동하는 유일한 센서이기 때문에 자연히 그것이 선택될 가능성이 높다. 그러나 높은 비용과 상대적으로 신기술이기 때문에 우리는 그것을 선택하는데 망설일 수밖에 없다. 하지만 몇 년 이내에 비용의 저하와 기술의 안정으로 좀 더 실용적이 될 것이라고 희망한다.

② 신뢰도 및 중복성 문제

모든 형태의 철도사고는 안전과 보안에 대해 대형사고가 발생될 가능성이 있기 때문에 모든 형태의 침입자 및 장애물 검지장치는 높은 신뢰도 즉, 매우 낮은 고장의 확률을 가져야 한다. 검지 플랫폼은 여분의 카메라나 검지기 같은 주 카메라나 검지기가 고장인 경우에 일시적으로 사용할 수 있는 백업 또는 중복 구성품을 포함하여야 한다. 실제 운영상황에서 이미 입증된 높은 품질의 장치의 사용과 함께 이는 장치의 신뢰도를 증가시킬 것이다.

철도사고의 전형적인 대형사고의 가능성과 국가 기반시설에 대한 테러에 대한 높은 위험을 고려하여 모든 장치는 비상안전장치를 가지도록 설계되어야 할 것이다. 이것은 장치의 어느 구성품이 고장의 가능성을 경험하는 경우에는 다가오는 열차에 적절한 경보를 제공해야 한다는 것을 의미한다. 일상적인 자기 진단기능이 이들 장치에 포함되어서 모든 검지장치와 통신구성품의 고장을 주기적으로 점검하고 고장정보를 적절한 경로(열차, 지상경보장치와 또는 관제센터)에 전달하여야 한다.

운영 및 유지보수 계획도 각종 검지장치에 대해 개발되어야 할 것이다. 검지 오류나 경보장치의 고장까지의 범위를 다룰 수 있어야 한다. 가능한 모든 상황을 포함하는 프로토콜 시나리오를 작성 비치하여 기관사와 기타의 모든 지정된 당국에 올바른 비상조치를 취할 수 있도록 해야 한다.

③ 야외 설치장비의 요건 충족

철도변 선로를 따라 설치되는 안전설비는 열차가 운행되는 한 어떠한 기후조건하에서도 그 기능이 정지되어서는 안 된다. 특히 확실한 성능요건 즉, 진동과 낙뢰 보호 물성과 또한 각종 기후조건에 적응시키기 위하여 사용되는 기술에 대한 요건을 충족해야 한다. 특히 태양광선과 지진 등을 포함한 환경조건의 변화에 의해 영향을 받지 않고 정상적으로 흠 없이 주어진 기능을 수행한다는 것을 검증하고 평가해야 한다.

(나) 3D 레이저 레이더 센서의 구성

① 개요

철도 승강장으로 차량의 진입시 고의 또는 과실로 승강장 선로에 사람 또는 장애물이 진입할 경우 인명의 사상 및 차량 운행 지연 등으로 심각한 손해를 초래하게 된다. 최근 들어 지하철의 승강장에서의 정신이상자, 취객, 자살 기도자 등의 낙상에 의한 인명사고, 출퇴근 혼잡 시간대에 옷이나 신체 일부가 열차의 출입문에 끼이는 사고, 승강장과 철도차량 사이의 틈에 승객의 일부가 빠지는 사고 등 철도내의 안전사고는 더욱 빈번해지고 있어 철도분야에서 해결해야할 가장 시급한 문제로 떠오르고 있다.

이에 대해 승객의 선로 추락 사고를 사전에 차단하기 위해 승강장에 안전펜스를 설치하거나, 스크린도어(Platform Screen Door, PSD)라고 하는 이중 안전문을 설치하여 안전사고를 방지하려는 다수의 고안이 제시되어 있다. 그러나 안전펜스의 경우 안전펜스를 지나 승강장 선로측으로 언제든지 들어갈 수 있기 때문에 안전장치로서의 역할을 더 이상 기대하기 어려웠고, 스크린 도어의 경우 모든 승강장에 설치하는 것은 막대한 비용이 들기 때문에 이용객이 많은 역이나 환승역에 우선적으로 설치 운영되고 있다.

특히 지상 승강장일 경우에는 주변 경관을 차단하여 승객들의 답답함을 가중시킬 수 있는 단점도 가지고 있다. 또한 열차가 승강장의 정위치에 정차하지 못할 경우 스크린도어의 개폐에 문제가 발생할 수 있고, 스크린 도어와 열차 사이의 틈에 인체나 물체가 끼였을 경우에 대한 처리방안이 필요하다. 이러한 환경 하에서 3D 레이저 레이더 센서를 이용하여 승강장 안전설비를 구축하는 것이 시급하다.

세계적으로 3D 레이저 레이더 장치는 군수, 교통안전, 보안분야 등 여려 분야에서 목표물의 실시간 위치 파악, 장애물 검지 등에 활용되고 있다. 최근 들어 철도 안전 분야에서도 건널목 장애물 검지장치, 터널, 교각 및 고속화에 따른 승강장 안전사고방지 대책의 일환으로 3D 레이저 레이더를 이용한 물체 검지 방법 연구의 필요성이 제기되고 있다.

3D 레이저 레이더를 이용한 장애물 검출방법은 목표물에 레이저 펄스를 방사하고 반사된 레이저 값을 분석하여 물체의 위치 및 모양을 3차원으로 인식한다. 지속적인 레이저 펄스 궤환을 통해 데이터 값의 변화를 추적하여 장애물의 움직임과

방향까지 파악할 수 있다.

철도 건널목의 장애물 검지장치의 경우 레이저광선 교차방식과 루프코일 방식이 있지만 3D 레이저 레이더 방법에 비해 검지의 범위 제한과 설치비용 및 유지보수의 복잡성 측면에서 적용가능성이 낮다. 또한 이미지 처리 방법은 기존의 감시카메라 방식이 이점으로 갖고 있지만 낮 시간에 그림자에 의해 크게 영향을 받으며 비와 눈과 같은 기후에 의해서도 크게 영향을 받는 등 문제점을 갖고 있다. 그러나 레이저 레이더는 장비 1set의 검지영역이 넓어 상대적으로 설치비용을 절감할 수 있고 장소에 따른 제약을 받지 않으며 다른 장치와 비교하여 상대적으로 유지보수가 용이하다. 뿐만 아니라 비와 눈과 같은 악천후에도 효과적으로 성능을 발휘한다는 것이 특징이다.

② 장애물 검지 원리

- 장애물 검출 처리 절차

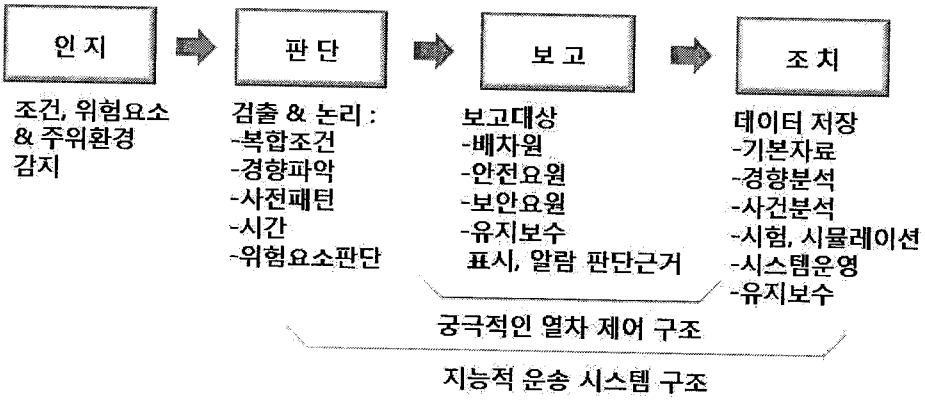


그림 3.10.11 장애물 검지 테이터 흐름도

열차운영 시스템에서 3D 레이저 레이더를 사용한 장애물 검지 방법에 관한 데이터 흐름도는 그림 3.10.11과 같다. 장애물 검출방법은 시스템의 데이터 흐름에 따라 4단계로 설명할 수 있다. 최초 인지 단계에서는 장애물과 주위환경을 대상으로 센서의 레이저 빔 피드백 검지작업을 진행하며 시간에 따른 범위영역의 장애물 위치 변화값을 데이터로 전환한다. 축출된 데이터는 사용자가 사전에 설정한 기준에 따라 위험요소(장애물) 여부를 판단하며 3차원 크기와 시간에 따른 패턴 변화를 통하여 속도와 방향을 판단할 수 있다.

장애물 판단정보는 보고대상자(배차원, 안전요원, 보안요원 등)에 보고되어 2차 판단의 근거로 사용된다. 또한 알고리즘에 따라 동작을 지시하는 전기신호를 출력한다. 사용자는 장애물을 검지하여 판정하는 단계와 상황에 맞는 조치를 실행하는 단계사이의 인터페이스를 목적과 설정범위에 따라 다양하게 적용할 수 있다. 최종 조치단계에서의 데이터 저장은 정보기록, 사후 사건분석, 시스템 유지보수를 위한 테스트와 패턴분석의 자료로 활용된다.

- 스캐너 모델

스캐너 장치는 독일, Wagen의 Zoller 및 Froehlich(Z+F)가 설계한 레이저, 및 PA, 피츠버그의 K2T가 설계한 2축 기계 스캐닝(scanning) 기구로 구성되어 있다. 스캐너는, 고도(高度) 시야각 30도 및 방위각 360도를 통해서 레이저 에너지를 조정하여 3차원 정보를 수집한다. 센서는 나선(螺線) 스캐닝(helical scanning) 양태로 배열된 시야(視野) 값 및 3차원 거리 점의 스트림(stream)을 만든다.

스캔장치는 금도금 알루미늄 거울, 거울이 수직방향으로 선회할 수 있도록 허용하는 요크 어셈블리, 요크 어셈블리를 회전시키는 스핀들 어셈블리, 공간에 거울의 위치를 확정하는 전자 회로, 거리 데이터를 수집 저장하는 전자 회로, 거리탐지 센서의 장착에 사용하는 기계 하우징, 및 상업적으로 이용할 수 있는 거리탐지 장치로 구성되어 있다.

레이저는 거울 어셈블리 밑에 배치되어 있으며 위쪽을 향해 있다. 스캐너는 자유도가 2인 거울을 지속적으로 회전시키면서 작동한다. 데이터는 거울의 초기 하방향 피봇(하강) 및 상방향 복귀 영역(상승)에 수집된다. 각 순간에, 거울은 레이저 광선을 알고 있는 방위(요크 어셈블리에 의해서 결정) 및 고도(高度)(거울의 수직위치에 의해서 결정)로 굴절시킨다. 레이저는 바깥으로 이동하는데, 물체나 반사(反射) 물질(먼지나 안개와 같은)에 부딪히면 산란된 레이저 에너지의 일부는 동일한 경로를 따라 탐지기로 복귀한다. 물체까지의 거리는 레이저 신호가 왕복하는데 소요된 시간을 직접 또는 간접적으로 측정하여 산출한다.

모터 하나가 거울 축을 잡고 있는 요크 샤프트를 구동시킨다. 거울의 수직위치는 캠 어셈블리에 의해서 결정된다. 캠 종동부(從動部) 휠은 가변 고도(可變 高度) 고리모양 캠 위에서 작동한다.

캠 종동부에는 거울 축과 기어장치로 연결되어 있는 랙(rack)이 장착되어 있으므로, 캠 표면의 국소 높이가 수직거울의 각도를 결정한다. 고리모양 캠은 요크 샤프

틀 감싸고, 회전하는데, 이것은 2번째 모터가 구동시킨다. 캠 표면과 요크 샤프트의 회전속도 차이가 수직 노딩(nodding)율을 결정한다.

그림 3.10.12는 거울 굴절 시스템에서, 회전하는 요크 샤프트가 거울 축을 잡고 있다. 모터 하나가 요크를 회전시키고, 요크가 레이저 광선의 방위방향을 제어한다. 고도 표면이 가변(可變)인 고리모양 캠은 2번째 모터가 회전시킨다. 캠 종동부 휠은 캠 표면 위에서 작동한다. 캠 종동부에는 종동부가 캠 표면 위에서 위와 아래로 이동함에 따라 기어를 통해서 거울 축을 회전시키는 랙이 장착되어 있다. 간단히 하기 위해서 요크 샤프트와 캠 종동부 어셈블리 사이의 견고한 커넥터는 생략했다.

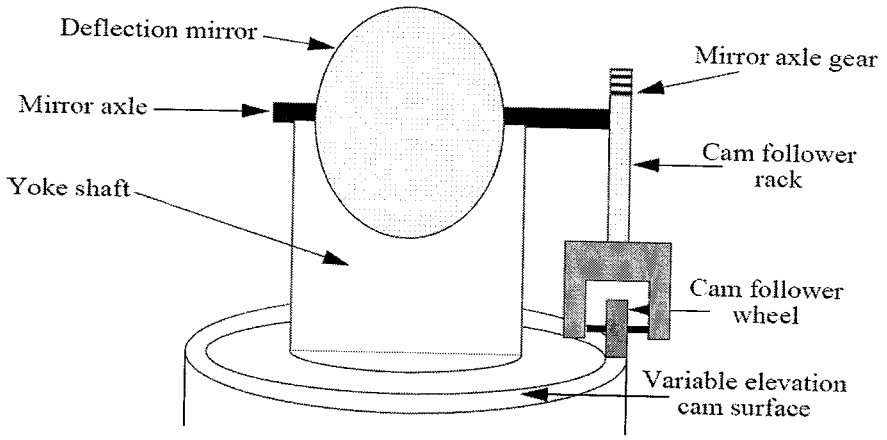


그림 3.10.12 레이저 스캐너 구조 일례(1)

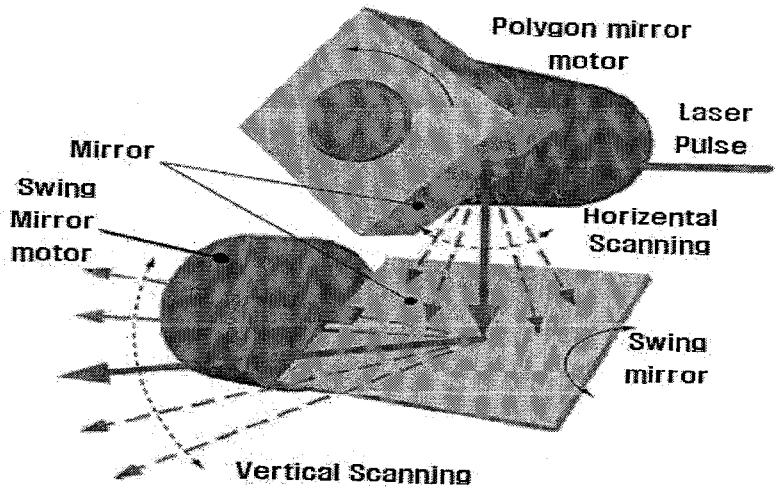


그림 3.10.13 레이저 스캐너 구조 일례(2)

- 장애물 검지원리

3D 레이저 거리계의 작동은, 레이저 에너지를 방출하고 또 그 에너지가 센터를 떠나, 표면에 부딪히고, 다시 복귀하는데 소요되는 시간을 측정하는 것이다. 이 시간 간격을 측정하는 방법에는 기본적으로 3가지가 있다. 즉, 펄스형 비행시간, AM 위상 시간차, 및 FM 맥놀이 주파수이다. 모든 방법의 목표물까지의 거리는 $z = (c\Delta t)/2$인데, 여기서 Δt는 레이저 에너지의 왕복이동 시간이고, c는 빛의 속도다. 우리의 스캔 기구는, Riegl이 개발한 펄스식 비행시간 레이저 조명지점 센서 모델 2개 및 독일, Wagen의 Zoller 및 Froehlich(Z+F)가 개발한 진폭 변조식 연속파(AMCW) 레이저 거리계(距離計)를 포함하여, 여러 대의 거리탐지 장치로 테스트했다. 3종류의 레이저 모두 근적외선 파장으로 작동한다. 기본적인 3종류의 거리탐지 방법의 작동원리를 간단히 설명하면 다음과 같다.

㉮ 펄스식 비행시간(Pulse time-of-flight)

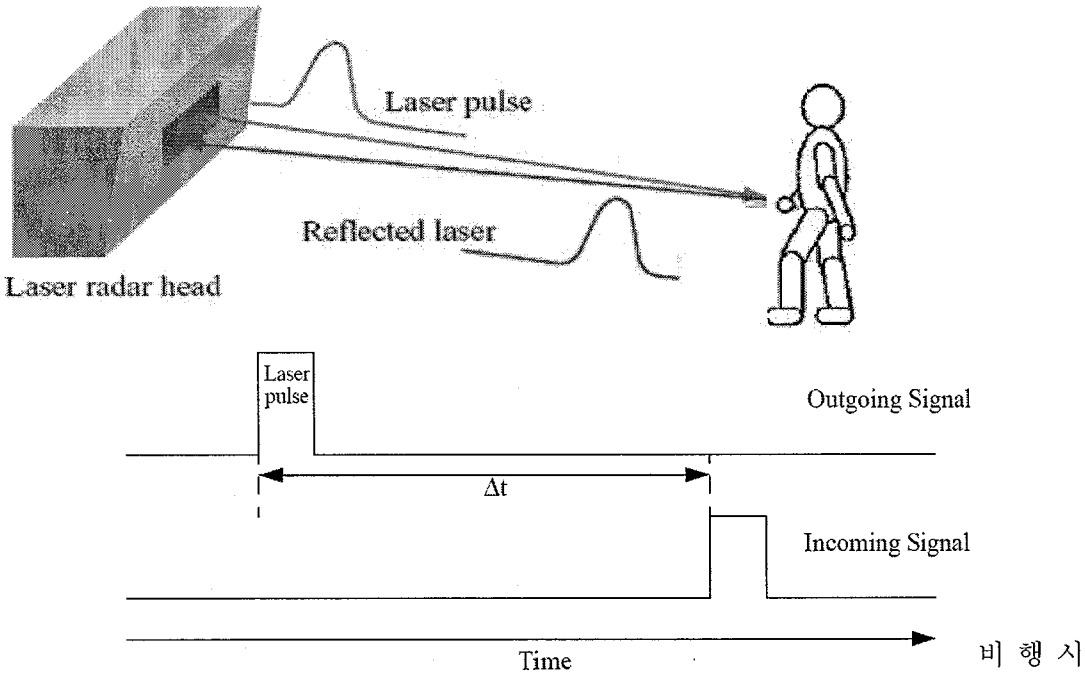


그림 3.10.14 펄스식 비행시간 레이저 센서의 작동

비행기간 레이저 센서의 작동은 집중된 각 픽셀의 레이저 에너지 펄스를 방출하는 것이다. 그 펄스는 센서를 떠나, 어느 표면에 부딪힌 다음, 다시 복귀한다. 시계가 펄스 시작과 수신기의 복귀펄스 선단(先端) 사이의 경과시간을 측정한다

빛의 속도는 3x108 m/s이므로, 짧은 거리는 매우 짧은 펄스와 복잡하고 빠른 전자장치만이 측정할 수 있다. 우리가 테스트한 Riegl 장치의 정확도는 +/- 3cm이고, 해상도는 2cm, 그리고 최대 데이터 수집율은 매초 12,000점이다.

해상도와 정확도는 많은 펄스를 평균하고 또 데이터 수집율을 낮게 하여 휴지시간(Dwell Time)을 늘리면, 이를 개선시킬 수 있다. 레이저의 최대 거리는 반사기가 좋은 경우에는(ρ>0.8) 150m이고, 반사기가 나쁘면(ρ>0.1), 50m이다. 최대 1000m 거리의 역(逆)반사기를 탐지할 수 있다. 레이저 역시 각 픽셀에 대한 세기가 8-bit이다. 센서가 측정할 수 있는 최소 거리는 1m이다.

그림 3.10.14에서 펄스식 비행시간 레이저 센서의 작동은 하나 또는 일련의 밀집된 강력한 레이저 펄스를 방출하고, 또 수신기가 그 레이저 펄스를 탐지할 때까지의 시간을 측정하는 것이다.

Riegl은 먼지구름이나 안개를 관통하여 볼 수 있는 다른 또 하나의 펄스식 레이저 시스템을 고안했다. 어느 환경에서 작동하는 경우, 밖으로 나가는 레이저 에너지의 일부는 먼지나 안개에 의해서 반사되는 한편 그 에너지의 잔여부분은 계속 이동하여 어느 고체 표면에 도달한 후에 탐지기로 복귀한다. 이 경우에, 수신기는 다수의 복귀 펄스를 수신한다. 레이저는 펄스 시작과 수신기로 복귀한 최종 펄스 사이의 경과시간을 측정한다 먼지나 안개가 밀도가 너무 크지 않으면, 이것으로 최초의 고체 표면까지의 거리를 알 수 있다.

최종펄스 탐지방법은 그 레이저 시스템에서 구현(具現)되어 침투력이 높은 시스템이 생성되었다. 센서의 이렇게 침투력이 높은 버전의 정확도는 +/- 10cm이고, 해상도는 10cm, 그리고 반사율 데이터는 8-bit이다. 거리가 동일한 목표물을 탐지하더라도 먼지 및 안개를 통과해야 하는 경우에는, 최종 목표물에 도달하는 에너지가 작기 때문에, 더 강력한 레이저가 필요한 것은 분명한 사실이다.

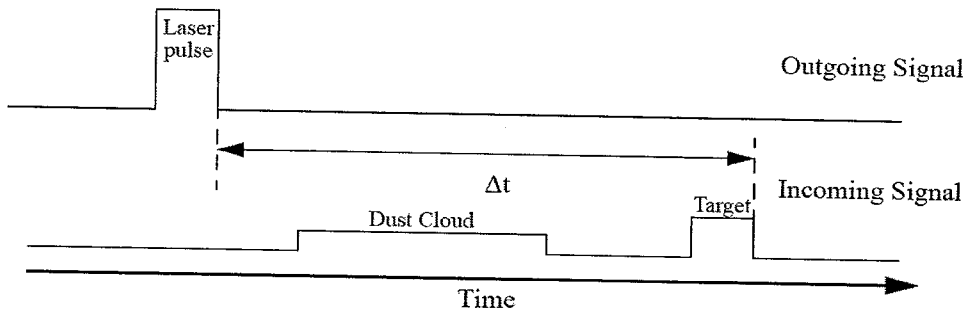


그림 3.10.15 침투력이 높은 레이저 사용

그림 3.10.15에서 침투력이 높은 레이저를 사용하면 먼지나 안개를 관통하여 목표물을 볼 수 있다. 센서의 작동은, 레이저 펄스를 방출하고 또 최종 복귀 에너지(최대 시간 또는 거리까지)를 기다리는 것인데, 이 경우 관심의 대상은 일반적으로 고체표면이다. 먼지나 안개는, 레이저 광선이 작은 미립자에 부딪히면 시간이 경과함에 따라 분산된 일부 레이저 에너지로서, 복귀 신호에 나타난다. 먼지나 안개로부터의 레이저 복귀 신호는 목표물로부터의 그것보다 세기가 더 크다.

㉯ 주파수 변조식 연속파

주파수 변조식 연속파(Frequency-Modulated Continuous Wave, FMCW)는 2번째 형식의 레이저 거리계는 주파수 변조식 연속파(FMCW) 장치다. 방출된 빛은 주파수가 다양한 사인파(sine wave)에 의해서 변조되고, 반사된 에너지와 혼합된다. 그 거리는 최종 맥놀이(beat) 주파수를 측정하여 추정한다. 여타 주파수 변조 스킴(scheme)도 가능하지만, 주파수 "첩(chirp)"은 일반적으로 주기적인 삼각 파형과 유사하다. 삼각 주파수 변조로, 목표물까지의 거리는(최대) 맥놀이 주파수 즉, 복귀신호와 방출된 신호 사이의 주파수 절대 차이에, 비례한다.

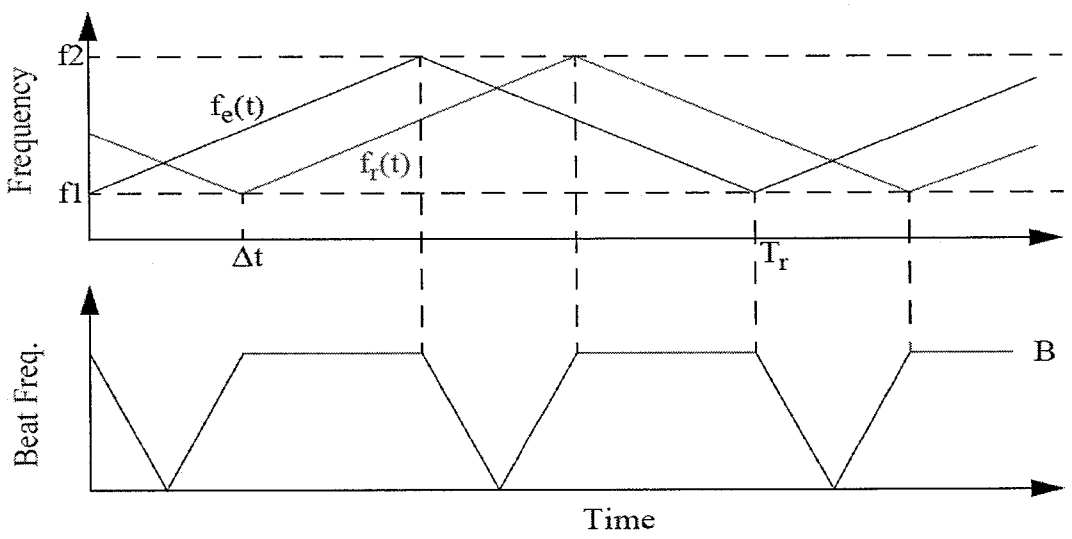


그림 3.10.16 FMCW 레이저의 맥놀이 주파수 및 대표적인 첩(chirped) 파형

그림 3.10.16에서 FMCW 레이저의 맥놀이 주파수 및 대표적인 첩(chirped) 파형 fc(t)는 방출된 주파수, 그리고 fr(t)는 수신된 주파수이다. B는 측정정 침두 맥놀이 주파수이다. Δt는 반사된 신호의 지연 값이고, Tr은 주파수 첩(chirp) 기간이다.

목표물까지의 거리는 다음과 같이 계산한다:

$$z = \frac{c\Delta t}{2} = \frac{cBT_r}{4\Delta f}$$

위 식에서 FMCW 레이저의 거리 c 계산. c는 빛의 속도이고 B는 맥놀이 주파수, Tr은 주파수 스윕(sweep)의 변화량이다.

FMCW 레이저용 시스템 매개변수 선택에는 수많은 경쟁 요소가 있다. 적절한 맥놀이 주파수 B는 그 시간 중 일부 동안에만 측정할 수 있음을 유의해야 한다. 그것의 측정이 불가능한 경우에, 시간 길이 Δt를 우리는 불감시간(不感時間, dead time)이라고 부른다. 불감시간의 분율(分率, fraction)은 2Δt/Tr이고, 이론 최대 측정 가능 거리는 zmax=(cTr)/4인데, 그 때에 B점은 단일 순간에만 측정할 수 있다. 소음을 줄이기 위해서는, 불감시간이 가능한 작게 되도록 Tr을 비교적 크게 하고 또 맥놀이 주파수를 측정하기 위한 표본채취 가능 시간을 증가시키는 것이 중요하다. 그러나 Tr이 짧게 되면, 센서의 잠재적 데이터 수집 율이 증가한다. 실제로는, 레이저 시스템의 최대 거리를 센서 파워와 소음 레벨로 관리하는데, 이것은 이론적 최대값에 가까워 지지 않는다.

시스템이 측정할 수 있는 최소 거리는 맥놀이 주파수 신호의 표본을 적절히 채취하는데 소요되는 시간에 따라 다르다. 베이진(Bazin) 및 저네트(Journet)은 맥놀이 신호 주기의 반(1/2)이 필요하여, 결국 zmin = c/(4Δf)로 된다고 주장한다. 따라서 swept 주파수가 더 커지면 작은 거리를 탐지하기는 더 쉬워지지만, swept 주파수를 증가시키면 필요한 필터 대역폭이 증가되고 또 첩(chirp) 파형의 비선형성(非線形性)이 유도되는 경우가 발생하는데, 이것은 그 다음에 거리를 불량하게 추정하는 원인이 된다.

㉯ 주파수 변조식 연속파

진폭 변조식 연속파((Amplitude Modulated Continuous Wave, AMCW)는 AMCW 레이저의 작동은 방출된 빛의 파워를 어느 주어진 주파수의 사인(sine)파로 변조하는 것이다. 복귀한 에너지 파형은 이동 시간 Δt 만큼 지연되고 또 방출된 에너지와 비교하면 이것의 위상이 비례적으로 이동된 것으로 나타난다. 거리는 위상에 비례하는데, 위상차가 2π인 때에 애매성(曖昧性)이 최대가 된다.

$$z = \frac{\phi}{2\pi}\Delta R$$

위 식에서 거리 z는 위상차 Φ 및 애매성 간격 ΔR에 비례한다. 위상의 애매성은 애매성 간격이라고 부르는 거리 크기 ΔR의 유사한 애매성으로 귀착된다. 거리 x+ΔR에서의 목표물까지는 거리 x에서 측정한다.

거리와 반사율을 극좌표로 표시하면 다음과 같다:

$$Ie^{i\phi} = \iint cI(\theta, \alpha)e^{i\phi(\theta, \alpha)}d\theta d\alpha$$

위 식에서 복귀한 신호의 위상 Φ 및 세기 I는 신호 에너지를 순간시야(瞬間視野)(IFOV)에 대해서 적분한 것이다. Θ는 방위각이고 α는 복각(伏角)이다.

위상을 레이저의 순간 시야에 대해서 일정하다고 가정하면, 최종 위상은 각 성분의 위상과 같고 또 세기는 각 dΘ 및 dα에 대한 개별 기여도의 단순한 합(合)이다. 이 가정이 거짓인 경우에는, 바람직하지 않은 결과가 발생할 수 있다. 이 가능성은 혼합된 픽셀에서 논의할 수 있다. 그림 3.10.17은 거리와 세기 값 사이의 기하학적 관계를 표시하는 것이다.

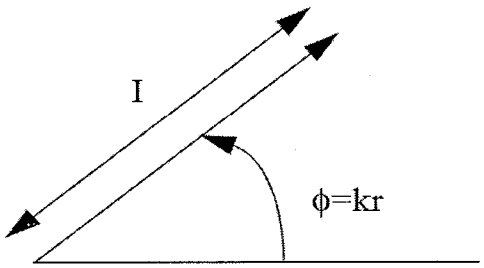


그림 3.10.17 수신된 레이저 신호의 페이저(phasor) 다이어그램

그림 3.10.17은 수신된 레이저 신호의 페이저(phasor) 다이어그램이고, I는 세기이고, Θ는 신호 위상, 그리고 r은 목표물까지의 거리이다. k는 비례상수다.

Z+F 레이저는 이중 주파수 진폭 변조식 신호를 사용하여 일반적 AMCW 방법을 개선한다. 수신기는 양 변조 주파수에서 복귀한 레이저 신호와 원 신호 사이의 위상차를 측정한다. Z+F 레이저는 변조 주파수 2개가 결합된 것을 사용하여 표준 단일 변조 스킴(scheme)에 대한 정확도를 개선시킨다. 높은 주파수 변조(23 MHz)의 위상 쉬프트(shift) 값의 12-bit 정확도에 의한 거리의 해상도는 다음과 같다:

$$\Delta r = \frac{c}{2^{(b+1)}f} = 1.6 \text{ mm}$$

위 식에서 거리의 해상도 Δr은, 광속도 c, 위상차 정확도 bit 수 b=12, 그리고 변조 주파수 f=23 MHz에 의해서 결정된다.
낮은 주파수 변조(2.875 MHz)의 위상 쉬프트를 이용하여 높은 주파수의 여러 사이클들 사이의 애매성을 제거하고, 또 이것은 다음과 같이 표시되는 전반적 애매성 간격을 허용한다:

$$\Delta R = \frac{c}{2f} = 52.2 \text{ meters}$$

상기 식에서 애매성 간격 ΔR은 광속도 c, 및 변주 주파수 f=2.875 MHz에 의해서 결정된다. 채널 2개를 결합시키면, 명백한 거리 52m에 대한 해상도를 효과적으로 15-bit가 되게 한다. 레이저의 전반적 정확도는 +/- 2cm이고, 또 어둠 속에서 최대 100m까지를 볼 수 있다. 거리측정 이외에, 각 픽셀의 레이저 반사율 값은, 높은 주파수 채널로 결정되는 16-bit이다. Z+F 센서는 매우 빠르다. 즉 그것은 매 초 500,000이나 되는 높은 픽셀 율로 작동할 수 있다. Z+F 레이저를 사용하면, 스캐너는 시야각(視野角) 30도 x 360에 대해서 최대 6000 열(列) x 수백 행(行)의 이미지를 만들 수 있는데, 이것의 각(角) 해상도는 매 픽셀마다 0.06°이다.

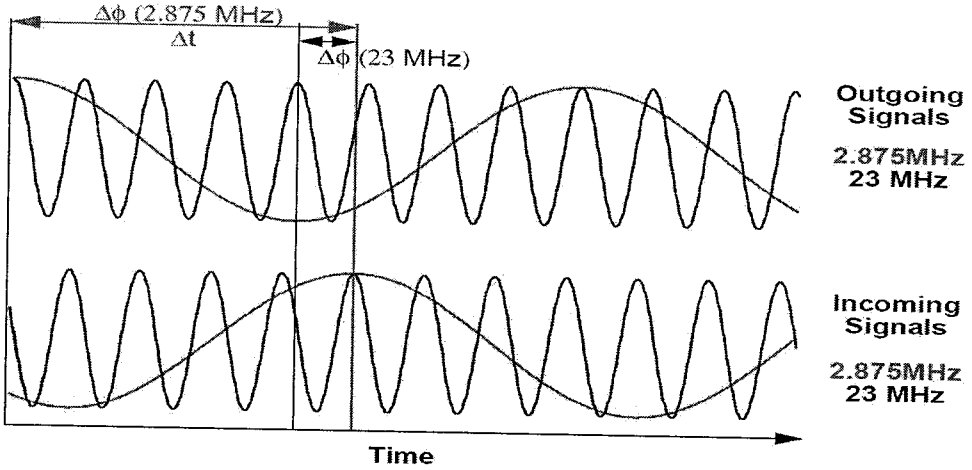


그림 3.10.18 다른 2개의 변조 주파수

그림 3.10.18에서 거리계산의 기초는 서로 다른 2개의 변조 주파수에서 복귀한 신호와 나가는 신호 사이의 위상차를 측정하는 것이다. 2.875MHz 신호의 위상차는 그 애매성 간격이 52m인데, 이 위상차를 사용하여 23MHz 신호의 애매성을 제거하는데, 이것으로 거리의 해상도는 크게 개선된다.

③ 시스템 구조

다음의 그림 3.10.19와 그림 3.10.20는 3D 레이저 레이더의 전체적인 시스템 구조를 보인 것이다. 이 시스템은 크게 레이저 레이더 해드(raser radar head)와 제어기(controller)부로 구성되어 있다.

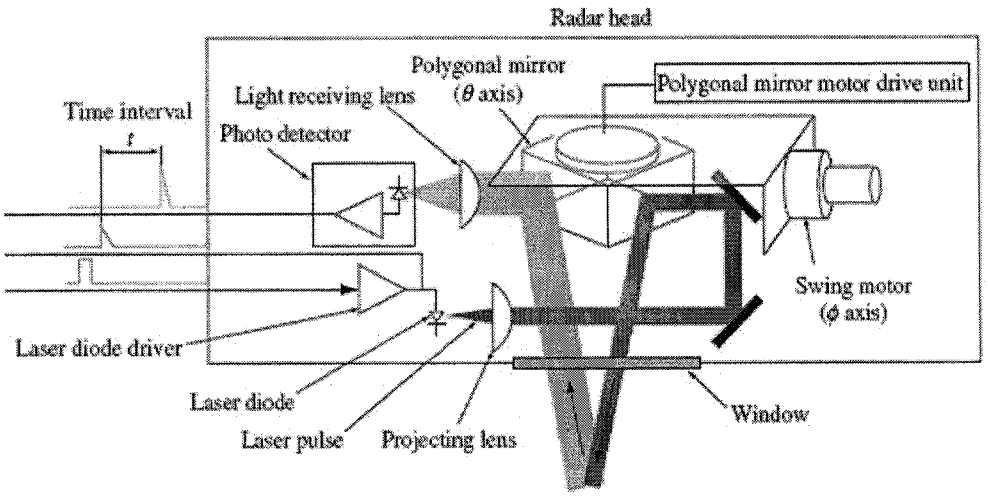


그림 3.10.19 3D 레이저 레이더의 장애물 검출 시스템 구조(1)

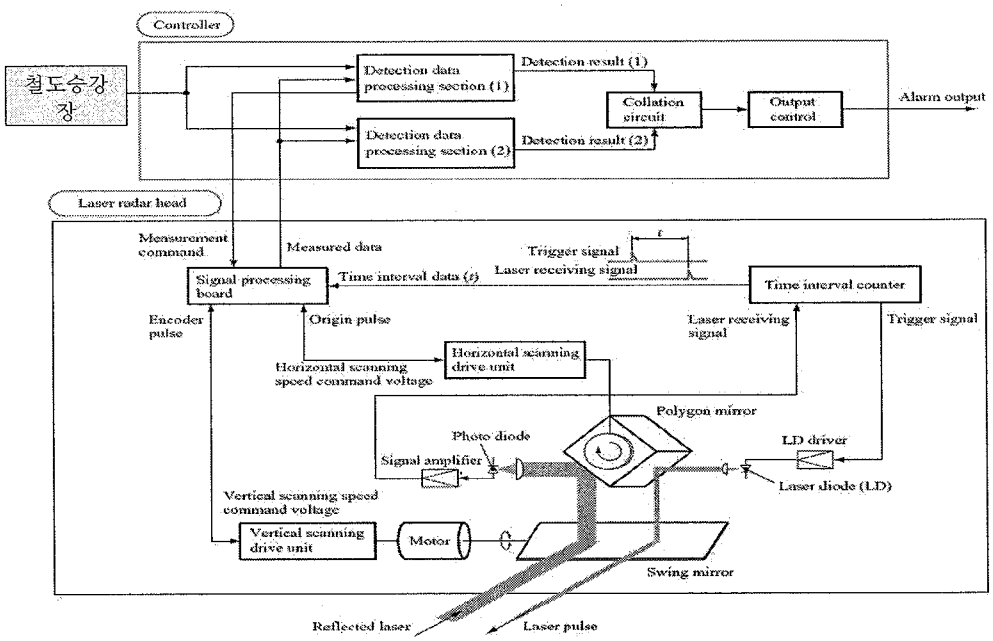


그림 3.10.20 3D 레이저 레이더의 장애물 검출 시스템 구조(2)

레이저 레이더 해드는 매 초마다 2번씩 수평 및 수직방향의 전체 영역을 스캔하는 레이저 펄스를 만들기 위해 다각형거울(polygon mirror)과 스윙거울(swing mirror)을 통해 레이저 펄스를 송출한다. 물체로부터 반사되어 돌아온 레이저 신호는 고감도 포토다이오드(photo diode)를 통해 고속으로 전기신호로 변환된다.

Time Interval Counter는 포토다이오드에 의해 생성된 레이저 수신신호의 출력과 레이저 펄스를 송출하기 위한 트리거 신호사이의 시간 간격에 기초하여 물체와의 거리를 측정한다. 일반적으로 Time Interval Counting 방식은 레이저의 발사 및 검출시간 사이에 발생한 펄스의 수를 세어 시간을 측정하는 방식이며, Epoch Event Timer 방식은 레이저의 발사 및 검출 사건(event)이 발생한 시각(epoch time)을 기록한 후 두 시간 차이를 구하여 시간을 측정하는 방식이다.

이들 중 Epoch Event Timer는 Time Interval Counter방식과는 달리 Counting의 한계가 없고, 측정의 한계 및 count의 reset에 소비되는 시간이 없어, High Frequency 및 장거리 거리 측정기에 적합한 반면 장비가 고가인 것이 단점이다.

신호처리보드(signal processing board)는 다각형거울과 스윙거울의 모션을 제어하며, 3차원 공간 데이터를 측정한다. 이들 측정된 3차원 공간데이터는 제어기내 검출데이터처리부(detection data processing section)로 보내진다. 검출데이터처리부에서는 물체의 인식과정이 실행되고, 장애물인지 아닌지를 순간적으로 판단한다. 만일 장애물로 판단되었을 경우에는 알람을 발생한다. 이 시스템에서 검출과정을 처리하는 하드웨어는 2중화로 되어 있어 고장 안전 기능을 확보하고 있다.

3차원 레이저 레이더는 그림 3.10.20에서 보여주는 바와 같이 레이더 헤드와 제어기로 구성되어 있다. 레이저 다이오드로부터 방사되는 레이저 펄스는 투사하는 렌즈에 의해 평행광선으로 만들어지고 회전/진동 다각형 거울에 의해 2차원 방향에서 주사된다. 물체로부터 반사된 펄스 레이저 광선은 빛을 받아들이는 렌즈에 의해 다각형 거울을 통하여 모아지고 광검파기에 의해 전기신호로 변환된다.

제어기에 있는 시간간격 카운터는 레이저 다이오드의 펄스를 만드는 시기와 동기화된 개시 펄스와 광검파기로부터 방사되는 중단 펄스의 시간간격을 측정한다. 신호처리판은 반사된 빛이 검지된 때에 시간간격 데이터 t를 출력하며 또한 극 좌표계 데이터(t, Θ, ø)로서 다각형 거울의 회전각 Θ와 스윙 각 ø을 출력한다. 결정처리장치는 신호 처리판으로부터 극 좌표 데이터를 그 근원으로서 레이더 헤드셋 위치와 함께 3차원 공간 데이터(X, Y, Z)로 변환시키며 인지 처리를 수행한다.

(다) 시스템 운용 조건

① 일반요구사항

- 환경조건

다음은 한국철도에 대한 환경조건이다. 공급자는 설계 가이드라인과 운용 요구조건으로서 다음 환경기준을 적용한다.

· 외 기 온 도 : -35℃~+40℃

· 상 대 습 도 : 5%~100%

· 최대 폭우량 : 120㎜/h (414㎜/day)

· 최대 풍속도 : 45㎧(연속), 50㎧(순간)

· 최대 폭설량 : 125㎜/h (296㎝/day)

- 승강장 선로조건

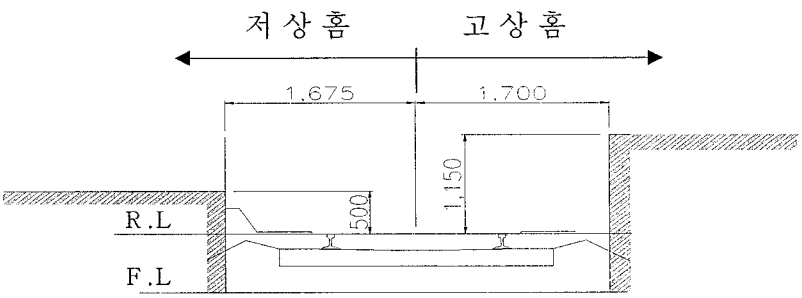


그림 3.10.21 승강장 유형

③ 전력공급

· 공급전원 : AC 220V, 60Hz

④ 장애물 검지 조건

승강장에서 추락자 또는 장애물 검지시스템에 대한 연구는 일찍이 오사카시 교통국에서 추락자 방지대책으로 2002년도부터 개발한 연구 내용을 발췌하여 한국철도차량의 시설이 맞도록 다음과 같이 정리하였다.

· 검지거리

직선 기준으로 설치되는 승강장의 최대 길이 400m에서도 장애물 검지 정도가 저하되지 않아야 한다.

· 빔 조사 높이

레이저 레이더 센서의 빔 조사 높이는 주어진 승강장 거리의 레일상면에서부

터 약 15cm 이상 위에 설정한다.

· 장애물의 최소 크기

승강장 선로의 장애물의 최소 크기는 200×200mm의 물체를 주어진 승강장 검지 거리에서 검지가 가능하여야 한다.

· 낙하물에 대한 오정보 방지

레일 상면에서부터 약 15cm 이상에서 순시로 통과하는 것을 낙하물, 일정시간(ex : 5~10초)경과하는 것을 추락자로서 인식하여 추락자와 낙하물(휴지, 가방 등의 휴대물)의 판별이 가능토록 한다. 또한 비둘기, 개, 고양이 등과 같은 추락자 이외의 물체와 구별이 가능해야 한다.

표 3.10.10 승강장 제원

항 목		기 준	비 고
궤 간		1,435mm	
곡선반경		직선, L=0	최소 1200m 이상
선로의 기울기(정거장)		없음(2‰이하)	
선로의 중심간격(정거장)		4.3m이상	
유 효 장		600m이상	
승강장의 폭	섬식	8m 이상	
	상대식	5m 이상	
승강장 높이	고상홈	레일면에서 1150mm	
	저상홈	레일면에서 500mm	
승강장 끝과 선로중심의 간격	고상홈	승강장 끝에서 1700mm	
	저상홈	승강장 끝에서 1675mm	
승강장 시설물	각종 기둥	1.0m이상	기둥: 승강장 끝에서 1.0m 이상
	벽 체	1.5m이상	벽 구조물: 승강장 끝에서 1.5m 이상
선로중심과 승강장 등과의 거리		1,675mm	

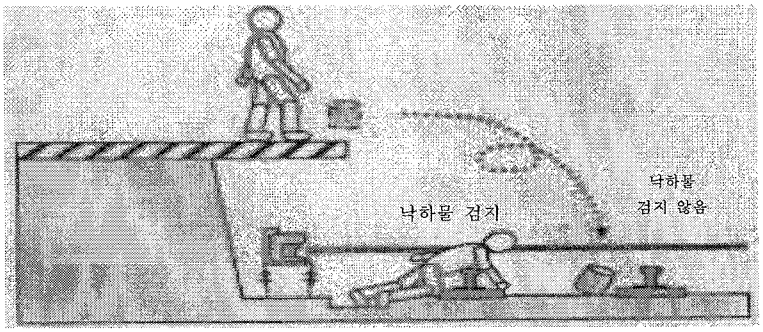


그림 3.10.22 낙하물 검지

- 추락자와 열차 보수원을 식별하기 위한 영역 설정
  · 레이저의 특성상 감시영역내의 모든 물체에 대해 검지신호를 출력하기 위해 유지보수요원이나 열차를 검지하여 출력한다.
  · 승강장 선로에 추락한 사람만을 구별하기 위해서는 레이저 센서의 영역설정 기능을 이용하여 A, B, C의 3개 영역으로 구분하여 분할하고 각각의 검지신호의 조건을 조합하여 추락자가 어떠한지를 판정하는 로직을 구성한다.
  · B영역은 승강장에서 사람이 추락했을 때 추락자 검지 영역을 상정한 위치로 영역폭을 설정하고 그 사방을 포함할 수 있게 보수원 열차검지용 A, C영역을 설정한다.

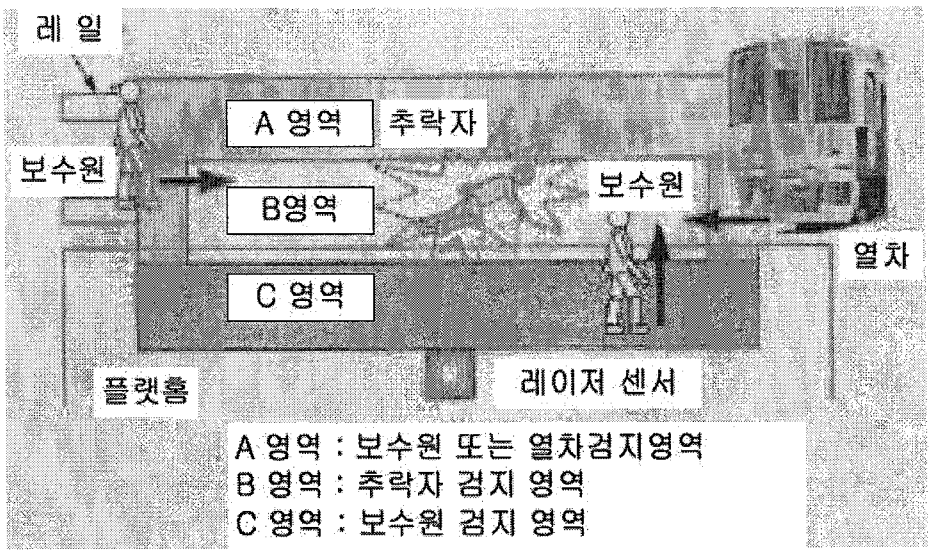


그림 3.10.23 레이저 센서의 감시영역

· 제어장치에는 레이저 센서의 영역구분 검지신호를 근거로 추락자가 판단을 수행하는 논리부가 있다. 논리구조는 보수원이 영역내를 이동할 경우에는 필히 A영역→B영역, C영역→B영역으로 이동한다.

· 레이저 센서의 검지신호는 A→B 또는 C→B로 변화한다. 이 신호변화를 "보수원"으로 판정한다. 즉, A영역 또는 C영역으로부터 이동한 유지보수원이 B영역에 진입해도 추락자 경보는 진행되지 않는다.

· 열차도 A영역→B영역으로 이동하기 때문에 레이저 센서의 검지신호는 A-B로 변화한다. 이러한 신호변화를 "열차"로 판정한다.

· 사람이 승강장으로부터 추락하면 직접 B영역으로 들어오게 되며 레이저 센서의 검지신호는 B신호를 출력하고 "추락자"로 판정한다. 즉, 추락자가 그 이후 A영역이나 C영역으로 이동해도 추락경보는 계속 진행된다.

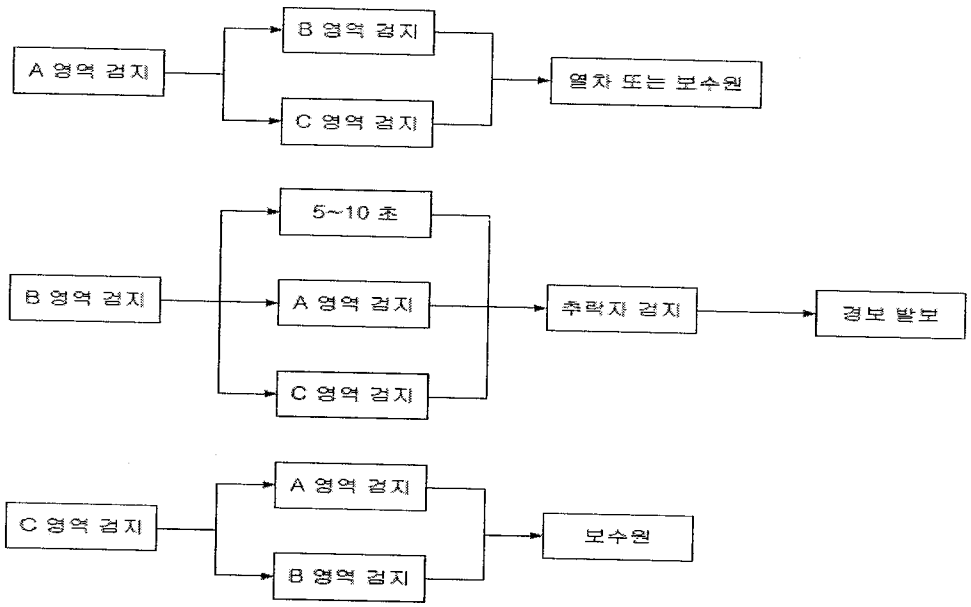
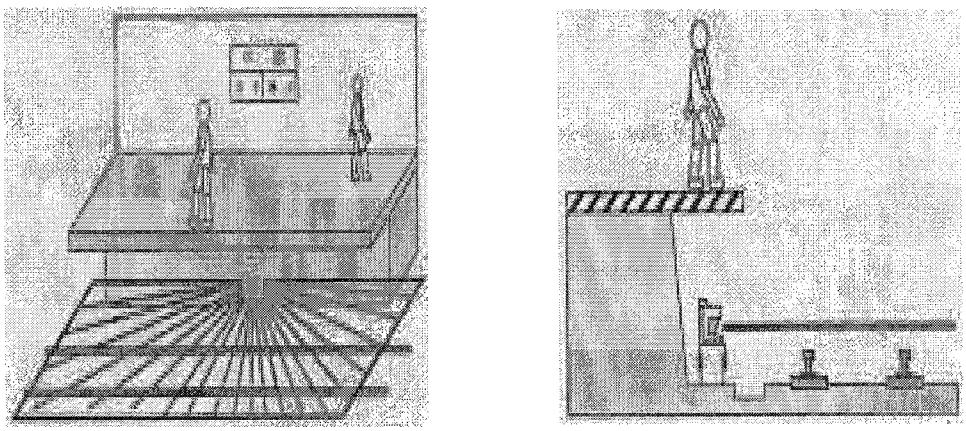


그림 3.10.24 레이저 센서의 감시영역 동작 계통도

⑤ 설치조건

· 승강장 하부에 설치 시

승강장 하부에 설치시, 레일 상면에 레이저 레이더 광을 조사할 수 있게 설정한다. 조사 각도는 구조물의 특성에 맞도록 조정이 가능해야 한다.



(a) 평면 (b) 단면

그림 3.10.25 설치 모형도(승강장 하부)

· 승강장 외측에 설치 시

승강장 외측에 설치시, 레일 상면에 레이저 레이더 광을 조사할 수 있게 설정한다. 조사 각도는 구조물의 특성에 맞도록 조정이 가능해야 한다. 또한 여분의 카메라(camera)는 사건(event)이 발생할 경우, 영상의 저장, 현장관측 등에 사용되는 장애물 검지기의 보조장치이다.

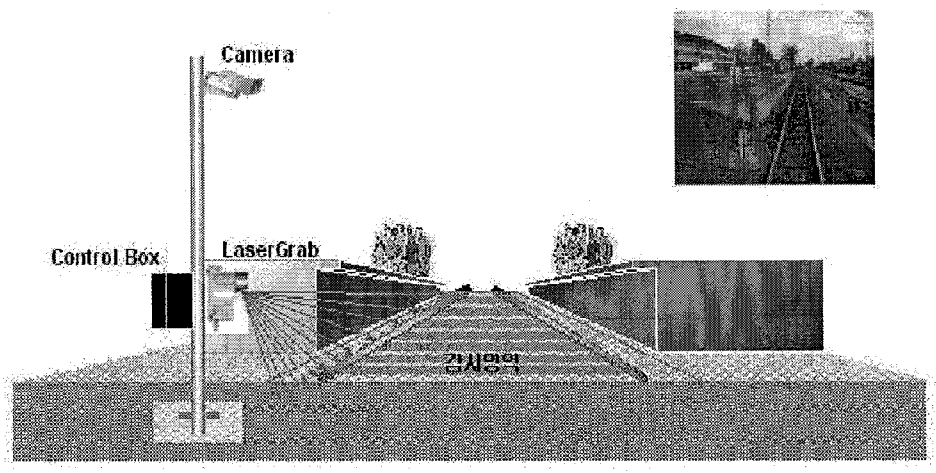


그림 3.10.26 설치 모형도(승강장 외측)

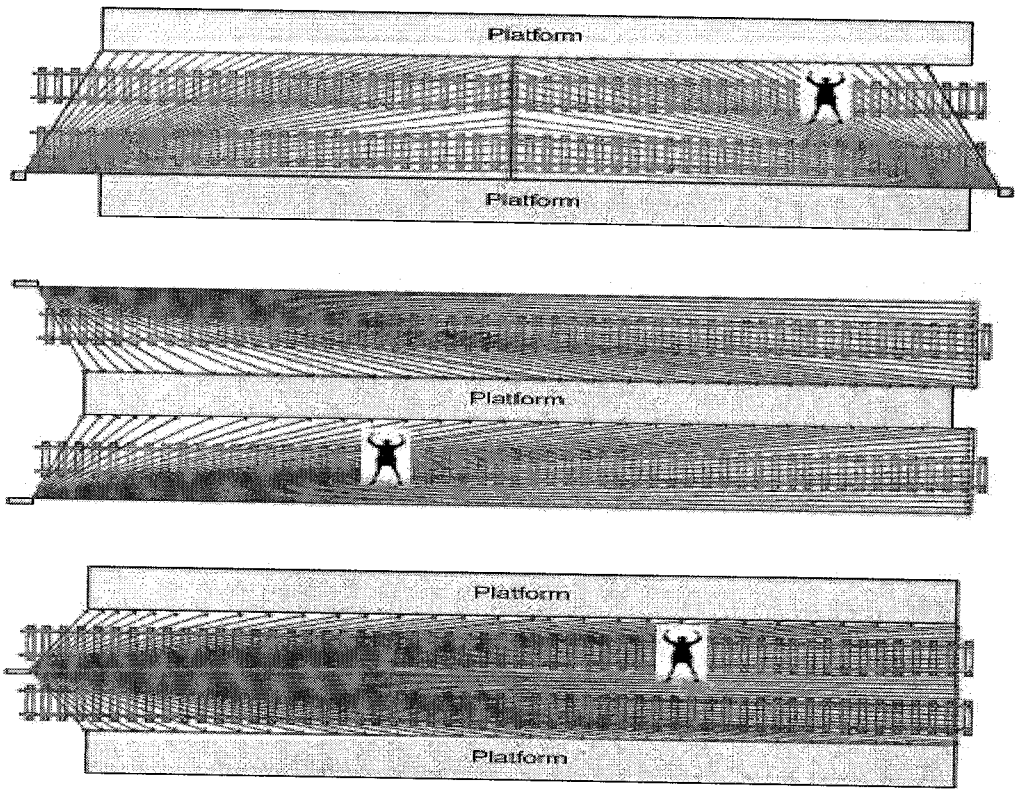


그림 3.10.27 3D 레이저 레이더 스캔(승강장 외측)

② 시스템 기능 설계

- 시스템 구성

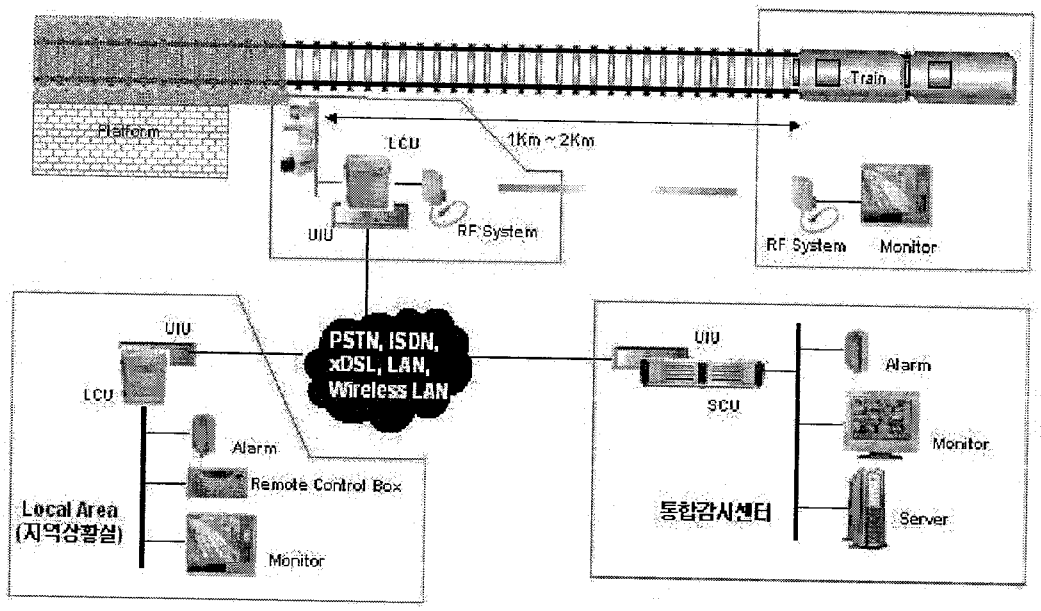


그림 3.10.28 승강장 선로 장애물 검출시스템 구성도

- 기능 및 성능

㉮ 하드웨어

· LaserGrab((Laser Scan Unit): Laser Radar System으로 특정 지역을 Scan하여 물체를 포착/감시하는 기능을 수행하며, LCU와 연동하여 3D 이미지 분석/제어 및 경보를 발생한다.

· LCU(Local area Control Unit): LaserGrab과 영상카메라를 제어하며, PC와 연동하여 원격 제어에 따른 명령을 수행한다.

· UIU(User Interface Unit): LCU와 PC 사이에 구성되는 다양한 통신 매체와의 연동을 담당하며, 사용자 요구에 맞게 구현되는 통신 정합을 담당한다.

㉯ 소프트웨어

· Linux Server를 이용한 시스템 통합관리

· Scan 이미지 분석 및 경보 발생

· 감시 영역 내 물체의 정확한 식별 및 감시

· 필요시 타 보안시스템과의 연동 및 통합 가능

· 고객 요구사항에 대한 보완/수정/추가 개발

- 인터페이스

㉮ 차량과의 연계

· 추락자 또는 장애물을 검지하면 열차무선전송장치(RF system)를 통하여 승강장으로 진입하는 열차로 사건 정보를 전송할 수 있는 단자 및 기능을 가지고 있어야 한다. 전송 주파수는 10-30GHz 내에서 별도 협의한다.

㉯ 비상 신호 정지장치 연계

· 추락자 또는 장애물을 검지하면 그 검지 신호를 비상 신호 정지장치와 연계할 수 있는 출력 단자를 가지고 있어야 한다.

㉰ MMI 인터페이스

· MMI를 위한 기본 문자는 영어를 우선으로 하며, 필요시 한글로 변환이 가능할 수 있는 구조로 설계되어야 한다.

(다) EMC 요구사항

· 공급되는 기기 및 그 설치는 철도 어플리케이션 전자파 적합성에 관한 표준

(예, EN 50121) 요구 사항을 만족시켜야 한다.

- 모든 재료 및 기기는 다른 기기(철도 부품 여부에 상관없이)에 의해 전자파 간섭(EMI) 영향 하에서도 지속적으로 올바르고 안전하게 작동해야 한다. 공급자는 그와 같은 EMI 소스를 규명하고, 전자파 적합성(EMC)을 보장할 수 있도록 적절한 심사, 차폐 또는 기타 구제책을 제공해야 한다.
- 공급되는 기기의 모든 구성품은 전차선 전압(25kV, 60Hz) 또는 다른 간섭원으로부터 안전해야 한다.
- 공급되는 기기 구성품에 대해 근방에서 동작하는 가정용 혹은 산업용 설비와 같이 여러 소스로부터의 원하지 않는 간섭을 제거하거나 또는 그 동작에 영향을 미치지 않도록 보장해야 한다.
- 공급되는 기기는 작동 시 허용 수준을 넘는 전자파가 방사되지 않아야 한다.
- 공급자는 모든 기기, 재료 및 설계가 전자파 적합성을 갖는다는 것을 입증하는 자료를 제출해야 한다.

(라) 접지 및 낙뢰보호

- 공급되는 기기는 낙뢰에 대한 접지 및 보호 방법과 관련된 국제 표준의 요구사항을 만족시켜야 한다.
- 공급되는 기기는 과전압뿐만 아니라 낙뢰에 의해 철도 전원 회로에 생기는 간섭과 전압 스파이크 등에 대해서 견딜 수 있어야 한다.
- 공급되는 기기는 궤도 및 철도 전원 선로를 따라 설치되므로 25KV 60Hz로부터 생기는 전기 간섭 및 과전압에 대비하여 차폐되어야 한다.
- 공급자는 모든 기기, 재료 및 설계가 접지 및 낙뢰보호에 대해 적합성을 갖는다는 것을 입증하는 자료를 제출해야 한다.

(마) RAMS 요구사항

- 공급되는 기기는 철도용 전기설비의 신뢰성, 가용성, 유지보수성, 안전성(RAMS)에 관한 국제 표준(IEC 62278) 요구 사항을 만족시켜야 한다.
- 각 장치들은 최대한의 신뢰도를 보장할 수 잇도록 설계되어야 하며, 주어진 환경에서 요구하는 기능을 수행할 수 있어야 한다.
- 어떠한 환경에서도, 시스템은 안전하게 작동되어야 하며 안전한 방법으로 배

치되어야 한다.

- 시스템의 가용도는 최소 99.99%를 유지하며, 그 이상이어야 한다.
- 진단장비에 의해 제공된 자가진단 데이터(Self-Diagnostics Data)를 기반으로 한 시스템을 유지보수하기 위한 시스템은 운용 및 유지보수 요원들을 위해 설계되어야 한다.
- 시스템은 보드 또는 모듈이 교체될 때 전체 시스템의 재시험을 최소화하기 위해 설계되고 제작되어야 할 것이다.
- 시스템에 결함이 발생하였을 경우, 자격을 갖춘 요원이 유지보수 작업을 하였을 때, 이러한 결함의 유지보수는 최소 30분 이하로 이루어져야 한다.

(바) 장애물 검지영상처리

① 개요

영상처리란 영상을 대상으로 하는 신호처리(Signal Processing)의 한 분야로써, 영상으로부터 원하는 정보를 얻기 위해 행하는 모든 종류의 처리를 의미한다. 영상처리 분야에서 주로 다루는 분야는 영상의 화질 향상, 소실된 정보의 복원, 데이터의 압축, 영상의 인식 등이 있다. 대부분의 영상 처리 기법은 화상을 2차원 신호로 보고 여기에 표준적인 신호 처리 기법을 적용하는 방법을 사용한다.

디지털 영상 처리 기술의 대부분은 1960년대 제트 추진 연구소, MIT, 벨 연구소, 메릴랜드 대학교 등에서 개발되었는데, 위성영상, 유선사진 표준 변환, 의료 영상, 영상전화, 광학문자인식, 그리고 사진개선 등에 응용된다. 그러나 처리 비용이 그 시대의 컴퓨터 장비로는 꽤 고가였다. 1970년대 값싼 컴퓨터와 전용 하드웨어가 이용 가능해지면서, 디지털 영상 처리는 급격히 증가하였다. 그 후 텔레비전 표준 전환과 같은 몇몇 전용 문제를 위해, 영상은 실시간으로 처리 가능하게 되었다. 범용 컴퓨터가 빨라지면서, 그것들이 가장 특화되고 컴퓨터 집약적인 작업을 위한 전용 하드웨어의 역할을 떠맡기 시작했다. 2000년대 빠른 컴퓨터와 신호 처리가 가능해지면서, 디지털 영상 처리는 영상 처리의 가장 일반적인 형태가 됐고, 방법이 다양할 뿐만 아니라, 가격도 저렴하기 때문에 일반적으로 사용되고 있다.

② 영상처리 시스템의 구성

㉮ 일반적인 디지털 영상처리 단계

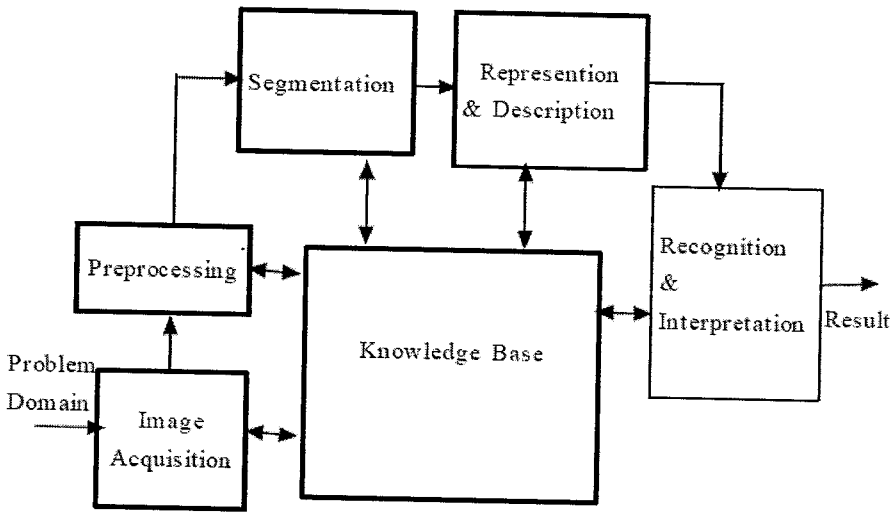


그림 3.10.29 일반적인 디지털 영상처리 단계

일반적으로 넓은 의미의 디지털영상처리는 영상획득, 전처리, 세그멘테이션, 해석, 인식의 단계로 이루어진다. 이 중에서 영상 획득부분과 전처리 부분만을 좁은 의미에서 영상처리라고 하며, 나머지 부분을 영상인식이라고 한다. 처리영상 획득(Image Acquisition) 부분은 디지털 캠코더나 카메라, 스캐너 등을 이용해서 영상처리에 사용할 수 있는 영상 데이터를 만드는 부분이다. 영상 데이터는 BMP와 같이 디지털 형태로 저장된다. 이 영상은 물리적 장치에서 얻어진 그대로 사용할 수도 있지만 일반적인 경우는 각종 필터나 히스토그램 이퀄라이제이션(Histogram Equalization)등의 방법을 이용하여 노이즈를 제거하거나 인식에 더 유용한 영상으로 만드는 과정이 추가된다. 이것을 전처리(Preprocessing)라고 한다. 영상의 전처리는 꼭 필요한 절차는 아니며 영상의 상태나 인식 목적에 따라 생략 될 수도 있다. 전처리까지 마친 영상은 실제 처리에 이용된다. 대부분의 영상처리에서는 영역 및 물체(Object) 추출(Segmentation)이 중심이 된다. 즉, x , y방향의 Projection이나 가능한 필터를 사용하여, 이미지 내부의 경계선(boundary)이나 영역 정보를 구하게 된다. 이런 정보는 사람이 보기에 명확하지 못하다. 따라서 사람에게 맞도록 정보의 해석(Representation & Description)이 필요하게 된다. 마지막으로 원하는 결과에 적합하도록 인식하고 해석하면 된다.

㈏ 흐름도

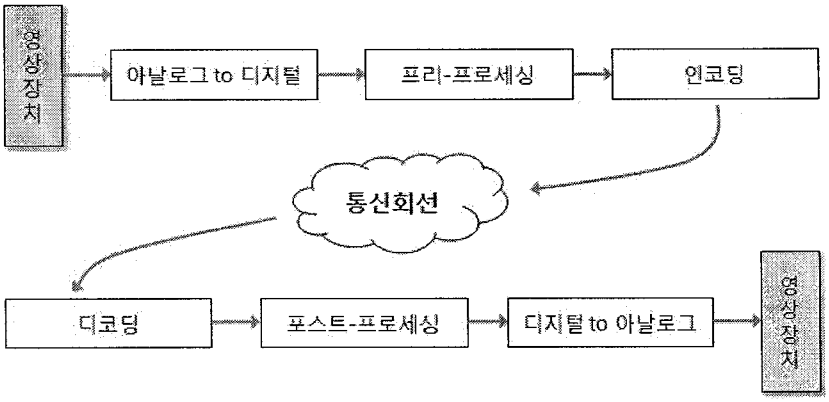


그림 3.10.30 영상장치 흐름도

일반적으로 영상이 입력된 데이터를 다른 장치에 보이기 위해서는 통신장치를 이용하여야 한다. 통신을 위해서는 먼저, 아날로그 데이터를 디지털 데이터로 변경해 주는 과정이 필요하다. 모든 전송은 아날로그가 아닌 디지털 정보를 가지고 전송이 되기 때문에 필수적이다. 이렇게 변환된 데이터를 논리적 오류를 최소화 하고 프로그래밍의 단순화 및 용이성을 한 단계 높이기 위해 프리프로세서를 이용하여 통일된 언어로 맞추는 등의 일을 수행한다. 다음으로 보안을 위해 인코딩을 함으로써 전송준비가 완료된다. 그렇게 만들어진 데이터를 통신회선 등과 같은 장치를 통해 전송한 후 통신이 이루어지면 데이터를 다시 영상정보로 확인하기 위해 반대되는 과정이 필요하게 된다. 이 과정에서 디코딩, 포스트-프로세싱, 디지털에서 아날로그로의 변환이 이루어지고 전송이 완료된다.

㉯ 처리순서

영상처리에서는 신호가 가지고 있는 유용한 정보 또는 파라메터를 이용하여 원하는 처리결과를 나타낸다. 여러 가지 영상을 전기적인 신호 형태로 변환한 후 이를 컴퓨터로 처리할 수 있는 디지털 형식으로 변환하여 원하는 처리 알고리즘을 수행함으로써 원하는 결과를 얻을 수 있게 된다. 즉, 원하는 정보를 추출, 전달, 축적하거나 시스템을 관측, 제어할 수 있도록 신호에 어떤 가공처리를 수행한다. 기본적으로 영상이 입력 된 후 그 결과를 나타내기까지의 과정은 그림 3.10.31와 같다.

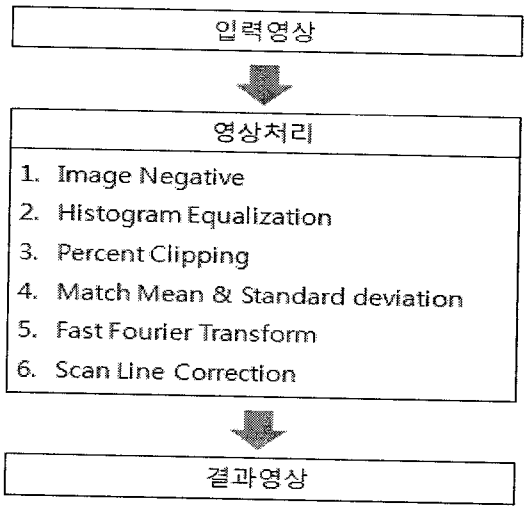


그림 3.10.31 영상처리 과정

③ 감시 시스템에서의 영상처리

㉮ 동영상 파일

동영상의 확장자는 AVI로 저장되는데 Audio Video Interleaving의 약자이다. AVI 파일 포맷은 오디오와 비디오를 함께 포함할 수 있으며, 여러 개의 오디오 또는 비디오 스트림을 가질 수 있다. 압축하지 않은 비디오와 압축된 비디오 포맷을 동시에 지원하며 압축된 비디오 포맷의 AVI 파일은 해당 압축 방법을 해제할 수 있는 코덱이라는 프로그램이 필요한 경우도 있다.

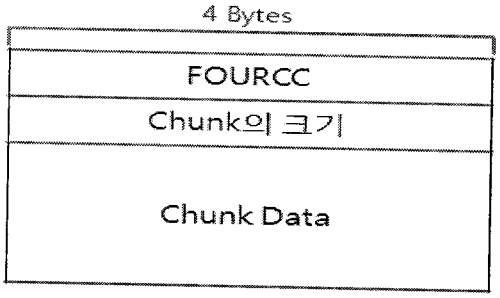


그림 3.10.32 영상 파일 포맷

AVI 파일 포맷은 RIFF의 특별한 형태로 청크(Chunk)라고 불리는 데이터의 단위로 나눠지며, 각각의 청크는 AVI파일의 영상코덱을 구분하는데 쓰이는 FOURCC(Four character code)라는 4개의 문자로 이루어진 코드로 구분된다. AVI

나 WAV 파일의 음성코덱 구분에는 2바이트가 사용된다. 그 다음에는 해당 청크의 크기를 나타내는 4바이트, 그리고 청크 데이터로 구성된다.

AVI 파일의 구조

```
RIFF('AVI '
      LIST ('hdrl'
            'avih'(<Main AVI Header>)
             LIST ('strl'
            'strh'(<Stream header>)
            'strf'(<Stream format>)
            [ 'strd'(<Additional header data>) ]
            [ 'strn'(<Stream name>) ]
            ...
            )
         ...
        )
      LIST ('movi'
             {SubChunk | LIST ('rec'
                               subChunk1
                               subChunk2
                               ...
                               )
             }
           )
       [ 'idx1' (<AVI Index>) ]
     )
```

㉯ 산술연산

산술연산이란 덧셈, 뺄셈, 곱셈, 나눗셈과 같은 기본적인 산수 계산을 의미하며 이러한 연산 방법은 영상에서도 유사하게 적용될 수 있다. 산술 연산 중 뺄셈을 이용하여 선로변 물체를 검지할 수 있다.

차이 연산은 두 입력 연산에 대하여 뺄셈 연산을 수행한 후, 그 결과값의 절대값을 이용하여 결과 영상을 생성하는 연산이다. 이를 수식으로 나타내면 다음과 같다.

$$h(x,y)=|f(x,y)-g(x,y)|$$

일반적인 뺄셈 연산의 경우 순서에 영향을 받기 때문에 뺄셈을 당하는 영상의 밝기가 전반적으로 어둡거나 뺄셈을 하는 영상이 전체적으로 밝을 경우, 결과 영상

의 그레이스케일은 0이 되거나 0에 가까운 값을 가지게 된다. 그러나 차이 연산은 순서에 상관없이 두 영상의 차이점을 그대로 나타낼 수 있는 장점이 있다. 그렇기 때문에, 차이 연산은 두 영상의 변화된 부분을 찾는 용도로 적합하다.

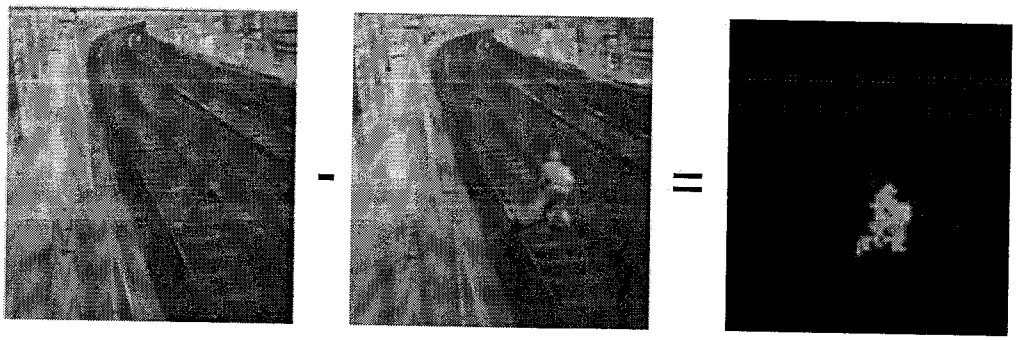


그림 3.10.33 차이연산을 통한 물체감지

그림 3.10.33은 영상의 차이를 연산을 이용하여 물체를 검출하는 예를 보여준다. 왼쪽의 영상은 물체가 없는 배경 영상이고, 두 번째는 사람이 선로변에 떨어진 경우를 보여준다. 이 두 영상을 이용하여 차이 연산을 수행하면 세 번째 영상과 같이 사람이 있는 부분이 두드러지게 된다. 이 연산을 이용하여 선로변에 사람이 감지될 경우 위험경보를 알리는 데 적용할 수 있다.

㉯ 감시 영역

승강장의 경우 단순히 배경 그림과의 비교만으로 위험상황을 판단하기는 어렵다. 영상의 감지도 중요하지만 감지하는 영역을 설정하고 그 영역에서만 물체를 인식, 판단해야 하기 때문이다. 승강장에서는 선로변 영역을 기준으로 하여 물체를 인식하고 감지하게 된다. 다음 그림은 선택된 영역을 나타낸 것이다.

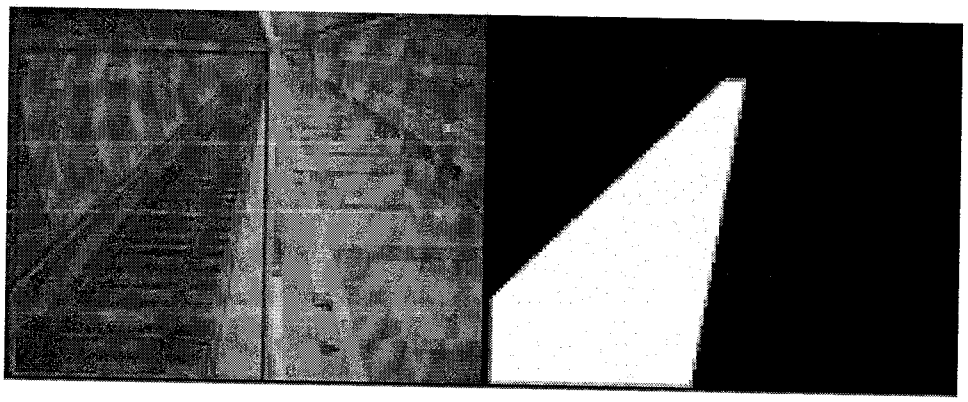


그림 3.10.34 승강장 감시영역 설정

④ 이동 물체 검지 기법

㉮ 영역분할 기법

영역분할 기법은 고수준의 이미지인식을 위한 기초적인 물체인식처리 기술 중의 하나로 알려져 있으며, 여러 물체인식처리 응용분야에서 반드시 필요한 필수적인 기술이라 할 수 있다. 일반적으로, 물체 인식처리에서 서로 다른 특징을 가지는 영역들을 분할하기 위해 다음과 같은 방법들을 주로 사용한다.

- 밝기값의 분포에 의한 영역분할
- 칼라정보에 의한 영역분할
- 텍스쳐 정보에 의한 영역분할
- 윤곽에 기반한 영역분할
- 영역에 기반한 영역분할
- 혼합 기법에 의한 영역분할

㉯ 영역분할을 위한 칼라와 텍스쳐 특징 추출

일반적으로 밝기값, 칼라 정보, 텍스쳐 정보 등과 같이 개별적인 특징만을 이용하여 영상을 분할할 경우에는 영상의 특성에 따라 성능에 큰 차이가 있을 수 있다. 즉, 칼라 정보를 이용하여야 좋은 결과를 얻을 수 있는 영상이 있는가 하면 텍스쳐 정보를 이용하여야 좋은 결과를 얻을 수 있는 영상이 있다. 따라서 이러한 칼라 정보와 텍스쳐 정보를 함께 고려하여 영역을 분할할 수 있는 기법을 개발함으로써 좀 더 정확하고 안정적으로 영역을 분할할 수 있도록 해야 할 것으로 판단된다.

㉰ 이동영역의 군집화를 통한 이동물체 검지기법

일반적으로, 이동 영역들은 하나의 이동 영역이 하나의 물체를 나타낼 수도 있으며, 다수의 이동 영역들이 하나의 물체를 나타낼 수도 있다. 따라서 거리가 근접하고 유사한 크기의 동작벡터를 가지는 이동 영역들을 군집화하여 개별적인 이동 물체를 감지하는 기법을 사용한다. 또한 이동 물체가 존재하는 영상에서 이동 물체에 해당하는 영역은 배경 영역보다 작은 부분을 차지한다. 그리고 이동 영역으로부터 추출되는 동작벡터들은 유사한 값을 나타내며 공간적으로 근접하게 된다.

㉱ 이동 물체의 모델 생성

이동 물체 검지(추출)한 후에는 이동 물체와 배경을 대표할 수 있는 특징들로 각각의 모델을 생성해야한다. 이동 물체는 다음과 같은 특징들로 표현될 수 있다. 따

라서 이런 요소들의 대표값을 추출하여 이동 물체의 모델로 설정한다.

- 이동 물체 영역을 대표할 수 있는 칼라
- 이동 물체 영역을 대표할 수 있는 텍스쳐
- 이동 물체 영역의 크기
- 이동 물체 영역의 중심위치
- 이동 물체를 구성하는 영역의 개수
- 이동 물체가 실질적으로 이동한 거리
- 이동 물체가 존재하는 시간

(사) 영상자료의 저장 및 관리 시스템 구조

① 개요

데이터베이스에서 데이터를 저장하는 방법에는 여러 가지가 있는데, 이러한 저장 방식은 데이터의 저장이나 수정, 검색에 직접적인 영향을 미친다. 가령, 들어오는 순서에 따라 그 값이 무엇이든 간에 무조건 비어 있는 곳에 저장하는 방법은 아무래도 지정된 위치에 넣는 것보다 저장하는데 유리하다. 하지만 나중에 원하는 것을 찾기 위해서는 불리할 수밖에 없다. 나중에 찾기 좋도록 저장하는 형태는 상대적으로 저장할 때의 부하가 있겠지만 액세스 할 때는 유리하다. 이러한 면은 데이터의 저장 목적이나 활용 목적에 따라 결정해야 한다. 또한 저장된 다수의 파일은 후처리 작업이 많을 경우 자료의 누락 또는 변질이 발생할 가능성이 매우 높다. 또한 지역 등에 따라 여러 자료가 생산되기 때문에 자료들이 상충할 수 있다. 이러한 사항들을 모두 고려해야 하기 때문에 자료의 관리와 구조를 항상 고려해야 한다.

② 자료의 종류 및 특징

- 진본성(Authenticity)

기록이 그 취지와 맞는지, 그 기록을 생산하거나 보내기로 되어 있는 사람에 의해 생산되거나 보내졌는지, 명시된 시점에서 생산되거나 보내졌는지를 증명할 수 있는 것을 말한다. 진본성을 보장하기 위해서는 기록의 생산, 수령, 전달, 유지 및 처분을 통제하는 정책 및 절차 등이 문서화되어야 한다. 이를 통해 기록의 생산자가 확인될 수 있고 인가를 받았는지 증명할 수 있게 하며 기록이 인가받지 않은 접근에 의해 부가, 삭제 변경, 이용 및 은폐되는 것을 막아줄 수 있다.

- 신뢰성(Reliability)

기록의 내용이 업무처리, 활동 혹은 사실을 충분히 명확하게 표현하고 있다고 믿을 수 있는지, 그리고 이후의 업무처리나 활동을 수행하는 과정에서 근거로 할 만한 것인지를 의미한다.

- 무결성 (Integrity)

기록의 완전함과 변경되지 않았음을 의미한다. 즉, 무결성은 기록이 인가받지 않은 변경으로부터 보호되었을 때 충족될 수 있다. 인가를 받은 어떠한 주석, 추가 혹은 삭제도 명백하게 드러나야 하고 추적할 수 있어야 한다. 이를 위해서는 기록 수정시의 정책과 업무절차가 필요하다. 기록이 생산된 이후의 변경에 대한 정보를 포함하게 함으로써 기록물의 무단변경에 대한 추적이 가능하게 해야 한다.

- 이용가능성 (Usability)

기록의 위치를 찾을 수 있고, 기록이 검색될 수 있으며, 보일 수 있고, 해석될 수 있음을 의미한다. 기록과 그 기록을 생산한 업무처리, 행위 등이 연결되어 보일 수 있어야 하며, 일련의 활동과정에서 생산된 기록들 간의 연계성도 유지되어야 한다.

③ 영상자료의 보존 및 관리방법

영상자료 구축작업은 동영상이 모든 콘텐츠에서 활용될 수 있도록 가장 좋은 품질로 포맷 되어야 하며, 하드웨어나 네트워크 환경을 고려하여 가장 적절한 포맷방식으로 제작되어야 한다.

- 제작

· 기록보존 : 기록보존용 영상파일은 윈도우 운영체계에서 기본적으로 지원하는 AVI 원본파일과 DVD의 기본 포맷으로 제작한다.

· 최근/현재 영상 : 자료 압축 및 서비스 형태는 Real Media, Windows Media Player와 호환되어야 하며 서비스가 가능해야 한다. 또한, 현재의 환경에서 가장 적합한 방식의 포맷을 사용하여 제작할 수 있다.

- 파일형식의 특징

표 3.10.11 파일형식

파일형식	특 징
AVI	윈도우 운영체계에서 기본으로 지원하는 동영상 파일 포맷이다. 화질은 뛰어나지만 용량이 크기 때문에 인터넷 서비스를 위한 실시간 동

	영상에는 적합하지 않으며 기록보존용 파일의 원본으로 관리한다. 최근에는 MPEG-4 기술을 활용한 서비스용 AVI파일도 사용되고 있다.
MPEG-1	비디오CD를 제작하기 위한 압축기술로 사용되고 있으며, 320×240의 화면사이즈를 기본으로 압축된다. 기본적으로 채택되는 방식이다.
MPEG-2	디지털 TV, 대화형 TV, DVD 등은 높은 화질과 음질을 필요로 하는 분야에 MPEG-1을 개선하여 만든 것이다. 720×480DML 화면사이즈를 갖는다.
MPEG-4	낮은 전송률로 동영상을 보내고자 개발된 데이터 압축과 복원기술에 대한 새로운 표준이다. 매초 64Kbps, 19.2Kbps의 저속 전송으로 동영상을 구현할 수 있다.
WMV	윈도우 운영체계에서 사용되는 오디오 포맷의 하나이다. 소리나 음성을 듣거나 녹음하는데 사용하며, 윈도우에서 표준으로 부속되어 있는 Media Player로 재생할 수 있다.

④ 저장구조 기법

- 특징

표 3.10.12 저장구조 특징

구분	특 징
Batch 처리 방식	· 시간이 많이 걸림. 유사한 작업도 다시 배치작업을 해야 함 · batch 작업 후, 데이터 Set을 지우기 때문에 과거 데이터 존재하지 않음
SAM File 가공방식	· PC에서 여러 분석을 하므로 호스트의 부하를 줄일 수 있음 · PC에서 GB단위 이상의 자료처리가 불가능하고 시간이 많이 걸림 · 분석가의 처리방식에 따라 결과가 상이할 수 있음
통합 데이터 베이스 방식	· 기존 운영계 시스템에서 데이터를 추출하여 통합 데이터베이스에 넣고 보관함 · 사용목적에 따라 목적별 데이터베이스를 구축함 · 4GL 프로그램이나 C/S 툴로 사용자가 접속하여 사용함 · 개발기간이 길고, 비용이 많이 들며 분석 및 예측기능이 없음

구분	특 징
데이터 웨어하우스 방식	· 기존 운영계 시스템에서 데이터를 추출하여 데이터 웨어하우스에 넣음 · 데이터 웨어하우스에만 적용되는 다차원 모델링을 함 · 여러 방식과 도구로 사용자가 접속하여 사용함 · 분석 및 예측을 할 수 있음

- 인덱스

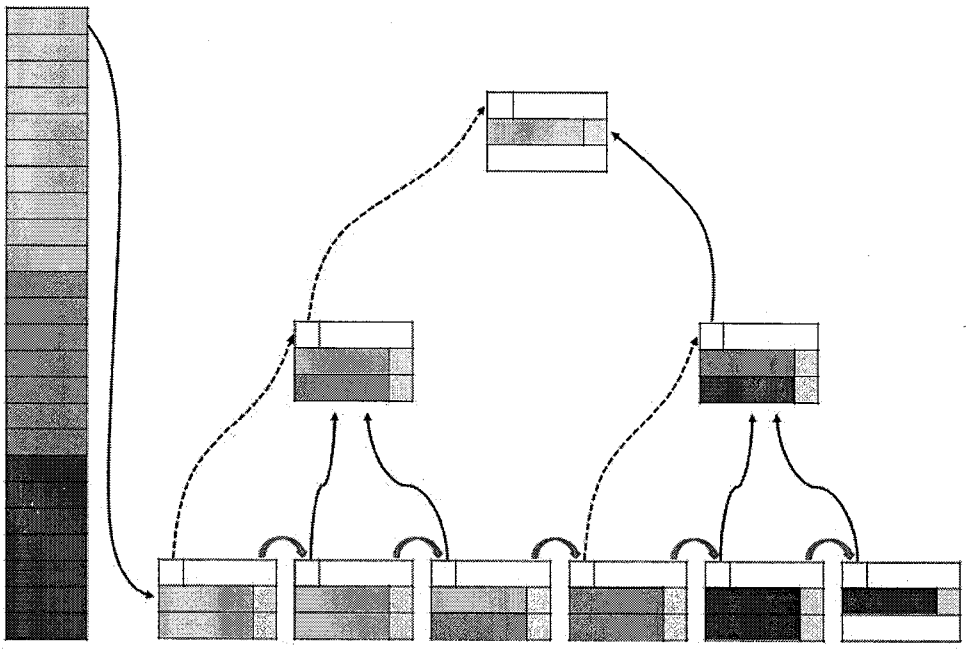


그림 3.10.35 인덱스를 이용한 자료분할

인덱스는 데이터 접근 경로를 단축시키는 기능을 한다. 테이블에 수백만개의 정보가 저장되고 특정정보를 이용해 데이터를 검색 할 때 인덱스가 없다면 전체자료를 읽어야 한다. 인덱스는 구성 칼럼 값으로 정렬되어 있고 테이블 내 값들의 위치를 갖고 있다. 인덱스를 이용하면 전체 테이블을 읽지 않고도 찾고자 하는 데이터를 찾을 수 있다. 테이블에 데이터가 수천만 개로 증가해도 인덱스를 이용한 접근 경로가 동일하다면 속도변화는 없을 것이다.

1개 이상의 데이터를 이용하여 비교 연산을 효과적으로 하기 위해 시스템은 정렬(Sort) 후 값을 비교한다. 비교 연산 때마다 정렬하지 않기 위해서 정렬된 결과를 데이터와 별도 인덱스를 생성하고 비교 연산이 필요할 때마다 이용한다. 정렬된

값을 효과적으로 스캔하고 유지하는 방법으로 트리구조와 알고리즘을 이용한다.

- 액세스 최적화 방안

데이터 관리에서 중요한 사항 중 하나는 자료에 접근하는 방식이다. 자료를 저장, 관리 하는 이유는 자료에 관한 정보를 얻기 위해서이다. 때문에 정보를 얻기 위해 데이터에 접근하는 방식 또한 중요할 수밖에 없다. 또한 접근을 위해서는 처음 자료저장을 용도에 맞게 구성하는 것이 중요하다. 특히 데이터를 처리하면서 힘든 점은 처리할 범위가 넓을 때 대책을 찾는 일이다. 소량의 데이터를 처리할 경우에는 상관없지만 넓은 범위의 데이터를 처리하는 순간부터는 고려해야 할 사항이 많아지게 된다. 그렇기 때문에 자료를 정렬하는 방식을 지정하는 것은 매우 중요한 것이다. 기본적으로 데이터를 전체범위로 처리하는 경우와 부분범위로 처리하는 경우를 고려하여 자료를 저장해야 한다.

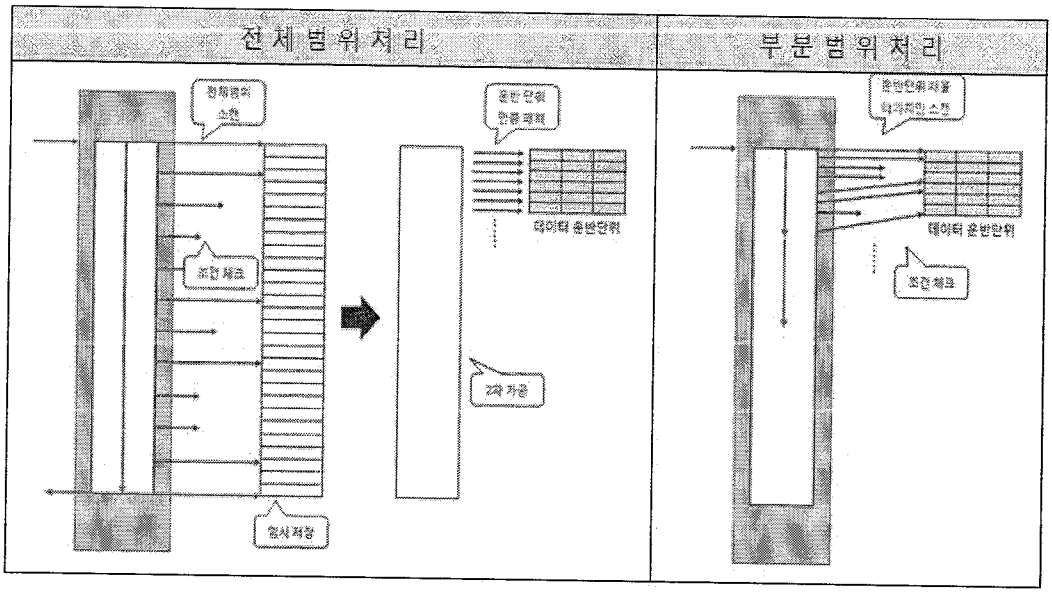


그림 3.10.36 범위에 따른 데이터 처리 방법

⑤ 감시 시스템에서의 자료관리

센서로 감지된 값과 그에 따른 영상데이터를 문서로 작성하기 위해서는 영역별 저장이 중요하다. 그렇기 때문에 서버에는 센서감지자료, 영상파일, 영상파일의 자료동기화에 따른 공통자료, 그 외의 자료처리 내역 등이 각각 연관되어 저장되어 있어야 한다. 이러한 서버의 데이터를 통신을 이용해 화면에 나타낼 수 있는데 각

각의 자료는 아래와 같이 연관되어 있다.

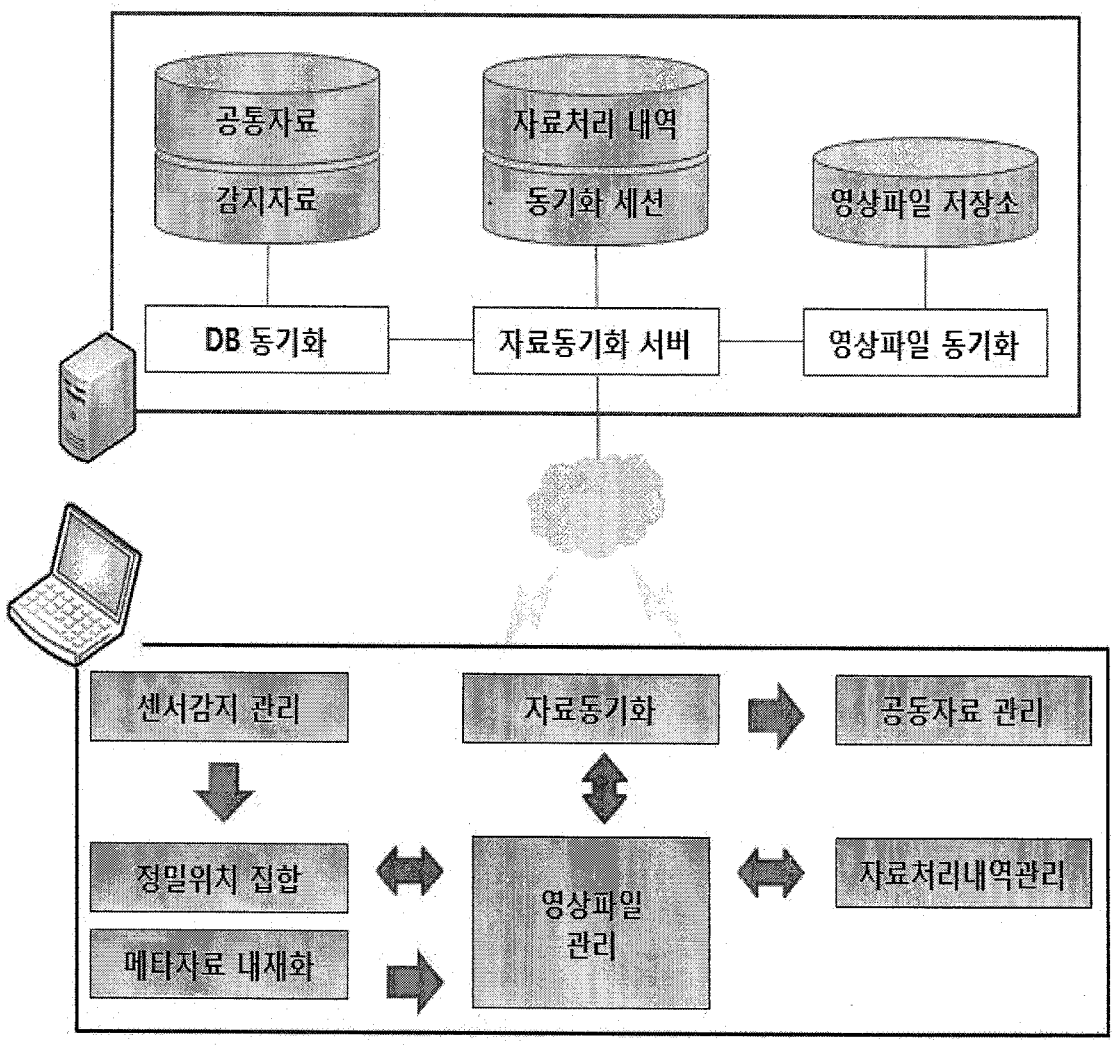


그림 3.10.37 영상자료관리

(4) 3D 레이저레이더를 이용한 안전설비 시제품 제작

(가) 시제품 제작

① 시제품 사양

6차년도 플랫폼 공중사상사고 저감을 위해 3차원 레이저 레이더를 이용한 안전설비 상세설계 사양은 표 3.10.13과 같다.

표 3.10.13 시제품 제작 사양

No	구 분	사 양
1	온도	- 35～+50℃

2	습도	0~100%
3	최대강수량	· 시스템은 다소 많은 강우량에도 작동되도록 설계한다. · 사양서의 강우량에 대해서는 시험 후 제작사와 최종 결정한다. 다만, 강우에 대해 오동작을 하지 않도록 두 개의 펄스 구조를 사용하는 방식을 채택한다.
4	바람	· 바람은 측정에 영향을 미치지 않지만 강풍은 경보실패를 유발할 수 있다.
5	최대강설량	· 최대강수량과 같다.
6	설치높이	· 선로 위 150~200mm 위에 레이저 빔의 중앙이 오도록 설치한다. · 감지 영역은 확산이 빔의 지름을 증가시키기 때문에 선로 위에 매우 가깝게 설치한다. · 빔이 직선으로 스캔하므로 감지영역은 평면이라는 것이 중요하다. · 평면에서의 편차는 정확도와 선명도를 감소시킨다.
7	검지능력	· 최소 200x200 mm의 물체를 감지하도록 설계한다. · 최고의 반발 검지능력이 있기 때문에 대부분의 빔이 물체를 지나쳐도 물체를 검지할 수 있게 한다.
8	반응시간	· 설정에 따라 1~5초이다. · 신문지처럼 날라 다니는 물체로 인한 오류를 방지하기 위해 3-5초의 마진을 둔다.
9	사용전압	· 220 VAC ± 10%, 60Hz · 시스템은 과전압보호장치를 갖추고 있다.

② 시제품 제작 및 시험

상세설계 단계에서 그림 3.10.38과 같이 3D 레이저 레이더 장치를 3차원으로 모델링하였으며, 이것으로부터 그림 3.10.39와 같이 시제품을 제작 완료하였다. 제작된 시제품에 대한 상세한 제원(중량, 크기 등) 및 주요부품 사양에 대해서는 최종 보고서에 내용을 보완할 예정이다.

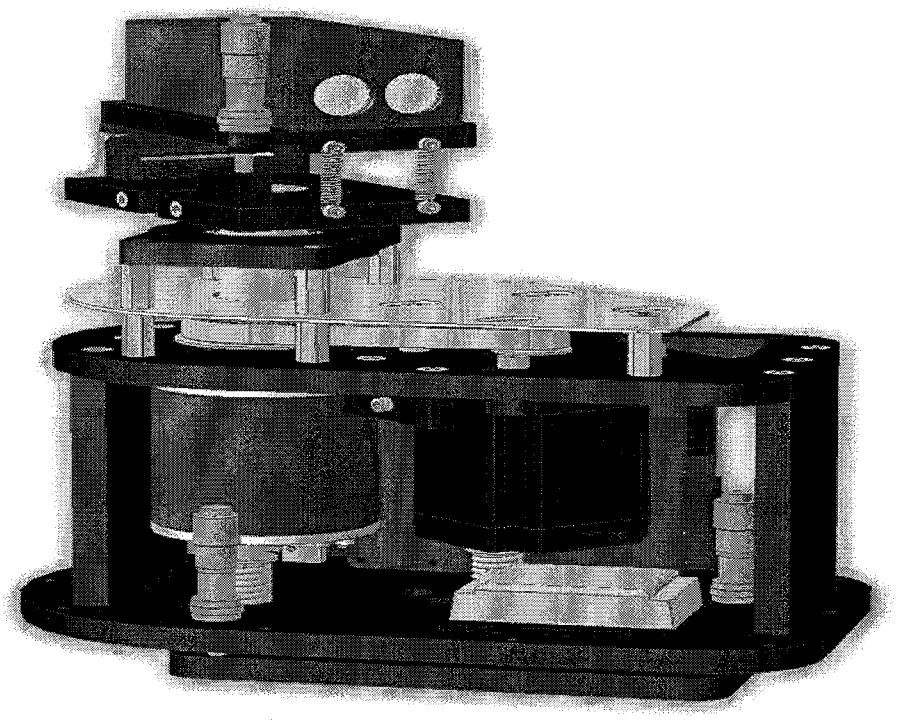


그림 3.10.38 3D 레이저 레이더 시제품 모델링

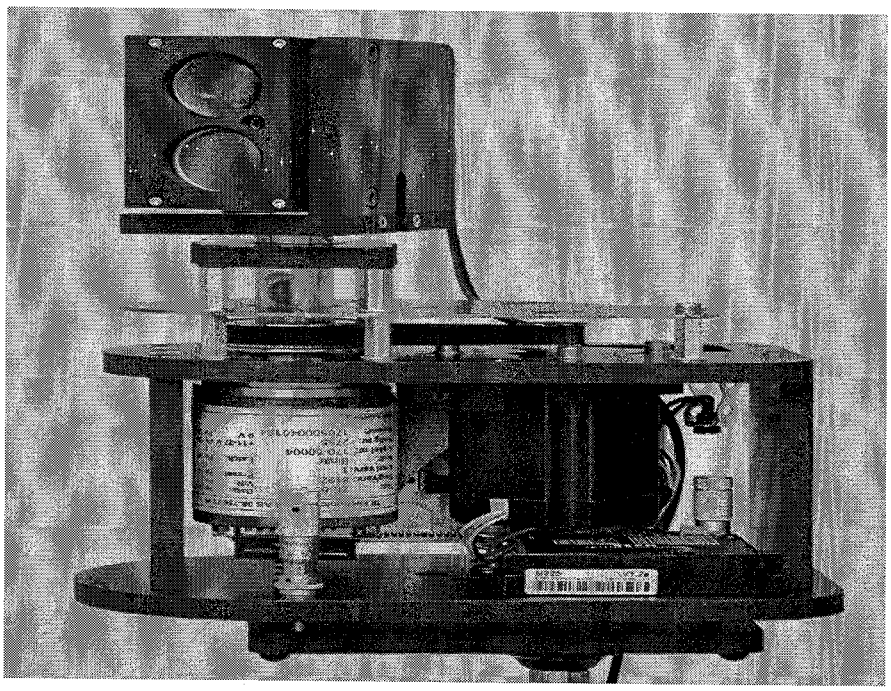


그림 3.10.39 3D 레이저레이더 센서 제어부 시제품 사진

개발 시제품에 대한 기능 시험을 위해서 센서부를 개발한 스웨덴 현지에서 1차 시험이 시행되었으며, 이를 통해 검지알고리즘에 대한 보완이 진행 중에 있다, 5월

중순에서 6월 초에 시제품에 대한 보완이 완료된 후 2차 시험이 수행될 예정이며, 이 시험이 마무리 된 후 개발 시제품을 국내로 반입하여 플랫폼에 적용을 위한 응용 프로그램의 분석 및 개발이 수행될 예정이다.

1차 시험 장소는 스웨덴 스톡홀름의 Af Chapman Youth Hostel 인근의 호수 및 도로에서 수행이 되었으며, 검지 데이터의 수집 및 분석을 위해 노트북을 통한 인터페이스를 하였으며, 검지 데이터 분석은 3D 레이저레이더에 적합하도록 개발한 전용 Viewer를 통해 수행되었다. 이 응용 소프트웨어의 분석 데이터를 통해 철도의 플랫폼 환경에 적합하도록 분석 및 응용 소프트웨어에 대한 추가적인 연구를 필요로 한다. 2차 시험결과 및 분석내용은 당해연도 최종보고서에 반영될 예정이다.

그림 3.10.40는 개발 시제품의 1차 시험을 위해 시험 현장에 설치한 사진으로 개발 센서부는 최대 600m의 측정범위를 가지며 정확성은 대략 ±10cm(at single shot), 스캔속도는 1000 Hz 이상이고, 회전각도는 약 90°이다. 검지 영상의 분석을 위해서 전용 응용소프트웨어가 탑재된 노트북을 사용하였으며, 응용 소프트웨어의 옵션 선택에 의해 검지된 영상을 다양한 형태로 출력해 볼 수 있도록 하였다.

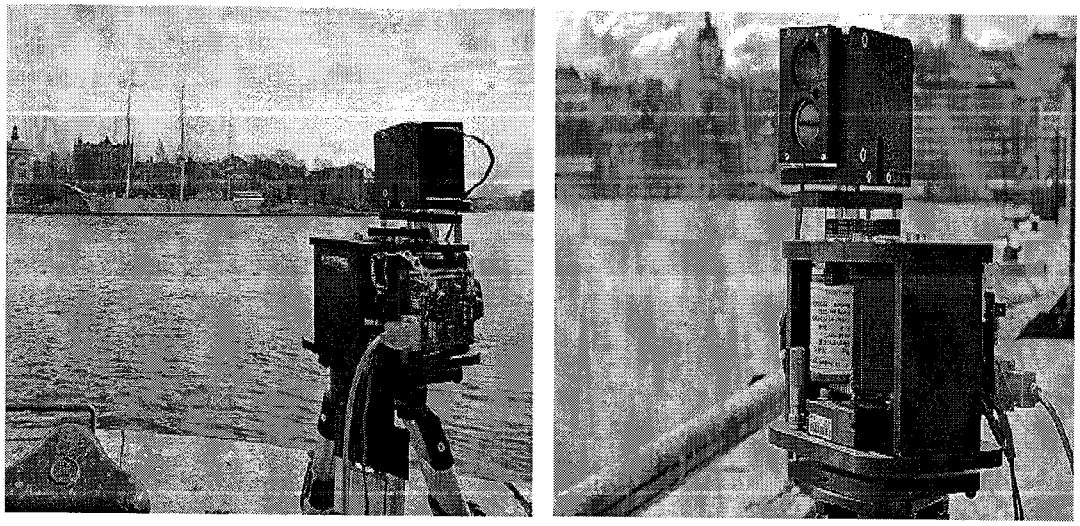


그림 3.10.40 개발 시제품 사진

그림 3.10.41은 시제품으로 센싱한 화면과 동일 지역을 위성촬영한 사진을 겹쳐서 표출한 사진으로, (a)는 측정지점의 반대편 부두의 약간 높은 지역의 여러 곳에

대해 스캔함. 노란색 마크들은 레이저에 의해 스캔된 데이터를 나타내고 있고, (b)는 동일한 지역을 스캔한 것이지만, 약간 더 높은 지역을 스캔한 데이터임. 왼쪽 다리 위의 가로등 기둥들이 스캔됨을 볼 수 있다. 스캔된 정보의 표출 색은 표시된 것은 전용 프로그램에 의해 옵션 선택을 통해 컬러 조정가능하다.



(a)



(b)

그림 3.10.41 레이저 레이더를 이용한 물체 스캔 데이터(1)

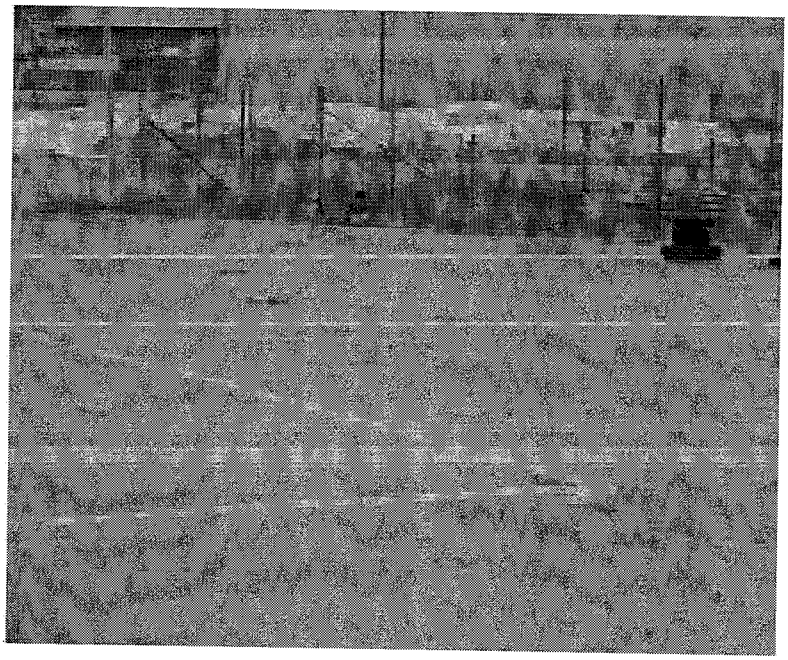


그림 3.10.42 센서부 시험을 위한 실제 전경

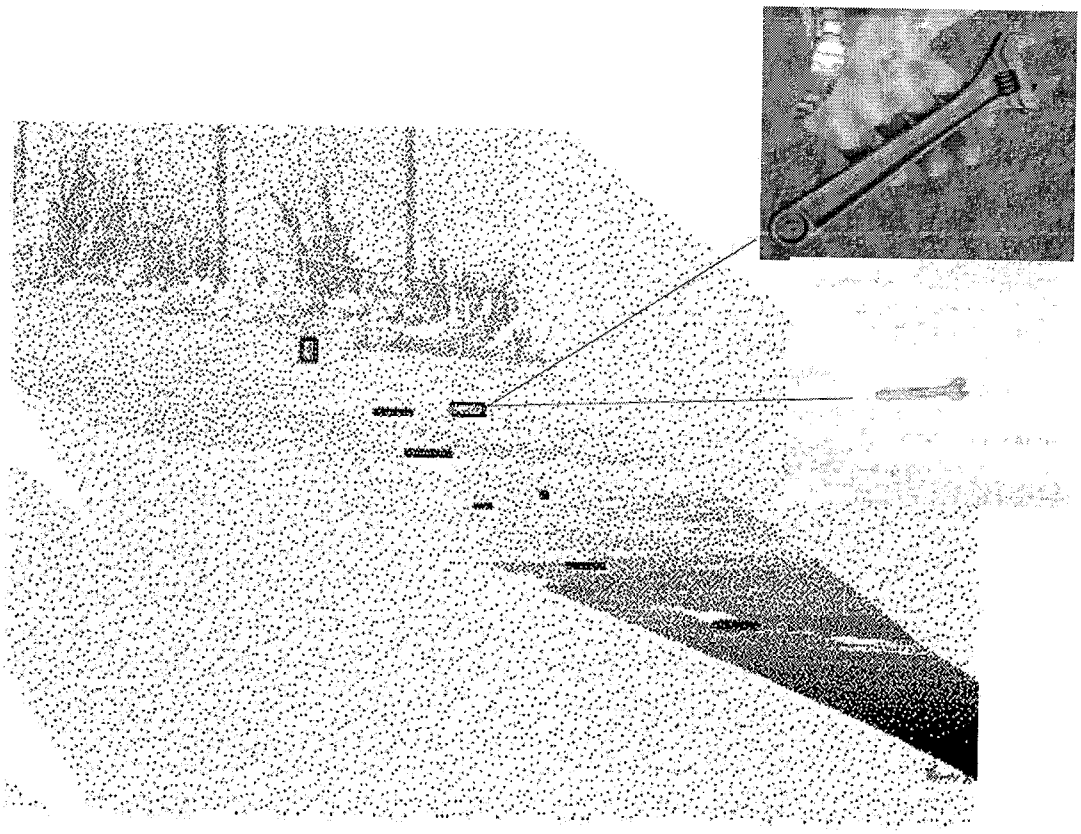


그림 3.10.43 분석 소프트웨어를 거친 스캔 데이터

앞의 시험 사진은 전체적으로 개발한 시제품의 스캔 성능을 확인한 사진이며, 보다 구체적으로 개발 센서부의 성능 확인을 위해 도로 바닥에 렌치, 나사 등의 물건을 놓고 스캔하여 해당 물체를 인식할 수 있는지 시험을 수행하였다. 그림 3.10.42는 센서부 시험을 위한 실제전경이며, 그림의 상단에 시험을 위한 스캔 대상인 렌치 등이 나타나 있다. 시제품과 이들 피사체와의 거리는 약 45m 정도로 하였다. 그림 3.10.43은 분석 프로그램을 통한 스캔 이미지를 나타낸 것으로 약 45m 거리에서 렌치를 검지할 수 있음을 확인하였다.

다음 사진은 좀 더 먼 거리에서 스캔하였을 경우를 나타낸 것으로 거리는 약 150 m이다. 앞의 시험에서와 동일하게 도로변에 작은 물체를 놓고 스캔하였을 경우 그 물체를 검지할 수 있는지 시험하였으며, 시험 결과에서와 같이 해당 물체를 정상적으로 검지할 수는 있었지만 해당 물체가 어떠한 물체인지 인식하는 부분은 지속적인 시험을 통해 전용 분석 프로그램에 입력되어야 한다.

이러한 1차 시험을 통해 개발한 시제품의 기본적인 성능은 확인하였으며, 실제 플랫폼 공중 사상사고 저감을 위한 안전설비에 활용하기 위해서는 실제 시범설치를 통한 해당 지역의 스캔을 통한 데이터 축적을 통해 사람이 추락되었는지 여부를 구별할 수 있는 응용 프로그램의 개발을 위한 후속연구가 필요하다. 즉, 개발된 시제품이 실제 안전설비로 활용되기 위해서는 실제 적용 대상에 대한 많은 스캔 데이터가 필요하며 이를 통한 검지 물체의 구분이 이루어 질 수 있다.

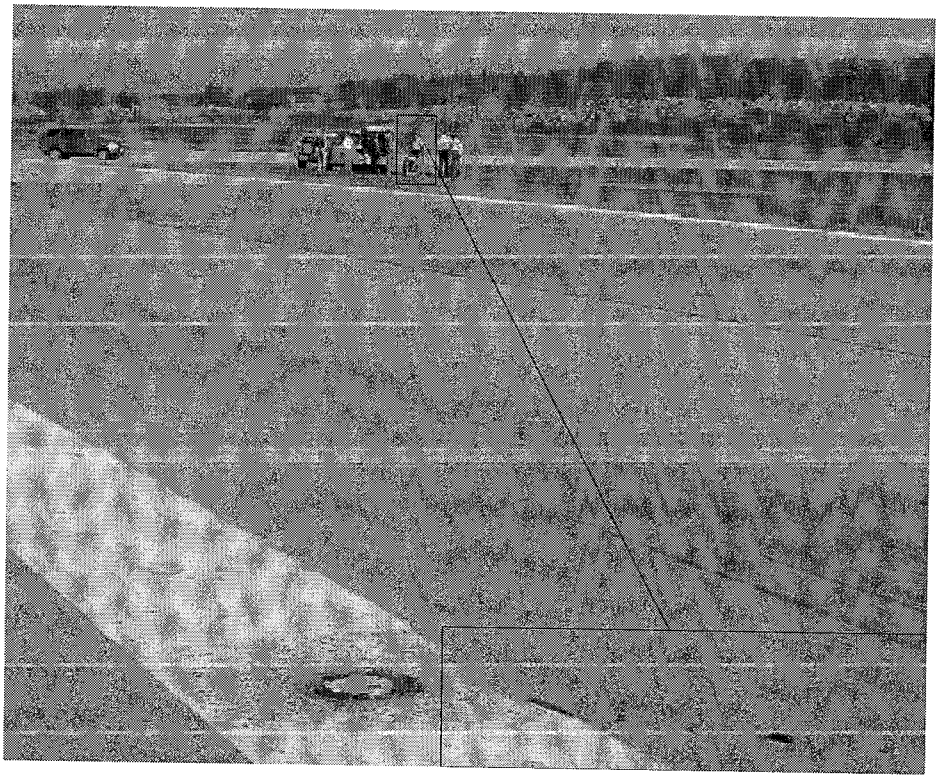


그림 3.10.44 센서부 시험을 위한 실제 전경(150m)

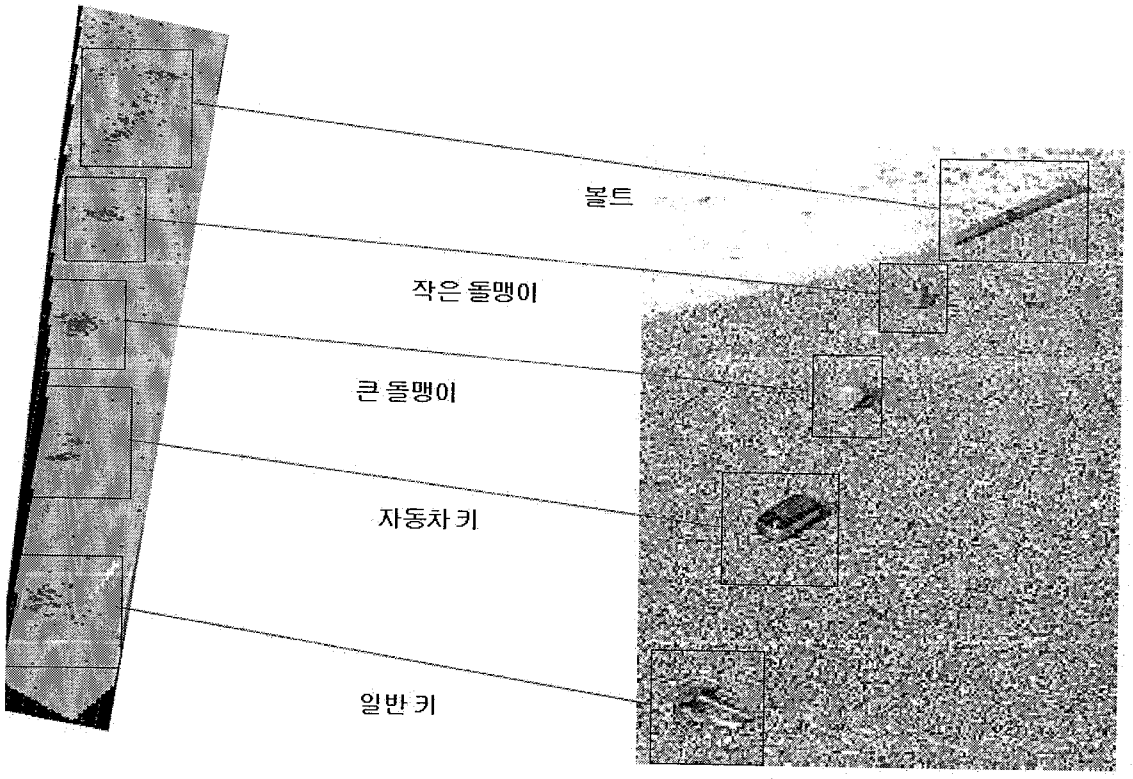


그림 3.10.45 분석 소프트웨어를 거친 스캔 데이터(150m)

(5) 선로변 작업자를 위한 안전설비 시제품 보완제작

(가) 개요

철도의 선로변에서 선로나 신호설비를 유지보수작업을 할 경우에는 작업 전후방 일정거리에 유지보수작업자 이외에 안전경보자를 위치시켜 이들이 열차의 접근을 인식하면 깃발이나 경광등 같은 경보장치를 통해 유지보수 작업자에게 열차의 접근정보를 전달하는 방식을 사용하고 있다. 이처럼 작업자 전후방 일정거리에 있는 안전경보자를 통한 열차접근의 경보를 하더라도 단조로운 유지보수 작업을 장시간 지속하면 유지보수자는 감각차단 현상이 발생하여 안전경보자에 의한 경보신호를 인지 못하여 열차가 유지보수 작업장 인근까지 접근하여도 열차의 접근을 인식하지 못하여 열차와 충돌사고가 발생하는 사상사고가 발생하고 있다.

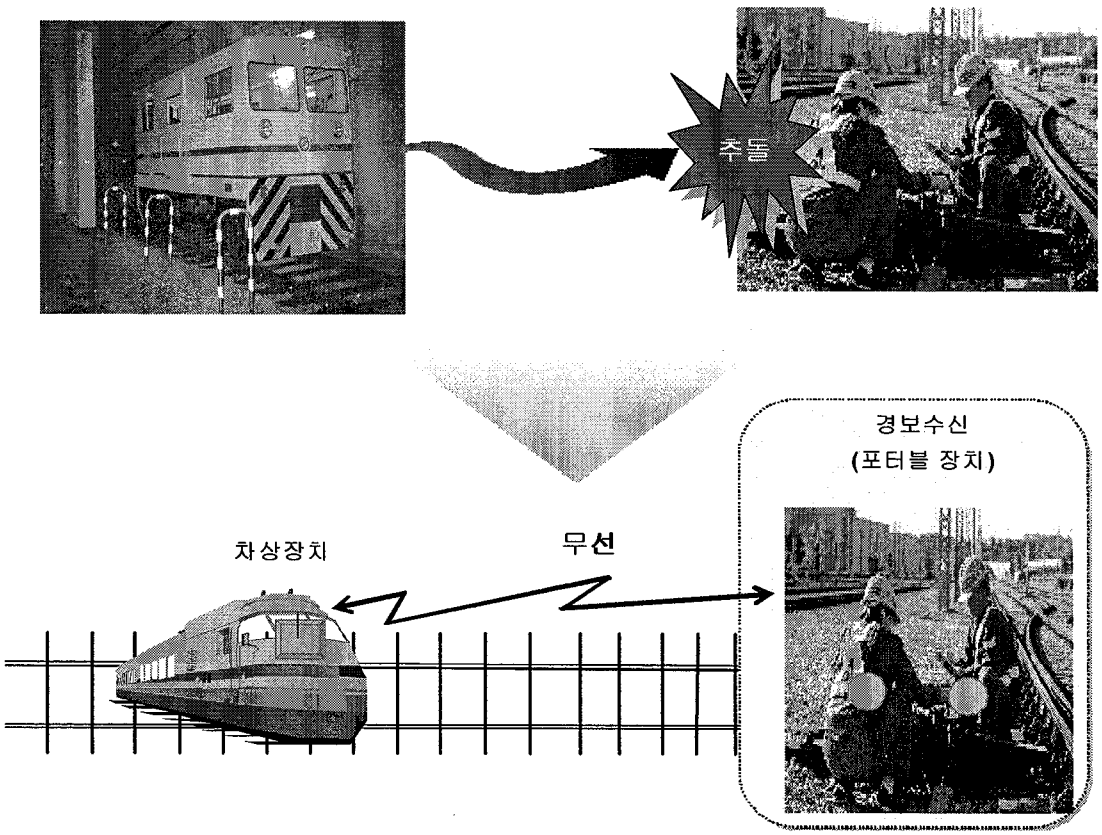


그림 3.10.46 개발 안전설비 개요

철도의 선로변에서 선로나 신호설비를 유지보수하는 자들은 단조로운 유지보수 작업을 장시간 지속하면 감각 차단현상이 발생하여 열차가 유지보수 작업장 인근

까지 접근하여도 열차의 접근을 인식하지 못하여 열차와 충돌사고를 발생할 수 있다. 이러한 철도유지보수자의 사상사고 예방하기 위한 안전장치를 전년도에 설계 및 제작하였고, 당해 연도는 전년도의 연구를 바탕으로 시제품의 현장시험 및 이를 통한 보완제작을 수행하였다. 특히 당해연도에는 개발 시제품의 실용화를 위하여 시연회를 개최하여 철도 운영기관 현장의 요구사항을 수집하였다. 또한 현재 개발 시제품을 도시철도 운영기관의 일부 유지보수차량에 시범적용하여 운용 중에 있으며, 시범운용을 통한 철도 운영기관의 의견을 수렴할 예정이다.

(나) 무선을 이용한 사상사고 저감 안전설비

철도 선로변에서 선로나 신호설비의 유지보수 작업자의 접근열차와의 충추돌에 의한 사상사고 저감을 위해 열차에서 특정 신호를 무선으로 주기적으로 전송하고 선로변의 작업자가 가지고 있는 단말장치에서 차상으로 부터의 무선신호를 수신하여 작업자에서 진동, 소리, LED 등 다양한 경보신호를 제공하여 사고를 예방하는 안전설비를 제안하였다. 즉, 전방의 일정거리 이내에 열차가 접근하면 작업자의 안전설비가 접근열차를 인지하여 작업자에게 다양한 형태의 경보신호를 제공하여 열차와의 충추돌 사고를 저감하고자 하는 설비이다.

그림 3.10.46은 앞에서 설명한 작업자 사상사고 저감을 위한 안전설비 개요를 나타낸 것으로, 전방의 일정거리 이내에 열차가 접근하면 작업자의 안전설비가 접근열차를 인지하여 작업자에게 다양한 형태의 경보음을 제공하여 대피할 수 있도록 하고, 반대로 열차에서도 전방에 작업자의 존재유무를 확인할 수 있도록 하여 주의운전을 하도록 유도하는 안전설비이다. 즉, 열차에 설치하는 차상장치와 작업자가 휴대하는 단말장치 간, 차상장치 간 각각 양방향 통신이 되도록 하였다. 이는 열차의 운전자에게도 전방의 일정거리에 작업자의 작업유무를 확인할 수 있도록 정보를 제공하여 주의운전을 유도하기 위함이며, 차상장치에서의 경고신호는 LED와 경고음으로 표출되도록 하였다. 이러한 무선통신 기반의 철도교통 사상사고 저감을 위해 제안한 안전설비는 선로변 작업자와 모터가의 다양한 운행 시나리오에 따라 각각 적절한 안전경보를 할 수 있는 동작 메커니즘을 구현하였다.

① 무선을 이용한 안전설비의 설계

선로변 작업자의 사상사고 저감을 위해 무선통신을 이용하여 경보신호를 양방향

으로 전송하는 안전설비를 설계하였다. 설계한 안전설비는 차상장치와 작업자용 포터블 장치로 구성되어지며, 각각 전방의 진입열차 정보나 작업자의 정보를 다양한 경보신호로 출력하도록 하여 주의운전 및 안전지역으로 대피할 수 있도록 하여 사상사고를 저감하기 위한 안전설비이다.

설계한 안전설비의 기본 메커니즘은 차량에서 특정 주파수대의 신호를 주기적으로 전송하고, 전방 일정거리 이내의 선로변 작업자가 가지고 있는 안전장치에서 차량으로부터 오는 주기적인 신호를 수신하여 부저, LED, 진동 등으로 경보신호를 전달하도록 하는 구조로 되어있다. 작업자가 가지고 있는 안전설비로부터 열차접근에 대한 경보신호 작업자가 인지하게 되면, 작업자는 안전구역으로 대피하게 되고 또한 경보음은 차단할 수 있도록 하였다. 반대로 차상에서도 전방의 작업자가 있는지 유무를 확인할 수 있도록 양방향 통신이 가능하도록 개발하였다.

그림 3.10.47은 안전 경보설비의 차상단말기의 구성을 나타낸 것으로, RF 신호를 주기적으로 송신하고 또한 수신하기 위한 RF 모듈, 주기적인 RF 신호의 발생 및 경보신호의 동작메커니즘을 처리하는 MCU 모듈, 빛에 의한 경보신호 출력을 위한 LED 모듈, 정보 표시를 위한 LCD 모듈, 소리에 의한 경보신호 출력을 위한 AMP와 스피커 부분, 그리고 모터카로부터 전원을 입력받기 위한 전원 모듈로 구성되어진다. 전원 모듈은 다양한 모터카의 전원을 입력받을 수 있도록 5V에서 40V까지 입력받을 수 있도록 하였다. 본 시제품에서 사용한 무선신호 주파수 대역은 ISM 대역인424 MHz로 하였다. LED에 의한 경보신호는 전방에 작업자가 있는지 또는 전방에 또 다른 모터카가 있는지에 따라 각각 다른 컬러로 표시되도록 하였다. 경보음은 모터카의 운전자에 조절이 가능하도록 하였고, LCD 판넬에는 접근한 작업자 단말기나 다른 모터카 단말기의 고유 번호가 표시되도록 하였다. 만약 접근구간 이내에 여러 대의 단말기로부터 무선신호를 피드백 받을 경우 무선신호가 피드백된 순서로 순차적으로 각각 단말기의 ID 번호가 표출되도록 하였다. 모터카의 차량 단말기와 작업자용 단말기의 무선신호 출력은 ISM 대역이고 또한 전파 도달거리가 도시철도에 적합하도록250~300m 정도가 되도록 10mW 이내로 조정하였다.

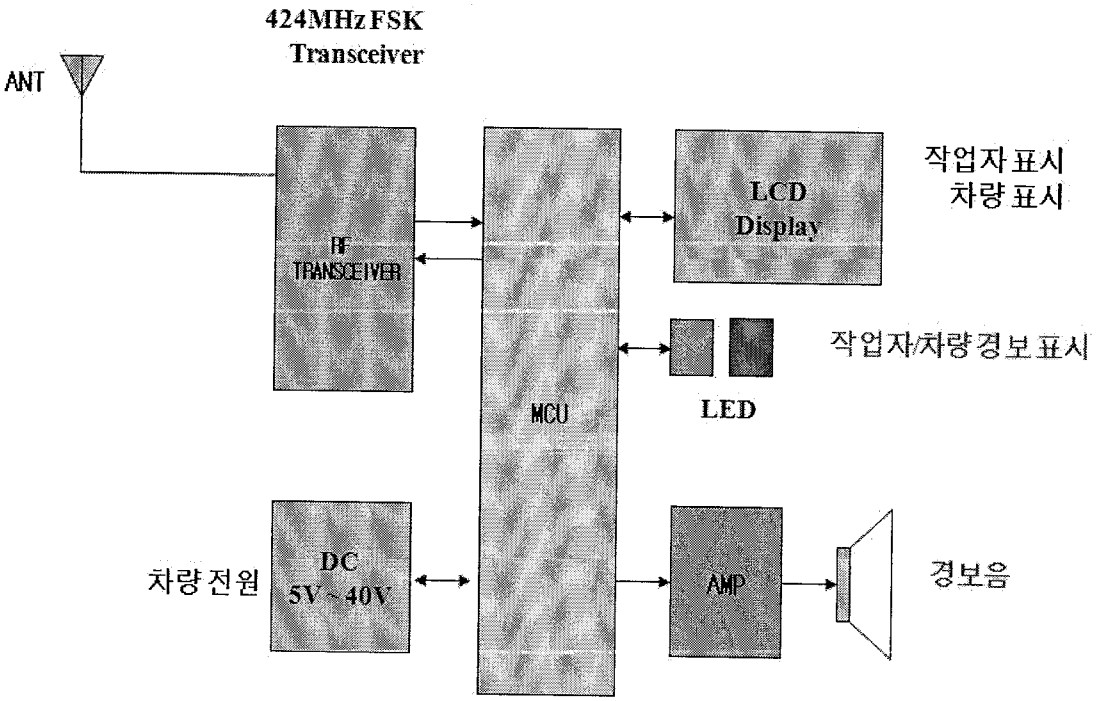


그림 3.10.47 차상 단말기의 구성도

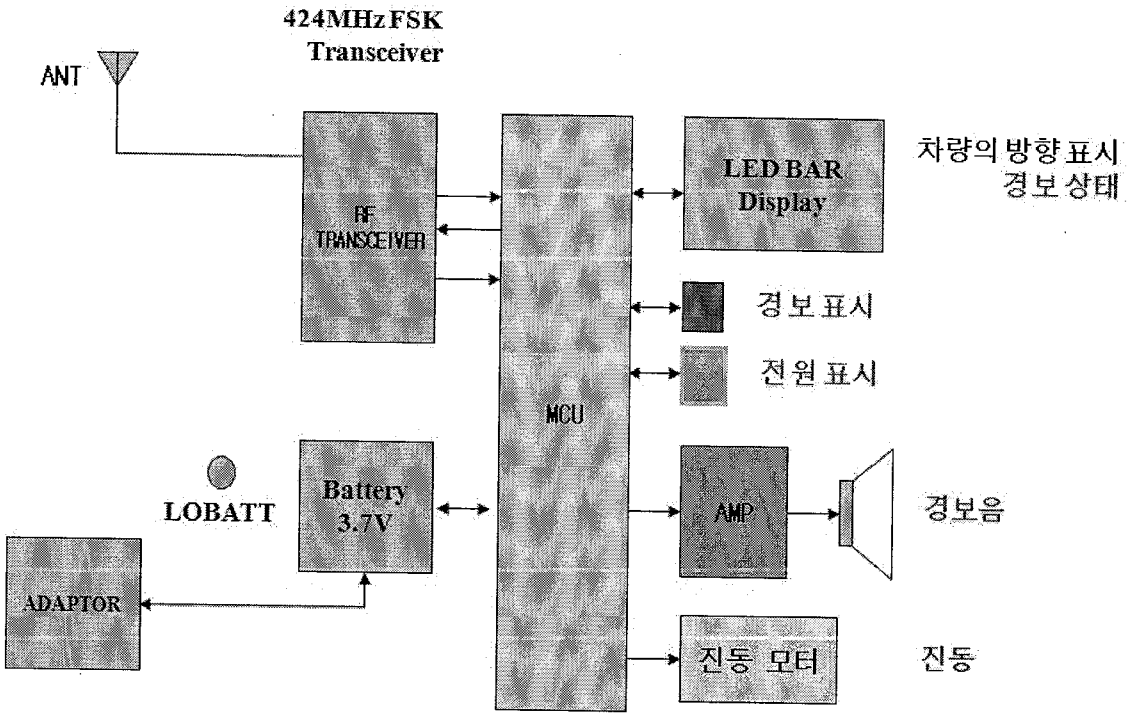


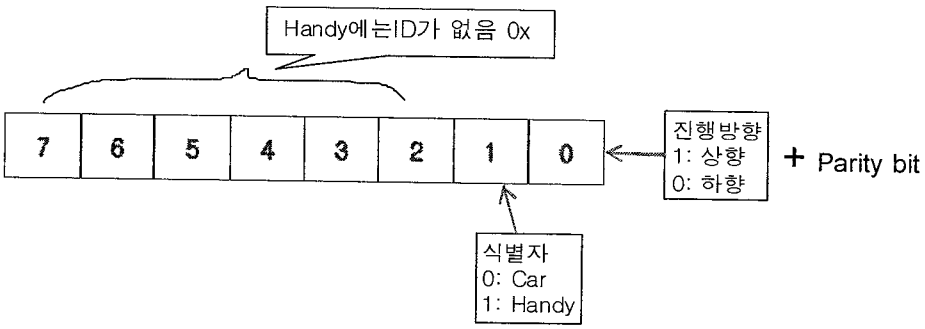
그림 3.10.48 작업자 단말기의 구성도

그림 3.10.48은 작업자용 단말기의 구성을 나타낸 것으로 기본적인 구성은 그림 3.10.47의 차상 단말기와 동일하지만 경보신호의 출력부분과 전원부분에서 차이점이 있다. 작업자용 단말기의 경보신호는 차상 단말기와는 달리 LED와 소리에 의한 경보신호 이외에 진동에 의한 경보신호를 추가하여 작업자에게 경보신호 전달기능을 향상시켰다. 따라서 작업자용 단말에는 진동 모터 부분이 추가되었으며, 또한 LED 경보는 모터카의 접근방향을 표시하는 LED와 일반고휘도 LED 두 가지로 구성하였다. 전원 부분은 차상 단말기는 모터카 차내의 전원을 직접 사용하지만 작업자용의 경우 휴대용이므로 배터리를 사용하여 외부에서 충전하여 사용할 수 있도록 하였고, 배터리의 충전이 3시간이하일 경우'LOBATT' LED의경보등이 동작되도록 하였다. 또한 작업자가 휴대하기 편리하도록 작업자 허리에 부착하거나 목에 걸 수 있는 구조로 하였다. 그림 3.10.49는 앞에서 설명한 작업자용 단말기와 차상용 단말기의 주요한 사양을 정리한 것이다.

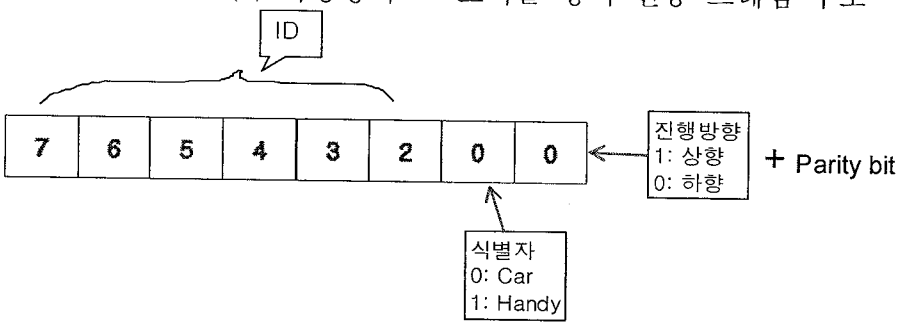
차상용 단말기	주파수	424Mhz
	출력	10mW 이내
	수신감도	-110dbm
	안테나	외장형 안테나 (150mm)
	입력 전압	12V~40V
	배터리	차량용 전원
	크기	190mm×130mm×50mm
작업자용 단말기	주파수	424Mhz
	출력	10mW 이내
	수신감도	-110dbm
	안테나	외장형 안테나 (50mm)
	입력 전압	3.3~4.2V
	배터리	축전지(충전형)
	크기	50mm×90mm×25mm

그림 3.10.49 차상용 및 작업자용 단말기의 주요 구성

전방의 첫 번째 열차가 작업자에게 접근하면 작업자의 포터블 안전설비가 차상장치로부터의 신호를 수신하여 경보를 표출하게 되고, 작업자가 경보신호를 인식하게 되면 확인버튼 동작을 통해 경보음을 차단한다. 이 후에 연속적으로 다른 열차가 작업자에게로 접근하게 될 경우 첫 번체 열차의 접근 인식에 따른 확인버튼 동작에 상관없이 두 번째 열차 접근 정보를 알리는 경보음이 표출되어야 한다. 이를 위해 그림 3.10.50 (a)와 같이 열차의 ID 정보를 같이 전송하도록 하였다. 그림의 전송프레임에서와 같이 64대의 열차 ID를 할당할 수 있으며, 이 이상의 열차 ID 할당이 필요할 경우 전송 프레임을 2바이트로 설정하면 가능하다. 또한, 이 프레임에서 확인되듯이 열차의 진행방향(상행 또는 하행) 정보를 추가하였다. 이는 열차의 진행 방향이 상행 또는 하행 두 가지 방향밖에 없으므로 이를 전송프레임에 같이 전송함으로서 작업자에게 열차의 접근방향이 어느 쪽인지 표출(LED 컬러를 구분하여 표시)하도록 하였다. 그림 3.10.50 (b)는 작업자용 포터블 장치에서 차상장치로 전송하는 프레임 구조를 나타낸 것으로 (a)와는 달리 차상에서는 작업자의 구분이 필요없어 ID번호를 할당하지 않았다.



(a) 차상장치 ⇒ 포터블 장치 전송 프레임 구조



(b) 포터블장치 ⇒ 차상장치 전송 프레임 구조

그림 3.10.50 차상제어장치 송신용 프레임 구조

앞에서 설명한 바와 같이 차상용과 작업자용 안전설비는 전원 스위치, 모드전환 스위치 등 몇 개의 조작 스위치를 가지고 있다. 전원 스위치의 경우 차량용 안전설비의 경우 차량의 전원이 투입될 경우 주기적으로 계속해서 전방으로 무선신호를 송신하고 운전자가 임의로 출력신호를 OFF할 수 없도록 차량용은 전원 스위치를 별도로 추가하지 않았다. 확인 버튼은 작업자가 열차의 접근을 인식하면 부저음을 차단할 수 있도록 하기 위해 추가된 버튼이다. 이 버튼을 동작시킬 경우 현재 접근 열차로부터의 무선신호는 수신하더라도 부저음이 표출되지 않지만 다른 접근하는 차량으로부터 새로운 무선신호를 수신할 경우 부저음이 다시 동작되는 메커니즘으로 설계하였다.

② 경보신호 동작 메커니즘

차량용 단말이나 작업자용 단말기는 각각 동일한 전파전달거리를 가지고 있어, 작업자 기준으로 전파전달거리 이내에 열차가 접근하면 차량용과 작업자용 단말기의 경보가 표출된다. 이후 작업자가 이 경보를 인식하면 경보정지버튼을 누르며 이에 따라 작업자용 및 차량용 단말기의 경보신호 표출은 중지되게 된다. 그림 3.10.51은 이러한 기본 경보동작 메커니즘을 설명한 그림이다. 즉 모터카 #1이 작업자 단말기의 전파전달 영역 이내에 들어오게 되면 모터카 #1의 단말기로부터의 RF 신호를 작업자용 단말기가 수신하고 경보신호를 발생시킨다. 그리고 바로 모터카 #1의 단말기로 피드백 하여 모터카 #1의 차량 단말기에도 전방에 작업자가 있다는 경보를 발생시켜 주의 운전하도록 한다. 선로변 작업자가 작업자 단말기의 경보신호를 확인하면 대피하게 되고, 이후에는 계속되는 경보신호가 발생될 필요가 없으므로 작업자용 단말기에 경보중지 버튼을 취급하여 작업자용과 차량용 단말기에 경보신호를 중지시키도록 한다. 이때에도 모터카 #1의 단말기는 주기적으로 RF신호를전송하고작업자용단말기도주기적으로 모터카 #1의 신호를 수신하지만 경보중지 버튼이 눌려지면 경보신호를 출력하지 않도록 하였다. 이후 그림과 같이 모터가 #2가 전파전달 영역 이내로 접근할 경우 작업자 단말은 그림 3.10.51과 같이 다시 경보신호를 발생시키고 동시에 차상 단말기로 피드백 시켜 모터카 #2에 경보신호를 발생시키도록 하는 메커니즘으로 구현되어 있다.

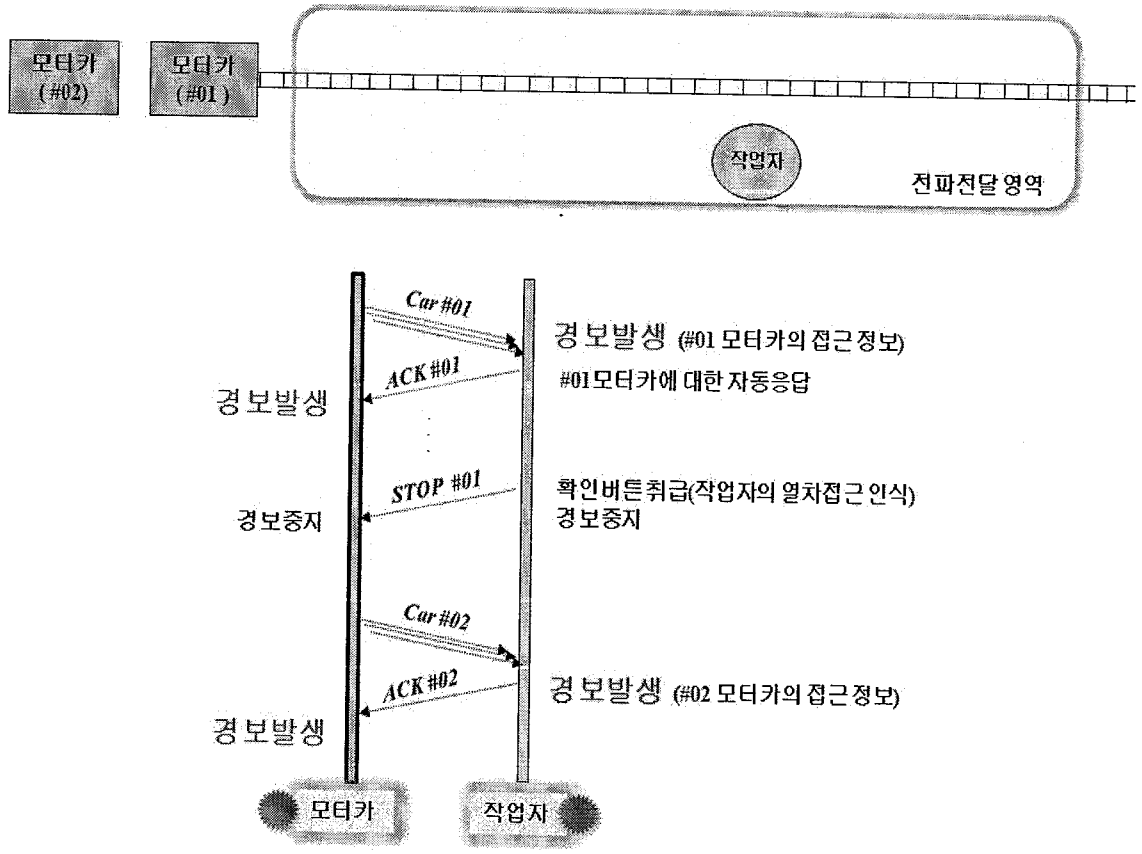


그림 3.10.51 기본 경보동작 메커니즘

이와 같은 기본적인 동작 메커니즘 이외에 하나의 모터카가 전파전달 영역 이내에 들어왔다가 벗어난 후 다시 재진입하는 상황이 발생할 수 있다. 이는 일반적인 영업 열차가 아닌 선로변 유지보수를 위한 작업용으로 사용되는 모터카의 운행이므로 좁은 영역에서 잦은 전진과 후진 운전을 반복 운전할 수 있다. 이러한 경우가 그림 3.10.51과 같은 경우로서, 이때는 작업자용 단말기에서 RF 신호가 수신되지 않으면 작업자용 단말기는 중지되고, 차상용 단말기도 작업자용으로부터 피드백신호를 받지 않을 경우 차상용 단말기의 경보신호도 중지된다. 이후 새롭게 모터카 #1이 전파전달 영역내로 진입할 경우 처음 진입했을 때와 동일한 메커니즘으로 경보신호를 표출하도록 하였다. 이는 그림 3.10.51과 같은 기본 메커니즘과는 달리 동일한ID의 차상용 단말기의 신호가 수신되더라도 RF신호가 끊긴 후 다시 수신되면 새롭게 처음부터 경보신호가 동작되도록 하는 메커니즘이다.

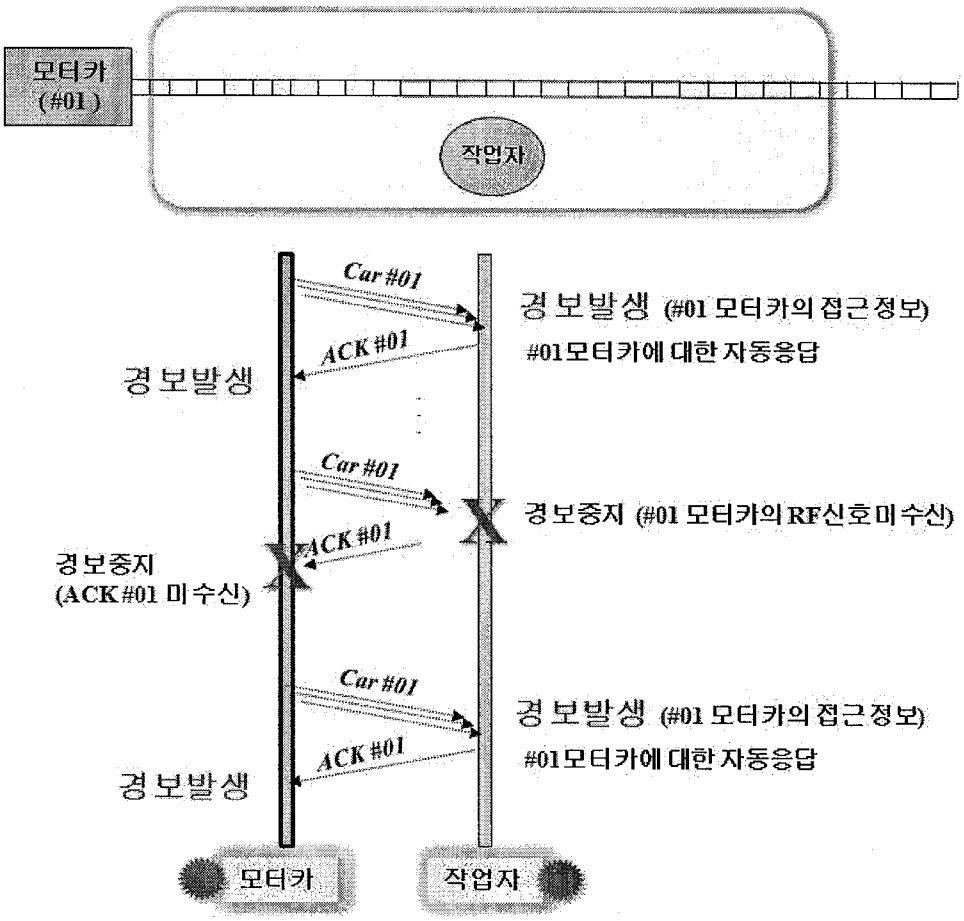


그림 3.10.52 모터카가 전파수신 영역 벗어난 후 후진하는 경우

그림 3.10.52는 모터카가 전파전달 영역을 벗어난 후 재진입하는 경우이지만, 모터카는 특성 상 좁은 영역 내에서 자주 운행을 하므로 작업자에 의한 경보중지 버튼 취급 후 전파전달 영역 내에서 후진하여 작업자에게로 다시 접근할 경우가 있다. 이러한 경우작업자 단말은 경보중지 버튼으로 인해 모터카의 진입을 경보하지 않음으로 사상사고가 발생할 가능성이 있다. 따라서 이에 대한 해결책으로 그림 3.10.53과 같이 일정시간 후 동일한 차상용단말기로부터 RF신호를 수신하면 다시 경보가 발생하도록 하는 메커니즘을 구현하였다. 설정시간은 운영기관의 모터카 운행 특성에 따라 가변되어질 수 있으며, 본연구의 시제품에서는 60초로 설정하였다.

그림 3.10.53에서는 모터카 #1과 작업자와의 경보동작 메커니즘은 앞에서 설명한 몇 가지 케이스와 동일하게 동작하지만, 추가적으로 모터카 사이의 경보동작 메커

니즘을 설명한 그림이다. 그림에서와 같이 모터카 #1이 접근할 경우 경보가 그림 3.10.53과 같이 동작을 하며, 만약 모터카 #2가 연속해서 작업자의 전차전달 영역 내로 접근할 경우에도 그림과 같이 작업자 단말기는 경보신호를 발생시키며, 또한 모터카 #1은 모터카 #2로부터 RF신호를 수신하면 경보신호를 그림과 같이 경보신호를 발생시키고 모터카 #2의 단말기로 피드백 시켜 모터카 #2의 차상단말기에 경보를 발생시키게 된다. 이때 차상단말기는 작업자에 의한 경보인지 다른 모터카에 의한 단말기인지에 따라 경보신호를 달리 표출토록 하여 운전자로 하여금 이에 따라 안전운전을 유도할 수 있도록 하였다.

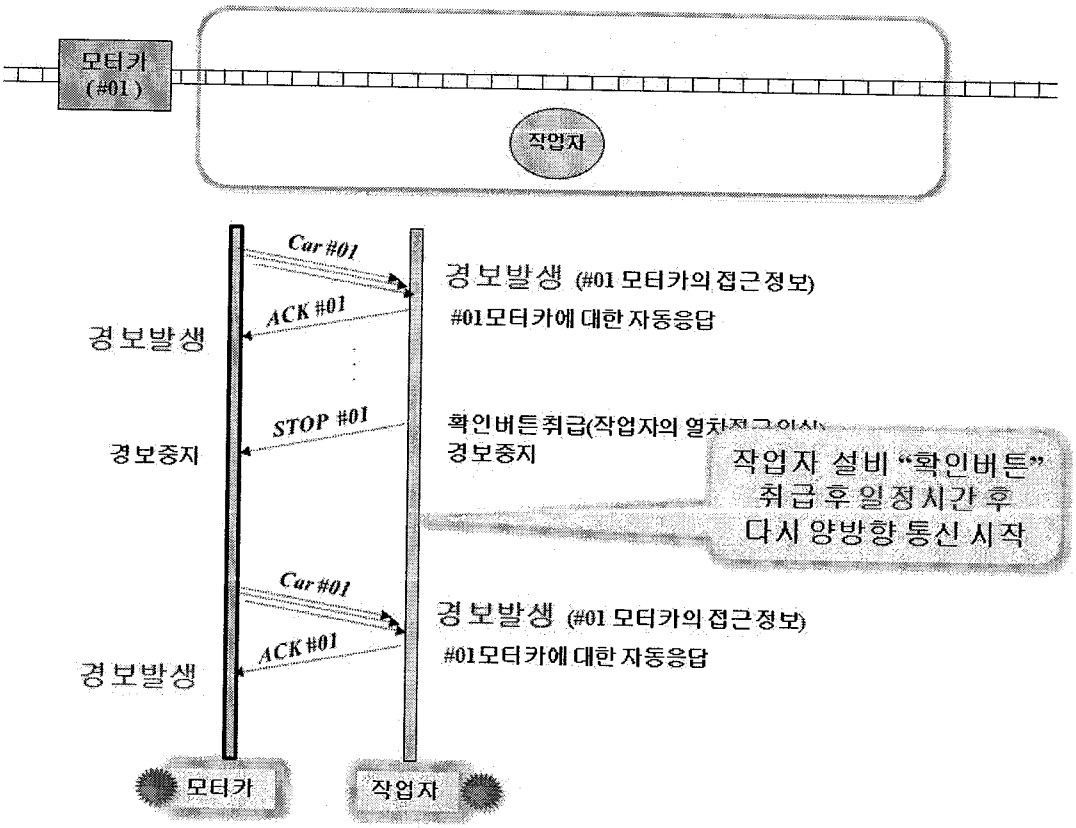


그림 3.10.53 모터카가 전파수신 영역 내에서 후진할 경우

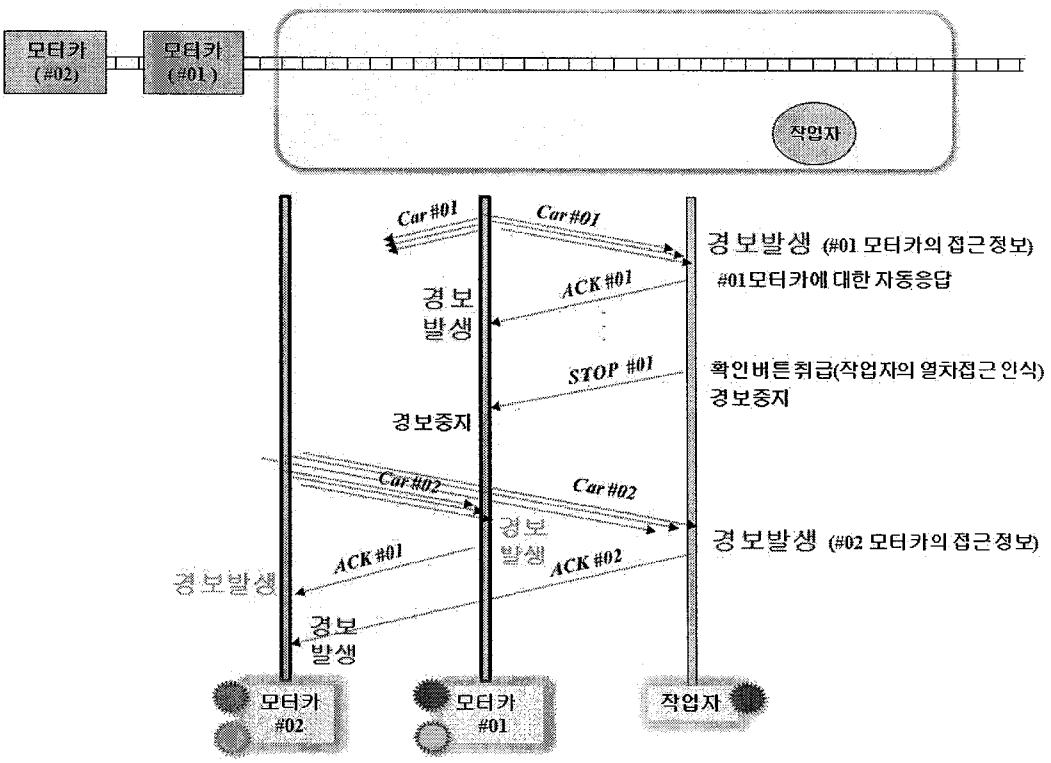


그림 3.10.54 모터카↔작업자 및 모터카 사이의 경보 동작 메커니즘

③ 시제품의 제작 및 현장 시험

앞에서 설계한 내용을 바탕으로 시제품을 제작하고 철도운영 현장에서 시험을 수행하였다. 그림 3.10.45는 본 연구를 통해 개발한 시제품의 작업자용 단말기이며, 그림 3.10.56은 차량용 단말기의 사진이다. 각 각 오른 쪽 사진은 경보신호가 표출되었을 경우의 사진으로, 작업자용의 경우 붉은 색 LED와 파란색의 고휘도 LED가 동작되어 작업자 본인뿐 아니라 인접하고 있는 작업자가 경보신호를 확인할 수 있도록 하였다.

작업자용 단말기의 경우 작업자가 휴대하기 편한 구조로 설계 되었으며, 작업자의 허리에 부착할 수 있는 구조로 되어 있다. 또한 단말기의 전원은 8시간 정도의 사용시간을 가지는 고용량 충전 배터리를 사용하여 작업자가 편리하게 사용할 수 있도록 하였다. 그림 3.10.56의 차량용 단말기의 경우 경보음의 소리를 조절할 수 있는 구조로 되어 있으며, LCD 표시 Panel을 통해 접근하는 작업자 단말기의 고유번호를 표시하도록 하였다. 또한 모터카의 차량전원을 사용하며, 별도의 전원 스위치를 설계하지 않음으로 인해 차량운행 중에는 반드시 본 안전설비의 전원이 인가

되도록 하였다. 즉, 운전자에 의해 임의로 본 설비의 전원을 차단하지 목하는 구조로 설계하였다. LED 경보의 경우 접근하는 다른 모터카인지와 작업자인지를 확인하여 다른 컬러 LED(붉은색, 초록색)를 사용하여 모터카인지 작업자인지 구분할 수 있도록 하였다.

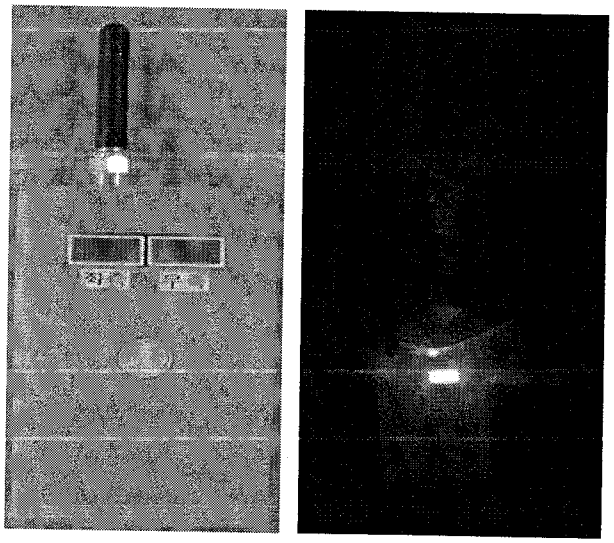


그림 3.10.55 작업자용 단말기 시제품

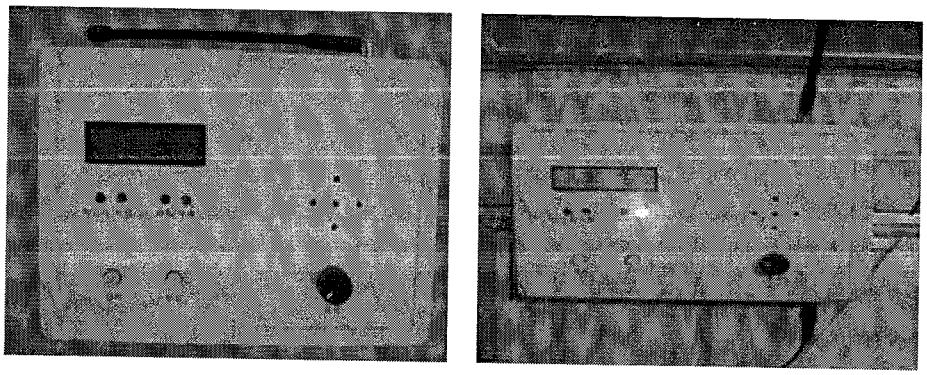
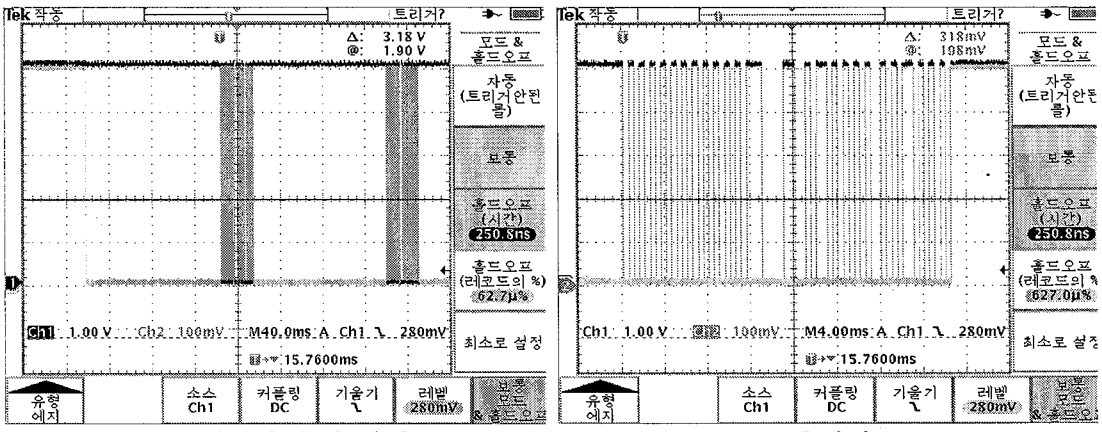


그림 3.10.56 차상용 단말기 시제품

그림 3.10.57은 차상장치에서 출력되는 신호의 파형을 나타낸 것으로 (a)는 주기적으로 신호를 송신하고 있는 파형이며, (b)는 전송 프레임 송신하는 출력파형을 나타낸 것이다. 이러한 차상장치로부터의 출력 신호는 일정 거리 이내에 작업자용 포터블 장치가 수신할 경우 이 전송신호를 디코딩하여 다양한 경보신호를 출력하게 된다.



(a) 주기적인 출력 파형 (b) 출력신호

그림 3.10.57 차상 안전설비 출력신호

④ 현장시험 및 시범설치

개발 시제품의 성능시험을 위해 서울메트로의 선로에서 몇 번의 현장시험을 수행하였으며, 현장시험에서는 차상장치에서의 주기적인 RF 신호가 작업자용 안전설비가 정상적으로 수신하여 진동, 부저 및 LED 형태의 경보음을 표출하는 지와 모드전환 스위치나 열차의 진행 방향이 정상적으로 표출되는지 등 기능시험을 수행하였다. 또한 차상설비와 작업자용 설비와의 전파전달거리는 현장시험을 통해 약 230~270 m 정도로 측정되었으며, 이러한 전파전달 거리는 본 안전설비의 요구사항을 충족하고 있음을 확인하였다. 시험현장은 지하구간, 지상구간, 플랫폼 구간 등 다양한 현장조건에 따라 수행되었으며, 특히 전파전달거리 및 성능시험을 위해 곡선반경이 150R인 구간에서 시험을 수행하였다. 그림 3.10.58은 차상설비 및 작업자 단말기의 현장시험 사진을 나타낸 것으로, 작업자 단말기 시험사진에서와 같이 다양한 철도운영환경에서 시험을 수행하였다. 지하구간에서 현장시험 결과 지상에서 시험한 경보표출 메커니즘이 충분히 표출되고 정상적으로 동작하는 최소 전파전달 거리는 약 230m 정도로 측정되었다. 230m 정도의 전파전달 거리는 도시철도 운영기관에서 요구하는 가장 이상적인 거리로서, 시제품의 전파전달 거리가 요구되는 성능을 만족함을 현장시험을 통해 확인하였다.

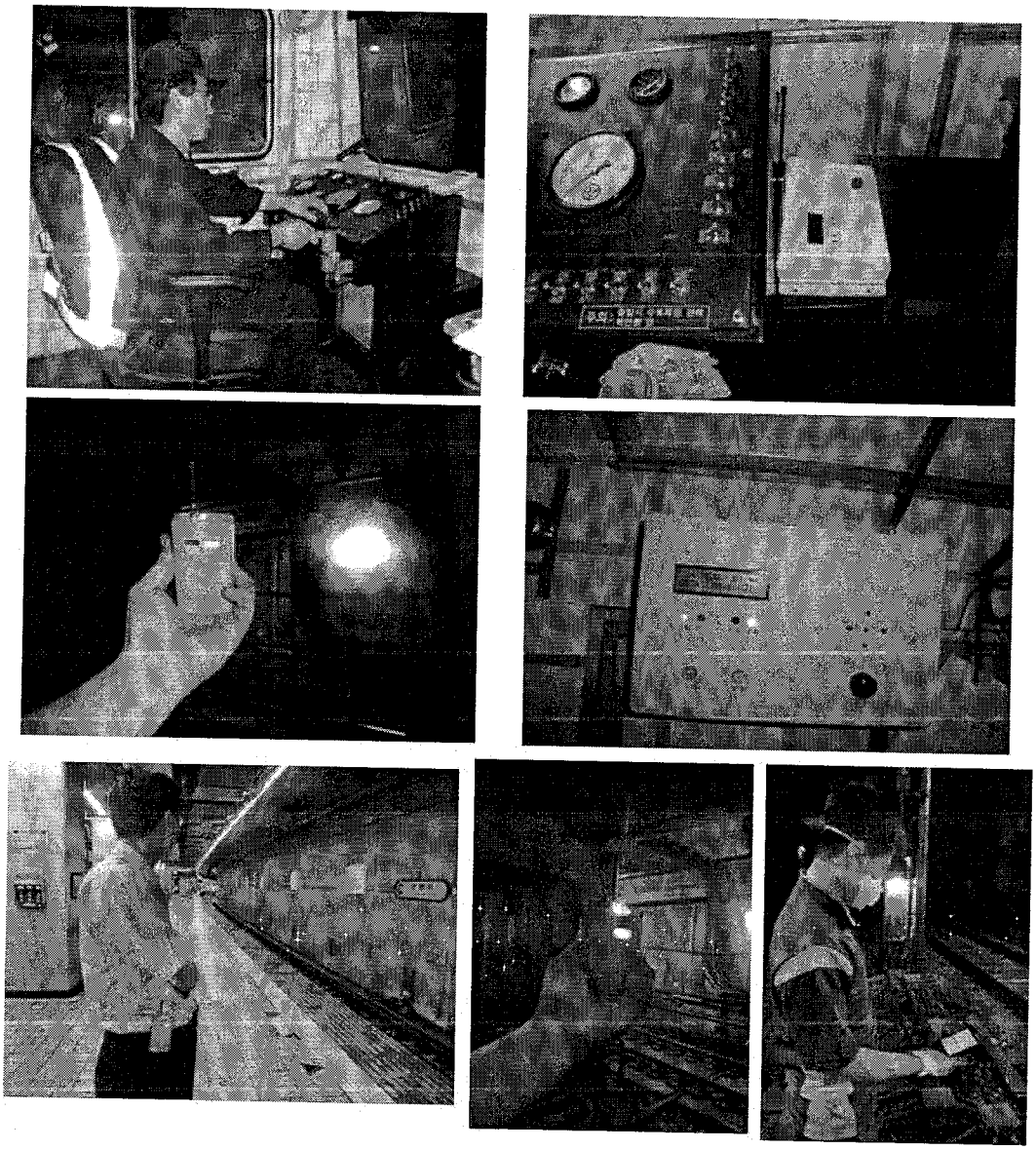


그림 3.10.58 현장시험 사진

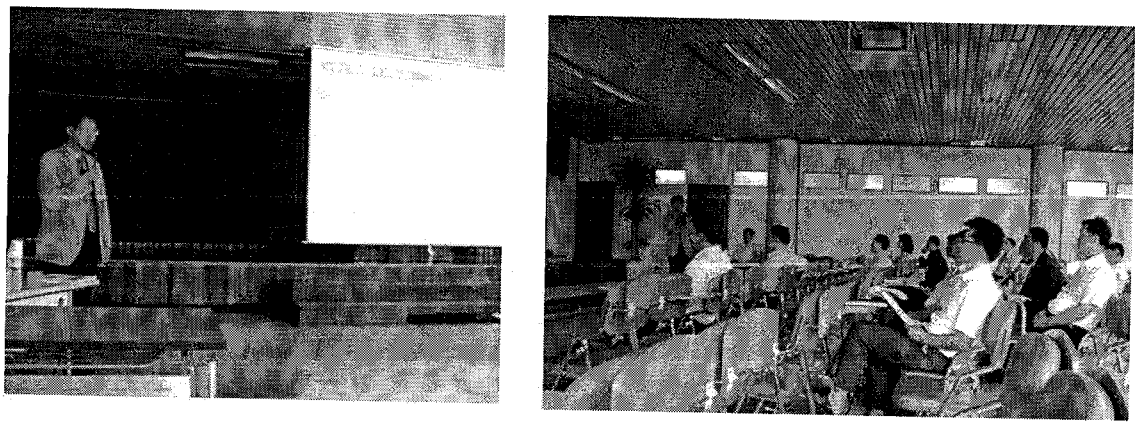


그림 3.10.59 개발시제품의 서울메트로 시연회 사진

당해연도에는 앞에서 설명한 바와 같이 시제품의 현장시험을 수행하여 그 성능을 검증하였으며, 또한 개발 시제품의 실용화를 위해 '09년 9월 서울메트로에서 시연회를 개최하였다. 이 시연회를 통해 철도운영기관에서의 본 개발 시제품의 효용성을 확인하였으며, 또한 다양한 의견을 수렴하였다. 시연회를 통해 수렴된 다양한 의견들을 서울메트로 담당부서와 협의를 통해 본 시제품에 일부 반영하여 시제품을 보완제작하였으며 이를 통해 '10.3월 말부터 서울메트로의 군자, 창동, 수서 차량기지의 모터카에 시범설치하여 현재 운용 중에 있다. 약 3개월간의 시범설치 및 운용을 통해 시제품의 성능, 효용성 등을 분석 후 차년도에 상용화를 추진할 예정에 있다.

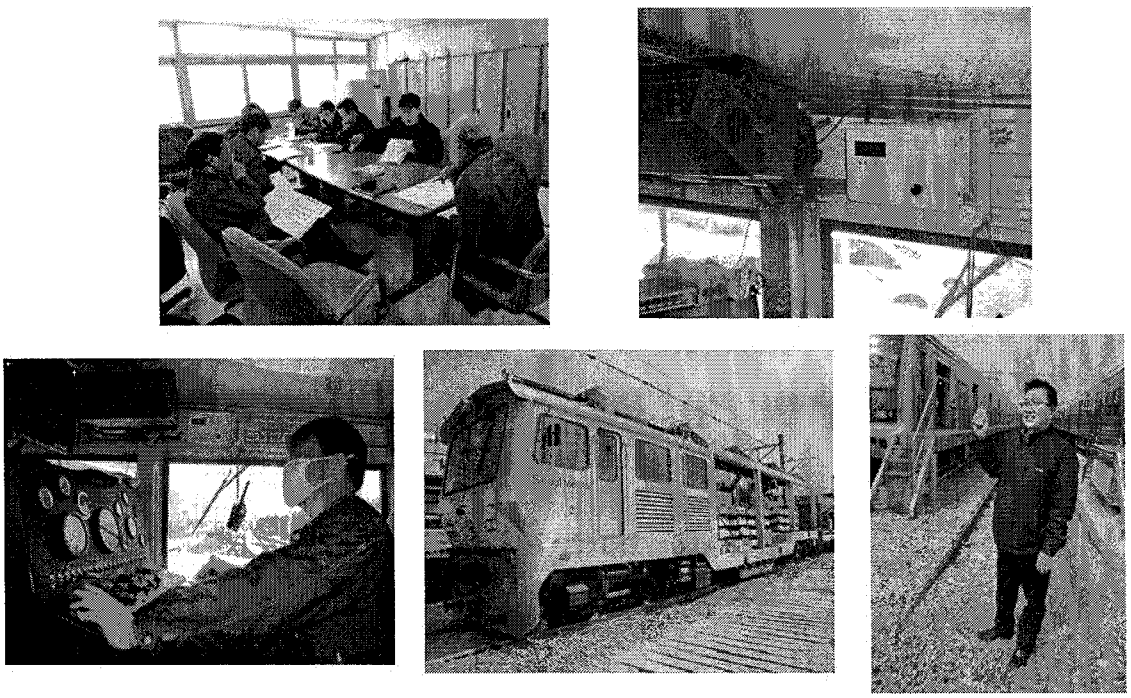


그림 3.10.60 시제품 시범설치 및 운용방법 교육 사진

제 4 장 연구개발 목표달성도 및 관련분야 기여도

1. 목표 달성도

가. 당해 연도 목표 및 평가의 착안점

○ 당해 연도 연구개발 목표

열차제어시스템 안전성 평가 및 향상기술의 보완

○ 당해 연도 주요 연구내용

- 철도안전SE 과제와의 연계사항 관리 및 조정
- 열차제어시스템 안전향상 핵심기술 개발(4)
  - · 고안전성 연산처리 장치 시제품 보완제작 및 통합시험 수행
  - · 고안전성 연산처리 장치 시제품 평가메트릭 제시
  - · 열차제어시스템을 위한 정형명세 작성 및 검증 절차 제시
  - · Zed와 Statechart를 이용한 정형명세 작성 및 검증절차 적용 예 제시
  - · 선로전환결함 방지기술 관련 각종 설비 및 요구사항 분석
- 열차제어시스템 안전성 평가기술 개발(4)
  - · 안전성 평가기술 적용성 연구를 위한 대상시스템 보완제작
  - · 대상시스템 시험을 위한 시뮬레이터 제작 및 시험
  - · 열차제어시스템 안전성 평가이드라인 보완작성
  - · 대상시스템 안전성 활동 수행 및 안전성 활동 기술지침 초안 작성
  - · 열차제어시스템 S/W 안전성 테스트 툴 설계 및 시제품 제작
- 열차제어측면의 사상사고 저감기술 개발(2)
  - · 플랫폼 공중사상사고 저감을 위한 3D 레이저레이더를 이용한 안전설비 상세 설계 및 시제품 제작
  - · 무선을 이용한 작업자 사상사고 저감 안전설비 시제품 보완 제작 및 현장시험

○ 당해 연도 정량적 성과지표

표 4.1.1 사업계획서의 정량적 성과지표

성과지표	목표치	성과물 명칭
논문	- 학술지 논문 게재 4건 - 학술회의 발표논문 2건	학술논문
특허	- 특허출원 및 등록 3건 (S/W 등록 포함)	특허 및 SW 출원증/ 등록증
기술지원	- 산학연 기술지원 2건	
홍보	- 기술개발결과 홍보 2건	언론기사 등
시제품 제작	- 시제품 3건 · 열차제어시스템 SW 테스팅 자동화 도구 3개 하부 모듈(Boundary Value Analysis 모듈, Equivalence Classes 테스팅, Fault Tree Analysis 테스팅 모듈) · 선로변 작업자 사상사고 저감 안전설비 시제품 · 고안전성 연산처리장치 시제품(TMR 시제품)	시제품

○ 당해 연도 연구개발 결과

연구내용	연구결과
◦ **열차제어시스템 안전성 향상 핵심기술 개발 (4)** - 열차제어시스템을 위한 고안전성 연산처리 장치 시제품 보완제작	◦ **열차제어시스템 안전성 향상 핵심기술 개발 (4)** **① 열차제어용 고안전성 연산처리장치 시제품 보완제작** -고안전성 연산처리 장치 시제품 보완제작 통합시험 수행 -시제품 인터페이스를 위한 바이탈 I/O 보드 제작 -열차제어용 고안전성 연산처리장치 평가메트릭 제시

	-시제품 Safety Case 작성 -열차제어용 고안전성 연산처리장치 설치 및 운용을 위한 기술지침(안) 작성
- 열차제어시스템을 위한 정형기법 적용방안 제시	**② 열차제어시스템을 위한 정형기법 적용 방안 제시** -열차제어시스템을 위한 정형명세 작성 및 검증 절차 제시 -Zed와 Statechart를 이용한 정형명세 작성 및 검증 절차 적용 예 제시
- 선로전환 결함 방지기술 분석 및 요구사항 제시	**③ 선로전환 결함방지기술 조사분석** -선로전환 결함관련 장애사례 조사분석 -선로전환 결함 방지관련 각종 설비 및 요구사항 분석
◦ **열차제어시스템 안전성 평가기술 개발(4)** - 안전성 평가활동 및 평가 적용성 기술 개발	◦ **열차제어시스템 안전성 평가기술 개발(4)** **① 안전성 평가기술 적용성 연구를 위한 대상시스템 보완제작** - 안전성 평가기술 적용성 연구를 위한 평가대상 시스템 시제품(CRD 시스템) 보완제작 및 시험
	② 평가대상 시스템 안전성 활동 수행 -대상 시스템 안전성 활동 수행(Consequence Analysis, Causal Analysis, SIL 결정 및 할당) -대상시스템 Safety Case 작성(1) -열차제어시스템 안전성 활동 기술지침 초안 작성
- 평가대상 시스템 시험을 위한 시뮬레이터 제작(2)	**③ 평가대상 시스템 시험을 위한 시뮬레이터 제작** -대상 시스템 시뮬레이터 보완제작(ATS 시

	뮬레이터, 차상 시뮬레이터, 신호시뮬레이터) -대상 시스템 안전측 동작 검증 시뮬레이터 제작 -평가대상 시스템과 인터페이스 시험 수행
- 열차제어시스템 안전성 평가 가이드라인 수정안 작성	**④ 열차제어시스템 안전성 평가 가이드라인 보완작성** -열차제어시스템 안전성 활동 기술체계 보완작성 -열차제어시스템 안전성 평가 가이드라인 보완작성 -리스크 분석기법(HAZOP-KR) 정리 -열차제어시스템 안전성 평가를 위한 체크리스트 작성
- 열차제어시스템 SW 테스팅 자동화도구 시제품 제작(3)	**⑤ 열차제어시스템 S/W 안전성 테스트 툴 설계 및 시제품 제작** -열차제어시스템 S/W 테스팅 자동화도구 설계 및 3차 시제품 제작(3개 하부모듈) -개발도구를 통한 평가대상시스템 소프트웨어의 테스팅 수행 -열차제어시스템 SW 테스팅 기술지침 초안 작성
◦ 열차제어측면의 사상사고 저감기술 개발(2)	**◦ 열차제어측면의 사상사고 저감기술 기본설계**
- 플랫폼 공중사상사고 저감 안전설비 상세설계 및 시제품 제작	**① 플랫폼 공중사상사고 저감 안전설비 상세설계 및 시제품 제작** -플랫폼 공중사상사고 저감을 위한 3D 레이저레이더를 이용한 안전설비 상세설계 -시제품 제작 및 시험
- 선로변 작업자 사상사고 저감 안전설비 시제품 보완제작 및 시험	**② 선로변 작성자 사상사고 저감 안전설비 시제품 제작 및 현장시험** -무선을 이용한 작업자 사상사고 저감 안전

	설비 시제품 보완 제작 및 현장시험 -작업자 사상사고 저감 안전설비 시제품 철도 운영기관 대상 시연회 개최 및 시범설치 운용 중(서울메트로 군자/창동/수서 차량기기)

○ 목표달성도 및 자체평가

연구내용	자체평가	달성도
열차제어시스템 안전성 향상 핵심기술 개발	-열차제어시스템 안전성 향상 핵심기술 개발 · 열차제어시스템을 위한 고안전성 연산처리장치 시험을 위한 바이탈 I/O 보드를 제작하는 등 시제품의 보완제작 및 시험이 수행되었으며, · 시제품의 시험을 통한 열차제어용 고안전성 연산처리장치 평가 메트릭을 제시하였음 · 국내에서 처음으로 정형기법에 대한 분석을 통해 평가대상 시스템 일부모듈을 Z와 Statechart에 의해 정형명세화 및 정형검증을 통한 실증연구에 의한 정형검증 방법을 제시하였음 · 선로전환 결함 방지를 위한 각종 설비들 및 요구사항을 조사분석하는 등 목표를 달성하였음 · 이러한 연구를 통한 특허를 출원하고 학술지 논문을 게재하는 등 연구결과가 우수함	110 %
사상사고 저감기술 개발	-사상사고 저감을 위한 안전설비 설계 및 시제품 제작 · 플랫폼 공중사상사고 저감을 위한 3D 레이저레이더 센서를 이용한 안전설비의 설계 및 시제품 제작이 수행되었음 · 또한 작업자 사상사고 저감을 위한 안전	120 %

	설비 시제품의 보완제작 및 철도운영기관 시연회 개최, 시제품의 시범설치하는 등 연구계획 이상의 연구성과를 달성하였음 · 본 연구를 통해 특허출원 및 학술지 논문을 게재하는 등 연구성과가 우수하며, 또한 철도운영기관을 대상으로 한 개발기술의 시연회 개최, 시범설치 및 시범 운용중에 있는 등 개발 기술의 실용화를 위한 많은 성과가 있었음	
열차제어시스템 안전성 평가기술 개발	-열차제어시스템 안전성 평가기술개발 · 적용성 연구를 위한 대상시스템 및 시뮬레이터의 보완제작, 대상시스템의 안전성 활동 수행, 국내 철도시스템에 적합한 안전성 활동 기술체계 및 HAZOP-KR 방법을 제시 등의 연구를 수행 · 전년도에 작성한 평가 가이드라인을 해외 전문기관의 기술자문을 통해 수정보완하였으며, · 열차제어시스템 소프트웨어 테스팅 자동화 도구 하부모듈 3개를 제작하였고, 대상시스템 SW에 적용성 시험을 수행하였음 · 외국의 안전성 평가전문기관(독일 TUV SUD)을 통한 연구내용에 대한 기술자문을 수행 · 개발한 SW 테스팅 자동화 도구 일부 하부모듈에 대해서는 당해연도에 기술이전을 실시하였고, 또한 실용화를 위한 SW 테스팅 기술지침 초안을 작성하는 등 개발기술 실용화를 위한 많은 성과가 있었으며, · 테스팅 자동화 도구 등 목표로 하는 시제품을 제작 하였으며, 또한 본 연구를 통한 많은 학술논문과 특허등록이 되는 등 연	110 %

	구성과가 우수함. -산·학·연 특성별 연구협조체계 구축에 의한 기술개발(LS산전, 대아TI, AB&I, 부경대)	
기타	본 과제의 당해연도 연구를 통해 다음과 같은 정량적 연구실적을 달성하였음 **o 지적재산권 확보 : 11건** - 국내특허 등록 : 3건 - 국내특허 출원 : 3건 - 소프트웨어 등록 : 5건 **o 학술지 논문 게재 : 6건** - 국내 전문학술지 : 4건 - 국내 전문학회 학회지 게재 : 2건 **o 학술대회 발표 : 16건** - 국제학술대회 발표 : 8건 - 국내학술대회 발표 : 8건 **o 시제품 제작 : 5건** - 열차제어시스템 SW 테스팅 자동화 도구 3개 하부 모듈(Boundary Value Analysis 모듈, Equivalence Classes 테스팅, Fault Tree Analysis 테스팅 모듈) - 선로변 작업자 사상사고 저감 안전설비 시제품 - 고안전성 연산처리장치 시제품(TMR 시제품) **o 기술자문 : 3건** - 산업계 개발기술 보급 외 · 제목 : "철도신호 RAMS 기술교육" 실시 · 대상 : 철도운영기관 신호시스템 실무 담당자 **o 연구개발관련 홍보 : 3건**	

	- 기술개발 결과의 철도운영기관 대상 시연회 개최 및 연구결과의 신문기사 **o 기술이전 : 1건** - 기술이전 협약체결 : SW 테스팅 자동화 도구 소스코드 분석 모듈('09.11.) - 기술이전 협의 중 : 선로변 작성자 사상사고 저감 안전설비	

2. 연구개발의 활용계획

가. 기대효과

◦ 기술적 측면

- 열차제어시스템 안전성 평가기술의 개발로 열차제어시스템의 안전성 확보 및 평가가 가능
- 안전성 향상을 위한 고안전성 연산처리 시스템 기술 및 정형기법에 의한 바이탈한 열차제어시스템의 소프트웨어 설계기술의 개발로 열차제어시스템의 안전성 향상이 기대됨
- 국내 기술로 열차제어시스템 안전성 향상 및 평가기술의 개발로 철도선진국과 동등한 안전성 관리가 가능

◦ 경제·산업적 측면

- 열차제어시스템 안전성활동 체계에 실행기술과 이의 평가기술 확보를 통한 안전성 관련 국제규격에 따른 시스템의 개발 및 운용이 가능하며, 또한 국내 열차제어시스템의 수입대체효과 기대
- 열차제어시스템의 안전성 평가기술의 국산화를 통해 국내 시스템이 기술 및

가격 경쟁력을 갖추게 되면 독자적인 세계시장 진출이 가능

- 열차제어시스템을 위한 안전성 활동 및 평가관련 전문 인력 확보가능

나. 활용방안

◦본 연구를 통해 확보할 열차제어시스템 안전성 활동 수행기술과 평가기술은 국내 운용기관, 제작사 등에 활용이 가능함

◦사고억제 및 안전성 향상을 위한 고안전성 연산처리 시스템 기술 및 정형기법에 의한 열차제어시스템 소프트웨어 설계 기술은 국내 열차제어시스템의 신뢰성 및 안전성 향상에 기여할 것으로 예상됨

◦또한 당해연도의 연구결과인 고안전성 연산처리 장치 시제품 제작 및 시험 결과는 열차제어시스템을 위한 고안전성 연산처리 장치성능평가 메트릭 분석에 활용되는 등 차년도 연구 수행에 활용

◦평가대상 시스템에 의한 적용성 연구를 통한 열차제어시스템 안전성 평가기술은 국내의 열차제어시스템의 평가 및 인증을 위한 기반 기술로 활용될 수 있으며, 국내에서 개발되는 열차제어시스템의 안전성 향상에 기여할 것으로 기대됨

◦당해년도에 설계 및 일부 제작한 열차제어시스템 소프트웨어 테스팅 자동화 도구는 본 과제에서 제작 중인 평가대상 시스템 S/W 테스팅에 우선적으로 활용할 예정이며, 또한 국내 열차제어시스템 시험 및 평가를 위한 기반 인프라 설비로 활용 가능

◦또한, 3차년도에 걸쳐 성공적인 테스트 자동화 툴이 개발하여 상용화를 추진할 계획이며, 이를 통해 국내 제작사나 평가기관 뿐만 아니라 외국에도 수출이 가능한 테스트 도구를 개발하고자 함.

◦열차제어시스템 안전성 활동 및 평가관련 기술은 국내 열차제어시스템 안전성 관련 기술교육 등을 통한 전파 및 홍보 예정임

다. 실용화 방안

본 연구를 통한 실용화 가능한 연구내용은 최대한 실용화를 할 수 있도록 연구과정에서 추진할 계획임

◦열차제어시스템 안전성 평가기술

- 열차제어시스템 안전성 활동 기술체계 및 평가 가이드라인 : 이 연구내용은 열차제어시스템 운영기관 및 제작사에 관련 연구결과를 홍보 및 전파를 통한 실용화를 추진 및 계획하고 있음. 예를 들어 본 연구과제에서 이미 수행한 바 있는 철도운영기관을 대상으로 한 "철도신호 RAMS 기술교육" 등을 통해 연구결과를 지속적으로 홍보 및 전파를 계획하고 있음
- 열차제어시스템 소프트웨어 테스팅 자동화 도구 : 본 연구과제를 통해 개발중인 소프트웨어 테스팅 자동화 도구는 평가단계는 물론이고 소프트웨어 개발단계에서도 적극적으로 활용될 수 있도록 개발 중에 있음. 또한 본 영구를 통해 개발한 자동화 도구는 일반 산업용 임베디드 소프트웨어 테스팅에도 커스터마이징을 통한 활용이 가능하므로 소프트웨어 테스팅 제작 전문기관에 기술이전 등을 적극적으로 추진 계획이며, 또한 SW 테스팅 자동화 도구 기술지침(안)을 작성하여 개발도구 실용화를 추진할 계획임
- 적용성 연구를 위한 평가대상 시스템 개발 : 안전성 평가기술 개발을 위한 평가대상 시스템 개발이지만 본 연구과제가 종료된 후 세부연구기관이면서 참여기업인 제작사에를 본 연구과제를 통해 개발한 평가대상 시스템을 활용하여 통신기반 열차제어시스템 개발에 활용될 수 있을 것으로 기대됨

◦ 열차제어시스템 안전성 향상 기술

- 열차제어용 고안전성 연산처리 시스템 기술 : 고안전성 연산처리장치는 열차제어시스템을 위해서는 필수적인 기술로서, 세부주관기관이면서 참여기업인 제작사가 본 연구과제를 통해 개발한 고안전성 연산처리 시스템 기술을 다른 열차제어시스템 제작에 적용될 수 있을 것으로 기대됨
- 정형명세 기술 : 본 연구과제를 통해 개발 중인 정형명세 기술이 확립되게 되면, 논문이나 기술교육 등을 통해 열차제어시스템 제작사에 전파하여 소프트웨어 개발에 적극적으로 활용할 수 있도록 추진할 계획임.

◦ 사상사고 저감기술

- 당해 연도에 개발한 선로변 작업자 사상사고 저감 안전설비의 경우 철도현장에서 시범설치 중이며, 시범설치 결과를 반영하여 시제품의 기능을 보완을 거쳐 기술이전 및 실용화를 추진할 계획임

제 5 장 참고문헌

1. 철도청 지시 제2001-49호, "열차제어시스템 안전성확보기술권고안(2001.7.13)".
2. CENELEC EN 50126, EN 50128, ENV 50129, EN 50159.
3. EN50126, "Railway Applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety(RAMS)", 1999.
4. J.Braband and et al, "The CENELEC-Standards regarding Functional Safety", Eurailpress, 2006.
5. MIL-882, "System safety program requirements", 1993.
6. Yuji Hirao, "New European Norms from a Japanese Viewpoin", Signal+Draft, No. 93, 2001.
7. 기술표준원, "국제전기위원회(IEC) 조직 및 현황", 산업자원부, pp. 3~104, 2003.
8. 平尾裕司외 2명, "鐵道信號における 安全性技術と 安全性技術指針", J-RAIL, 1997.
9. IEC 62278, IEC 62279, IEC 62280-1, IEC 62280-2.
10. IEC 62278, "Railway applications-Specification and demonstration of reliability, availability, maintainability and safety(RAMS)", 2002.
11. IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems", 1998.
12. IEC 61882, "Hazard and operability studies(HAZOP Studies)-Application guide", 2001.
13. NUREG-0492 U.S. Nuclear Regulatory Commission, "Fault Tree Handbook", 1981.
14. RAILTRACK, "Engineering safety management issue 2.0", Volume 3, 1997..
15. RAILTRACK, "Engineering safety management issue 3.0", 2000.
16. 철도청연구보고서, "철도신호제품에 대한 신뢰성과 안전성 검증기준 제정 연구", 2001. 10.
17. Neil Storey, "Safety-critical computer system", Addison-Wesley, 1996.
18. Nigel Hyatt, "Guidelines for process hazards analysis, hazards identification & risk analysis", DYADEM, 2003.

19. Daniel P. Siewiorek, "Reliability computer systems design and evaluation", Digital Press, 1992.
20. R. Ramakumar, "Engineering reliability: fundamentals and applications", Prentice Hall, 1993.
21. Lawrence M. Leemis, "Reliability-probabilistic models and statistical methods", Prentice-Hall International, Inc. 1995.
22. 장주수, "신뢰도예측 가이드", 교우사, 2005.
23. Trevor Kletz, "HAZOP and HAZAN-identifying and assessing process industry hazards", Taylor & Francis, 1999.
24. Felix Redmill, "System Safety: HAZOP and Software HAZOP", John Wiley & Sons, 1999.
25. Draft Defence Standard 00-56, "Safety management requirements for defence systems containing programmable electronics", Ministry of Defence, UK, 1995
26. RAILTRACK, "Systematic risk profiling of railway infrastructure & operations, 2-HAZARD Portfolio", Issue 1, p1-53, 1997.
27. HMSO, "Risk criteria for land use planning in the vicinity of major industrial hazards", UK, 1989.
28. MIL-STD-1629A, "Procedures for performing a failure mode, effects and criticality analysis", 1999.
29. Nicholas J. Bahr, "System safety engineering and risk assessment", Taylor & Francis, 1997.
30. Yacov Y. Haimes, "Risk modeling, assessments and management", Wiley-Interscience, 2004.
31. 송준엽 외 4명, "고장모드 및 영향, 치명도 해석", 교우사, 2005.
32. 철도청, "철도사고사례집. 철도청".
33. 교통안전공단, "철도교통사고예방에 관한 종합연구".
34. 한국철도기술연구원, "철도산업구조개혁 대비 철도안전규제 제도개선 방안연구".
35. 교통안전공단, "도시철도 신호분야 안전관리".
36. 나카무라, "철도수송 시스템의 신뢰성", 신뢰성분석연구센터, 2005.
37. Clifton A. Ericson II, "Hazard Analysis Tchniques for System Safety", John

Wiley & Sons, 2005.

38. ISO/IEC 9126, "소프트웨어 제품 품질 모델 및 측정 표준".
39. ISO/IEC 14598, "소프트웨어 제품의 평가 지침".
40. IEEE 1008, "소프트웨어 단위 테스트 표준".
41. IEEE 1012, "소프트웨어의 검증 및 확인 계획에 대한 표준".
42. 김수동 외 11명, "소프트웨어 테스트 전문기술", 한국정보통신기술협회. 2005.
43. ISO/IEC 9126 소프트웨어 제품 품질 모델 및 측정 표준
44. M. Fewster, D. Graham, "Software Testing Automation: Effective use of test execution tools", ACM Press, Addison Wesley, 1999.
45. 산업자원부 기술표준원, "국제 표준의 SW 품질평가기술과 임베디드 SW", 2005.
46. Dhiraj K. Pradhan, "Fault-Tolerant computer system design", Prentice Hall, 1996.
47. Barry W. Johnson, "Design and analysis of fault-tolerant digital systems", Addison-Wesley Publishing Company, 1989.
48. Parag K. Lala, "Self-Checking and Fault-Tolerant Digital Design", Morgan Kaufmann Publishers, 2001.
49. J.Braband and et al, "Risk-orientated Apportionment of Safety Integrity Requirements - An Example", SIGNAL+DRAHT, Vol. 1+2, 2000.
50. ISO/IEC 9796, "Information technology - Security techniques - Digital signatures scheme giving message recovery", 1991.
51. ISO/IEC 9797, "Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", 1994.
52. ISO/IEC 9979, "Information technology - Security techniques - Procedures for the registration of cryptographic algorithms", 1999.
53. ISO/IEC 10118-1, "Information technology - Security techniques - Hash-functions - Part 1 : General", 2000.
54. ISO/IEC 10118-2, "Information technology - Security techniques - Hash-functions - Part 2 : Hash-functions using an n-bit block cipher", 2000.
55. ISO/IEC 11770-1, "Information technology - Security techniques - Key management - Part 1 : Framework", 1997.

56. ISO/IEC 11770-2, "Information technology - Security techniques - Key management - Part 2 : Mechanisms using symmetric techniques", 1996.
57. ISO/IEC 11770-3, "Information technology - Security techniques - Key management - Part 3 : Mechanisms using asymmetric techniques", 1999.
58. FIPS PUB 46, "Specifications for the Data Encryption Standard", 1977.
59. RFC 1321, "The MD5 Message-Digest Algorithm", 1992. 4,
60. NIST Special Publication 800-67 Ver.1, "Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher", pp.13-15, May 2004.
61. TTAE.IF-RFC3562, "TCP MD5 서명 옵션을 위한 키관리 고려사항", 2006.
62. TTAE.IF-RFC 3217, "TRIPLE DES와 RC2 Key 싸기", 2005.
63. Laprie J. C., "Dependable Computing and Fault Tolerance: Concepts and Terminology", Proceeding of FTCS-25, Vol. 3, pp. 2-11, 1996.
64. Bowen J. P., Stavridou V., "Safety-Critical Systems, Formal Methods, and Standards", IEE/BCS Software Engineering Journal, Vol. 8, No. 4, pp. 189-209, 1993.
65. Dehbonei D., Mejia F., "Formal Methods in the Railway Signalling Industry", in Naftalin et. al., pp. 26-35, 1994.
66. Gnesi S., Latella D., Lenzini G., Abbaneo C., Amendola A., Marmo P., "A Formal Specification and Verification of a Safety Critical Railway Control System", Proceedings of the 5th International Workshop on Formal Methods from Industrial Critical Systems, 2000.
67. Hussey A., "HAZOP Analysis of Formal Models of Safety-Critical Interactive Systems", Fowler & Bennett, pp. 250-263, 2000.
68. Bohn J., Damm W., Wittke H., Klose J., Moik A., "Modeling and Validating Train System Applications Using Statemate and Live Sequence Charts", Proceedings of Integrated Design and Process Technology, 2002.

Wiley & Sons, 2005.

38. ISO/IEC 9126, "소프트웨어 제품 품질 모델 및 측정 표준".
39. ISO/IEC 14598, "소프트웨어 제품의 평가 지침".
40. IEEE 1008, "소프트웨어 단위 테스트 표준".
41. IEEE 1012, "소프트웨어의 검증 및 확인 계획에 대한 표준".
42. 김수동 외 11명, "소프트웨어 테스트 전문기술", 한국정보통신기술협회. 2005.
43. ISO/IEC 9126 소프트웨어 제품 품질 모델 및 측정 표준
44. M. Fewster, D. Graham, "Software Testing Automation: Effective use of test execution tools", ACM Press, Addison Wesley, 1999.
45. 산업자원부 기술표준원, "국제 표준의 SW 품질평가기술과 임베디드 SW", 2005.
46. Dhiraj K. Pradhan, "Fault-Tolerant computer system design", Prentice Hall, 1996.
47. Barry W. Johnson, "Design and analysis of fault-tolerant digital systems", Addison-Wesley Publishing Company, 1989.
48. Parag K. Lala, "Self-Checking and Fault-Tolerant Digital Design", Morgan Kaufmann Publishers, 2001.
49. J.Braband and et al, "Risk-orientated Apportionment of Safety Integrity Requirements - An Example", SIGNAL+DRAHT, Vol. 1+2, 2000.
50. ISO/IEC 9796, "Information technology - Security techniques - Digital signatures scheme giving message recovery", 1991.
51. ISO/IEC 9797, "Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm", 1994.
52. ISO/IEC 9979, "Information technology - Security techniques - Procedures for the registration of cryptographic algorithms", 1999.
53. ISO/IEC 10118-1, "Information technology - Security techniques - Hash-functions - Part 1 : General", 2000.
54. ISO/IEC 10118-2, "Information technology - Security techniques - Hash-functions - Part 2 : Hash-functions using an n-bit block cipher", 2000.
55. ISO/IEC 11770-1, "Information technology - Security techniques - Key management - Part 1 : Framework", 1997.

56. ISO/IEC 11770-2, "Information technology - Security techniques - Key management - Part 2 : Mechanisms using symmetric techniques", 1996.
57. ISO/IEC 11770-3, "Information technology - Security techniques - Key management - Part 3 : Mechanisms using asymmetric techniques", 1999.
58. FIPS PUB 46, "Specifications for the Data Encryption Standard", 1977.
59. RFC 1321, "The MD5 Message-Digest Algorithm", 1992. 4,
60. NIST Special Publication 800-67 Ver.1, "Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher", pp.13-15, May 2004.
61. TTAE.IF-RFC3562, "TCP MD5 서명 옵션을 위한 키관리 고려사항", 2006.
62. TTAE.IF-RFC 3217, "TRIPLE DES와 RC2 Key 싸기", 2005.
63. Laprie J. C., "Dependable Computing and Fault Tolerance: Concepts and Terminology", Proceeding of FTCS-25, Vol. 3, pp. 2-11, 1996.
64. Bowen J. P., Stavridou V., "Safety-Critical Systems, Formal Methods, and Standards", IEE/BCS Software Engineering Journal, Vol. 8, No. 4, pp. 189-209, 1993.
65. Dehbonei D., Mejia F., "Formal Methods in the Railway Signalling Industry", in Naftalin et. al., pp. 26-35, 1994.
66. Gnesi S., Latella D., Lenzini G., Abbaneo C., Amendola A., Marmo P., "A Formal Specification and Verification of a Safety Critical Railway Control System", Proceedings of the 5th International Workshop on Formal Methods from Industrial Critical Systems, 2000.
67. Hussey A., "HAZOP Analysis of Formal Models of Safety-Critical Interactive Systems", Fowler & Bennett, pp. 250-263, 2000.
68. Bohn J., Damm W., Wittke H., Klose J., Moik A., "Modeling and Validating Train System Applications Using Statemate and Live Sequence Charts", Proceedings of Integrated Design and Process Technology, 2002.

주 의 사 항

1. 본 보고서는 국토해양부가 출연하고 한국건설교통기술평가원에서 위탁시행 한 미래철도기술개발사업의 연차 연구보고서입니다.
2. 본 보고서의 내용을 발표할 때에는 반드시 국토해양부가 출연하고 한국건설교통기술평가원에서 위탁시행 한 미래철도기술개발사업임을 밝혀야 합니다.
3. 국가보안 차원에서 필요하다고 인정되는 내용은 대외적으로 발표 및 공개하여서는 아니됩니다.

본 보고서와 관련하여 문의를 원하시는 분은 아래의 문의처로 연락을 주시기 바랍니다.

■ 문의처 : 한국건설교통기술평가원 TEL 031)389-6472
한국철도기술연구원 TEL 031)460-5400
LS산전(주) TEL 031)450-7502
대아티아이(주) TEL 032)680-0895
에이알텍(주) TEL 02)837-5576

R&D /

열차제어시스템 안전성능 평가 및
사고방지기술 개발 연구보고서

■ 발행일 / 2010. 06 . .
■ 발행처 / 한국철도기술연구원
경기도 의왕시 월암동 360-1
TEL : 031-460-5000(대)
■ 인쇄처 / 도서출판 성균사