열차제어시스템 안전성 활동 기술체계의 분석 및 적용

황종규† · 조현정 · 한찬희* · 조우식* · 안 진*
한국철도기술연구원 열차제어통신연구실 · *대아티아이(주) 연구소
(2009. 9. 12. 접수 / 2010. 1. 22. 채택)

Development and Application of Safety Activity Process for Railway Signaling Systems

Jong-gyu Hwang† · Hyun-jeong Jo · Chan-hee Han* · Woo-sick Cho* · Jin Ahn*
Korea Railroad Research Institute(KRRI)
*DaeaTI R&D Center
(Received September 12, 2009 / Accepted January 22, 2010)

Abstract : As safety-related regulations for signaling systems are standardized to IEC 61508/62278/62425, and others at the international level, safety activities and its assessment are required to be performed. And also there is the need to develop technologies for safety improvement to secure safety signaling systems in terms of technologies for safety activities on each life-cycle. In this paper we have developed the safety activity processes and technologies each steps of proposed processes respectively for railway signaling systems. And the proposed process and technologies are applied to the safety activities for mock-up signaling systems.
Key Words : safety activity system, hazard identification, risk analysis and estimation

1. 서 론

철도 시스템에서 열차제어시스템(Railway Signaling System)은 열차의 안전운행을 책임지는 바이탈한 제어설비로, 높은 안전성과 신뢰성이 요구된다. 이러한 열차제어시스템은 기존에는 기계 및 전기식 장치에 의해 안전성이 보장되었지만, 최근의 컴퓨터 기술 발달에 따라 열차제어시스템이 소프트웨어에의 의존성이 증가되게 되되고 있다. 이처럼 컴퓨터와 소프트웨어에 대한 의존성이 높은 열차제어시스템의 경우 시스템의 안전성을 검증하거나 평가기가 매우 어렵다. 이러한 이유로 유럽을 중심으로 철도시스템의 안전성 확보를 위한 RAMS 관리 및 평가에 대한 요구사항들이 국제규격화 되었다. 유럽을 중심으로 시작된 철도시스템의 RAMS(Reliability, Availability, Maintainability and Safety) 관리에 대한 규격화가 IEC에 의해 국제 규격화되고 있다[1-3]. 이러한 국제 규격에서는 철도시스템의 신뢰성, 가용성 및 안전성에 대한 요구사항들을 정의하고 있고, 또한 이 규격들 중 IEC 61508과 IEC 72278은 철도시스템 RAMS 전체를 설명하고 있고, IEC 62425 규격의 경우 철도 운영기관이나 인증기관에서 시스템의 안전성을 승인(Approval) 및 수용(Acceptance)하기 위한 안전관리 조직이나 품질관리 시스템 등 안전성(Safety) 측면의 요구사항을 설명하고 있다.

Fig. 1은 이러한 철도시스템 RAMS 관련 국제규격들을 나타낸 것으로, 그림에서와 같이 IEC 61508과 IEC 62278 규격을 기준으로 하여 철도 소프트웨어, 철도통신에 관련된 요구사항들이 각각 설명되어져 있고, 철도신호의 안전성관련 요구사항은 앞에서 언급하였듯이 IEC 62425로 규격화되어 있다.

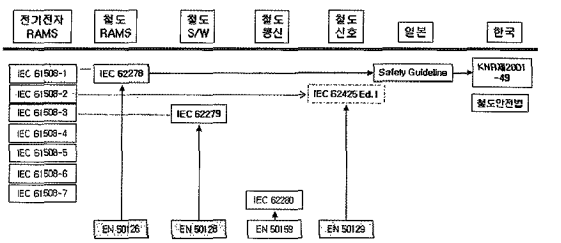

Fig. 1. Railway RAMS related Standards.

† To whom correspondence should be addressed.
jghwang@krri.re.kr

철도시스템 중 열차제어시스템은 다양한 설비와 서브시스템으로 구성되는 매우 복잡한 제어시스템 이기에 각각의 기능과 인터페이스에 대한 안전성이 더욱 중요한 바이탈 제어시스템이다. 유럽을 중심으로 이러한 열차제어시스템의 안전성을 확보하기 위한 규격을 제정하고 이에 따른 프로세스와 방법을 지속적으로 연구하고 있고 또한 실제 프로젝트에 적용하고 있다. 국내에서도 철도안전법[4]이 제정되는 등 국제 규격에 따른 열차제어시스템의 안전성 확보에 심혈을 기울이고 있지만, 아직은 시작 단계에 불과한 수준이다. 따라서 본 논문에서는 국제규격에 따른 열차제어시스템의 안전성 활동 및 평가를 위한 기술체계의 정립이 필요하다. 본 논문에서는 열차제어시스템에 적용하기 적합한 안전성 활동 수행체계 및 이에 따른 각 단계별 적용기술을 제시한다.

본 논문의 2장에서는 관련된 국제규격 및 선행연구의 분석 등을 통한 열차제어시스템을 위한 기술체계를, 3장에서는 기술체계 단계별 적용기술을 선정하고 실제 적용을 통해 도출한 세부기술의 적용결과를 제시하고, 4장에서는 본 논문의 결론을 설명한다.

2. 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[5-8], 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 Table 1에 나타내었다. 즉, 안전성 활동은 Table 1과 같이 시스템 수명주기 내에서 프로젝트 시스템의 안전성 향상 및 입증을 위해 수명주기 각 단계에서 수행되어진다. Fig. 2는 시스템 수명주기 단계와 비교 없이 국제규격에 따른 안전성 활동 중심으로 해서 표현한 블록도로서 안전성 평가에 필요한 안전성 활동 절차를 나타낸 것이다.

Table 1. Analysis of Safety Activities through System Life-cycle

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, 2단계
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 3단계
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, 5단계
안전대책 수립 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 9단계
안전성 인증	-안전성 활동의 완성도의 판단을 위임하는 기관에서 작성하는 평가보고서에 따라 안전성 인증 진행	수명주기 10단계
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, 14단계

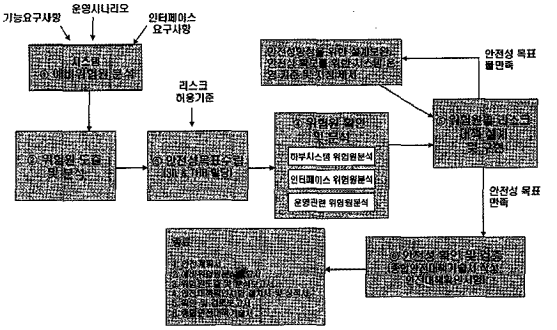

Fig. 2. Safety Activity Procedure for Signaling Systems.

Table 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 위험원이 안전성 활동을 통해 허용수준 이하로 제어되었는지를 입증함으로써 안전성 입증이 이루어지도록 하고 있다. 즉, ① 예비 위험원 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.

본 논문에서는 Table 1과 Fig. 2에서의 분석결과를 바탕으로 국내의 열차제어시스템 안전성 활동을 위한 절차를 Fig. 3과 같이 나타내었다. 이 안전성 활동 절차는 Fig. 2에서 나타낸 기본적인 절차와 유사하지만 안전성 활동을 수행하기 위한 구체적인 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.

또한 세 번째 단계인 리스크 분석 단계에서는 위험원별 리스크를 예측 및 분석하고, 동시에 수용가능한 리스크 기준(Tolerable Risk Criteria) 입력과 과 비교를 통해 수용가능한 리스크 기준을 초과하는 위험원에 대해서는 이를 제거 또는 기준이하로 줄일 수 있는 안전요구사항이 도출되게 된다. 작성된 안전요구사항은 개발하는 시스템의 구조에 따라 하부시스템으로 각각 할당하게 되며, 이때 하부시스템별로 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.

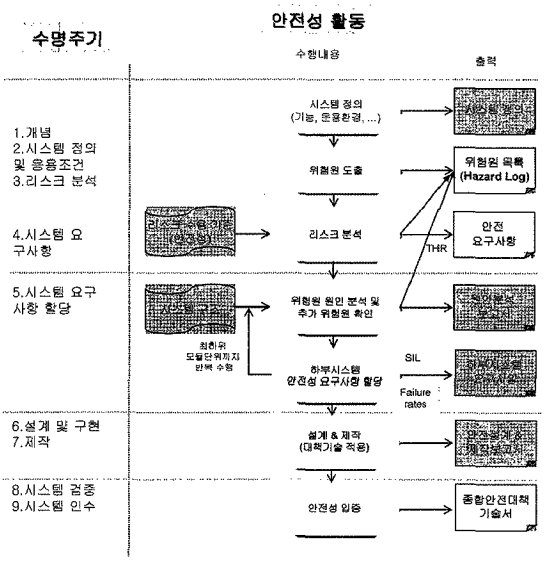

Fig. 3. Proposed Safety Activity Procedure with System Life-cycle for Signaling Systems.

3. 안전성 활동 기술체계 단계별 적용기술 제시

3.1. 위험원 분석 기술

안전성 활동의 첫 번째 단계인 위험원 분석을 위한 기술에는 여러 가지 방법들이 있다[3,9,10]. 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

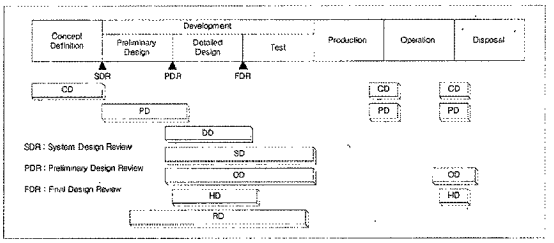

Fig. 4. Hazard Analysis Type according to System Life-cycle.

Table 2. Hazard Analysis Methods for IEC 62425

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 타입은 전체 시스템 개발 수명주기에서 Fig. 4와 같이 배치되어질 수 있다. 이처럼 수명주기 각 단계별 위험원 분석 타입이 조금씩 다르며, 이에 따라 수명주기별 또는 타입별 각각 다른 위험원 분석기술이 적용되는 것이 바람직한 접근방법이다. 이러한 위험원 분석을 위한 방법에는 매우 다양한 방법들이 있으며 관련 국제 규격에서도 위험원 분석을 위해 Table 2와 같이 다양한 방법들을 권고하고 있다[3].

위험원 분석 기술은 Table 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. Table 2에서 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 Table 3과 같이 나타낸 것이다. 각 분석기법이 수행되는 수명주기의 단계를 Fig. 4를 활용하여 분석 타입으로 구분하였으며, 위험원을 도출할 수 있는지의 여부와 정량적·정성적 분석인지를 분석하여 제시하였다.

Table 3. Relations between Hazard Analysis Type and Methods

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 제어시스템의 위험원 분석을 위해 가장 많이 활용되는 기법 중의 하나이다. SHA, SSHA, O&SHA는 위험원 분석 기법으로 적용대상의 범위에 따라 분류되는 방법이다. 따라서 이러한 세 가지의 위험원 분석을 위해서는 FMECA나 HAZOP 기술들이 적용되어 질 수도 있다.

이러한 검토를 바탕으로 본 논문에서는 열차제어시스템의 위험원 분석을 위해서 FMECA와 HAZOP 기법을 선정하였다. 이 중 HAZOP 기법은 화학공

정 분야에서 개발되어 적용되어 온 방법으로[11,12], 입출력이 디지털이고 컴퓨터에 의해 제어되는 열차제어시스템에 적용하기에 다소 어려움이 있다. 본 논문에서는 선행연구[13]를 통해 철도의 열차제어시스템에 적합하도록 가이드워드를 보완하는 등 기존 방법을 변경한 새로운 방법을 HAZOP-KR (HAZOP for Korean Railway)을 적용하였다.

3.2. 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.

이러한 리스크 분석 기법에는 Fig. 5와 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[14-16].

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[16] 결과에 자세히 설명되어져 있다.

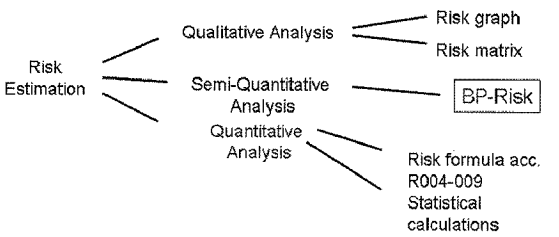

Fig. 5. Risk Analysis Methods.

3.3. 안전성 활동 수행기술 및 적용결과

앞에서 설명한 바와 같이 안전성 활동을 수행하기 위한 다양한 기법 및 기술들이 존재하지만, 각 기법별 고유한 특성들이 있다. 본 논문에서는 앞 절에서 제시한 각 기법들을 Fig. 6과 같은 대상 열차제어시스템을 통한 적용을 통해 열차제어시스템에 적합한 안전성 활동 절차와 각 단계별 적용기술을 포괄하는 안전성 활동 기술체계를 제시하였다.

앞 절에서 제시한 안전성 활동 절차 및 기술들을 적용하기 위한 대상 열차제어시스템을 본 논문에서는 CRD(Control of Route and Distance system)라 부르며, 이는 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 앞 절에서 제시한 안전성 활동 체계 및 이에 따른 단계별 수행기술에 대한 적용성 연구를 수행하였다.

Table 4는 위험원 분석 타입별 선정한 위험원 분석 기법을 나타낸 것이다. 이 표에서와 같이 적용

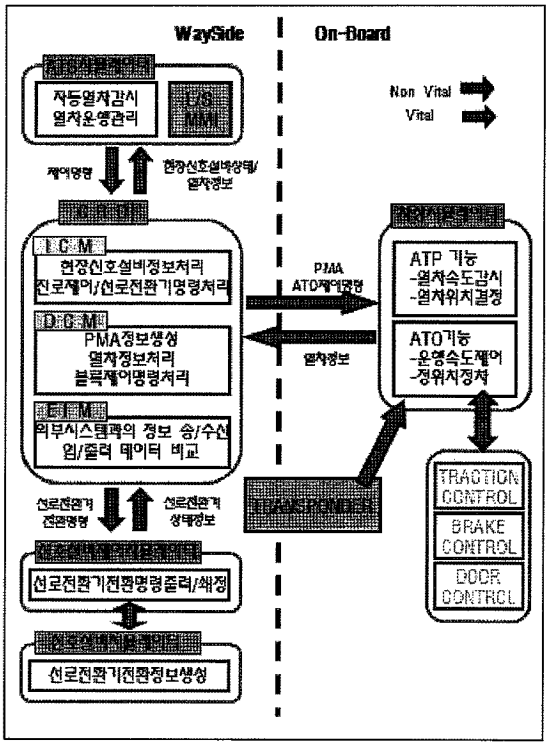

Fig. 6. Configuration of CRD Systems for Feasibility Study.

Table 4. Deduction of Hazard Analysis Methods for Analysis Types

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

되는 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 Table 3과 4의 분석결과와 같이 PHL과 PHA 활동을 수행하도록 하였으며, 그 결과의 일부분을 Table 5와 6에 나타내었다. 이러한 PHL과 PHA를 통해 도출된 위험원을 바탕으로 다음 단계(DD, SD)에서 SSHA, IHA를 수행하였다.

앞 절에서도 설명하였듯이 SSHA와 IHA를 위해서는 FMECA 방법을 적용하였고, 또한 시스템의 상세한 위험원 도출 및 분석을 위해 HAZOP-KR을 적용하였으며 그 결과는 Table 7과 같다. SSHA와 IHA는 기본적으로 FMECA 기법을 적용하였으며, 실제 본 연구에서는 3.2절에서 설명한 BP-risk 기법과 결합한 형태의 템플릿을 적용하였다. Table 8은 CRD 시스템의 하부 모듈인 EIM 모듈에 대한 SSHA 결과로서, 전체적으로는 FMECA를 수행하면서 리

Table 5. PHL Results for CRD systems

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	
⋮	⋮	⋮	⋮

Table 6. PHA Analysis Results for CRD Systems

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
		⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Table 7. HAZOP-KR Results for CRD Systems

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 열차고장정보 확인
Outside	Other	강풍에 의한 과속	강풍에 의한 과속	열차탈선	날씨에 따른 열차간격 및 속도 제어
Data	No	차상제어정보 없음	ATS 속도제어명령 없음	열차탈선/충돌	경보 이벤트 출력

Table 8. SSHA results for EIM Module of CRD Systems

Subsystem	EIM																					
Failure Identification			Failure Effect		S=E+V+A						D=T+C+H							U		S D U	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			
Hazard -1	열차위치 확인 설패	EIM 처리 오류	열차진로 및 허용이 동권한 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 확인실패	EIM 처리 오류	DCM 열차속도정보 처리 불가	열차충돌 및 탈선	5	충돌로 인한 다수 사상	5	최대운행속도 초과	5	열차간 충돌	1	유효성 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

스크 분석을 위해 BP-risk 방법을 적용하였다. Table 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. Fig. 7은 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.

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 논문에서는 관련된 국제규격 및 선

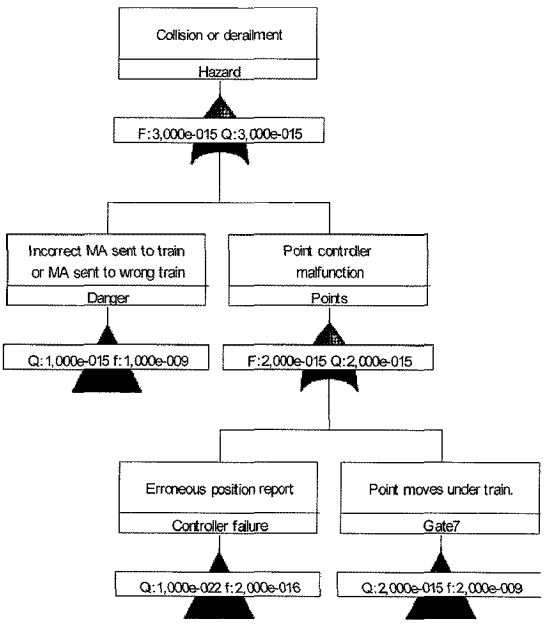

Fig. 7. FTA of Top Level Hazards for CRD Systems.

행연구의 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.

이를 통해 본 논문에서는 국내 열차제어시스템을 국제규격에 적합한 안전성 활동 절차 및 이에

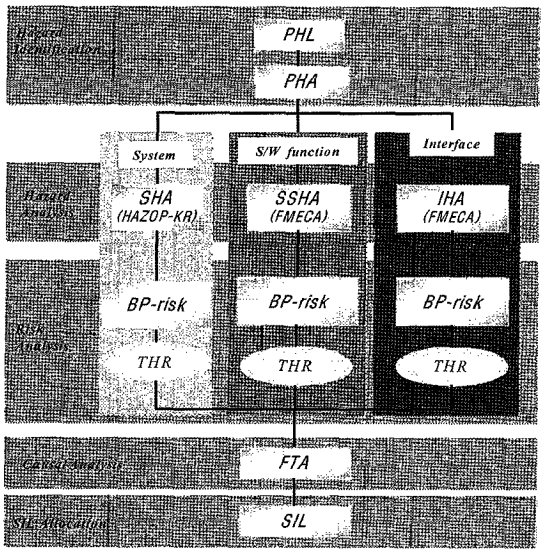

Fig. 8. Proposed Applicable Methods for Safety Activity.

따른 기술을 포괄하는 안전성 활동 기술체계를 Fig. 8과 같이 제시하였다. Fig. 8은 본 논문에서 제시하는 열차제어시스템을 위한 안전성 활동 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.

4. 결 론

높은 안전성이 요구되는 열차제어시스템은 관련된 국제규격과 국내의 철도안전법의 제정 등으로 인해 시스템 수명주기에 따른 안전성 활동이 요구되어지고 있다. 국내의 열차제어시스템의 경우 이러한 국제규격에 따른 안전성 활동 절차와 이를 위한 기법이나 기술들에 연구가 이루어지고 있지만, 아직 초기단계에 불과한 실정이다. 본 논문에서는 국제규격과 적합성을 가지는 열차제어시스템의 안전성 활동을 위한 기술절차와 이에 따른 적용기법 및 기술을 제시하였으며, CRD라는 대상시스템을 통해 그 적합성을 확인하였으며, 그 결과의 일부를 제시하였다. 특히 단계별 적용기술의 선정에 있어서 시스템, 기능, 및 인터페이스로 구분한 각기 분야별 특성을 고려한 SHA, SSHA, IHA 방법들을 제시하였고, SHA를 위해서는 열차제어시스템의 특성을 고려하여 HAZOP-KR 기법을 시스템의 위험원 분석에 적용하였다. 또한 리스크 매트릭스의 단점을 보완하여 보다 체계적이고 정량화시킨 BP-risk 방법을 리스크 분석 및 예측 기법을 본 기술체계에 반영하였다. 향후 본 연구의 결과는 철도안전법에 따른 열차제어시스템의 안전성 활동에 활용될 수 있으며, 또한 국내에서 국제규격에 따른 안전성 활동 및 평가를 위한 체계 구축에 기여가 예상된다.

감사의 글 : 본 논문은 국토해양부가 출연하고 한국건설교통평가원에서 위탁시행한 철도종합안전기술개발사업(열차안전C03)의 연구비지원에 의해 수행되었습니다.

참고문헌

1) IEC 61508, "Functional safety of electrical/ electronic/programmable electronic safety-related systems", 1998.
2) IEC 62278, "Railway Applications - The specification and demonstration of RAMS", 2002.
3) IEC 62425 Ed. 1, "Railway Application: Communications, signaling and processing systems - Safety related electronic system for signaling", 2005.
4) 건설교통부, "철도안전법", 제7245호, 2004.
5) J.G.Hwang and H.J.Jo, "RAMS Management and Assessment of Railway Signaling System through RAM and Safety Activities", Proceedings of ICCAS 2008, pp. 892~895, 2008.
6) 신덕호, 외, "안전입증에 과한 연구", 한국철도학회논문집, 제9권, 제4호, pp. 412~418, 2006.
7) 한국철도기술연구원, "열차제어시스템 안전성능평가 및 사고방지기술 개발", 연구보고서, 2008.
8) 한국철도기술연구원, "치상신호(ATP)시스템 구축사업의 위험원 도출 및 분석 보고서", 2006.

9) Clifton A. Ericson, "Hazard Analysis Techniques for System Safety", pp. 5~11, 31~54, 2005.
10) J.G.Hwang, H.J.JO and Y.K.Yoon, "Analysis of Safety methodology for Railway Signaling Systems", International Journal of Safety, Vol. 6, No. 2, pp. 38~42, 2007.
11) 노미영 외, "회분식 공정의 HAZOP 분석 자동화를 위한 지식기반구조 및 알고리즘", Journal of the Korean Institute of Chemical Engineers, Vol. 39, No. 3, 2001.
12) IEC 61882, "Hazard and Operability Studies(HAZOP Studies)-Application Guide", 2001.
13) 안진, 조우식, 외, "철도시스템 적용을 위한 HAZOP-KR에 대한 연구", 한국안전학회 춘계학술대회, 2009.
14) Jens Braband, "Risikoanalysen in der Eisenbahn-Automatisierung", Eurail Press by Siemens AG, 2005.
15) Jens Braband, "Improving the Risk Priority Number Concept", Journal of System Safety, pp. 21~23, 2003.
16) 조현정, 황종규, "열차제어시스템 안전성 확보를 위한 위험도 분석 방법 적용", 한국안전학회논문지, 제22권, 제5호, pp. 71~76, 2007.