신호보안시스템의 소프트웨어 신뢰성 향상에 관한 기초연구
A Basic Study on the Improvement of Software Reliability of Signaling Safety System

김종기* 이종우* 정의진** 조봉관**
Kim, Jong-Ki Lee, Jong-Woo Joung, Eui-Jin Cho, Bong-Kwan

ABSTRACT

Railway signaling safety system organizes equipments and facilities of railway, increases transport efficiency and assures safe operation of railway. In the early days of signaling system, railway managers made sure of safety by using relay logic technology based on fail-safe concept. But the development result of computer and science having been introduced to railway industry, railway signaling equipments begin to be operated through micro electronic control system. Accordingly high speed and high density operation of train became possible. Software reliability and safety technology that controls important systems of railway was highlighted. In the middle of 1990s the standard or guideline of railway reliability and safety were studied and established, and are being reviewing in Europe, Japan, etc. Our reliability and safety technology have depended largely on foreign countries. In this study we performed a basic study about the reliability of software that controls the railway signaling system.

1. 서론

철도신호보안시스템은 궤도상에서 주행하는 열차에 대하여 전방의 운행조건을 제시하여 주는 시스템으로 선로의 이용률을 향상시키고 열차상호간의 안전을 확보하며 운행열차를 방호함으로써 철도의 수송력 증가, 안전성 확보, 경영 합리화와 서비스 향상에 기여하고 있는 매우 중요한 시스템이다. 신호보안시스템에는 자동열차정지장치(ATS), 자동열차제어장치(ATC), 열차집중제어장치(CTC), 자동폐색장치(ABS), 자동열차운전장치(ATO), 전기 및 전자연동장치, 신호정보분석장치, 신호기장치, 선로전환장치, 궤도회로장치, 건널목보안장치, 기타 안전설비 및 이에 부대되는 각종 시설이 유기적으로 연결되어 있다. 철도의 신호보안시스템 기술은 철도의 수송능률을 극대화시킬 수 있는 철도의 핵심기술이나, 국내에서는 아직 관련기술을 독자적으로 확보하지 못하고 대부분을 해외기술에 의존하고 있는 실정이다.

철도선진국에서는 전자제어·정보통신의 눈부신 발달 성과를 철도에 도입하여 신호제어설비의 전자화를 구축하면서 이에 따라 철도의 획기적인 고속화, 고밀도화, 고기능화가 이루어지기 시작하였다. 복잡한 제어논리와 섬세한 기기들로 시스템이 구성되면서 고장의 예측이 어려워지고 치밀한 설계와 제작과정을 거친 시스템의 검증절차도 새로운 기법이 필요하게 되었다. 특히, 사소한 고장이나 오작동이 대형사고를 유발할 수 있다는 점에서 신뢰성과 안전성 문제가 대두되었다.

선진외국에서는 안전하고 정확한 철도운행을 위하여 신뢰성 기술 구축을 위한 연구의 필요성을 일찍이 인식하고 연구에 착수하였으며, 현재 그 결과를 현장에 활용하고 있다. 신뢰성 활동은 우

* 한국철도기술연구원 철도신호·통신연구팀 책임연구원, 정회원
** 한국철도기술연구원 철도신호·통신연구팀 주임연구원, 정회원

주선, 무기체계 또는 원자력 발전설비 등에서부터 활용되어 왔으며, 이들은 비용 요소보다는 신뢰성이나 안전의 문제가 훨씬 중요하므로 철저한 분석과 시험을 거쳐 신뢰성을 추구하여 왔다. 그러나 상업용 제품에서는 비용 증가가 경쟁력에 많은 영향을 주므로 분석과 시험보다는 주요부품의 관리에 치중하여 왔다. 국가의 핵심 신경망인 철도에서도 기본적으로 장치의 성능과 기능을 중시하여 개발하는 것이 중요하다. 고장이나 사고가 빈발하면 열차의 안전운행을 보장할 수 없게 되고 국가적으로 막대한 손실을 가져다주므로 철도시스템의 신뢰성관리는 열차운행의 전 수명주기(Life Cycle)를 통하여 관리되어야 한다. 수명주기 RAMS(Reliability, Availability, Maintainability, Safety) 관리는 유럽의 CENELEC(Comité Européen de Normalisation Électrotechnique) 규격에서도 제시되고 있는 방법이다.

다음 그림은 신호보안시스템의 변천과정을 나타내고 있는 것으로 왼쪽 하단의 시스템은 전기기술을 바탕으로 열차운행효율보다는 안전운행을 지향하던 1970년대 기술을 근간으로 안전측 동작원칙(Fail-Safe) 기술을 하드웨어적으로 구현한 것이며 오른쪽 하단의 시스템은 최근 마이크로 일렉트로닉스 제어기술을 도입하여 열차의 고속화 및 높은 운행효율을 도모한 것이다.

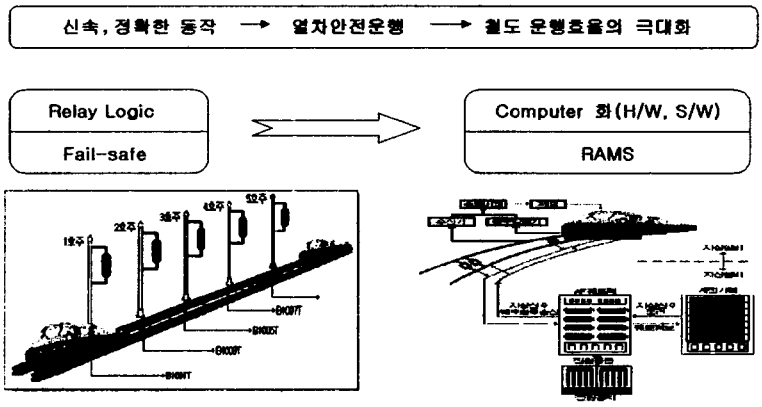

그림 1. 신호시스템 제어로직의 변화

1980년대 스웨덴에서 최초로 전자연동장치가 실용화되면서 철도신호설비에도 마이크로 컴퓨터시대가 시작되었다. 그후 마이크로 일렉트로닉스 제어가 철도 전분야로 확산됨에 따라 열차의 고속·고밀도 운행이 가능해지고 많은 주요 철도설비가 소프트웨어로 제어되고 있다. 신호보안시스템에도 컴퓨터제어로직을 응용함으로써 소프트웨어가 필수적으로 사용되기 시작했다. 따라서 이에 대한 고도의 안전성과 신뢰성의 확보는 매우 중요한 문제가 되었다. 최근의 철도시스템에서는 장비의 사소한 오작동이 대형사고를 야기할 수 있으므로 RAMS 체계 구축이 유럽과 일본 등의 철도 선진국을 중심으로 시도되고 있다.

우리나라도 마이크로 컴퓨터를 이용한 열차집중제어장치와 전자연동장치의 확대설치 등 자동화·전자화를 위한 설비개량, 전산화 및 신뢰성·안전성 기술 도입에 총력을 기울이고 있다. 그러나 1996년에 발생했던 강동역 오진로 진입사고는 선로전환장치의 잘못된 소프트웨어 제어로직에 그 원인이 있었던 것으로 나타났으며 미국과 프랑스의 철도기술에 전적으로 의존하여 제어로직을 보완하고 안전성을 점검했다. 따라서 이러한 대외 의존도를 낮추고 고속철도시대를 맞이하는 우리의 철도산업분야의 기반기술을 더욱 확고하게 구축하고자 2000년부터 이러한 철도기술의 변화에 따라 새로 부각되고 있는 신호보안시스템 소프트웨어 신뢰성 향상에 관한 기초 연구를 수행하였다.

2. 국내 철도신호시스템의 신뢰성·안전성 기술 동향

최근 철도기술의 세계적인 추세는 철도의 높은 안전성과 신뢰성을 향상시켜 경영의 합리화를 도모하기 위해 신호제어설비의 전자화가 빠르게 이루어지고 있으며, 근래 우리도 컴퓨터를 이용한 열차집중제어장치, 전자연동장치의 확대설치 등 자동화, 전자화를 위한 설비개량을 추진하고 있다. 특히 신호제어 설비의 신뢰도와 안전도 향상을 위한 자기진단 기능을 향상시켜 보수업무의 전산화를 구축하였으며 낙뢰 및 전철구간에서의 유도대책 등 각종 재해대책 수립과 고속철도의 건설 등 신기술 개발에 총력을 기울이고 있지만, 핵심적인 고급기술은 선진외국에 의존하는 실정으로

기술발전에 많은 노력과 지원이 절실히 요구되고 있다.

그리고 대부분의 철도신호설비들은 철도연변에 인접하여 설치되어 있어 열차의 빈번한 통과에 따른 진동과 외부 노출로 인한 설비의 열화 진행도 빨라 기기의 신뢰성 및 수명에도 악영향을 주는 등 가혹한 환경조건을 갖고 있으며, 설비의 점검이 열차가 운행을 중지하는 시간대에 이루어져야 하므로 단시간에 효율적인 작업을 하여야하는 유지보수상의 문제점을 항상 내포하고 있다.

따라서 향후 열차속도가 향상되고 열차운행 밀도가 증대되면 신호설비에서의 고장이 발생될 경우에 철도경영에 미치는 영향이 커질 것이며, 이에 따른 신호설비는 높은 신뢰도와 안전도가 요구될 것으로 예상된다. 다음은 도시철도와 국철, 고속철도 등에서 사용하고 있는 신호보안시스템 현황자료를 요약한 것이며, 최근에는 각 운영기관과 정책기관에서 신호설비에 대한 안전성과 신뢰성 기술 연구에 대한 지원이 시작되고 있다.

2.1. 도시철도

도시철도용 신호보안설비는 현재 4개 도시(서울, 부산, 대구, 인천)에서 운영중이며, 설비 모두 외국기술에 의존하고 있는 실정이며, 제어로직이 모두 컴퓨터에 의존하는 첨단설비로 설치되어 있다. 서울지하철은 1974년 1호선이 개통된 이래 1985년에 2, 3, 4호선이 개통되면서 우리나라의 본격적인 지하철시대를 열었다. 1, 2호선에 도입된 열차운행제어시스템은 기관사의 불안전한 요소를 보완하는 자동열차정지장치(ATS)이었고, 3, 4호선에서는 자동화의 개념이 처음 도입되어 자연적인 위해요소나 인간의 실수로부터 안전을 확보할 수 있는 자동열차제어장치(ATC)가 설치되어 열차사고를 미연에 방지하고 있다.

산업과 경제의 발전에 따라 차원 높은 서비스를 원하는 승객에게 효과적인 서비스를 제공하고, 효율적인 경영을 달성할 목적으로 지하철 5, 6, 7, 8호선(2기 지하철)에서는 가능한 모든 부분을 자동화하여 승객을 만족시키는 한편, 열차의 안전한 운행을 도모하며, 운영과 경영의 효율화를 꾀하도록 설계된 컴퓨터의존형 신호보안시스템이다.

표 1. 도시철도용 신호제어설비

도시명	노선구분	주요 제작사	비고
서울	1, 2호선 3, 4호선 5~8호선 과천선, 분당선, 일산선	경삼 및 대동신호(일본) US&S(미국) US&S 외(미국 외) 유경통신(한국)/US&S(미국)	제작사에 따라 신호제어설비 구성 및 성능이 다름
부산	1호선 2호선	일본신호(일본) ADtranz(스웨덴)	
대구	1호선	GRS(미국)	
인천	1호선	Siemens(독일)	

2.2. 국철

우리나라 철도신호는 1899년 9월 18일 노량진~제물포간에 최초로 철도가 부설되고 동시에 완목식 신호기가 설치된 이래 1942년 영등포~대전 사이에 자동폐색신호기가, 1955년에는 대구역 남부에 제1종 전기연동장치가 설치되었다. 이와 같이 기계식을 시초로 1940년대 전기식에 이어 1968년 전자기술을 도입하기에 이르게 되었으며, 1977년에는 수도권 일원, 1988년에는 태백선, 1991년에는 경부선에 CTC를 설치하여 운용함으로써 신호보안장치에 많은 발전을 이룩하게 되었다.

표 2. 국철용 주요신호제어설비

노선명	신호체계	주요제작사	비고
경부선	5현시	샬롬엔지니어링(한국) 또는 경삼신호(일본)	신호현시체계에 따라 열차제어 방식이 다름
경부선 외	3현시		

한국철도 100년의 역사에서 열차운행의 안전을 담당해온 신호보안설비의 제어로직의 변화는 기계식, 전기식, 전자식, 컴퓨터에 의한 제어방식으로 발전해 왔다.

2.3. 고속철도

현재 건설중인 경부고속철도용 신호보안설비는 4분 간격으로 시속 300㎞로 주행하는 열차의 안전운행 확보가 최대 목표이다. 시속 300㎞이면 1초에 83m를 달리는 초고속 열차가 안전하게 운행하기 위하여 신호설비의 주요장치는 2중화 또는 3중화하여 신뢰성을 높여서 만일 장비가 어떠한 고장이 발생하더라도 안전한 측으로 기능이 작동되도록 하는 Fail-Safe개념으로 시스템이 구성되어 안전성이 확보되어 있다.

경부고속전철은 남서울~부산 409km, 중간역 4개소(천안, 대전, 대구, 경주), 운행 최고속도 300km/h, 운행 최소운전시격 4분으로 건설된다. 신호설비의 주된 임무는 진로구성에 관한 명령과 제어, 열차간격을 조정하는 기능, 안전운행 확보, 기관사의 순번 및 역할 조정, 각종 보호기능에 관한 역할을 수행하며, 자동열차제어장치(ATC), 전자연동장치(IXL), 열차집중제어장치(CTC) 및 안전감시장치로 이루어져 있으며, 이들 장치를 통틀어 TCS(Train Control System)라 한다.

표 3. 경부고속전철용 주요신호제어설비

주요설비명	설치위치	주요제작사
열차집중제어장치	남서울역	알스톰(프랑스)
전자연동장치	각정차역 신호기계실 및 현장	알스톰(프랑스)
열차제어장치	지상설비 : 선로 전구간 차상설비 : 동력차 92대	CSEE(프랑스)
선로전환기	선로분기점	알스톰(프랑스)

경부고속철도 신호설비는 중앙제어실, 역 및 건넘선 등에 대부분 시설되어 있다. 중앙제어실(Operation Center)의 위치는 남서울역이며, 이곳에서 열차운행시간표(Timetable) 준비, 운행중인 열차를 위한 역과 궤도의 상태 등을 검사, 제어, 열차의 진행을 감시, 운용과 중앙집중화된 유지보수 정보의 입수, 운행조건의 감시, 특별한 조건하에서의 열차운행제어, 역의 승객을 위한 정보제공(TIDS: Train Information Display System), 전력공급상태의 표시(SCADA: Supervisory Control And Data Acquisition), 기관사와 역무원, 유지보수 인력과의 통신(Radio Data Transmission), 기타 장치와의 통신 기능을 수행한다.

3. 국외 철도신호시스템의 신뢰성·안전성 기술 동향

3.1. 유럽

영국철도는 1970년대부터 설비의 전자화로 인해 설계단계에서 결함 확인이 어렵게 되자 시스템 단계의 신뢰성 분석기법인 FTA(Fault Tree Analysis), FMEA(Failure Mode and Effect Analysis) 등을 도입하여 중복설계, 고장허용 설계, 신뢰성에 치명적인 부품 관리, 예비부품 관리, 유지보수 계획 등을 수행하려 했으나 분석에 필요한 데이터 부족으로 인해 제대로 수행되지 못했다. 그후 1980년대부터 철도의 민영화 및 사업분할이 이루어지고 신뢰성 요구사항이 설정되자 신뢰성 요구사항의 달성가능성, 현실성, 실연성(Demonstration), 측정가능성 등의 항목을 계약사항으로 제시하여 공급업체에 신뢰성관리 요구를 하기 시작하였으나 촉박한 개발기간과 현장데이터 부족 및 현장 접근이 어려워 공급업체의 형식적 대응만 이루어졌다. 그러나 수명주기 비용 분석을 시작하고 신뢰성 정보시스템을 보완하고 수리정비내용의 현장데이터화를 위한 신뢰성 엔지니어 그룹을 결성하는 등 신뢰성 기술체계를 구축하면서 신뢰성 목표를 달성하고 아울러 유지보수 비용을 절감하는 효과를 얻기 시작하였다.

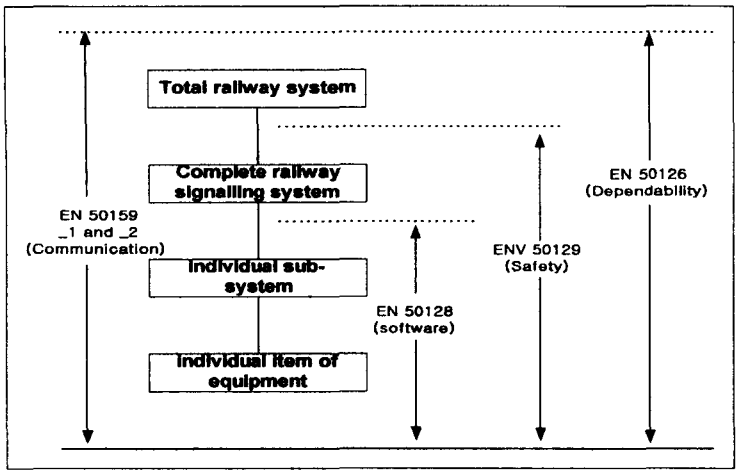

그림 2. CENELEC 규격의 범위

1990년대 중반 유럽에서는 과학기술적 요구사항을 반영하여, 실질적인 구속력을 가지고 운영되는 CENELEC 규격을 제정하여 EU내 철도신호 시장의 개방화를 도모하고 국가간에 상이한 신호보안시스템의 안전성 요건을 공통화하여 타국의 신호시스템의 도입을 용이하게 하고 EU 고속철도망의 구축 및 열차제어시스템의 개발을 촉진하고 있다. 철도신호보안시스템의 대표적인 규격인 CENELEC 규격은 신뢰성과 안전성의 표준규격으로 EN 50126, EN 50128, ENV 50129로 구성되어 있다

EN50126은 가장 넓은 범위에서 철도시스템에 대한 RAMS 전 수명주기에 걸쳐서 RAMS 관리의 일관성 있고 일반적인 기준과 절차 및 적용사례를 제시하고 있다. 여기서는 RAMS 요건을 명세화하고 철도 RAMS의 체계적인 관리를 위해 RAMS 고장의 범주(3단계: Significant, Major, Minor), RAMS와 보급지원을 정량화하는 파라메터, 리스크 분석과 평가, 안전성 등급(SIL: Safety Integrity Level) 등을 정의하고 RAMS 수명주기를 거치면서 수행되어야 하는 각종 활동을 개념단계에서 폐기처분에 이르기까지 규정하고 있다. EN 50128은 철도보안시스템의 소프트웨어측면에서 신뢰성과 안전성을 확보하기 위한 기준으로 소프트웨어의 안전성 요건을 규정하고 있다. 이 규격은 안전성 등급을 0에서 4까지 다섯단계로 구분하고 0등급은 안전과 관련이 없는 수준이며 1에서 4등급으로 갈수록 안전에 치명적인 영향을 미친다는 것을 의미한다. 이 규격에서 현재의 기술수준은 모든 시스템의 절대적인 안전을 보장할 수는 없으며 상당히 복잡한 안전에 관련된 소프트웨어의 결함, 특히 사양과 설계결함이 없다는 것을 증명할 방법이 없다는 점을 지적하고 있다.

3.2. 일본

일본의 철도기술은 세계에서 가장 먼저 고속철도를 개발하여 실용화한 저력에서 알 수 있듯이 열차제어기술 등이 꾸준히 발전해 왔다. 일본의 열차제어기술은 지상신호방식과 차상신호방식을 사용 중에 있으며, 최근 디지털 ATC를 개발하여 1단 제동방식에 의한 고밀도 운전을 고려하고 있다. 유럽의 ETCS(European Train Control System)프로젝트와 유사하게 약10여년전부터 무선통신방식에 의한 열차제어시스템(CARAT: Computer And Radio Aided Train Control System)을 개발하여 현재는 실용화 단계에 있다.

일본은 1970년대부터 안전성과 신뢰성 연구활동을 시작하여 이후 20여년동안 철도신호분야에서 개발한 제품에 대해 설계에서 폐기까지 안전성과 신뢰성에 대해 검증한 자료와 노하우를 가지고 있다. 또 1994년에는 안전성 관련 기술에 풍부한 지식과 경험을 가진 전문가(학자, JR, 公民鐵, 제작사)들로 구성된 위원회를 조직하고 그간 축적된 기술과 경험을 바탕으로 2년여간 조사 및 검토를 실시하고 IEC(International Electrotechnical Commission), CENELEC 등의 안전성 기술규격의 국제동향, 일본신호보안기술 등을 참고하여 「열차신호시스템의 안전성기술지침」을 작성하였다.

본문, 해설, 자료의 3부로 구성된 안전성 기술지침의 본문은 총7장으로 되어 있으며 1장은 적용범위, 2장은 용어정의, 3장은 Fail Safe 기본과 안전성 확보방향, 4장은 라이프 사이클 전반에 걸친 안전성 관리와 기술활동의 방향, 5장은 시스템 안전성 라이프 사이클을 정하고 각 단계의 기술적

요건을 설명하고 있으며 6장은 시스템 설정 보안기능 달성, 7장은 문서화에 대해 설명하고 있다. 여기에는 마이크로 컴퓨터를 사용한 신호보안시스템의 설계, 제조, 운용에 관한 안전성 확보의 개념, 기본적인 작업순서, 안전성 라이프 사이클, 안전성의 해석, 위험도 해석 및 안전성 요구, 신호보안시스템 설계 및 제작에 관한 사항, 설치 검증 및 타당성 검사, 시스템 개조/수리 시의 안전성 해석 등을 포함하고 있다. 이 안전성 기술지침의 작성에 고려된 기본적인 개념은 다음과 같다.

- 열차신호시스템의 제조, 운영을 규제하는 것이 아니라 수명주기 전체에 걸친 안전성 기술 관리 및 활동에 대해 사용자와 제작사에게 정보를 제공하는 것이다. 따라서 이들의 사용은 사용자와 제작사 간에 협의하여 결정한다.
- 안전성 기술지침 본문에서는 구체적인 설계수법과 각종 목표치를 규정하지 않았으나 해설에서는 안전성 등급에 적합한 기법, 수단, 심사기관 등의 목표치를 기술한다.
- 안전성 기술지침의 본문 또는 해설과는 다른 기법을 채택할 때는 그 이유와 대체 방법을 명확하게 하고 기록하는 것을 권장한다.

3.3. 미국

미국의 FTA(Federal Transit Administration)가 후원하는 연구 프로젝트인 TCRP(Transport Cooperative Research Program)를 통해 CBTC(Communication Based Train Control) 표준화가 진행되었다. IEEE(Institute of Electrical and Electronics Engineers Inc)를 통하여 작업이 진행되면서, 1996년 경량 및 중량철도 차량에 대한 시스템 및 하부 시스템 인터페이스에 대하여 자유 조화에 의한 표준개발 절차의 설계를 목적으로 하는 RTVISC(Rail Transit Vehicle Interface Standards Committee)가 구성되었다. 현재까지 9개 분야로 구성되어, 차량 내부의 통신 프로토콜, 추진 시스템이나 마찰 제동, 차량 주간 제어기 사이의 기능 및 인터페이스, 차량 감시 및 진단 시스템, 승객 정보 시스템, 프로세서를 사용하는 제어 시스템의 안전 검증 등에 대한 주제를 다루고 있으며, 특히 제2작업그룹(WG2)이 CBTC 시스템에 대한 표준을 다루고 있다.

IEEE RTVISC 제2작업그룹은 CBTC 시스템에 지상-차상 및 차상-지상간의 인터페이스에 대하여 자유 조화에 의한 표준을 제정하는 것이었다. WG2는 북미의 모든 CBTC 시스템의 주요 공급회사 및 잠재 공급회사들과 자리를 함께 하여 새롭게 전개되고 있는 열차 제어기술에 대한 표준을 개발하기 위한 복잡한 문제들을 토론하였다. 공개 토론회를 개최하여 각 사의 CBTC 시스템에 대한 정보를 공유하도록 하였으며, 이를 통하여 현재 사용하고 있거나 개발중인 여러 종류의 CBTC 시스템 사이의 유사성 및 주요 차이점을 확인하였다.

경쟁 조달 방식에 의한 표준화가 진행되고 있는 NYCT(New York City Transit Committee) 카나지선의 경우, 최선의 CBTC 시스템을 선정하여 NYCT의 표준 시스템이 되어 상호 운영이 가능하도록 인터페이스 사양과 함께 각 공급회사에 요구될 것이다. 이러한 서로 다른 두 가지 방식의 표준화를 통하여 같은 목적을 달성함과 동시에 상호 보완적인 영향을 미치고 있으며, 서로 상당한 시너지 효과를 얻고 있다.

4.. 소프트웨어 신뢰성 향상

소프트웨어의 신뢰성을 평가하고 향상시키고자 하는 기법은 1970년대부터 연구되기 시작하여 소프트웨어의 오류와 고장의 의미 분석, 메트릭스(Metrics)를 이용한 소프트웨어 품질평가 및 품질특성의 표준화, 각종 소프트웨어의 신뢰도 추정기법, 소프트웨어 최적시험기간 설정기법, 소프트웨어 신뢰도 성장모형 등이 개발되어 왔다. 그러나 소프트웨어 신뢰성 기술의 역사가 짧고 정량적인 평가 및 예측이 어렵고 고장도 하드웨어와는 매우 다른 양상을 보이고 있어 아직 신뢰성 높은 소프트웨어의 설계, 구현, 테스트 방법이 명확하게 정립되어 있지 않다.

그러나 철도 소프트웨어 분야에서는 최근 부각되고 있는 형식기법(Formal Method)을 활용하여 안전성과 신뢰성을 높이고자 하는 움직임이 유럽과 일본을 중심으로 일고 있다. 형식기법의 기본

개념은 다음과 같다.

① 컴퓨터 프로그램은 수학적인 문장이며 올바른 프로그램의 설계는 수학이론의 유도 및 증명과 유사한 과정이다. 형식기법은 수학적인 개념을 기초로 만들어졌다.

② 어휘, 문법, 추론의 방법을 수학적으로 정의하는 시스템을 사용하며 엄격한 방법을 사용함으로써 시스템의 기능과 안전성을 확보하고자 한다.

③ 소프트웨어의 구현 과정에서 설계 명세화, 구현모델 구축, 검증 등의 단계를 수행한다.

④ 프로그램의 특징과 데이터 구조를 공리(Axiom)와 추론 방법으로 처리하고 요구되는 명세(Specification)에 해당되는 정리(Theorem)의 증명을 시스템의 안전성으로 간주한다.

⑤ 배우기가 어렵고 시간조절, 제어, 행위를 표현하기 어렵다.

⑥ 프랑스의 ATC와 스웨덴의 전자연동장치의 데이터 검증에 사용하고 있으며 일본에서는 현재 연구 중에 있다.

형식기법은 프로그램 설계부터 수학적인 엄밀성과 수학정리 증명과정의 객관성을 프로그래밍에 도입함으로써 발생할지도 모르는 버그를 근원적으로 차단하는데 있으며 일반적인 절차는 다음과 같다.

① 형식 명세(Formal Specification)의 준비
- 시스템의 동작행위 및 특성을 명확하고 일관성있고 엄밀하게 서술한다.
- 집합론과 형식 논리 기호를 사용한다.
- 시스템이 운용될 환경에 대한 가정, 시스템이 달성해야할 요구사항, 요구사항에 부합하기 위한 설계 등이 포함된다.
- 목적(Object) 시스템을 모델링하고 상태변수와 작동함수로 시스템을 표현하고 불변조건, 사전조건, 사후조건을 결정한다.

② 형식 검증(Formal Verification)
- 정리증명(Theorem Proving): 시스템의 특성을 수학적 논리 내에서 공식으로 표현하고 증명하는 것이다. 공리와 추론규칙, 유도되는 정의, 중간 이론 등을 이용하며 정리증명기(Theorem Prover)를 사용한다.
- 증명과정에서 불완전성이나 불일치성을 자동으로 발견할 수 있다.

③ 검증된 명세를 최종 프로그램화한다.

다음은 형식기법의 일종인 VDM(Vienna Development Method)으로 영역정보의 불변조건을 표현한 예이다.

Inv-area(Is : Line-set, ar : Area-set) ret : B

$$ret = (\forall l1 \in \mathrm{Is} \cdot \forall aid1 \in l1.areas1) \cdot$$

post

$$\exists a2 \in ar \cdot a2.id = aid1) \wedge$$
$$(\forall a1 \in ar \cdot \forall a2 \in ar \cdot (((a1.id = a2.id) \wedge$$
$$(a1 = a2)) \wedge (a1.id \neq a2.id)));$$

프랑스 파리 지하철에 MTI(Matra Transport International)에서 개발한 자동열차운행시스템에 형식기법을 사용하여 소프트웨어 신뢰성을 향상시켜 안전성을 확보한 것으로 알려진 프랑스의 'Météor 프로젝트'가 있다.

MTI는 시스템과 장비의 각 단계별로 수행되는 안전성 분석에 의거하여 자동 열차운행시스템의 소프트웨어를 안전에 치명적인 소프트웨어와 안전에 치명적이지 않은 소프트웨어 두 가지로 구분하고 소프트웨어 결함을 다음 두 가지로 분류했다.

① 설계 또는 코딩에러: 소스코드가 소프트웨어 요구사항을 만족하지 않는 경우

② 코드생산과정(컴파일, 링크)이나 하드웨어 결함으로 인한 에러

그리고 MTI는 안전에 치명적인 소프트웨어를 개발할 때 다음 두 가지의 방법을 채택했다.

① 단일 소프트웨어 설계와 개발단계에서 B 형식기법을 사용하여 요구사항에 따라 버그가 없는

소프트웨어의 정확성을 수학적으로 증명한다.

② VCP(Vital Coded Processor)를 사용하여 코드생산과정과 하드웨어결함에 따른 에러를 검출한다.

VCP는 1980년대 MTI가 개발한 방법으로 중복으로 코드화된 데이터 요소를 사용하여 각 안전성 주기를 실행한 후에 코드의 정확성을 체크해가며 소프트웨어 실행의 안전성을 확인하는 확률적인 접근방법이며 기대 총안전수준을 보증한다.

'Météor 프로젝트'는 소프트웨어의 명세화부터 자동설계, 개발단계에서 B 형식기법을 사용하여 소프트웨어의 정확성을 수학적으로 증명하는 검증절차를 거치고, 소프트웨어 실행의 안전성을 증명해 가는 VCP를 사용하여 코드생산과정의 에러와 하드웨어 결함으로 인한 에러를 검출하고 방지했다. B 형식기법과 VCP는 서로 보완관계에 있으며 이를 적절하게 사용하여 높은 신뢰성을 보증하게 되었다.

5.. 결론

철도의 신호보안시스템은 기계, 전기, 전자, 제어, 통신 등 다양한 시스템으로 이루어진 대규모 복합시스템으로 열차의 고속·고밀도 주행에 필수적인 장비이다. 신호용품은 열차안전 운행과 직결되므로 고장률이 낮아야 하며, 유지보수가 편리하여야 한다. 또한 개발 및 설계과정은 물론 운용과정에서 분석과 시험을 거쳐야 한다. 철도 선진국에서는 이미 신뢰성 기술을 확립하여 우주선, 무기체계 또는 원자력발전설비 등에 활용되어 왔으며, 이미 유럽에서는 철도의 경우에도 이와 유사하게 추진해 왔다. 그러나 우리의 경우 철도용품에 대한 신뢰성과 안전성 기술에 대한 연구가 아직 시작단계이며, 철도용품은 일반 상업용 제품보다는 훨씬 엄격한 신뢰성분석과 안전성시험이 요구된다. 철도용품은 기획단계에서부터 설계 및 제작, 운용에 이르기까지 관련 신호보안시스템의 설계, 신뢰성 및 안전성, 품질관리 등의 기술 검증을 위한 판단근거를 마련하고, 안전성 및 신뢰성 평가의 검증 절차 등 기준을 마련하여 시행해야한다. 이를 통해 국내 철도산업의 기술을 선도하고 장비운영의 효율화 및 과학적 유지보수를 수행하고 세계적으로 이루어지고 있는 표준화 구축에 대한 대처 능력이 확보될 수 있다.

시스템은 하드웨어와 소프트웨어가 유기적으로 얽혀 있기 때문에 시스템 신뢰성도 소프트웨어와 하드웨어간의 상호 의존적인 고찰을 통해 분석함으로써 높은 신뢰성 요구를 정확하게 달성할 수 있다. 고도의 정밀함과 안전성이 요구되고 사람의 생명과 안전에 직결되는 철도신호보안시스템은 더욱 절실히 요구된다.

그러나 아직 소프트웨어에 관한 신뢰성 분석은 미미한 편이며 이제서야 관심을 끌고 있다. 일각에서는 지식정보화 사회로 빠른 발전속도에 비해 체계화된 소프트웨어의 설계, 개발, 평가, 분석기법의 부재를 가리켜 '소프트웨어의 위기'라고 규정하고 이 분야 연구개발을 촉구하고 있다.

소프트웨어 분야에서 신뢰성 접근 방법도 형식기법 등의 소프트웨어 공학적인 접근과 확률통계 개념을 기초로한 정량적인 접근 등이 있으나 아직 철도신호분야에 적용하기에는 다각적인 측면에서 검토가 필요하고 좀더 많은 연구가 필요하다. 따라서 이러한 접근법들의 장단점을 체계적으로 분석하여 국내의 철도신호분야에서 고신뢰도와 안전성을 보장하는 새로운 방법들의 개발이 절실히 요구된다.

참고문헌

1) CENELEC Standard EN 50126, EN 50128, ENV 50129, 1997.
2) 平尾裕司, 渡辺郁夫, "列車保安制御システムの安全性技術指針," RTRI REPORT, Vol. 10, No. 11, pp. 5-10, 1996. 11.
3) Faivre, Alain and Benoit, Paul, "Safety Critical Software of Météor Developed with the B Formal Method and the Vital Coded Processor," The 4th WCRR Conference, Tokyo, 1999.