열차제어 통신시스템의 안전성 평가를 위한 연구

조현정*, 황종규, 정락교
한국철도기술연구원 철도시스템연구센터 열차제어통신연구실

Study on Safety Assessment for Train Control Communication Systems

Hyun-jeong Jo*, Jong-gyu Hwang, Rak-gyo Jeong
Train Control & Communication Engineering, Korea Railroad Research Institute

Abstract - Safety-critical systems related to the railway communications are currently undergoing changes. Mechanical and electro-mechanical devices are being replaced by programmable electronics that are often controlled remotely via communication networks. Therefore designers and operators now not only have to contend with component failures and user errors, but also with the possibility that malicious entities are seeking to disrupt the services provided by theirs systems. This paper discusses the safety strategies employed in the railway communications and proposes a security mechanism for Korean railway communication system.

1. 서 론

최근 철도 열차신호제어 통신에서 사용되는 기계적이고 전자적인 장치들이 통신망을 통해 원격 제어되고 프로그램 가능한 전자장치들로 대체됨에 따라 철도 통신망에서의 안전성에 대한 관심이 증가되고 있다. 철도 통신망에서 안전성을 위협하는 요소로는 시스템 부품과 소프트웨어의 오류 또는 고장에 의한 안전성 문제와 철도 통신망이 폐쇄형 전송 시스템에서 개방형 전송 시스템으로 변화함에 따라 발생하는 보안 문제로 나눌 수 있다. 즉, 폐쇄형 전송 시스템에서는 물리적 전용의 유선회로를 사용함으로써 오류나 고장에 대한 안전성 확보를 위한 대책만 요구되었지만, 무선통신이나 인터넷 등을 중심으로 하는 물리적으로 독립되지 않은 전송회로를 사용하는 개방형 전송 시스템으로 변화함에 따라 안전뿐만 아니라 인증 받지 않은 접속으로 고의 방해 등에 대한 엄격한 보안 대책이 필요하다[1][2][3].

열차제어시스템의 통신 부분 안전성과 관련하여 유럽의 경우 유럽 철도 신호안전관리규격인 EN50159-1(폐쇄형 기준) 및 EN50159-2(개방형 기준)를 국제 규격화하여 IEC62280-1(폐쇄형 기준) 및 IEC62280-2(개방형 기준)로 국제 규격화하고 안전 통신을 위한 요구사항으로 제시하고 있다[4][5]. 본 논문에서는 열차신호제어 통신망의 전송 데이터 보안연구를 위해 먼저 철도 열차제어 시스템 통신부분 안전성 평가 체계를 분석하고 안정성 평가 항목과 기준 정의 및 평가 절차를 제시한다. 이를 바탕으로 안정성을 위한 통신 안전성 검증 및 판단 도구 구현에 대한 요구사항 분석을 통해 열차제어시스템 통신망 보안 위험원을 도출 및 제시하고 열차제어시스템 통신망 데이터링크 보안 방법을 제시한다. 또한 본 논문에서는 앞에서 분석 및 제시한 기본 설계를 바탕으로 개방형 안전성 평가를 위한 평가 도구의 구현에 대해 기술하고 그 내용과 결과 적용에 대해 논의한다. 본 도구의 전체적인 내용은 국제 규격인 IIEC62280-2를 기반으로 구현하였다.

2. 열차제어 통신시스템의 안전성 평가기술 체계

2.1 개방형 전송시스템 기반 안전성 평가기술체계

개방형 전송 시스템의 양단간에 사용자에게 알려져 있지 않은 외부 영향에 대한 민감한 전송 특성을 지닌 하나 이상의 종류의 전송 매체로 구성된 임의의 경로를 통해, 사용자에게 알려져 있지 않은 프로그램에 따라서 메시지의 경로 설정이 가능한 네트워크 제어 및 관리 시스템을 기본 능력으로 한다. 개방형 전송 시스템은 먼저 제어 및 보호 시스템 설계자에게 알려져 있지 않으며, 미지의 포맷으로 미지의 정보량을 보내는 전송 시스템의 타 사용자가 있을 수 있고, 둘째로 시스템 관리자로부터 승인 없이 데이터를 읽고 또는 모방하기 위하여, 타 사용자로부터 보내지는 데이터에 대한 접속을 시도할 가능성이 있는 전송 시스템의 사용자도 존재할 수 있다. 마지막으로 안전 관련 데이터의 무결성에 대한 추가적인 위협을 주는 종류에 관계없는 위협들에 의해 영향을 받는다.

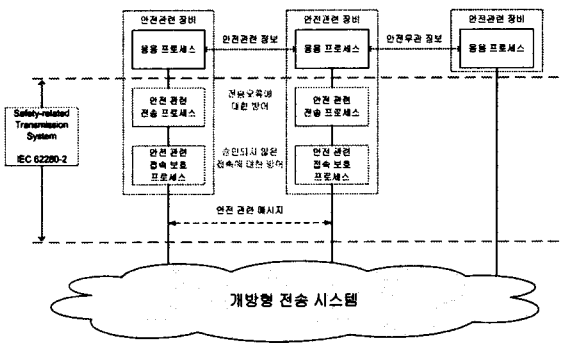

그림 1. 비신뢰 전송시스템을 사용하는 안전관련 시스템의 구조

또한, 개방형 전송시스템 전송링크는 전송 시스템에 연결되어 있는 둘 이상의 안전 관련 장비간의 모든 사항 하드웨어, 소프트웨어, 전송 매체 등으로 구성되는 것으로 간주된다. 시스템 참조구조는 어떠한 내부적 전송 보호 방식이 포함 되었는가 와는 상관없는 비신뢰 전송시스템에 안전과 관련된 및 안전과 무관한 시스템들이 연결되는 개방형 전송 시스템을 사용하는 <그림 1>과 같은 구조이다. 안전 관련 전송시스템은 비신뢰 전송 시스템과 관계되고 어떠한 안전 요구 사항도 개방형 전송 시스템의 비신뢰 특성에 부과되지 않아야 한다. 이 구조는 안전관련 전송 기능과 안전 관련 접속 보호 기능에 바탕을 둔다. 안전 관련 전송 기능에 대한 기능적이고 기술적인 안전에 대한 입증은 IEC62280-2 표준체계를 따라야 하는데, 비신뢰 전송시스템에 대해서는 어떠한 안전 요구 사항도 부과되지 않고 다만 안전성과 관련한 측면

들은 안전 관련 장비 내에서 동작하는 안전 절차와 안전 부호화를 적용함으로써 <그림 2>와 같은 전송 매체 상에서의 안전 관련 메시지 표현 모델을 얻는다.

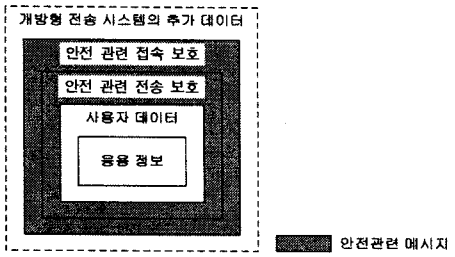

그림 2. 전송매체 상에서의 안전관련 메시지 표현모델

표 1. 개방형 전송시스템 기반 위협 및 위험 사건 및 방어 대책

위험 사건	위협						
	반복	삭제	삽입	순서 재배열	손상	지연	허위
하드웨어의 규칙적인 고장	X	X	X	X	X	X	X1)
소프트웨어의 규칙적인 고장	X	X	X	X	X	X	X1)
혼선		X	X		X		X1)
통신 선로 파괴		X			X	X	
안테나의 잘못된 정렬		X			X		
배선 오류		X	X		X	X	X1)
하드웨어의 불규칙적인 고장	X	X	X	X	X	X	X1)
하드웨어의 노화	X	X	X	X	X	X	X1)
조정이 안 된 장비의 사용	X	X	X	X	X	X	X1)
적합하지 않은 장비의 사용	X	X	X	X	X	X	X1)
부정확한 하드웨어 교체	X	X	X	X	X	X	X1)
페이딩 효과		X		X	X	X	
EMI		X			X	X	
인적 실수	X	X	X	X	X	X	X1)
열잡음		X			X		
자기 폭풍		X			X	X	
화재		X			X	X	
지진		X			X	X	
번개		X			X	X	
전송 시스템의 과부하		X				X	
통신 선로 도청	X	X	X	X	X	X	X1)
하드웨어 손상 또는 파괴		X			X	X	
공인되지 않은 소프트웨어의 수정	X	X	X	X	X	X	X2)
공인되지 않은 메시지의 전송	X		X				X2)
채널의 청취							
방어 대책	- 순서번호 사용 - 시간날인	- 순서번호 사용	- 순서번호 사용 - 출처와 도착지 식별자 - 개별 메시지 식별절차	- 순서번호 사용 - 시간날인	- 안전코드 사용 - 암호화 가법사용	- 시간날인 - 만기	- 개별 메시지 식별절차 - 암호화 가법사용

1) 이와 같은 경우, 잘못된 경로 설정 등과 같은 오류로 인해 올바른 메시지가 잘못된 수신단에 전달된다.
송신단 주소의 명기가 한 가지 가능한 대처 방안이다.
2) 이와 같은 경우, 메시지는 초기부터 그릇된 것이다. Key의 사용 등과 같은 강력한 방어가 요구된다.

개방형 통신망 기반 안전성 평가를 위해 안전에 대한 위협으로 네트워크 및 외부 환경에서 발생하는 위험 사건과 위협과의 관계 및 방어대책은 <표 1>에 나타내었다. <표 1>에서는 폐쇄형 전송망 기반에서의 위험 사건에 개방형 전송망 기반에서 고려되어야 하는 보안에 관한 위협 관련 요소가 추가 되었다. 즉, 외부 환경 개체의 위험사건 확인 단계에 파괴자와 침입자가 위험 관련 요소로 추가되었다. 파괴자에 의해서 발생할 수 있는 위험 사건으로는 통신 선로 도청, 하드웨어 손상 또는 파괴, 공인되지 않은 소프트웨어의 수정이 발생할 수 있고, 침입자에 의해서는 채널의 청취나 공인되지 않은 메시지의 전송이 발생할 수 있다.

2.2 열차제어시스템의 통신 안전성 검증/판단 도구

개방형 안전성 평가 도구 구현을 위한 기본 구조는 <그림 3>에 제시된 것과 같이 크게 2개의 모듈로 구성되어 있다. 우선 안전 관련 전송 기능(IEC 62280-2)과 관련하여 개방형 안전성 테스트 기능 모듈과 비신뢰적 개방형 전송 시스템에 기반 한 전송 매체를 대신한 개방형 기반 논리 전송 매체 모듈로 구성되어 있다.개방형 안전성 테스트 기능 모듈은 송신부와 수신부로 구성되어 있으며 하위의 개방형 기반 논리 전송 매체 모듈을 통해 통신이 이루어진다. <그림 4>는 개방형 안전성 테스트 기능 모듈 구조를 보여준다.

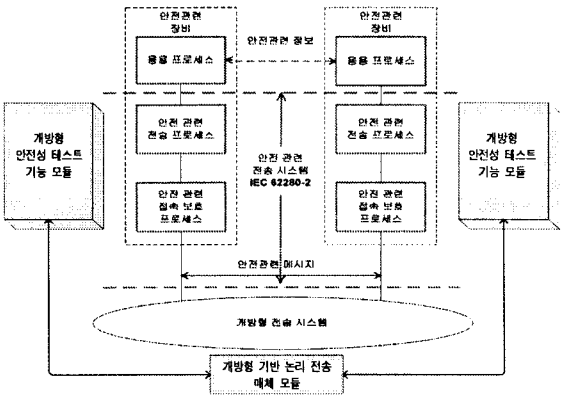

그림 3. 개방형 안전성 평가를 위한 테스트 도구 전체 구조

먼저 개방형 안전성 테스트 기능 모듈(송신부)는 개방형 안전성 기능 시뮬레이션으로 크게 7가지 기능 세부 모듈로 구성된다. 첫째 "순서 번호 생성 세부 모듈", "시간 날인 생성 세부 모듈", "출처와 도착지 식별자 생성 세부 모듈", "식별자 생성 세부 모듈", "안전 코드 생성 세부 모듈", "암호화 생성 세부 모듈", 마지막으로 "수정된 메시지 조합 세부 모듈"로 구성된다. 그리고 "순서 번호 생성 세부 모듈"은 개방형 전송에서의 반복 위협, 삭제 위협, 삽입 위협, 순서 재배열 위협에 대한 예방으로 순서 번호 생성에 대한 기능을 수행하는 세부 모듈이며, "시간날인 생성 세부 모듈"은 반복 위협, 순서 재배열 위협, 지연 위협에 대비하기위한 메시지 생성 시간 생성의 역할을 하는 세부 모듈이다.

그리고 "출처와 도착지 식별자 생성 세부 모듈"은 삽입 위협에 대비해 출처와 도착지 식별자를 생성하는 세부 모듈이며 "식별자 생성 세부 모듈"은 삽입 위협과 허위 위협에 예방의 목적으로 사용자 데이터에 출처 식별자 생성 역할을 담당하는 세부 모듈이다. 또한 "안전 코드 생성 세부 모듈"은 손상 위협에 대한 안전 코드를 생성하는 세부 모듈이며 "암호화 생성 세부 모듈"은 허위 위협에 대한 암호화를 생성하는 세부 모듈이다. 끝으로 "수정된 메시지 조합 세부 모듈"은 위에서 설명된 각종 세부 모듈에 의해 생성된 정보들을 모아서 수정된 메시

지로의 조합을 담당하는 세부 모듈이다. 이렇게 조합된 메시지는 아래의 개방형 기반 논리 전송 매체 모듈로 송신된다.

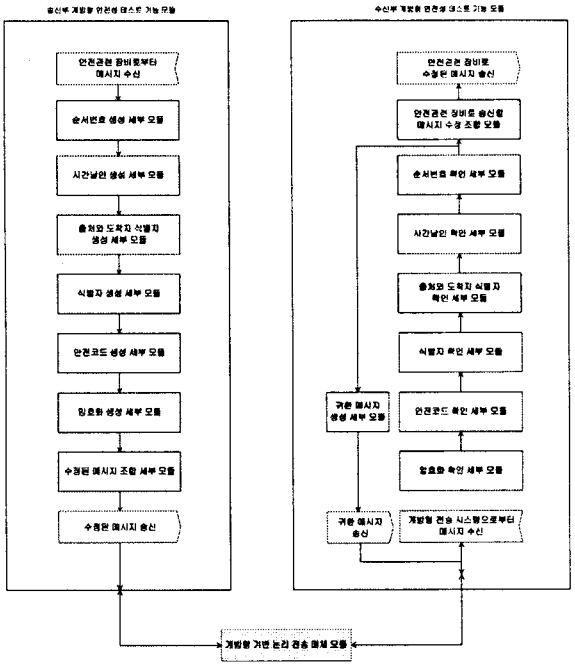

그림 4. 개방형 안전성 테스트 기능 모듈

한편, 개방형 안전성 테스트 기능 모듈(수신부)는 개방형 안전성 기능 시뮬레이션으로 크게 8가지 기능 세부 모듈로 구성된다. 첫째 "암호화 확인 세부 모듈", "안전코드 확인 세부 모듈", "식별자 확인 세부 모듈", "출처와 도착지 식별자 확인 세부 모듈", "시간 날인 확인 세부 모듈", "순서 번호 확인 세부 모듈", "귀환 메시지 생성 세부 모듈", 마지막으로 "안전 관련 장비로 송신할 수정 메시지 조합 세부 모듈"로 구성된다.

3. 결 론

안전 중심의 응용을 위한 기존의 철도 통신은 설치비용이 고가이고, 유지와 보수가 어려운 폐쇄형 통신망에 기반을 두고 있다. 이러한 시스템은 많은 부분에서 명확한 대체 통신 방법의 부재로 인해 융통성 있는 열차 제어 시스템의 도입이 늦어지는 결과를 초래하였다. 그러나 새로운 통신 기술의 기반이 되는 무선 통신 및 TCP/IP 프로토콜의 사용은 개방형 통신기술의 설치와 관련된 기반구조 구축비용의 감소에도 불구하고 다양한 철도 통신 서비스를 제공할 수 있다. 경제적인 관점에서 이러한 해결책이 나타나는 반면에 개방형 통신 시스템의 사용은 안전과 관련된 보안에 문제점이 발생하였다. 열차를 개방형 기반 원거리 제어로 바꾸고자 하는 것은 최근의 문제가 아니지만, 최근에는 추진력을 얻어서 증가되는 추세이다. 전송 또는 통신 기반의 열차 제어에 관한 이러한 경향은 안전과 보안 측면에서 특유의 문제점을 나타내고 있다. 공교롭게도 이러한 광범위 통신의 설치와 관련된 많은 비용을 안전 이득적인 면에서 판단할 수 없고, 좀 더 필수적인 응용을 위해 무선통신 기반의 열차제어시스템에서 개방형 통신망의 사용을 강력하게 원하고 있다.

안전성은 시스템 설계와 시스템이 사용되는 환경의 조합이다. 철도 제어 응용의 환경은 현재 기본 구조 동작 환경과 상당히 다르다. 폐쇄형 통신망 관점에서의 일대일 통신 링크에 대한 주요한 위험요소는 에러와 고장 때문이라는 가정 하에 안전 최우선 시스템을 설계하는 것이 충분하였지만, 그러나 개방형 통신망 관점에서 시스템의 안전성은 악의적이고 고의적인 공격자의 증가에도 안정적인 동작을 필요로 한다. 결론적으로 철도 통신 안정성에 대한 위협은 더 복잡하고 더 다양한 위험원으로부터 안전성을 보장하기 위해서는 개방형 통신망 관점 모두 안전과 보안 측면에서 위협에 대한 대처를 강구하여야 하므로 본 논문에서 연구한 열차제어 통신시스템의 안전성 평가기술 체계 및 통신 안전성 검증/판단 도구가 크게 요구되고 활용될 것으로 기대한다.

[참 고 문 헌]

[1] Winther R. and Johnsen O., Gran B. A., "Security Assessments of Safety Critical Systems Using HAZOPs," Proceedings of 20th International Conference on Computer Safety, Reliability and Security, SAFECOMP, Lecture Notes in Computer Science, Vol. 2187, pp. 14-24, 2001.

[2] Knight J. C., "Safety Critical Systems: Challenges and Directions," Proceedings of the 24th International Conference on Software Engineering, pp. 547-550, 2002.

[3] Eames D. P. and Moffett J., "The Integration of Safety and Security Requirements," Proceedings of 18th International Conference on Computer Safety, Reliability and Security, SAFECOMP, Lecture Notes in Computer Science, Vol. 1698, pp. 468-481, 1999.

[4] IEC-62280-1, "Safety-related communication in closed transmission systems," 2002.

[5] IEC-62280-2, "Safety-related communication in open transmission systems," 2002.