

철도신호용 통신프로토콜의 설계 및 표준화 고찰

황종규, 조현정, 이재호
한국철도기술연구원 열차제어연구팀

Review of Communication Protocol Design and Standardization for Railway Signalling System

Jong-Gyu Hwang, Hyun-Jeong Jo, Jae-Ho Lee
Korea Railroad Research Institute(KRRI)

Abstract - 철도신호제어장치는 열차의 안전운행을 책임지는 매우 바이탈한 제어장치이다. 이러한 바이탈 제어장치는 최근 들어 컴퓨터 및 통신기술의 발달에 따라 각 장치들간 인터페이스를 통한 통합 시스템화 되어가고 있다. 이에 따라 이들 각 장치들간 인터페이스를 위한 통신 프로토콜 또한 높은 안전성이 요구된다. 국내에서 몇 년간의 연구를 통한 이러한 철도신호설비들간 인터페이스를 위한 통신프로토콜에 대한 연구가 이루어 졌으며, 이를 통해 표준으로 제정되어 현재 적용되고 있다. 본 논문에서는 이러한 바이탈한 제어장치인 철도신호설비들간 통신프로토콜의 설계, 검증 그리고 표준화 과정의 분석을 분석하였다. 이러한 프로토콜의 설계 및 표준화 과정의 분석을 통해 높은 안전성이 요구되는 국내 적용 중인 통신프로토콜이 가지고 있는 안전성 특성을 확인하였다.

1. 서 론

전자기술과 정보기술의 급속한 발전으로 컴퓨터망의 획기적인 발전이 가능하게 되었고, 그 결과 많은 통신망들이 구현 및 운용되고 있다. 이러한 다양한 통신망을 경유하는 응용개체(Entity) 사이의 인터페이스는 통신 프로토콜(Communication Protocol)의 정의에 의해 가능하다. 이러한 통신망과 프로토콜은 일반 정보통신 망뿐만 아니라 제어시스템에도 다양하게 응용되고 있으며, 최근 들어 철도제어용 설비들간에도 이러한 통신기술이 적용되고 있다.

철도분야에서의 신호제어장치들은 각자 고유의 기능을 수행하면서 각 장치간 통신링크를 통하여 하나의 통합된 시스템을 이루고 있다. 외국의 경우는 철도신호시스템을 위한 표준 통신 프로토콜들이 존재하며, 그 대표적인 국가표준 프로토콜로는 SAAT와 BR 1631이다[2]. SAAT 프로토콜은 프랑스 철도신호시스템을 위한 프랑스 표준 프로토콜이며, BR 1631 프로토콜은 영국의 국가 표준 프로토콜이다. 이들 각각의 국가표준 프로토콜은 단지 그 나라에서만 적용되고 있다. 이에 따라 국내에서도 국내의 철도신호시스템에서도 국내에서 높은 신뢰성 및 안전성을 갖는 표준 프로토콜의 필요성이 증가함에 따라, 최근 들어 국내 철도신호시스템을 위한 표준 프로토콜이 설계되어 국가표준으로 제정 및 운용되고 있다[1][2].

본 논문에서는 이러한 국내 철도신호시스템을 위한 통신 프로토콜의 설계 및 표준화 과정을 검토하였으며, 이를 통해 바이탈한 철도신호설비들간 인터페이스를 위한 통신프로토콜에 요구되는 안전성 특성을 확인하였다.

2. 표준 프로토콜의 설계 및 검증

2.1 신호제어시스템의 구성

철도신호제어시스템은 다음 어느 제어시스템보다 바이

탈한 제어시스템으로서 많은 장치들 사이에 인터페이스가 이루어지고 있다. 국내에서는 이들 중 그림 1에서와 같이 CTC 통신서버와 선로변 신호기기실에 위치하는 LDTS와 전자연동장치(EIS) 사이의 인터페이스를 위한 통신프로토콜이 설계되어 표준으로 제정되었으며[1], 이 표준 프로토콜은 현재 철도공사에 의해 추진 중인 통합 CTC 관계센터 구축 프로젝트에 적용되어 시험 중에 있다.

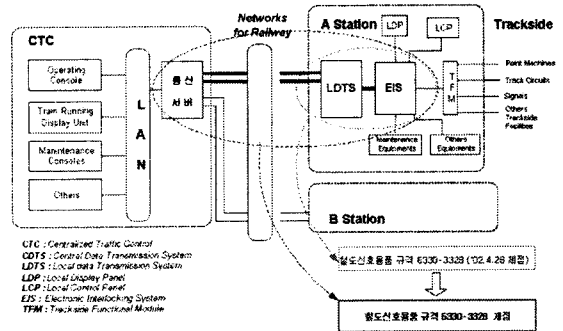


그림 1 프로토콜 표준화 대상

이들 두 장치사이의 통신링크는 관계실 CTC를 통한 제어명령이 전송되고, 반대로 선로변의 현장설비들의 상태정보가 관계실의 CTC로 전송되는 통신링크로서 다른 어느 통신링크보다 더 높은 신뢰성과 안전성이 요구된다. 이 통신링크에는 프로토콜 표준화 이전에 몇 개의 서로 다른 프로토콜이 적용되고 있었다. 이에 따라 시스템의 안전성 및 유지보수에 어려움 등이 있어 표준프로토콜이 매우 필요했던 부분이라 할 수 있다. 이들 사이의 프로토콜은 신호기기실 내부의 LDTS와 EIS 사이에 프로토콜이 우선적으로 표준화 되었으나, 그 후 CTC 통신서버와의 링크를 위해 확대되어 개정되었다. 본 논문에서는 이 표준 프로토콜의 설계 및 표준화 과정을 분석하였다.

2.2 프로토콜의 설계 및 검증 [2]

앞 절에서 설명한 표준 프로토콜의 설계를 위해서 우선적으로 기존에 이들 링크에 적용되었던 프로토콜을 분석하였으며, 이를 통해 이 링크에 요구되는 요구사항을 도출하였다. 이러한 분석과 높은 신뢰성과 안전성 확보를 위한 방향에 준하여 이들 링크를 위한 프로토콜(안)이 설계되었다.

설계된 프로토콜의 검증을 위해서 세단계의 과정이 수행되었다. 신뢰성 확인을 위한 컴퓨터 시뮬레이션, 안전성 확인을 위한 정형검증(Formal Verification) 그리고

최종적으로 적용성 검증을 위한 실험실 레벨에서의 테스트 과정이다. 일반적으로 새로운 프로토콜의 개발에서 신뢰성 확인을 위한 시뮬레이션과 실험실 시험을 거치지 않, 안전성 검증을 위한 정형기법의 적용은 지금까지 정보통신 프로토콜의 일부에서만 적용되어오던 방법으로 철도신호용 프로토콜에는 국내에서 처음 적용된 방법이다. 따라서 본 논문에서는 안전성 확인을 위한 정형검증 방법과 그 결과에 대해 다음 절에 별도로 설명한다.

먼저 신뢰성 검증을 위해 신뢰성 모델링에 의한 시뮬레이션을 통해 기존에 사용되어 오던 프로토콜과 새롭게 설계한 프로토콜의 성능을 비교분석하였다. 그림 2는 이러한 신뢰성 분석 결과를 비교한 것으로, 세로축은 FER(Frame Error Rate)이고 가로축은 E_b/N_0 를 의미한다. 이 결과에서 보듯이 새롭게 설계한 프로토콜이 기존에 사용되어 오던 프로토콜보다 높은 신뢰성을 가짐이 확인되었다.

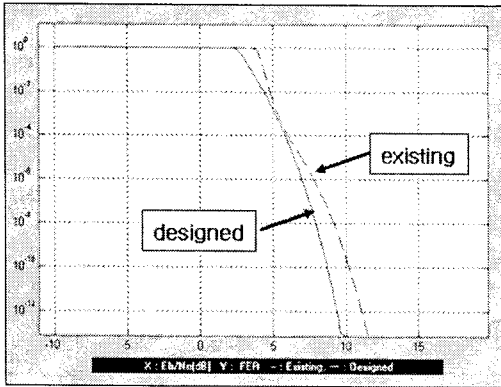


그림 2 프로토콜 신뢰성 분석결과

설계된 프로토콜의 현장적용성 확인을 위해 실험실에서 실제 EIS와 LDTS 그리고 현장 시뮬레이터 등을 모의로 구축하여 설계된 프로토콜을 구현하여 실험을 수행하였다. 실험실 테스트에서는 철도공사 경부선 역 중 하나인 경산역을 모델로 하여 현장설비들은 소프트웨어에 의한 시뮬레이터로 구성하고 LDTS와 EIS는 실제 운용되고 있는 설비들을 이용하였다. 이러한 실험실 테스트를 통한 설계한 프로토콜에서의 몇가지 개선사항을 확인하였고 이 실험 결과를 반영하여 프로토콜(안)을 보완하였다.

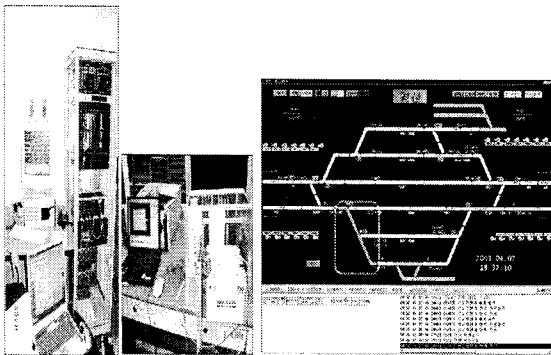


그림 3 적용성 확인을 위한 모의 테스트

2.3 정형기법을 통한 안전성 검증 [2][3]

철도신호시스템은 다른 어느 제어시스템보다 높은 안

전성이 요구되는 바이탈 시스템이다. 따라서 이를 위한 통신 프로토콜 또한 높은 안전성이 요구되고, 프로토콜의 설계과정에서 안전성이 확인되어야 한다. 하지만 지금까지 철도신호용 프로토콜은 대부분 비정형적인 방법 (Informal Method)에 의해 설계 및 구현되어져왔다. 이러한 비정형적인 방법에 의해 개발된 프로토콜은 오류와 비효율성을 내포하고 있을 수 있으며, 이러한 프로토콜이 바이탈한 철도신호시스템에 적용되게 되면 치명적인 결함이나 사고를 발생시킬 수 있다[3]. 하지만 최근에 표준으로 제정된 표준 프로토콜은 이러한 정형적인 방법 (Formal Method)에 의해 안전성이 검증되었음을 확인하였다.

그림 4는 이러한 정형검증 기법에 의한 프로토콜의 개발과정을 나타낸 것으로 일반적인 프로토콜의 개발과정에서 안전성 확인을 위한 마킹된 두 부분이 추가되는 방법이다. 이러한 정형검증 방법은 철도신호용 통신시스템의 안전성 요구사항에 대한 국제 규격인 IEC 62280[4]에서도 권고하고 있는 방법으로 국내에 표준화된 프로토콜이 국제규격에 준하여 개발되었음을 의미한다.

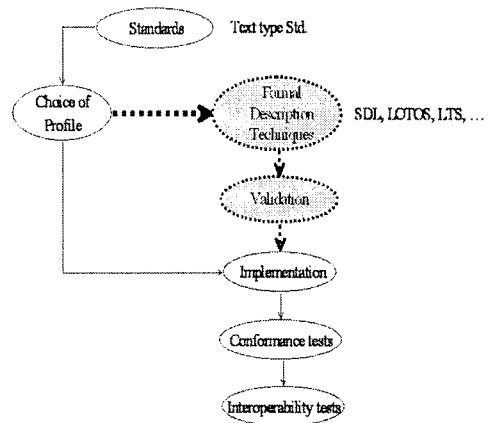


그림 4 정형기법에 의한 프로토콜 개발 과정

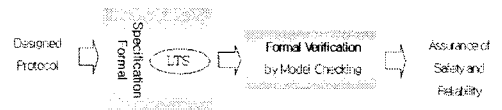


그림 5 프로토콜 정형검증 과정

프로토콜 검증은 프로토콜 명세의 정확성, 안전성과 필연성을 검증하는 것으로 모형검사에서 보다 구체적으로 검증해야 할 프로토콜의 특성은 다음과 같은 안전성 (Safety)과 필연성(Liveness)이며 이 두 특성을 이루는 구성요소는 그림 6과 같이 네 가지가 있다. 안전성 특성은 Deadlock이나 Livelock과 같이 절대로 발생되어서는 안되는 상태나 행위를 프로토콜에서 배제하는 특성을 나타낸다. 필연성은 프로토콜이 초기 상태로부터 정의된 전이의 순서에 의해 결국에는 도달되어야 하는 상태와 반드시 발생해야 하는 행위 즉, Reachability와 Liveness를 만족하는 특성이다.

이러한 검증항목들의 검증을 위해 우선적으로 정형명세(Formal Specification) 언어 중의 하나인 LTS(Labelled Transition System)으로 명세화하고, 이 명세를 모델체킹(Model Checking)에 검증하였다. 그 결과 설계한 프로토콜(안) 높은 안전성을 가짐이 확인되었다.

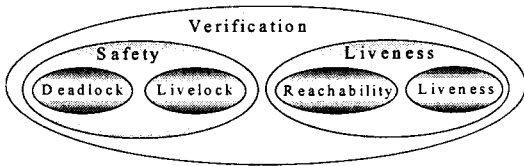


그림 6 프로토콜 정형검정 대상

3. 프로토콜의 표준화

앞 절에는 철도신호용 프로토콜의 설계과정을 설명하였다. 특히 컴퓨터 시뮬레이션을 통한 신뢰성 확인, 정형검증을 통한 안전성 검증 그리고 현장적용성 확인을 위한 실험실 테스트 등 설계한 프로토콜의 검증과정과 그 결과를 분석하였다.

이러한 설계 및 검증과정을 통해 얻어진 프로토콜(안)이 표준으로 채택되기 위해서는 이를 운용할 운영기관과 이를 구현할 제작사의 의견 수렴 과정이 필수적이다. 본 프로토콜은 5차례에 걸친 의견수렴을 거쳐 최종안이 준비되었고, 이를 통해 최종적으로 표준안으로 제정되었음을 확인하였다. 그림 7은 이러한 프로토콜의 설계에서 표준화까지의 일련의 과정을 나타낸 것이다. 표준화된 프로토콜이 올해 11월 완공을 목표로 하고 있는 철도공사의 통합 관제센터 구축 프로젝트에 적용되어 그 성능을 테스트 중에 있다. 이 프로젝트에 따른 실제 시스템에 포팅되어 시스템과 함께 테스트 중에 있으며, 그 결과에 따라 일부 보완사항 발생 시 표준 프로토콜은 개정되어질 수 있을 것이다.

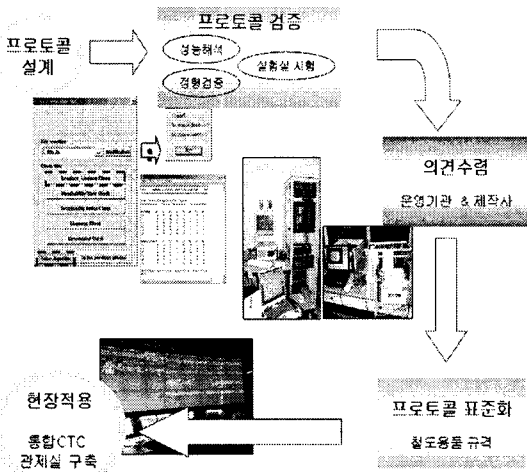


그림 7 프로토콜 설계 및 표준화 절차

4. 프로토콜의 안전특성 분석

앞에서 설명하였듯이 철도신호용 프로토콜은 높은 안전특성을 갖는 것이 매우 중요하다. 이러한 바이탈 신호 제어시스템을 위한 통신의 안전성 요구사항이 IEC 62280의 국제규격에 정의되어 있다. 이 국제규격에 의하면 철도신호용 전송시스템의 구조는 그림 8과 같으며, 이 전송구조에서 통신기능인 '안전관련 전송기능'에서 그림 9와 같이 안전절차(Safety Process)와 안전코드(Safety Code)의 적용을 요구하고 있다. 표준 규격의 분

석결과 IEC 62280 규격에서 요구하는 안전절차 요구사항 대부분이 구현되어 있음을 확인하였고, 안전코드는 표준 프로토콜에서는 CRC-16 코드가 적용되었음을 확인하였다.

따라서 본 논문에서 분석 대상으로 한 국내의 철도신호용 표준 프로토콜은 안전성 요구사항을 명시한 국제규격을 준수하고 있고, 이에 더하여 정형검증을 통한 안전성 확인을 거친 프로토콜로서 높은 안전성이 요구되는 바이탈한 철도신호용 프로토콜로 적절함을 확인할 수 있었다.

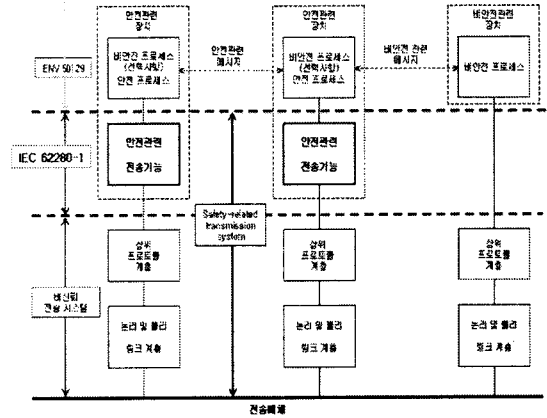


그림 8 국제규격에 의한 안전관련 전송시스템 구조

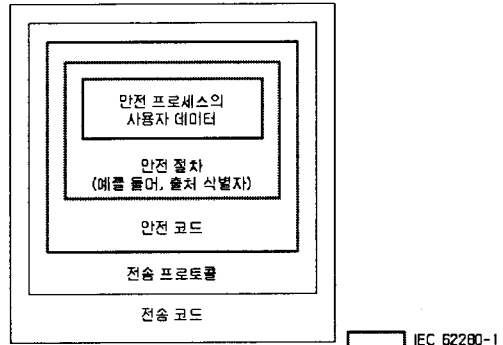


그림 9 전송매체에서의 메시지 표현모델

[참고 문헌]

- [1] 철도용품규격6330- 3348, '철도신호시스템 점대점 정보전송 방식', 2004.
- [2] 황종규, 이재호, '철도신호시스템을 위한 새로운 통신 프로토콜의 성능해석 및 검증', 전기학회논문지, 53B권 6호, pp.380-387, 2004년 6월.
- [3] D. Schwabe, 'Formal Techniques for the Specification and Verification of Protocol', Ph.D Thesis, Univ. of California Los Angeles, 1981.
- [4] IEC 62280, 'Railway application - Safety-related communication in closed transmission systems', 2002.