한국철도학회논문집
제7권 제2호 2004년 | pp.114-119

철도신호설비 상호간 정보전송을 위한 통신 프로토콜 검증시험

Verification Test of Communication Protocol for Interface between EIS and LDTS

황종규[1] · 이재호[1] · 윤용기[1] · 신덕호[2]
Hwang Jong-Gyu · Lee Jae-Ho · Yoon Yong-Gi · Ducko Shin

Abstract

According to the computerization of railway signalling systems, the communication protocol for interface between these systems are required. Therefore the new communication protocol for railway signaling system is required. Generally, there are two verification method for new designed protocol in the industrial and academic fields. One is the laboratory testing method which is very popular and general technique. In our research the comparison between existing and new designed protocol for signaling is described and the verification test results are also represented. From these laboratory test, we are verified the conformance of new designed protocol. Another method is verified by formal method. The formal verification method is widely used at safety-critical system design but this approach is nor popular at verification communication protocol. However it is very important to verify the safety of new designed protocol for railway signaling system because signaling systems are very safety-critical systems. So, the methodology for formal verification of designed protocol is also reviews in this paper.

Keywords : Communication Protocol(통신 프로토콜), Railway Signaling Systems(철도신호시스템), Formal Method(정형기법), Model Checking(모형검사)

1. 서 론

철도 신호제어장치들은 각자 고유의 기능을 수행하면서 각 장치간 통신링크를 통하여 하나의 신호제어시스템을 구성하고 있다. 이러한 신호제어장치들이 기존에는 대부분 기계적 또는 전기적인 계전기 로직에 의해 그 고유의 기능을 수행하여 왔으나, 최근 들어 각 장치별로 전자화된 시스템들로 대체되어가고 있다. 이처럼 신호제어장치들이 전자화 되어감에 따라 각 장치간 인터페이스를 위한 링크 구성도 디지털 통신채널을 통하여 구성되고 있다. 따라서 이러한 각 장치간 인터페이스를 위한 통신채널에 대한 중요성이 증대되고 있다.

현재 철도청의 주요 신호제어장치들간 통신 프로토콜들은 각 제조회사별, 각 노선별 서로상이함으로 인해 통신시스템을 포함한 신호제어시스템의 안전성 저하는 물론이고 유지보수에도 어려움이 있다. 또한 기존에 많이 사용하고 있는 통신 프로토콜의 경우 특정 하드웨어에 종속되어 있거나 멀티드롭 방식이 적용된 비정상적인 프로토콜을 사용하고 있어 새로운 철도신호용 통신프로토콜이 필요하였다. 외국에서는 철도신호시스템을 위한 표준 통신 프로토콜들이 존재하며, 그 대표적인 국가표준 프로토콜로는 SAAT와 BR 1631이다[3,4]. SAAT 프로토콜은 프랑스 철도분야에서 SNCF(French National Railway Authority)에 의해 적용된 철도신호시스템을 위한 프랑스 표준 프로토콜이며, BR 1631 프로토콜은 영국의 국가 표준프로토콜이다. 이들 각각의 국가표준 프로토콜은 단지 그 나라에서만 적용되고 있으며, 신호시스템을 위한 안전성, 신뢰성 및 유지보수의 효율성은 그들 표준 프로토콜을 적용함으로써 개선되어졌다. 따라서 그러나 그들 각 나라의 프로토콜은 국제표준으로 고려되고 있지는 않다.

이에 따라 철도청에서 운용 중인 여러 신호제어장치들 중 대표적인 전자연동장치(EIS : Electronic Interlocking

1 정회원, 한국철도기술연구원, 선임연구원
2 정회원, 한국철도기술연구원, 주임연구원

System)와 역정보전송장치(LDTS : Local Data Transmission System) 사이의 인터페이스를 위한 프로토콜을 설계 및 제시하였으며, 철도청에 의해 표준으로 채택되었다[1,2].

새로운 표준 프로토콜은 시뮬레이션을 통한 성능해석으로 철도현장에서 적용되고 있던 기존의 프로토콜에 비해 성능면에서 우수함을 확인하였다[2]. 새롭게 설계한 프로토콜은 기 발표된 바와 같이 컴퓨터 시뮬레이션에 의한 성능검증을 한 후 실제 적용 전에 반드시 적합성 시험을 수행하여야 한다. 시뮬레이션에 의한 성능해석은 프로토콜이 가지고 있는 지연시간이나 처리율 등에 대한 성능평가지수들에 대한 검증을 위한 단계이고, 이를 통해 프로토콜에 요구되는 성능이 확인되면 설계된 프로토콜이 논리적으로 적절한지 또는 모순된 부분이 없는지, 실제 적용 상에 모호성이 없는지 등을 확인하기 위한 검증시험이 이루어져야 한다.

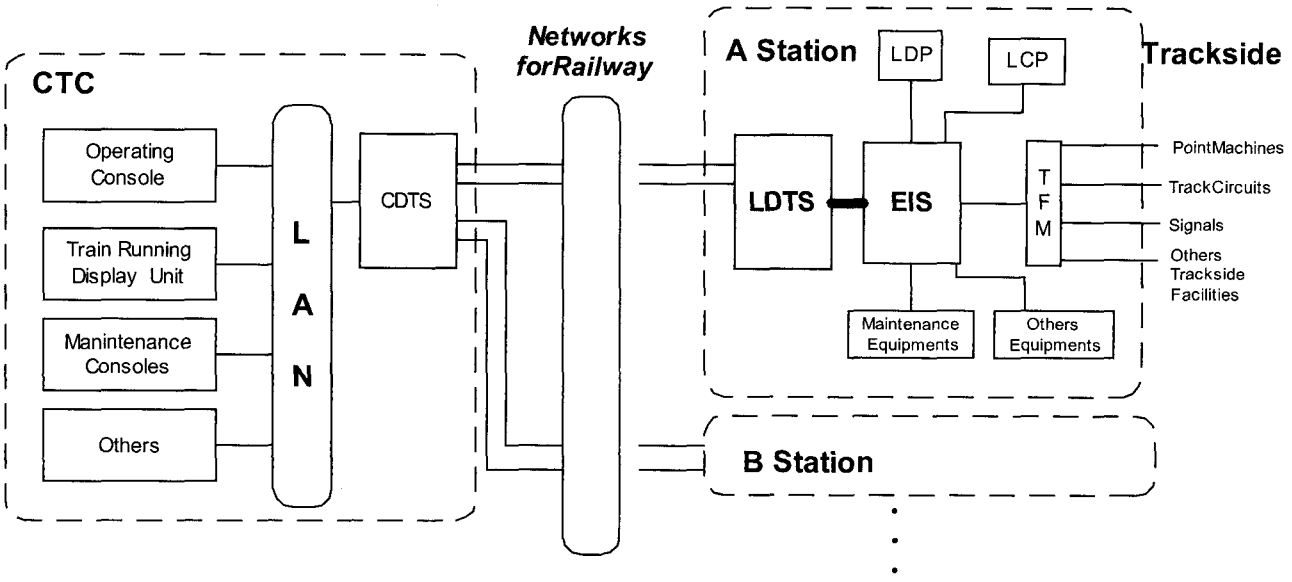
일반적으로 프로토콜의 검증시험에서는 직접적인 시험에 의한 실험적인 방법이 많이 적용되고 있는 방법으로, 프로토콜을 실제 장치에 탑재하여 시험을 수행하는 것으로 이 시험을 통해 실제 적용 전에 설계된 프로토콜의 안전성이나 적합성을 검증하는 방법이다. 본 논문에서는 철도신호용 표준 통신프로토콜의 검증을 위해서는 실제 LDTS와 EIS 각 장치에 표준 프로토콜을 탑재하여 정보전송하여 프로토콜 분석기와 각 콘솔을 통해 확인하는 실험적인 방법을 적용하였다.

그리고 바이탈 제어시스템 설계에 적용되어오던 정형기법(Formal Method)을 프로토콜의 안전성 검증에 적용하려는 연구가 외국을 중심으로 진행되어오고 있다[5]. 특히 철도신호시스템과 같이 바이탈한 제어장치에 사용되는 프로토콜의 경우는 심각한 오류 등을 정형기법을 통해 제거하여 프로토콜의 안전성을 확보하는 것이 매우 중요하다. 이에 따라 본 논문에서는 설계한 프로토콜을 형식언어(Formal Specification Language)에 의해 명세화하고 이를 바탕으로 안전성과 필연성 특성을 정형검정(Formal Verification) 하는 방안을 연구하여, 철도신호용 프로토콜에 적합한 방법론을 제시하였다[6-8].

2. 표준 프로토콜

철도청의 신호시스템 구성은 그림 1과 같이 매우 많은 컴퓨터화된 제어장치들로 구성되고 있다. 이들 장치들 중 본 연구에서는 철도청의 신호장치들 중 대표적인 EIS와 LDTS 간 통신 프로토콜을 연구하였다.

이들 두 장치사이의 통신 링크에 사용되는 통신 프로토콜은 여러 가지가 적용되고 있지만 그 중 가장 많이 사용되는 프로토콜이 I/O 프로토콜이다. 표 1은 이 I/O 프로토콜과 표준 프로토콜의 주요 내용을 비교한 것으로서, 표준 프로토콜에서는 기존 프로토콜에서의 불합리한 점들이 개선되었



***CTC** : Centralized Traffic Control*
***CDTS** : Central Data Transmission System*
***LDTS** : Local data Transmission System*
***LDP** : Local Display Panel*
***LCP** : Local Control Panel*
***EIS** : Electronic Interlocking System*
***TFM** : Trackside Functional Module*

그림 1. 철도신호시스템의 구성

표 1. 기존 프로토콜과 표준 프로토콜의 비교

내용	기존 프로토콜	표준 프로토콜
바이트 구성	9 Bit(1 byte)	8 Bit(1 byte)
프레임 구성	[표 2]	[표 3]
	Destination Type/ID+Source Type/ID : 일반적인 점대점 통신에는 필요 없는 필드	해당필드 삭제(필요 없음)
	Sequence No. : 없음	전송 데이타의 안전성 확보를 위한 필드
	· 프레임 시작 구분 : 9th 비트값 · 프레임 끝 구분 : Length 필드로 계산	· 프레임 시작 구분 : STX 필드 · 프레임 끝 구분 : ETX 필드(안전성 향상)
최소길이	4 Bytes(36 Bits)	7 Bytes(56 Bits)
최대길이	133 Byte(1197 Bits)	262 Bytes(2096 Bits)
에러검지	Checksum	CRC-16(에러검지 확률 증가)

표 2. 기존 프로토콜의 전송메시지 구조

Destination Type/ID	Source Type/ID	Message Type	Message Length	Data	BCC
1 byte	1 byte	1 byte	1 byte	N byte	1 byte

표 3. 표준 프로토콜의 전송메시지 구조

STX	Data Length	Sequence No.	Message Type	Data	CRC	ETX
1 byte	1 byte	1 byte	1 byte	N byte	2 byte	1 byte

으며, 또한 시뮬레이션을 통해 표준프로토콜이 기존 프로토콜에 비해 성능이 우수함을 확인하였다[2]. 기존 프로토콜과의 비교 및 표준 프로토콜에 대한 내용은 [1]과 [2]에 상세히 설명되어져 있다.

3. 검증시험

3.1 시험현황

LDTS와 EIS 사이의 표준 프로토콜을 검증하기 위하여 실제 두 장치에 표준 프로토콜을 탑재하여 시험을 수행하였다. 검증시험을 위해 그림 2와 같이 경부선의 경산역을 실험실 시험을 위한 모델역으로 선정하였다. 선정한 모델역은 건널목 정보를 제외한 두 장치사이의 인터페이스에 필요한 모든 정보들을 포함할 수 있어 프로토콜의 검증시험을 위한 대상으로 적절하다.

그리고 표준 프로토콜의 검증시험을 위해 실험실에 구성

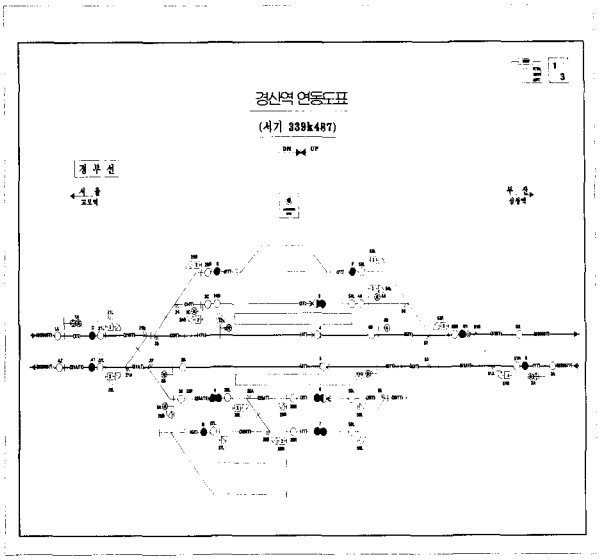


그림 2. 검증시험을 위한 모델역

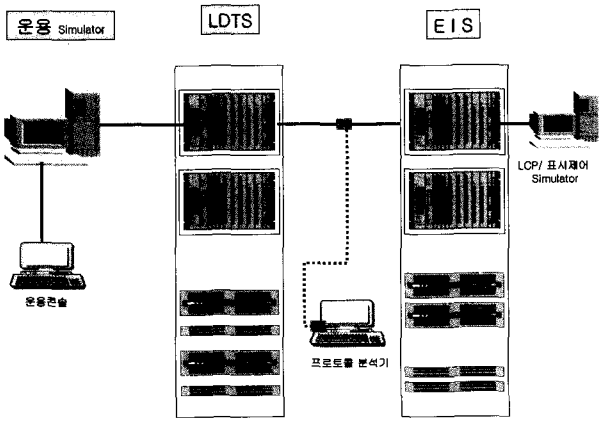


그림 3. 검증시험을 위한 시스템 구성

한 시스템 구성은 그림 3과 같다. 이때 궤도회로, 선로전환기, 신호기 등의 현장 신호설비들은 소프트웨어에 의한 시뮬레이터로 대신하였다. 이러한 현장 신호설비들은 대부분 전기적인 계전기 접점의 On/Off를 통해 제어되고 또한 이 계전기 접점의 상태가 피드백되어 연동장치의 운용콘솔에 표시되므로, 이러한 On/Off 접점을 소프트웨어에 의한 디지털 접점으로 대신하여도 연동장치나 LDTS 등 제어장치들의 관점에서는 실제 현장설비들로 제어정보를 내리고 또한 피드백 받는 것으로 인식할 수 있다. 따라서 본 프로토콜의 검증시험에는 실제 설비들과 거의 유사한 조건으로 볼 수 있다.

검증시험 시 각 장치에 연결되어 있는 시뮬레이터에서 통신모듈을 통해 송수신되는 프레임을 Hex 값으로 모니터링 할 수 있도록 하여, 두 장치 사이의 프로토콜 분석기와 이들

각각의 시뮬레이터 값들을 통해서 표준 통신프로토콜의 검증시험을 수행하였다.

3.2 시험결과

검증시험에서는 표준 프로토콜에 제시된 모든 전송메시지를 발생시켜 링크 중간에서 프로토콜 분석기와 각 장치들에 연결되어 있는 시뮬레이터 및 운용콘솔을 통해 정상적으로 데이터가 전송되는지를 확인하였다. 그림 5는 LDTS에서 EIS로 초기 폴링 메시지를 전송하고 이에 대한 응답으로EIS의 초기 상태정보를 업데이트하는 전송정보를 시뮬레이터 콘솔을 통해 확인한 것을 보인 것이다.

위의 "수신" 메시지는 EIS에서 LDTS로부터 주기적인 업데이트를 위한 폴링 메시지를 나타내고, 아래의 "송신" 메시지는 이에 대한 응답으로 LDTS로 추기 EIS의 상태정보 131 바이트를 업데이트 하는 것을 확인할 수 있다.

그림 6은 LDTS에서 제어메시지를 전송하고 EIS가 이에

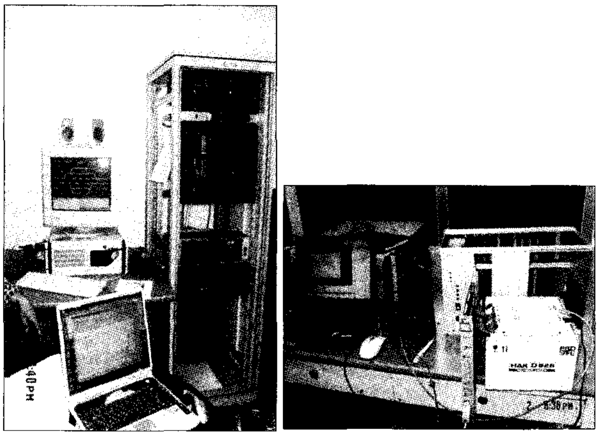
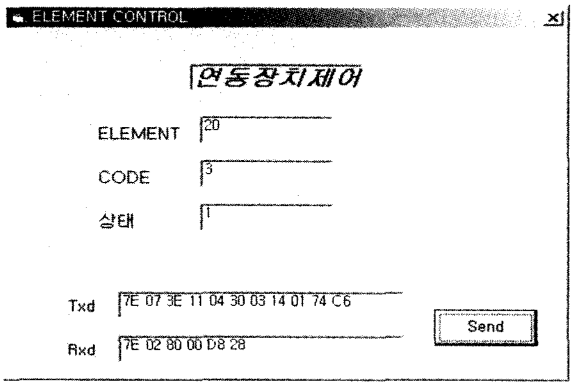


그림 4. 시험현황

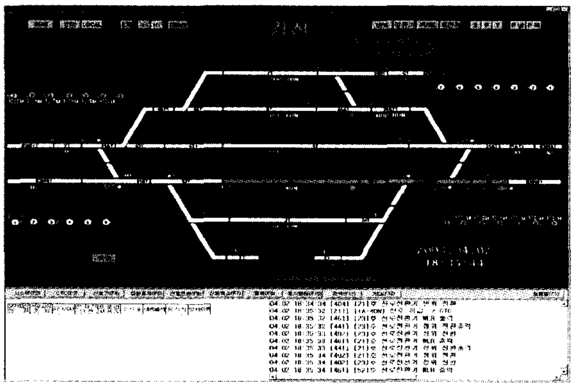
수신 = <02><04><00><10><00><00><00><84><F1><E7>
<03>
Packet = [F1]-[E7], Cal = [00]-[00]
RequestAllInfo...[0]-[131]
송신=[02][84][00][11][01][00][01][01][01][01][01][01][01][01]
[01][01][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][00][00][00][00][00]
[00][00][00][00][00][00][00][00][00][03][00][00][03]

그림 5. LDTS ⇒ EIS 폴링요청 및 응답 메시지

응답하는 송수신 메시지를 표시하는 콘솔과 LCP 화면을 나타낸 것이다. 그림 6(a)는 진로제어명령을 설정하는 LDTS 운용 시뮬레이터 화면을 나타낸 것으로 "1A-4D" 진로설정 명령이고, 이 제어메시지를 전송받은 EIS는 이 제어명령에 따라 진로제어를 하고 LCP 화면에 표시한 예를 보여주고 있다. 이 진로제어 메시지 이외에 LDTS에서 전송될 제어 메시지는 선로전환기 제어, 입환진로 설정, 운용모드 절체



(a) LDTS 콘솔의 진로제어명령 설정



(b) EIS LCP 출력

그림 6. 제어 메시지 전송 및 응답확인 출력화면

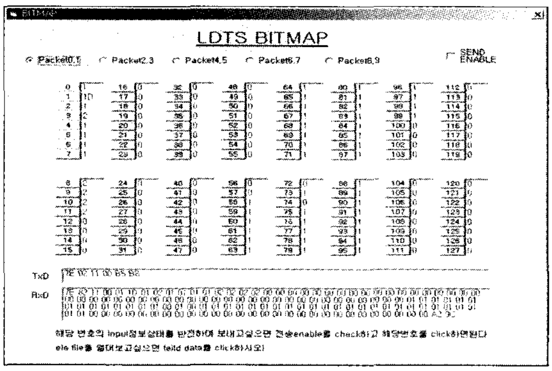


그림 7. LDTS 시뮬레이터

명령 등이 있다. 이러한 제어메시지를 LDTS 시뮬레이터를 통해 발생시키고 LCP 화면과 프로토콜 분석기를 통해 이를 송수신되는 메시지의 정확성을 확인하였다.

4. 정형기법에 의한 검증방안

통신 프로토콜에 대한 사용자의 요구사항이 복잡화, 다양화, 대형화되어짐에 따라 개발에 따르는 어려움은 더욱 증대되었고, 비정형적 방법에 의한 개발은 많은 오류나 결함을 내포할 수 있다. 특히 철도신호시스템 같은 바이탈 제어시스템에 적용을 위해서는 이러함 오류나 결함이 제어되어져야 한다. 이에 따라 일반적으로 바이탈 제어시스템의 설계에 적용되어오던 정형기법을 프로토콜 설계에 적용을 위한 연구를 수행하여, 본 논문에서는 설계한 프로토콜을 정형검증을 위한 방법론을 제시한다.

프로토콜 검정은 프로토콜 명세의 정확성, 안전성과 필연성을 검증하는 것으로 모형검사에서 보다 구체적으로 검정해야 할 프로토콜의 특성은 다음과 같은 안전성(Safety)과 필연성(Liveness)이며 이 두 특성을 이루는 구성요소는 다음과 같이 네 가지가 있다[5]. 안전성 특성은 Deadlock이나 Livelock과 같이 절대로 발생되어서는 안되는 상태나 행위를 프로토콜에서 배제하는 특성을 나타낸다. 필연성은 프로토콜이 초기 상태로부터 정의된 천이의 순서에 의해 결국에는 도달되어져야 하는 상태와 반드시 발생해야 하는 행위 즉, Reachability와 Liveness를 만족하는 특성이다. 본 연구에서는 이러한 안전성과 필연성 검증을 프로토콜의 정형검증 기준으로 설정하였다.

이러한 대상들을 검정하기 위해서는 설계한 프로토콜을

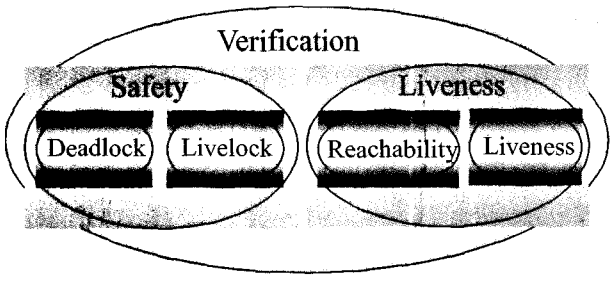


그림 8. 프로토콜 정형검정 대상

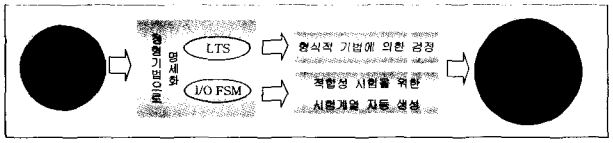


그림 9. 프로토콜의 정형검증 절차

형식언어(Formal Specification Language)로 표현하여야 하는데, 본 연구에서는 정형검증을 위한 중간모델인 LTS (Labeled Transition System)로 하기로 하였다. 이 LTS의 경우는 시스템의 상태천이에 대한 모델링을 위한 형식언어로 프로토콜 같은 순차적인 프로세스의 표현에 적절하다. 그리고 이 형식명세를 바탕으로 정형검증을 위해서는 형식명세가 안전성과 필연성 특성을 만족하는지를 분석하는 과정이 필요하다, 이러한 과정이 모형검사(Model Checking) 기법으로, 일반적으로 시제논리에 기반을 둔 방법들이 많이 사용되어 왔으나 시스템 요소의 증가에 따라 상태가 기하급수적으로 증가하는 상태폭발 문제가 있어, 본 프로토콜의 검증을 위해서는 Modal μ-calculus 논리를 이용한 검정방법이 적절할 것으로 보인다.

이 중 Solve 알고리즘의 모형검사 알고리즘을 적용하고자 한다[6]. 그리고 정형검증이 마무리된 후 실제로 프로토콜이 구현되었을 경우, 구현된 프로토콜이 정확하게 구현되었는지 시험을 위한 시험계열 생성을 위해 I/O FSM(Input/Output Finite State Machine)으로 모델링하고 이를 바탕으로 시험계열을 생성하여 구현된 프로토콜의 정확성을 검증할 예정이다.

5. 결 론

철도청에서 운용 중인 여러 신호제어장치들 중 가장 대표적인 전자연동장치와 역정보전송장치 사이의 인터페이스를 위한 표준 프로토콜이 설계되어 제시되었다. 하지만 이 프로토콜이 실제 적용에 앞서 설계된 프로토콜의 적합성이 검증되어야 한다. 본 논문에서는 이를 위해 실제 장치에 본 프로토콜을 탑재하여 시험하는 실험적인 방법에 의한 검증시험 결과를 설명하였다. 이 시험결과 제시된 프로토콜이 정상적으로 동작됨을 확인할 수 있었다.

또한 설계된 프로토콜의 정형검정을 위해 본 논문에서는 정형검정 대상, 정형검정을 위한 형식언어, 검정알고리즘, 시험계열 생성을 위한 방법론을 제시하였다. 이러한 방법론에 따른 정형검정이 이루어지게 되면 철도신호시스템을 위한 프로토콜의 정형검정은 보다 높은 신뢰성과 안전성이 확보될 것이다.

감사의 글

본 프로토콜의 검증시험에 도움을 주신 철도청, 유경제어(주), LG산전(주) 담당자 여러분께 감사드립니다.

참 고 문 헌

1. 철도용품 규격, "철도 6330-3328 : 열차집중제어장치와 전자연동장치간 정보전송방식(Protocol)", 철도청, 2002.
2. 황종규, 이재호, "전자연동장치와 역정보전송장치간 인터페이스를 위한 데이터링크 프로토콜 성능해석", 한국철도학회 논문지, 제6권 제2호, pp.135-141, 6. 2003.
3. NF F72-010(Norm de French), "Procedure for Transmission of Bi-directional Serial Asynchronous Point-to-point : French Railway Protocol", SNCF, French, 1991.
4. G7 고속전철기술개발사업 연구보고서, "전기신호시스템 엔지니어링 기술개발", 한국철도기술연구원, 1999. 10.
5. D. Schwabe, "Formal Techniques for the Specification and Verification of Protocol", Ph.D Thesis, Univ. of California Los Angeles, Apr., 1981.
6. D. Kozen, "Results on the Propositional Mu-calculus, Theoretical Computer Science", 27:333-354, 1983.
7. R. Cleaveland, "Tableau-Based Model-checking in the Propositional Mu-calculus", Acta Informatica 27:725-727, 1990.
8. E. M. Clarke, E. A. Emerson and A. P. Sistla, "Automatic Verification of Finite State Concurrent Systems Using Temporal Logic Specifications", ACM TOPLAS 8(2), 1986.