한국철도학회논문집
제10권 제3호 2007년 ▌pp.365-371

열차제어용 표준 통신 프로토콜의 안전 특성 분석 및 평가

Safety Characteristics Analysis of Korean Standard Communication Protocol for Railway Signalling

황종규† · 조현정* · 이재호**
Jong-Gyu Hwang · Hyun-Jeong Jo · Jae-Ho Lee

Abstract

The communication protocol for interface among railway signalling systems is designed and established as national standard in Korean from a few years ago. So the communication link for information transmission among railway signalling system can be a good example of application of this standard. Communication protocol which is standardized among Korean railway signalling is considered to apply information transmission. And we confirmed there is no the states of deadlock of livelock in std. protocol which is applied formal verification which is one of the analytic method for inspection of safety characteristics in the design course of protocol. But the safety of protocol has to necessarily accomplish this normal analysis approach about satisfying requirement matters with such this analytic approach. In this paper we analyzed the safety characteristics of standard protocol for Korean Railway signalling through the requirement matters for safety transmission of railway transmission system which is required in international standard. So through this study we confirm whether it satisfies safety requirement matters of the level which require in international standard and tried to confirm whether standard protocol has enough safety character in the real railway field.

Keywords : Standard Communication Protocol, Safety Characteristics, Formal Verification

1. 서 론

유럽을 중심으로 철도시스템의 안전성에 관련된 기준 및 지침들이 규격화되어 운용되고 있으며, 이 중 철도시스템 통신 관련된 안전성 부분은 유럽전기전자표준위원회인 CENELEC에 의해 유럽규격인 EN 50159로 규격화되었다가 최근 들어 IEC 62280 코드로 국제규격화 되었다[1][2]. 이 규격에서는 철도시스템의 전송시스템에 연결되어 있는 안전관련 장비들간 통신을 하기 위해 필요한 요구사항들이 제시되고 있으며, 전송시스템을 폐쇄형과 개방형의 두 부분으로 나뉘어져 각각에 대한 안전 요구사항을 제시하고 있다. 철도신호시스템은 다른 어느 시스템 보다 높은 안전성을 요구하고 있으며, 이러한 바이탈한 안전설비인 신호장치들간 인터페이스를 위한 통신링크는 이 규격을 적용하기에 가장 좋은 예가 될 수 있다.

이러한 철도시스템의 통신관련 안전요구사항의 국제규격화와는 상관없이 국내에서는 몇 년전부터 철도신호설비들간 인터페이스를 위한 통신프로토콜이 설계되어 국가표준으로 제정되었다. 표준화된 국내 철도신호설비들간 통신 프로토콜은 현재 CTC 통신서버와 현장설비인 LDTS나 전자연동장치 사이 또는 SCADA 장치사이의 정보전송에 적용이 고려되어지고 있다. 이 통신 프로토콜의 설계 및 표준화 과정에서 통신프로토콜이 가지는 신뢰성 확인을 위한 시뮬레이션이나 실험실 차원에서의 모의시험 등의 단계를 거쳐 프로토콜의 성능을 검증하려는 노력들이 전개되었다[6]-[8]. 또한 프로토콜의 설계과정에서 안전성 검증을 위해 해석적인 방법 중의 하나인 정형검증(Formal Verification) 방법을 적용하여 프로토콜 내부에 데드락(Deadlock)이나 라이브락(Livelock) 상태가 없음을 확인 하였다[8]. 하지만 프로토콜의 안전 특성은 이러한 프로토콜공학의 절차에 따른 해석적인 방법과 더불어 국제규격에서 명시한 요구사항을 만족하는지에 대한 정성적인 분석과정이 필수적으로 이루어져야 한다.

† 책임저자 : 정회원, 한국철도기술연구원, 열차제어연구팀, 공학박사
E-mail : jghwang@krri.re.kr
TEL : (031)460-5438 FAX : (031)460-5449
* 정회원, 한국철도기술연구원, 열차제어연구팀, 주임연구원
** 정회원, 한국철도기술연구원, 열차제어연구팀, 책임연구원, 공학박사

본 연구에서는 국제규격에서 요구하고 있는 철도전송시스템에서의 안전전송을 위한 요구사항을 통한 국내의 표준프로토콜의 안전특성을 분석하였다. 국내의 철도신호설비용 표준 통신프로토콜은 국가 표준으로 제정 후 철도현장에서 이제 막 적용하려는 단계에 있다. 따라서 국제규격에서 요구하는 수준의 안전요구사항을 만족하는지 여부 확인을 통하여 실제 철도현장에 표준프로토콜이 적용되기 전에 충분한 안전특성을 가지고 있는지 확인하는 것이 필요하다. 2장은 안전전송 국제규격의 요구사항을 간략하게 분석하였고, 3장에서는 국내 표준 프로토콜 개요, 4장은 해석적인 방법과 정성적인 방법에 의한 표준 프로토콜의 안전 특성 분석결과, 마지막으로 5장에는 결론으로 본 논문이 구성되어져 있다.

2. 안전전송 국제규격에 따른 요구사항 분석

철도시스템의 정보전송시스템의 안전요구사항은 IEC 62280에 명시되어져 있으며, 이 규격은 다음과 같이 개방형(Open) 전송시스템과 폐쇄형(Closed) 전송시스템의 두 부분으로 구분되어져 있다. 본 절에서는 이러한 국제규격에 의한 통신 안전성 요구사항을 분석하였다.

- Part 1 : Safety-related communication in closed transmission systems
- Part 2 : Safety-related communication in open transmission systems

철도시스템의 전송시스템을 개방형과 폐쇄형 시스템으로 구분하여 IEC 62280에서는 표 1과 같이 정의하고 있다. 철도신호시스템은 열차제어의 안전운행에 매우 중요한 시스템으로 분류하여 열차제어용 망 이외의 외부망과의 인터페이스를 하지 않으며, 또한 외부망과 인터페이스를 하더라도 방화벽 등의 안전장치를 두어 외부망에서 철도신호제어용 망에 접근을 막고 있다. 이에 따라 철도신호시스템에 사용되는 대부분의 통신링크는 폐쇄형 전송시스템으로 IEC 62280-1의 요구사항을 적용할 수 있다. 하지만 최근 들어 통신기반 열차제어 시스템(CBTC : Communication Based Train Control System)이 국내에서도 시범적용되고 있는 등 지상과 차상간의 통신방식이 개방된 RF 통신링크 방식의 적용에 따라 외부의 접근 가능성이 있는 등 개방형 전송시스템이 도입됨으로 인해 IEC 62280-2의 요구사항도 같이 고려되어져야 한다. 유럽의 ETCS 프로젝트의 경우 ETCS 레벨 1에서 선로상의 발리스에 의한 지상-차상간 통신링크는 폐쇄형 전송시스템으로 분류하여 IEC 62280-1을 적용하고, 레벨 2부터의 지상-차상간간 통신을 무선통신을 이용함으로 인해 개방형시스템으로 분류하여 보다 높은 안전성과 보완성이 요구되는 IEC 62280-2 규격을 적용하고 있다.

표 1. 폐쇄형 및 개방형 전송시스템 정의

폐쇄형 전송시스템	개방형 전송시스템
· 잘 알려지고 정해진 특성을 지니며, 권한이 부여되지 않은 접속에 대한 위험이 미비한 전송시스템으로, 연결된 장치의 수가 고정되거나 고정된 최대 수를 가짐	· 알 수 없는 원격통신 임무에 사용되는, 알려지지 않은, 변수와 신뢰할 수 없는 성질을 갖는, 알 수 없는 수의 참가자와의 전송 시스템으로, 여기서는 권한이 없는 접근이 접근될 수 있는 위험이 있음

2.1 폐쇄형 전송시스템

IEC 62280-1의 폐쇄형 전송시스템의 구조와 메시지 표현모델은 각각 그림 1과 그림 2와 같다. 이들 그림과 같이 이 규격은 별도로 표시한 부분인 "안전관련 전송기능 부분"에 한정되는 것으로, "안전절차(Safety Procedure)"와 "안전코드

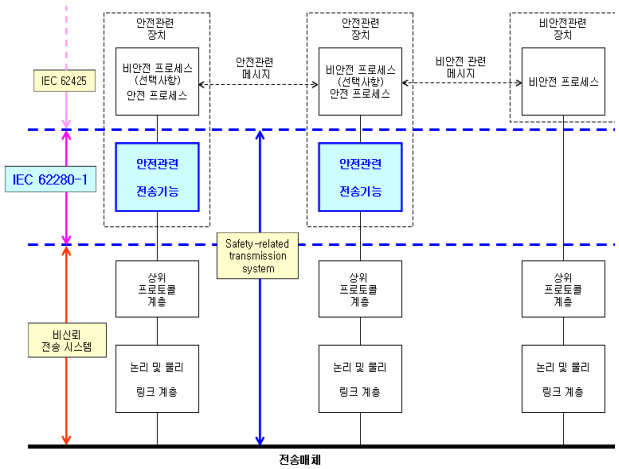


그림 1. IEC 62280-1의 전송시스템 구조

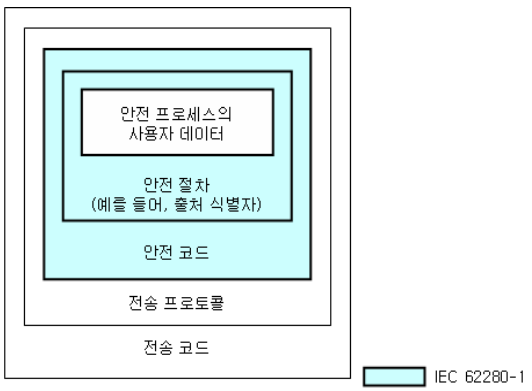


그림 2. IEC 62280-1의 메시지 표현모델

(Safety Code)"를 그 범위로 하고 있다. 따라서 전송계층 프로토콜과 응용측면에서의 전송코드(OP code 등으로 표현되는 전송데이터)는 본 규격의 범위 밖이다.

폐쇄형 전송시스템의 수신기 관점에서 오류가 포함된 정보(송신기 식별자 오류, 형태 오류, 값 오류)나 시간오류(지나치게 오래 지연된 데이터, 순서상의 오류)를 피하기 위해 수신기에 구현된 안전처리과정에서 사용하기 이전에 이러한 오류들이 검출되어야 한다. 이를 위해 다음과 같은 방법들이 폐쇄형 전송시스템에 제공되도록 요구하고 있다.

- 송신기 식별자 오류의 검출
- 데이터 형태 오류의 검출
- 데이터값 오류의 검출
- 기한이 지난 데이터 및 정해진 시간 내에 수신되지 못한 데이터의 검출
- 사전에 정의된 지연으로 인한 통신두절의 검출
- 안전관련 전송기능과 비신뢰 전송시스템에서 사용된 계층간의 기능적 독립성 보장

이 규격에서 요구하는 안전절차 요구사항은 안전관련 설비들간, 안전관련 설비와 안전무관 설비들간, 안전무관 장비간의 통신으로 구분하여 제시되고 있다. 하지만 국내에서 표준화된 철도신호설비들간 표준프로토콜은 모두 안전설비들인 철도신호제어장치들 사이의 통신링크에 적용되는 것으로 본 논문에서는 이 부분만 설명하며, 비안전 설비와 안전관련 설비간 전송절차 등은 본 논문의 범위 밖으로 한다. 안전관련 설비간 통신에서는 데이터의 확실성, 무결성 및 정시성을 보장하도록 하고 있다.

그림 1에서와 같이 본 규격의 범위에 속하는 안전처리과정이 비신뢰 전송시스템의 내부기능을 접근할 수 없으므로, 안전처리과정은 결함이 검출되지 않은 채 넘어가지 못하도록 비신뢰 전송시스템에서 제공하는 기능 이외에 추가적인 검사작업을 수행하여야 한다. 다음은 표준 프로토콜의 적용대상인 안전관련 장치들간 통신링크를 위한 안전절차 요구사항을 나타낸 것이다.

① 전송시스템 내에서 데이터 출처가 식별되지 않으면, 사용자 데이터에 출처 식별자를 추가하여 확실성을 제공하여야 한다.
② 사용자 데이터에 안전코드를 첨부하여 무결성이 제공되어야 한다.
③ 사용자 데이터의 적시성은 사용자 데이터에 시간정보(예를 들어, 시간 날인, 순서 번호, …)를 추가하여 제공하여야 한다.
④ 메시지의 순서는 안전 프로세스에 의해 검사되어야 한다.
⑤ 안전관련 장치에 대한 안전절차는 비신뢰 전송 시스템에 의해 사용되는 절차와 기능적으로 독립적이어야 한다. 특히, 양 절차가 동일한 코딩기법을 사용하는 경우, 파라미터 (예를 들어, 다항식)가 상이하여야 한다.
⑥ 모든 안전 관련 장치는 위의 요구사항들의 성능을 감시하여야 하며, 전송품질이 사전 정의되어 있는 수준 이하로 떨어지면, 적절한 안전반응이 일어나야 한다.

전송되는 데이터는 비신뢰 전송 하드웨어의 고장이나 전송매체에 있어서 외부적인 영향(예를 들어 EMI 등)으로 인해 전송데이터에 에러가 발생할 수 있다. 이러한 전송도중의 에러를 검출하고 또한 필요 시 정정하기 위하여 전송되는 데이터에 추가되는 코드를 안전코드(Safety Code)라 하며, 이 안전코드의 요구사항은 다음과 같다.

- 요구되는 안전 무결성 수준을 충족시키기 위해서는, 비신뢰 전송 시스템에서 발생하는 결함 검출 및 대응이 필요
- 요구되는 안전 무결성 수준을 충족시키기 위해 전형적인 오류의 검출 및 대응이 요구되어짐
- 안전코드는 전송코드로부터 기능적으로 독립적이어야 함

이러한 폐쇄형 전송시스템의 요구사항을 분석해보면, 최종적으로 폐쇄형 전송시스템에서는 데이터 출처 식별자 적용, 안전코드의 사용, 데이터 시간정보의 추가가 가장 중요한 안전절차를 위한 요구사항으로 분석되어진다.

2.2 개방형 전송시스템

IEC 62280-2의 개방형 전송시스템의 구조는 그림 3과 같다. 이 그림에서와 같이 이 규격의 적용범위는 폐쇄형 전송시스템과 같이 전송오류에 대한 방어를 위한 "안전관련 전송 프로세스" 부분을 포함하여, 폐쇄형에는 없지만 개방형 전송시스템의 특성에 따라 승인되지 않은 접속에 대한 방어를 위한 "안전관련 접속 보호 프로세스"를 그 범위로 한다.

이 규격의 범위인 개방형 전송시스템의 경우 전송시스템에 대한 위협(Threat)으로부터 적절한 방어대책이 통신링크에 구현되어야 한다. 개방형 전송시스템에 대한 주요 위협들에는 다음과 같다.

- 반복(Repetition)
- 삭제(Deletion)
- 삽입(Insertion)
- 위장(Masquerade)
- 손상(Corruption)
- 지연(Delay)
- 순서 재배열(Resequence)

이러한 위협들은 폐쇄성 전송시스템과 비교 시 가장 큰 차이점은 개방형 전송시스템 고유의 특성으로 인해, 통신하고자 하는 송수신자 이외의 제3자에 의해 전송되는 데이터가 삭제, 반복, 손상 등의 에러가 발생하게 되는 위협들이다. 따라서 이러한 위협들로부터 위험도를 줄이거나 제거하기 위해서는 폐쇄형 전송시스템과는 달리 보안문제 등 다른 안전대책을 필요로 한다.

본 논문의 연구대상으로 하는 국내의 철도신호용 표준 통신 프로토콜 2개는 모두 폐쇄형 구조로 되어 있어, IEC 62280-2의 요구사항을 적용받지 않고 2절에서 언급한 IEC 62280-1의 요구사항을 적용받는다.

3. 철도신호용 표준 프로토콜

그림 4는 현재 통신프로토콜이 표준화되어 있는 철도신호시스템 통신링크를 표시한 그림으로, 그림 4에서 ①은 CTC와 역 신호기기실의 LDTS/EIS 와의 점대점 기반 통신링크이며, ②는 CTC와 SCADA 장치사이의 네트워크 기반 통신링크이다.

이들 두 링크에 대한 프로토콜은 각각 점대점 및 네트워크 기반으로 하여, 그림 5와 같은 데이터 전송프레임 구조를 가진다. 그림 5의 (a)는 점대점 기반의 전송 프레임 구조로서 프레임의 시작과 끝에 'STX'와 'ETX'의 필드를 가지며 전송 프레임의 길이와 CRC-16의 에러검지 코드를 가진다. (b)는 네트워크 기반의 전송프레임 구조로서, 기본적으로 각각 Ethernet, TCP, IP 프로토콜을 각각 하위 계층으로 가지는 응용계층의 구조를 가진다. 그리고 하위계층에서 이미 반영되어 있는 에러검지 코드나 순서번호 필드 등의 정보를 응용계층의 데이터 필드 부분에 추가적으로 삽입하여 프로토콜의 안전성을 향상시킨 것을 특징으로 한다. 이러한 표준 프로토콜의 신뢰성 측면에서의 성능은 전송프레임 에러확률 모델링을 통한 시뮬레이션 결과 기존에 철도현장에서 적용되어 오던 다른 프로토콜들보다 우수함이 확인 되었다[6][7].

4. 표준 프로토콜의 안전특성 분석

본 절에서는 표준 프로토콜의 안전특성 확인을 위해 앞에서와 같은 Deadlock이나 Livelock 상태가 없음을 확인하는 정형검증 방법과, 국제규격의 요구사항과 비교분석을 통한 정성적인 방법에 의한 안전특성을 확인하고자 한다.

국내에서는 철도신호설비들간 인터페이스를 위한 통신프로토콜이 표준으로 제정되었다. 국내 철도신호용 통신 프로토콜은 3절에서 설명한 바와 같이 설계 과정에서 전송프레임 에러확률 모델링을 통한 컴퓨터 시뮬레이션과 모의실험을 통

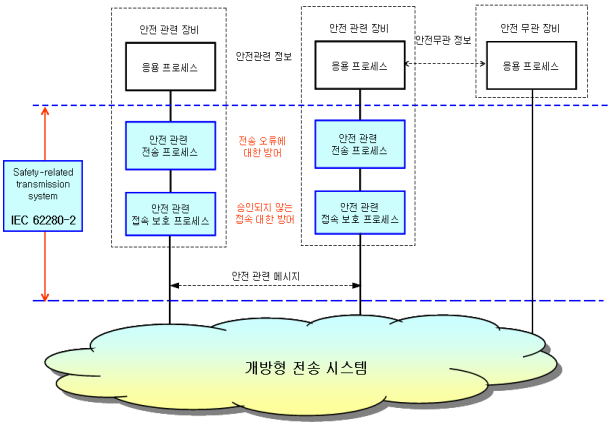


그림 3. IEC 62280-2의 전송시스템 구조

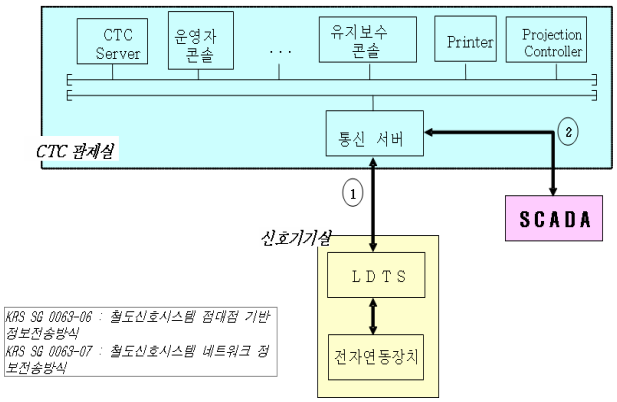
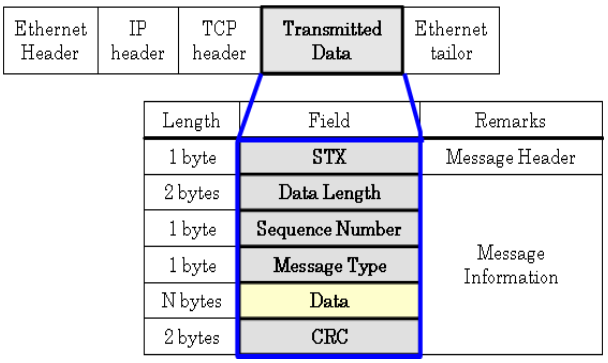


그림 4. 철도신호시스템 통신 프로토콜 표준화 현황

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

(a)점대점 기반 전송프레임 구조



(b) 네트워크 기반 전송프레임 구조

그림 5. 표준 프로토콜 전송프레임 구조

한 프로토콜의 신뢰성을 확인하였다. 철도신호용 프로토콜의 경우 다른 어떠한 프로토콜들보다 높은 안전성이 요구되어진

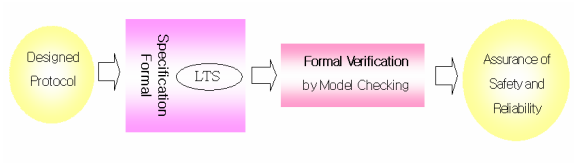


그림 6. 표준 프로토콜의 정형검증 과정

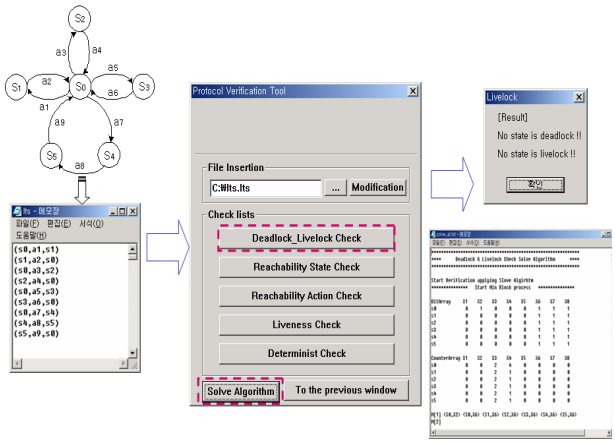


그림 7. 표준 프로토콜의 Deadlock 및 Livelock 검증

다. 이러한 안전성의 검증을 위해서는 정보통신분야에 적용되고 있는 모델체킹(Model Checking)을 통한 정형검증(Formal Verification) 방법과 철도전송시스템의 안전요구사항을 제시한 국제규격을 만족하는지 여부에 대해 분석하는 방법이 있을 수 있다. 본 논문에서는 프로토콜의 안전성 확인을 위한 이러한 국내의 표준 프로토콜에 대한 정형검증 결과를 간략하게 살펴보고, IEC 62280 국제규격에서 제시한 안전절차 요구사항과 표준 프로토콜과의 비교분석을 통한 안전특성을 확인한다.

자연어로 설계되어진 프로토콜 명세의 경우, 프로토콜 내부에 Deadlock이나 비정상 도달상태(Livelock)와 같은 잠재적인 설계에러들이 프로토콜 설계자가 인지 못하면서 포함되어 있을 수 있다. 이러한 잠재적인 설계에러들은 프로토콜의 실제 동작에 있어서 시스템의 치명적인 사고로 유발할 수 있는 등 잠재적인 위험원들이다. 따라서 이러한 인지 못하는 잠재적인 위험원들이 설계과정에서 또는 적용과정에서 확인되고 제거되어져야 한다. 이를 위한 방법으로 가장 확실하면서 우수한 성능을 지닌 방법이 정형검증 기법이다.

설계한 프로토콜이 적절한 통신을 하기 위해서는 프로토콜이 Deadlock 상태나 Liovelock 상태 등과 같은 잠재적인 설계에러가 없는지 확인을 위한 모델체킹 방법을 통한 정형검증 방법이 일반적으로 적용되어진다[4][5]. 정형검증기법을 적용한 프로토콜 검증은 프로토콜 명세의 정확성, 안전성과 필연성을 검증하는 것으로 모델체킹에서 보다 구체적으로 검정해야 할 프로토콜의 특성은 안전성(Safety)이며 이 두 특성을 이루는 구성요소는 다음과 같이 네 가지가 있다.

- Deadlock : 한 상태에서 다른 어떤 상태로의 천이가 존재하지 않기 때문에 다음 행위를 할 수 없는 경우. 즉, 그 상태에서 나가는 천이가 존재하지 않는다.
- Livelock : 프로토콜 상태들의 부분집합 내에서 그 상태들만을 무한히 반복적으로 천이하는 경우로써 그 부분집합 이외의 다른 상태로의 천이가 존재하지 않는다.

통신 프로토콜의 안전특성은 Deadlock이나 Livelock과 같이 절대로 발생되어서는 안되는 상태나 행위를 프로토콜에서 배제하는 특성을 나타는 것이고, 국내 철도신호용 표준 프로토콜도 정형검증을 통해 표준 프로토콜의 안전특성이 검증되었다[8].

다음 그림은 철도신호용 표준 프로토콜을 정형검증방법을 통해 검증하는 절차를 나타낸 것으로, 자연어로 명세화된 표준 프로토콜을 정형명세 언어(Formal Specification Language) 중의 하나인 LTS(Label Transition System)로 모델링하고 이를 모델체킹 기법을 통해 Deadlock이나 Livelock 등을 검증하는 과정을 나타내고 있으며, 이에 대한 보다 자세한 과정은 [8]에 설명되어져 있다.

그림 7은 툴에 의해 설계한 표준 프로토콜의 정형검증을 하는 과정을 나타낸 것으로, 설계한 프로토콜에는 Deadlock과 Livelock 상태가 없음을 확인하였고, 이에 따라 설계한 프로토콜은 기본적으로 기능상의 안전성은 확보한 것으로 평가할 수 있다.

점대점 링크기반의 표준인 6330-3348은 CTC와 LDTS/EIS 사이의 통신 프로토콜로서, 두 장치 모두 바이탈한 철도신호 제어장치이며 또한 전송시스템에 연결된 장치들이 알려져 있으며, 접속권한이 없는 다른 접속으로부터의 위협이 거의 없는 폐쇄형 전송시스템 특성을 가지고 있다. 네트워크 기반의 표준인 6330-3349는 CTC와 SCADA 사이의 통신 프로토콜로서 SCADA 설비가 신호시스템은 아니지만 전송시스템에 연결된 장치들이 알려져 있으며, 시스템 운용도중에 장치들이 추가되거나 삭제될 가능성이 적고 또한 접속권한이 없는 다른 접속으로부터의 위협이 적은 폐쇄형 전송시스템의 특성을 가지고 있다. 따라서 현재 국내에 제정 및 운용 중인 표준 프로토콜은 모두 IEC 62280-1 규격의 안전요구사항의 적용이 적절하다.

본 논문 2장에서 폐쇄형 전송시스템의 안전설비들간 통신 링크를 위한 안전절차 요구사항의 분석결과 데이터 출처 식

표 2. 표준 프로토콜과 규격의 비교분석

IEC 62280 안전절차 요구사항	KRS SG0063-06	KRS SG0063-07
① 전송시스템 내에서 데이터 출처가 식별되지 않으면, 사용자 데이터에 출처 식별자를 추가하여 확실성을 제공	- 점대점 통신기반으로 데이터 출처의 식별이 기본적으로 가능	- 전송 데이터 패킷의 “IP Header”에 송신자 주소를 나타내는 필드가 있음
② 사용자 데이터에 안전코드를 첨부하여 무결성이 제공	- “CRC-16” 코드를 전송메시지 프레임에 안전코드로 추가	- 전송메시지 프레임이 “CRC-16” 코드 추가
③ 사용자 데이터의 적시성은 사용자 데이터에 시간정보 를 추가하여 제공	- 상태정보를 주기적으로 전송하도록 하고 있고, 필요시 폴링메시지를 사용하여 필요시 상태정보를 업데이트 하고 있음 - 마스터클럭 메시지 추가하여 송수신장치의 시간을 동기화시킴 ☞ 메시지별 시간정보는 없으나 위의 두 가지를 통해 유사한 효과가 가능	- 상태정보를 주기적으로 전송하도록 하고 있고, 필요 시 폴링메시지를 사용하여 필요시 상태정보를 업데이트 하고 있음 ☞ 메시지별 시간정보는 없으며 위의 절차를 통해 시간정보를 제공함
④ 메시지의 순서는 안전 프로세스에 의해 검사	- 수신측에서 다음의 경우 송신측으로 ‘NAK’ 메시지 전송 · 안전코드에 의한 에러 검출 시 · 시컨스 번호 오류 시 · 타임아웃 발생 시	〃
⑤ 안전 관련 장치에 대한 안전절차는 비신뢰 전송 시스템에 의해 사용되는 절차와 기능적으로 독립적이어야 함. 특히, 양 절차가 동일한 코딩기법을 사용하는 경우, 파라미터 (예를 들어, 다항식)가 상이하여야 함	- 데이터링크 계층 프로토콜로서, 물리계층과 구별됨	- 데이터 필드 부분에 CRC-16, Ethernet 헤더에 CRC-32, IP 헤더에 Checksum의 안전코드를 달리 적용 - 각 계층별(MAC, IP, TCP, 데이터 필드) 별도의 절차를 가짐
⑥ 모든 안전 관련 장치는 위의 요구사항들의 성능을 감시하여야 하며, 전송품질이 사전 정의되어 있는 수준 이하로 떨어지면, 적절한 안전반응 절차를 가져야 함	- ④의 요구사항에 대한 안전대책에 의한 것처럼 전송메시지 오류 시 재전송 프로세스를 가짐 - 동일 메시지 3회 이상 전송 시 ‘Alarm’ 처리하도록 함	〃

별자 및 안전코드의 사용, 데이터 시간정보와 메시지 순서 확인, 전송품질이 일정 수준 이하일 경우 적절한 안전반응 수행 등 몇 가지로 요약된다. 이러한 요구사항들에 대해 국내 표준 프로토콜들이 어떻게 명세화되어 있는지에 대해 분석함으로써, 표준 프로토콜의 안전특성을 분석하고자 한다.

IEC 62280-1 규격의 폐쇄형 전송시스템의 안전절차 요구사항의 각 항목별로 국내의 표준 프로토콜에서 어떤 내용으로 반영되어 있는지 여부를 비교 및 확인하였다. IEC 62280-1의 안전절차 요구사항에서는 표 2와 같이 6개의 요구사항을 제시하고 있으며, 이 안전절차 요구사항과 더불어 안전코드의 사용도 제시하고 있다. 이 6개의 안전절차 요구사항은 안전관련 설비간 통신에서 데이터의 확실성, 무결성 및 정시성을 보장하도록 하고 있다. 통신에 있어서 안전처리과정이 본 규격에서 언급하는 바와 같이 비신뢰 전송 계층의 내부기능을 접근할 수 없으므로, 안전처리과정은 결함이 검출되지 않은 채 넘어가지 못하도록 비신뢰 전송시스템에서 제공하는 기능 이외에 표 3에서 제시하는 추가적인 안전절차들이 수행하여야 한다. 다음은 국제 규격에서 제시하는 안전절차 요구사항과 국내 표준 프로토콜의 비교분석 결과를 나타낸 것이다. 이 표에서 보는 바와 같이 국제규격에서 요구하는 각 항목별로 각각 국내 표준규격에 이미 안전요구사항들이 반영되어서 설계 및 표준화 되어 있음을 확인할 수 있다.

5. 결 론

국내신호설비들 상호간 정보전송을 위한 프로토콜들이 표준화 되어 있지 않아서 시스템의 유지보수 및 안정적인 동작에 어려움이 있어, 최근 들어 철도신호용 통신 프로토콜이 설계되어 현재 국가 표준으로 채택되어 있으며, 이 표준프로토콜에 이제 철도현장에 막 적용하려는 단계에 있다. 철도신호설비간 정보전송을 위한 통신링크는 매우 바이탈한 정보들이 전송되어지므로, 실제 철도현장에 적용되기 전에 표준 통신프로토콜의 신뢰성뿐만 아니라 안전특성 확인이 매우 중요하다. 본 논문에서는 최근 국내에서 설계 및 표준화된 철도신호용 통신프로토콜의 안전특성을 분석하였다. 이를 위해 우선적으로 해당 프로토콜의 설계과정에서 진행된 정형검증 결과

를 확인하였으며, 이와 더불어 철도통신시스템의 안전성관련 국제규격의 요구사항과 국내의 표준 프로토콜을 비교분석하였다. 즉, 프로토콜 내부적으로 안전성에 영향을 미칠 수 있는 Deadlock이나 Livelock 같은 상태가 없음을 확인하는 정형검증 방법과 같은 해석적 방법과 국제규격의 요구사항과 비교분석을 하는 정성적인 방법의 두 가지 측면을 모두 고려하였다. 이러한 두 가지 측면의 분석결과 국내에 설계 및 표준화된 철도신호용 통신 프로토콜은 내부에 데드락이나 라이브락 상태를 가지고 있지 않으며, 또한 국제 규격의 요구사항을 만족함을 확인하였고 이에 따라 프로토콜이 안전성을 가지고 있는 것으로 평가할 수 있다.

참 고 문 헌

1. 'IEC 62280-1 : Safety-related communication in closed transmission systems', 2002.
2. 'IEC 62280-2 : Safety-related communication in open transmission systems', 2002.
3. D. Schwabe, "Formal Techniques for the Specification and Verification of Protocols", Report No. CSD-810401, UCLA, (PhD Thesis), April 1981.
4. R. Cleaveland, "Tableau-Based Model-checking in the Propositional Mu-calculus", Acta Informatica, vol.27, No.3, pp.725-727, 1990.
5. B. Sarikaya, "Principles of Protocol Engineering and Conformance Testing", Ellis Horwood, New York, NY, 1993.
6. 황종규, 이재호, "전자연동장치와 역정보전송장치간 인터페이스를 위한 데이터링크 프로토콜 성능해석", 한국철도학회논문지, 제6권 제 2호, pp.135-141, 2003.06.
7. 황종규, 조현정, 이재호, "열차제어시스템과 SCADA 장치간 네트워크 기반 데이터 전송 프로토콜의 성능분석", 대한전기학회 논문지, Vol. 55B, no. 9, pp.485-490, 2006. 9.
8. J. G. Hwang, H. J. Jo and J. H. Lee, "Development .of Communication Protocol Verification Tool for Vital Railway Signalling Systems", Journal of Electrical Engineering & Technology, vol. 1, no. 4, pp.513-519, Dec. 2006.

(2007년 4월 25일 논문접수, 2007년 6월 1일 심사완료)