IEC 62280을 통한 철도신호용 표준 통신프로토콜의 안전특성 분석

Safety Characteristics Analysis of Korean Std. Protocol for Railway Signalling according to IEC 62280

황종규* 조현정** 윤용기** 김용규**
Jong-Gyu Hwnag*, Hyun-Jeong Jo**, Yong-Ki Yoon**, Yong-Gyu Kim**

ABSTRACT

The existing Europe Standard, EN 50159 with respect of safety of railway signalling communication protocol has been changed into International Standard, IEC 62280. This Standard presents the requirement for safe communication between safety-related devices which connects with transmission system, there are both closed and open transmission system. Regardless of this international Standards, the communication protocol for interface between CTC communication server and external facilities has been standardized several years ago in our country, so this is applied to integrated CTC system in KORAIL. Two Standards are currently standardized as a protocol between CTC and external facilities, these standard protocols are also required high level safety as a communication link which is transmitted vital control information in common with the train control system. For that reason, we have made analysis of requirement for the safe transmission required by international standard. Under this analysis, we have studied safety features of communication protocol applying to our standard. In other words, we have researched that how many the requirement from international standard for safe transmission is reflected in domestic standard protocol, and also whether our standard makes sure of safety enough or not.

---

1. 서론

철도시스템 통신 프로토콜의 안전성 관련하여 기존의 유럽규격이던 EN 50159-1/-2 규격이 IEC 62280-1/-2 로 국제규격화 되었다[1][2]. 이 국제규격은 전송시스템에 연결되어 있는 안전관련 장치들 간의 안전통신을 위한 요구사항을 제시하고 있으며, 폐쇄형과 개방형 전송시스템의 두 부분으로 나뉘어져 있다. 이러한 통신 안전성 요구사항은 철도신호시스템들에 적용되는 통신링크에 적용될 수 있다. 철도신호시스템은 다른 어느 시스템 보다 높은 안전성을 요구하고 있어, 이들 장치들 간 인터페이스를 위한 통신링크의 안전성 확보는 매우 중요하다.

이러한 국제규격과는 상관없이 국내에서는 몇 년전부터 CTC 통신서버와 다른 신호설비 또는 외부설비들간의 인터페이스를 위한 통신 프로토콜들이 표준으로 제정되어 철도공사의 통합 CTC 시스템에 적용되고 있다.

---

* 한국철도기술연구원 열차제어연구팀
E-mail : jghwang@krri.re.kr
TEL : (031)460-5438 FAX : (031)460-5449
** 한국철도기술연구원 열차제어연구팀

현재 철도신호설비들간 통신 프로토콜의 표준이 두개 제정되어 있으며[3][4], 이들 표준 프로토콜들 또한 열차제어시스템과 마찬가지로 바이탈 제어정보들이 전송되는 통신링크로서 매우 높은 안전성이 요구되고 있다. 이에 따라 본 연구에서는 국제규격에서 요구하고 있는 안전전송을 위한 요구사항을 분석하고, 이를 바탕으로 국내에 표준으로 제정되어 적용되고 있는 통신 프로토콜의 안전특성을 분석하였다. 즉, 안전전송을 위해 국제규격에서 제시하고 있는 요구사항들이 국내의 표준 프로토콜에 어느 정도 반영되고 있는지, 또한 국내의 표준이 충분한 안전성을 확보하고 있는지 여부 등을 분석하였다.

2. 안전전송 국제규격에 따른 요구사항 분석

철도시스템의 통신 안전성 관련 규격은 IEC 62280에 의해 정의되어 있으며, 다음과 같이 개방형(Open) 전송시스템과 폐쇄형(Closed) 전송시스템의 두 부분으로 구분되어져 있다. 본 장에서는 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

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 최대수를 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

개방형과 폐쇄형 전송시스템을 IEC 62280에서는 위의 표와 같이 정의하고 있다. 이러한 정의에 따르면, 국내의 철도신호용에 사용되는 대부분의 통신링크는 폐쇄형 전송시스템으로 IEC 62280-1의 요구사항을 적용할 수 있다. 하지만 최근 들어 통신기반 열차제어시스템(CBTC : Communication Based Train Control System)이 국내에서도 적용되고 있는 등 통신링크가 개방형으로 전송시스템도 적용이 되고 있다. 유럽의 ETCS 프로젝트의 경우 레벨 1에서 사용되는 발리스에 의한 지상-차상간 통신링크는 IEC 62280-1을 적용하고, 레벨 2부터의 무선통신에 의한 통신링크는 IEC 62280-2 규격을 적용하고 있다.

2.1 폐쇄형 전송시스템

IEC 62280-1의 폐쇄형 전송시스템의 구조는 그림 1과 같으며 메시지 표현 모델은 그림 2와 같다. 이 그림과 같이 이 규격의 적용범위는 안전관련 전송기능 부분에 한정되는 것으로, “안전절차(Safety Procedure)”와 “안전코드(Safety Code)”를 그 범위로 한다. 따라서 전송 프로토콜과 코드는 규격의 범위 밖으로 그림1에서와 같이 비신뢰 전송계층을 분류된다.

이 규격에서 요구하는 안전절차 요구사항은 안전관련 설비간, 안전관련 설비와 안전무관 설비간, 안전무관 장비간의 통신으로 구분하여 제시되고 있다. 하지만 국내에서 표준화되어 적용되고 있는 철도신호설비들간 표준프로토콜은 모두 안전설비들로 안전관련 설비들간 통신링크로 본 논문에서는 이 부분만 설명한다.

- 전송시스템 내에서 데이터 출처가 식별되지 않으면, 사용자 데이터에 출처 식별자를 추가하여 확실성을 제공하여야 한다.

- 사용자 데이터에 안전코드를 첨부하여 무결성이 제공되어야 한다.
- 사용자 데이터의 적시성은 사용자 데이터에 시간정보 (예를 들어, 시간 날인, 순서 번호, …)를 추가하여 제공하여야 한다.
- 메시지의 순서는 안전 프로세스에 의해 검사되어야 한다.
- 안전 관련 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.
- 모든 안전 관련 장치는 위의 요구사항들의 성능을 감시하여야 하며, 전송품질이 사전 정의되어 있는 수준 이하로 떨어지면, 적절한 안전반응이 일어나야 한다.

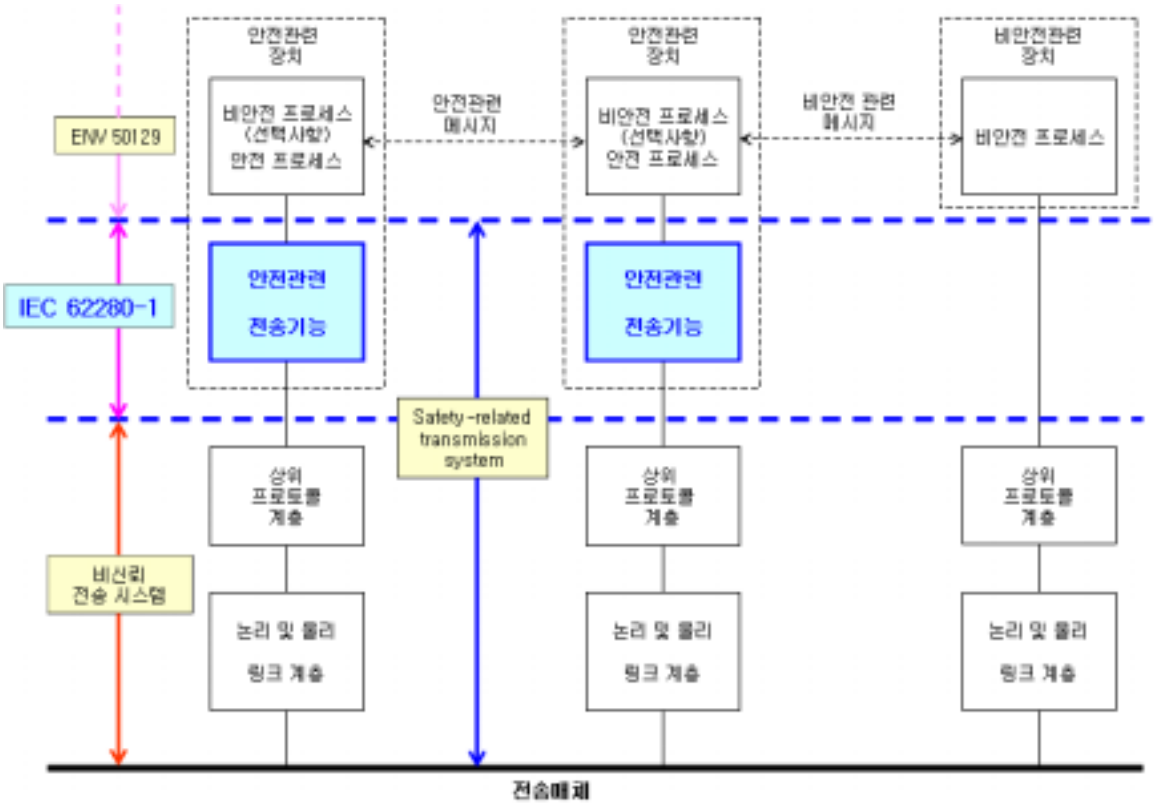

그림 1 IEC 62280-1의 전송시스템 구조

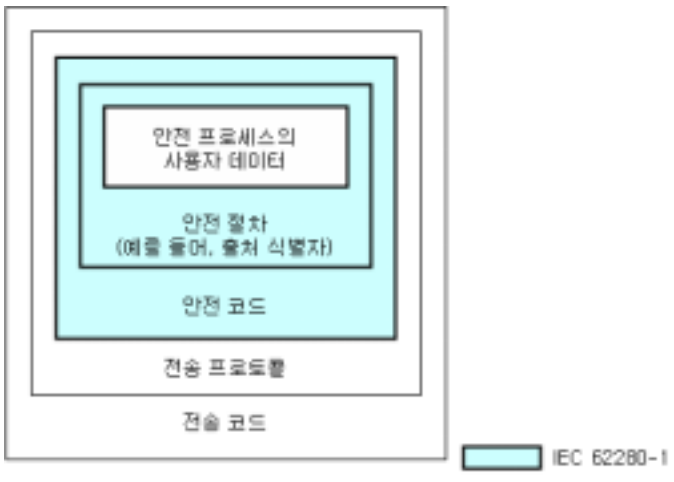

그림 2 IEC 62280-1의 메시지 표현모델

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 필요시 정정하기 위하여 전송되는 데이터에 첨가되는 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 안전 요구사항으로 정리되어진다.

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.

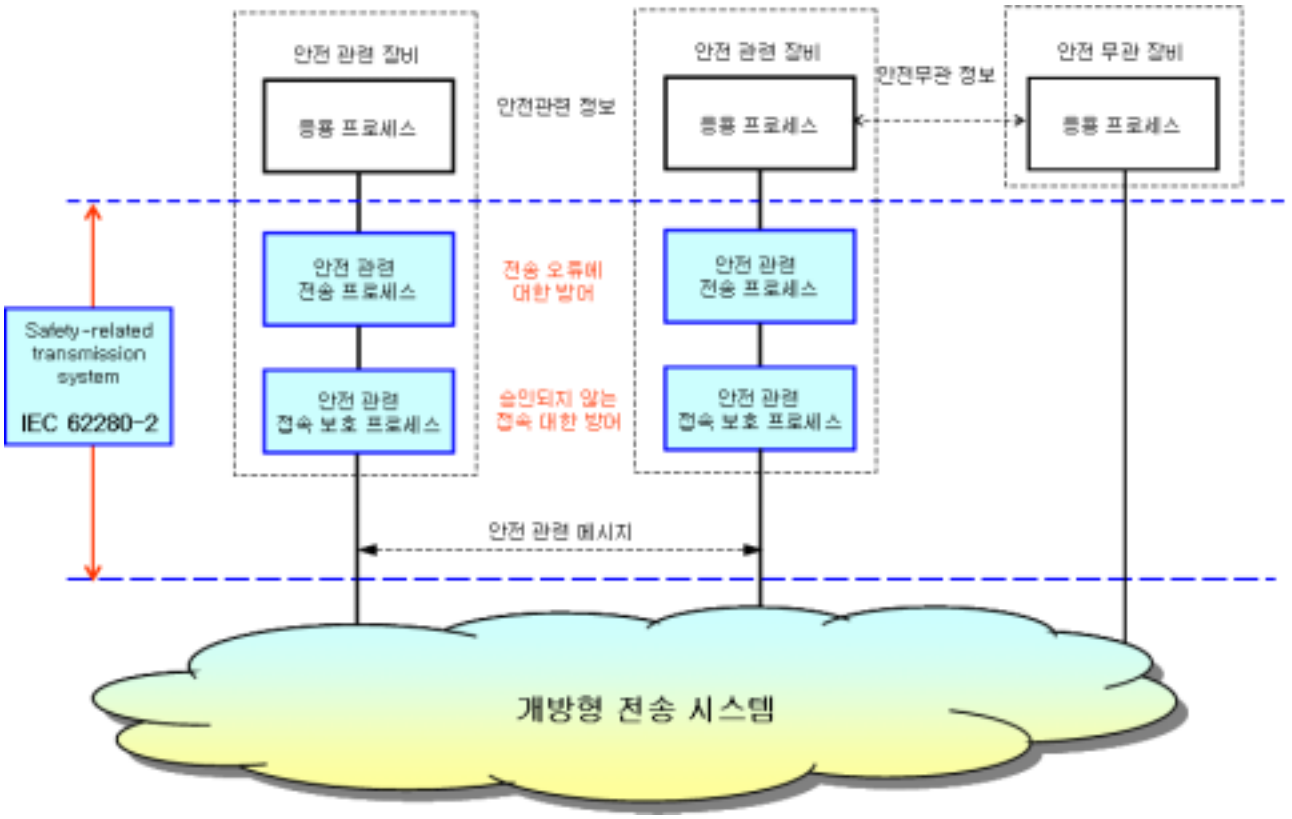

그림 3 IEC 62280-1의 전송시스템 구조

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

- 반복(Repetition)
- 삽입(Insertion)
- 손상(Corruption)
- 삭제(Deletion)
- 순서 재배열(Resequence)
- 자연(Delay)

- 위장(Masquerade)

이러한 위협들은 폐쇄성 전송시스템과 비교 시 가장 큰 차이점은 개방형 시스템 고유의 특성으로 인해, 통신하고자 하는 송수신자 이외의 제 3자에 의해 전송되는 데이터가 삭제, 반복, 손상 등의 에러가 발생하게되는 위협들이다. 따라서 이러한 위협들로부터 위험도를 줄이거나 제거하기 위해서는 폐쇄형 전송시스템과는 달리 보안문제 등 다른 안전대책을 필요로 한다. 규격에서는 위협들로부터 위험도를 줄이거나 제거하기 위한 전송시스템에 대한 안전대책으로 다음과 같은 방법들을 제시하고 있다.

- 순서번호(Sequence Number)
- 시간날인(Time Stamp)
- 타임아웃(Time-out)
- 출처와 도착지 식별자(Source & Destination Identifiers)
- 피드백 메시지(Feedback Message)
- 식별절차(Identification Procedure)
- 안전코드(Safety Code)
- 암호화 기법(Cryptographic Technique)

표 2는 개방형 전송시스템에 대한 위협과 해당되는 위협의 위험도를 제거 또는 저감시키기 위한 방어대책을 나타낸 표로서, IEC 62280-2 규격에서는 이들 표를 바탕으로 방어대책을 복수개를 사용하여 전송시스템의 위협으로부터 안전을 확보하도록 요구하고 있다.

표 2 개방형 전송시스템의 위협 및 방어대책

위협 (Threat)	방어 (Defences)							
	순서 번호	시간 날인	타임아웃	출처 & 도착지 식별자	귀환 메시지	식별 절차	안전 코드	암호화 기법
반복	X	X						
삭제	X							
삽입	X			X	X	X		
순서 재배열	X	X						
손상							X	X
지연		X	X					
위장					X	X		X

3. 표준 프로토콜과 규격의 비교분석

국내에서는 철도신호설비들간 인터페이스를 위한 통신프로토콜이 표준으로 제정되어 현재 운용되고 있다. 본 연구에서는 이러한 국내에서 제정 및 운용되고 있는 표준 프로토콜이 IEC 62280 국제 규격에서 요구하는 안전성 요구사항에 부합하는지에 대한 분석을 하였으며, 이를 통해 국내 표준 프로토콜의 안전 특성을 확인하고자 한다.

철도신호설비들간 통신 프로토콜의 표준이 현재 다음과 같은 2개 제정되어 운용되고 있다.

- 철도 6330-3348 : 철도신호시스템 점대점 정보전송방식
- 철도 6330-3349 : 철도신호시스템 네트워크 정보전송방식

점대점 링크기반의 표준인 6330-3348은 CTC와 LDTS/EIS 사이의 통신 프로토콜로서, 두 장치 모두

바이탈한 철도신호설비들이며 또한 표1의 정의에서와 같이 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 적용이 가능하다. 하지만 현재 진행 중인 철도공사 분당선의 지능형 열차제어시스템 구축사업의 경우 지상과 차상간의 인터페이스가 무선랜 기반으로 하고 있어 제 3자에 의한 통신링크의 간섭 및 훼손의 가능성이 있다. 이러한 경우에는 개방형 전송시스템으로 IEC 62280-2 규격이 적용되어야 한다. 이 지능형 열차제어시스템의 지상-차상간의 통신 프로토콜은 아직 표준화되지 않고 있어, 본 연구에서는 제외하였다.

본 논문 2장에서 폐쇄형 전송시스템의 안전 요구사항을 정리해보면 데이터 출처 식별자 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 명세되어 있는지에 대해 분석함으로써, 표준 프로토콜의 안전특성을 분석하고자 한다. IEC 62280의 안전요구사항을 표준 프로토콜이 모두 만족하면 안전특성을 가지고 있다고 말할 수 있을 것이다. 본 연구에서는 표3과 같이 IEC 62280의 안전요구항에 따른 국내 표준 프로토콜의 안전특성을 분석하였다. 이 표에서와 같이 국내의 철도신호용 표준 프로토콜은 IEC 62280의 안전요구사항에 대부분 부합하는 것으로 분석되었다.

표 3 표준 프로토콜과 규격의 비교분석

IEC 62280 안전 요구사항	철도 6330-3348	철도 6330-3349
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 시간정보를 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 두가지를 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 시	- 데이터링크 계층 프로토콜로서, 물리계층과 구별됨	- 데이터 필드 부분에 CRC-16, Ethernet 헤더에 CRC-32, IP 헤더

스템에 의해 사용되는 절차와 기능적으로 독립적이어야 함. 특히, 양 절차가 동일한 코딩기법을 사용하는 경우, 파라미터 (예를 들어, 다항식)가 상이하여야 함		에 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	〃

4. 참고문헌

[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] '철도 6330-3348 : 철도신호시스템 점대점 정보전송 방식', 철도용품 표준규격, 2005.
[4] '철도 6330-3349 : 철도신호시스템 네트워크 정보전송 방식', 철도용품 표준규격, 2005.