Safety characteristics analysis of Korean standard communication protocol for railway signalling

J.-G. Hwang & H.-J. Jo
Train Control Research Team, Korea Railroad Research Institute (KRRI), Korea

Abstract

The safety requirements for communication in the railway system were recently standardized as IEC 62280. The railway signalling system requires higher safety levels than any other system and it is very important to establish a safety communication link for an interface among safety equipment such as between the CTC communication server and field equipment, LDTS, or electronic interlocking system or among SCADA. The communication protocol for an interface among railway signalling systems was designed and established as a national standard in Korea a few years ago. So the communication link for information transmission among the railway signalling system can be a good example of the application of this standard. The communication protocol which is standardized among Korean railway signalling is considered to apply information transmission. We also confirmed there is no state of deadlock or livelock in the standard protocol to which is applied formal verification which is one of the analytic methods for inspection of safety characteristics in the design course of protocol. But the safety of the protocol has to necessarily accomplish this normal analysis approach by satisfying requirement matters with such an analytic approach. In this paper we analyzed the safety characteristics of the standard protocol for Korean Railway signalling compared the requirements for safety of the railway transmission system required by the international standard. Through this study, we confirm whether it satisfies the safety requirement to the level required in the international standard and tried to confirm whether the standard protocol has enough safety characteristics in the real railway field.

Keywords: IEC 62280, Safety of railway communication protocol, formal verification, closed transmission communication system.

WIT Transactions on The Built Environment, Vol 96, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/UT070571

1 Introduction

The standards and guides related to the railway system's safety are based on European standards. Among these, the part of safety related to communication of railway system is standardized as EN50159, Europe standardization, by CENELEC and was recently standardized as IEC 62280 [1, 2]. In this standardization, the requirement for the communication among safety related equipment connected to railway system is presented. It separates each safety transmission system into close and open types. Railway signalling systems require higher safety standards than any other system and it is very important to establish safe communication link interfaces among safety equipment such as between CTC communication server and field equipment, LDTS, or electronic interlocking system or among SCADA.

Regardless of an International Standard safety requirement related to communication in railway systems, a communication protocol for interface among railway signalling systems was designed and established as a national standard in Korean few years ago [3, 4]. 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. Through simulation for reliability estimation, which the protocol has, or by testing at laboratory level, there were efforts to inspect the protocol efficiency [5, 7]. We confirmed there is no situation of deadlock or livelock in the standard protocol; to which formal verification is applied, which is one of the analytic approaches for inspection of safety characteristics in the design course of protocol. However, the safety of protocol has to necessarily accomplish this normal analysis course, satisfying requirement matters with this analytic method.

In this paper, we analyzed the safety characteristics of standard protocol for Korean Railway signalling using the safety requirement for transmission system required in international standard. Standard protocol for railway signalling is about to apply in real railway field after establishment as the national standard. Through this study, we confirm whether it satisfies safety requirements to the level required in the international standard and tried to confirm whether standard protocol has enough safety character in the real railway field. In Section 2, we briefly analyze the safety requirement of international standard; in Section 3, we outline Korean standard protocol; in Section 4, analytic approaches and the result of standard protocol are given; and finally the conclusions are presented in Section 5.

2 Requirement analysis according to International standard safety requirements

Safety requirements of transmission systems in railway systems are specified in IEC 62280 and this standard is divided into open transmission systems and closed transmission system. In this section, we analyze the communication safety requirement set by international standard.

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

We define the difference between open and close systems in Table 1, as set out in IEC62280. Railway signalling is classified as a very important system in the train control's safety operation, and it doesn't do interface with external network and besides network for railway signalling. It is prohibiting the access to network for railway signalling from external network as having safety equipment like firewall although it does interface with external network. Therefore, most signalling links which are used in railway signalling an apply IEC 62280-1's requirement as the closed transmission system.

Table 1: Definition of closed and open transmission system.

Closed Transmission System	Open Transmission System
A fixed number or fixed maximum number of participants' links by a transmission system with well-known and fixed properties, and where the risk of unauthorized access is negligible.	A transmission system with an unknown number of participants, having unknown, variable and non-trusted properties, used for known tele-communication services, and for which the risk of unauthorized access shall be assessed.

But like CBTC (Communication Based Train Control) the system is also applied to the Korean metro line and there is exterior access possibility that ground vehicle communication link is by opened RF. Due to the introduction of open transmission system, IEC 62280-2 requirement has to be considered together. In case of ETCS project in Europe, ETCS level 1 is classified and apply IEC 62280-1. It applies IEC 62280-2 standard, which higher safety and complementary nature is required, classifying into opened type system by using communication between ground and vehicle communication from level 2.

2.1 Closed transmission system

The structure of a closed transmission system and message expression model is shown in Figs 1 and 2. In general, safety-related and non-safety-related equipment may be connected to a transmission system, which from a safety point of view is non-trusted. Figure 2 shows the model of message representation on the transmission media of closed transmission system. As shown, no safety requirements are placed upon the non-trusted transmission system. Safety aspects are covered by applying safety procedures and safety codes that are running inside safety-related equipment.

Shown in Figs 1 and 2, this standard is limited to safety related transmission function part indicated separately and contains procedure and safety code. So transmission class protocol and transmission code in the side of application transmission data. It is beyond the limits of a closed transmission system. In the receiver's view of a closed transmission system, these errors have to be detected to avoid information in which errors are continued, the error of receiver, type error, value error or time error (data which is delayed too long), the error of order before it is used in safety procedure's course. Closed transmission systems therefore have to include:

- Detection of transmitter identifier error
- Detection of data type error
- Detection of data value error
- Detection of outdated data of data not received in due time
- Detection the loss of communication after a predefined delay
- Ensure the functional independence of the safety-related transmission function and the used layers of the non-trusted transmission system

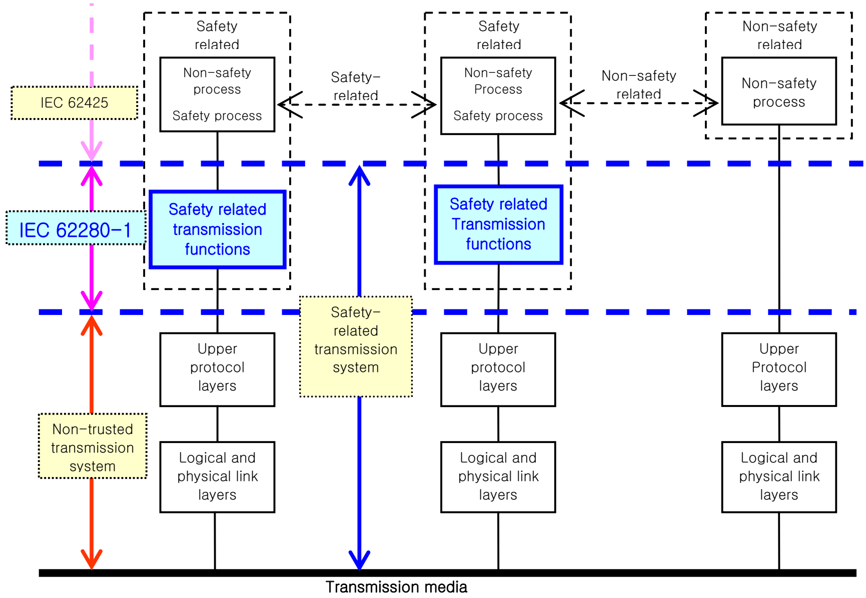


Figure 1: Structure of safety-related system using a non trusted transmission system.

The safety procedure requirements, which are required in this standard, are represented by dividing communication into safety related equipment and non-safety related equipment. However, in Korea the communication protocol for railway signalling is standardized for communication links among safety related equipment only. Therefore, in this paper, we explain only this part, and unsafe equipment and transmission procedures among safety related equipments, etc. is beyond the limit of this paper. We do to assure the authenticity, integrity, and punctuality of data in the communication among the safety related equipments. As shown in Fig. 1, safety procedures outside the limit of this standard cannot access internal functions of unreliable transmission systems; safety management procedures have to do additional inspection work to ensure that the unreliable transmission system does not pass on undetected errors. The safety procedures for communication links between safety equipment, as set out in the protocol, are represented below.

- If the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source identifier to the user data.
- Integrity has to be provided by adding safety codes to the user data.
- The timeliness of user data has to be provided by adding time information to the user data.
- If necessary, the sequences of messages have to be checked by safety process.
- The safety procedures for the safety-related equipment have to be functionally independent of the procedures used by the non-trusted transmission system.

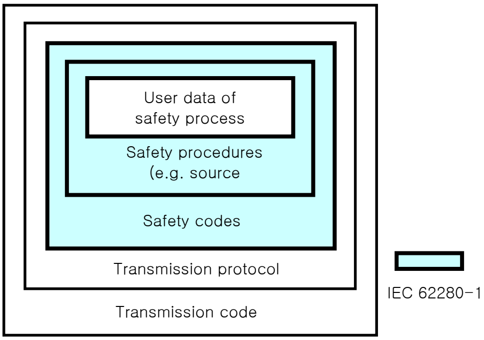


Figure 2: Model of message representation on the transmission media.

Safety codes are necessary to guard against data errors, unreliable data transmission and failure of transmission hardware. They detect errors during transmission and correct when needed. The requirement of safety code is as follows.

- To satisfy the required safety integrity level, it is necessary to detect and act on typical faults of the unreliable transmission system.
- To satisfy the required safety integrity level, it is necessary to detect and act on typical errors.
- The safety code has to be functionally independent from the transmission code.

In the closed transmission system, final application data origin discriminator using safety code, addition time information of data analyzed requirement for the most important safety procedure.

2.2 Open transmission system

The application range of IEC 62280-2 for opened transmission system contains safety related transmission processes for protection against transmission errors as in closed transmission system. It defines a range of safety related access protection processes for protection against unaccepted access in an open transmission system that doesn't exist in close type. In the case of open transmission systems, proper protection measures against unauthorized transmissions have to be embedded in the communication link. This threat is the biggest difference between closed and open transmission systems. The unique characteristics of open transmission systems are the threats of errors transmitted by third parties, deletion, repetition, corruption, etc. Therefore, to decrease and remove the degree of danger, other safety measures are needed. This standard suggests safety measures to decrease and delete the risk as follows.

Table 2: Threats/defences matrix.

Threat	Defenses							
	Sequence number	Time stamp	Timeout	Source & destination identifiers	Feedback message	Identification procedure	Safety code	Cryptographic technique
Repetition	X	X						
Deletion	X							
Insertion	X			X	X	X		
Resequence	X	X						
Corruption							X	X
Delay		X	X					
Masquerade					X	X		X

Table 2 represents the threats surrounding open transmission systems and defence measures to delete or decrease the risk of the equivalent threat. IEC 62280-2 standard based on this table requires establishing safety from threat of transmission system using multiple defence measures.

3 Standard protocol for railway signalling

Figure 3 represents the railway signalling system communication link with two standard codes in Korea. The CTC communication server located in the centralized control centre receives the control commands from CTC main computer for the control of field signalling equipment such as signal aspects, point machines, and others. Conversely, the LDTS and EIS transfers state information of the field signalling equipment CTC computer. If this link contains any faults or errors, they may lead to a severe accident because the interface link is the essential hub-link for controlling and monitoring railway signalling, so the interface link is a significant link from the point of view of the safety of the railway signalling operation. SCADA system has a role for control and monitoring of railway power systems such as catenaries system, railway power stations, etc. Very important information has to be exchanged between CTC communication server and SCADA systems. The importance of protocol for railway signalling systems was increased by the increase in the exchange of information among computerized signalling systems.

In Figure 3, ① link is a point to point based communication link with CTC and LDTS/EIS of signaling room located in a station or trackside area. The ② link is a network-based communication link between CTC and SCADA equipments. The protocols about these two links are based on each point-to-point, and network based one. The standard code 'KRS SG 0063-06 has point-to-point based transmission frame, and it has 'STX' and 'ETX' data fields in the beginning and the end of transmission frame, the 'Data Length' and error detection code of 'CRC-16'. The standard code 'KRS SG 0063-07' has network-based transmission frame structure, and it has the structure of an application layer which has Ethernet, TCP, and IP protocol as each sub-layer. It is inserted in addition to error detection code 'CRC-16', 'STX', 'Sequence Number' fields in transmission frame with overlapping of sub-layer functions. Those additional data fields increase the safety of standard protocol. On the side of reliability, two protocols are superior to other protocol which is applied in existing Korea railway. It was assured by the simulated results through transmission error probability modeling.

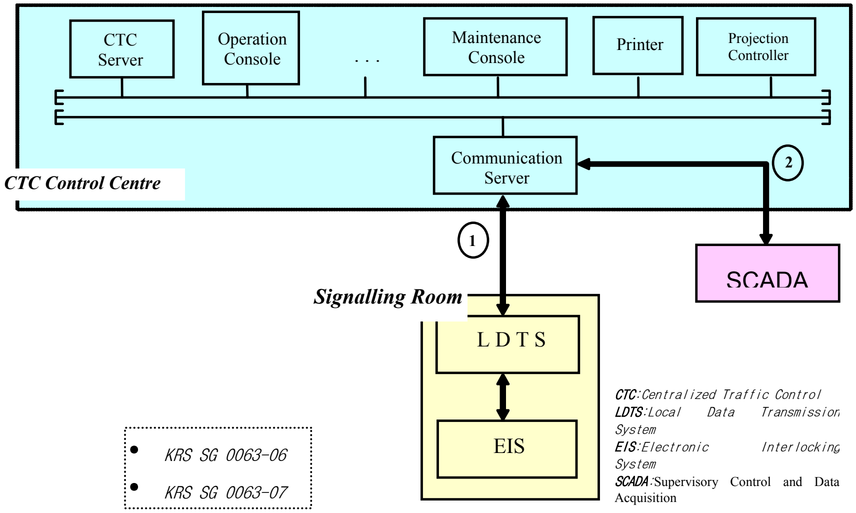


Figure 3: Configuration of standardization of Korean railway signalling.

4 Standard protocol's safety character analysis

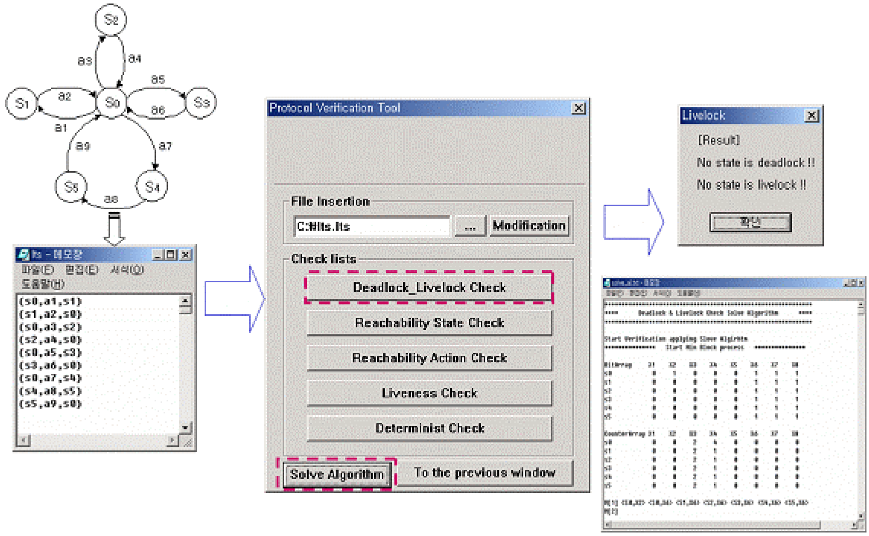
In Korea, communication protocol for interface among railway signalling systems was established as a national standard. We confirmed communication protocol for Korean railway signalling has the reliability through computer simulation and laboratory test with field signalling simulator. Communication protocol for railway signalling higher safety characteristics than any other field's protocol requires. For verification of safety characteristics, there is a formal verification method which is applied in information & communication field, and the analysis method about whether it satisfies IEC 62280 standard which safety requirement is explained in previous section. In this paper we briefly described the formal verification results in regard to two Korean standard protocols as a method for verification of safety characteristic [6], and confirm the safety characteristics through analysis between the requirement of safety procedure which is suggested in IEC 62280 standard and two Korean protocols.

For a communication protocol to properly communicate, the formal verification method is generally used to verify whether there is potential design error such as deadlock and/or abnormal reach states in designed protocol. The protocol has two properties that have a safety without deadlock and livelock, and liveness with some good state and action. A safety property states that some bad feature is always precluded. Safety can either be ascribed to states, that bad states can never be reached, or to actions, that bad actions never happen. A liveness property states that some good feature is eventually fulfilled. Again it can either be ascribed to states, that a good state is eventually reached, or to actions, that a good action eventually happens. Previous sectioned described two Korean standard protocol verified the safety property through formal verification. Figure 4 represents the course which does formal verification of two protocols by formal verification tool, and we confirmed there is no state of deadlock and livelock in two protocols. Therefore, we can analyze the designed protocol to ensure basic functional safety property.

In this section we try to confirm the safety property of two standard protocols. Safety property by formal verification method, which confirms deadlock and livelock as above, doesn't exist, and the normal approach through comparative analysis with the requirement of IEC 62280 standard.

As protocol 'KRS SG 0063-06', which is the standard of point-to-point link, is based on communication protocol between CTC and LDTS/EIS, both vital control equipment. This communication link has the characteristics of a closed transmission system in which there is no threat from unacceptable access. As protocol 'KRS SG 0063-07', which is the network-based standard is a communication protocol between CTC and SCADA. The SCADA equipment is not signalling equipment but the equipment connected to signalling system, this communication link has the characteristics of a closed transmission system, in which equipment added or deleted during system application is little and the threat from the other unacceptable access is low. So, two standard protocols are suitable to apply the IEC 62280-1 safety requirement.

The safety procedure requirement of closed transmission system by IEC 62280-1 is able to be summarized as follows: communication link data source identifier, usage of safety code, time stamp information, message order confirmation verification, and proper safety response execution and so on. By analyzing these requirements, two standard protocols are reflected as some contents by each item of safety procedure requirement of IEC62260-1. Table 3 shows six items of IEC 62280-1 safety procedure requirement. The six safety procedure requirements do so as to assure certainty of data in communication among safety related equipment, integrity and punctuality. Because the safety procedure cannot access unreliable transmission layer, this safety procedure has to be added to the safety procedures as represented in Table 3 in addition to the function to ensure that undetected errors are not passed on. Table 3 represents the safety procedure requirement, which the IEC 62280 standards represent, and the comparative analysis result of the two Korean standard protocols.



```
(s0,a1,s1)
(s1,a2,s0)
(s0,a3,s2)
(s2,a4,s0)
(s0,a5,s3)
(s3,a6,s0)
(s0,a7,s4)
(s4,a8,s5)
(s5,a9,s0)
```

C:₩lts.lts

[Result]

No state is deadlock !!

No state is livelock !!

```
****    Deadlock & LiveLock Check Solve Algorithm    ****
```

Figure 4: Deadlock and livelock verification of standard protocol.

5 Conclusion

The standardization of communication protocol for Korean railway signalling has recently progressed to reduce maintenance costs and to increase signalling safety. Now we are about to apply these standardized protocols to the real railway field. Not only reliability of standard communication protocol but also the confirmation of safety characteristics before applying to the real railway field is very important. In this paper, we analyzed the safety characteristics of communication protocol which was recently designed, and standardized protocols for railway signalling systems in Korea. For this we preferentially review the formal verification results, which were progressed in protocol design phase. Also, we analyzed the safety requirements of two Korean protocol with IEC 62280 standard. So the formal verification and comparative analysis approaches has been performed to verify the safety property of protocol for Korean railway signalling. The results of two verifying approaches show that the two communication protocols for Korean railway signalling have safety characteristics.

Table 3: Comparative analysis of two standard protocol and IEC 62280.

IEC62280 safety requirement	KRS SG0063-06	KRS SG0063-07
1. It the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source identifier to the user data.	Discrimination of data origin is basically possible on the point to point communication basis.	There is a data field which represents the receiver's address on IP Header of transmission data packet.
2. Integrity has to be provided by adding safety code to the user data.	Adding safety code CRC-16 code on transmission message frame	Adding code CRC-16 code on transmission message frame
3. The timeliness of user data has to be provided by adding time information to the user data.	-To transmitting periodically state information and doing update the state information using polling message when needed -Synchronization of transmission receiver equipment adding master message clock ☞There is no time information by message but similar effect is possible through above two things	-To transmitting periodically state information and doing update the state information using polling message when needed ☞ Offering time information through above procedure
4. If necessary the sequences of messages have to be checked by safety process.	-NAK message transmission from the reception side the transmission side ·Case of error detection by safety code ·Case of sequence number error ·Case of time out occurrence	
5. The safety procedures for the safety-related equipment have to be functionally independent of the procedures used by the non-trusted transmission system.	-As the protocol of data link class it is distinguished from physics class.	-CRC-16 on the data field, CRC-32 on Ethernet Header, checksum's safety code on IP header. They are differently applied. -MAC, IP, TCP and Data transmission layer has the each separate procedure by each layer.
6. All safety-related equipment has to monitor the performance of the requirements and if the quality of the transmission falls below, then an appropriate safety reaction has to be triggered.	-In case of transmission error, as being by safety measure about 4's requirement matter, it has retransmission process. -In case of over three transmission of same message management as alarm.	Equal with the left side

References

[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] 'KRS SG0063-06: Communication Protocol through Point-to-point Transmission Type for Korean Railway Signalling System', 2005.

[4] 'KRS SG0063-07: Communication Protocol through Network-based Transmission Type for Korean Railway Signalling System', 2005.

[5] Lee, J.H., Hwang, J.G. and Park, G.T., Performance Evaluation and Verification of Communication Protocol for Railway Signalling Systems, *Computer Standards & Interfaces*, **27**, pp. 207-219, 2005.

[6] Hwang, J.G., Jo, H.J. and Lee, J.H., Development of Communication Protocol Verification Tool for Vital Railway Signalling Systems, *Journal of Electrical Engineering & Technology*, **1**(4), pp. 513-519, Dec. 2006.

[7] Hwang, J.G., Jo, H.J. and Lee, J.H., Performance Analysis of Network-based Data Transmission Protocol between Railway Signaling and SCADA Systems, *Journal of Korea Institute of Electrical Engineering*, **55B**(9), pp. 485-490, 2006.