Proposal of the standard-based method for communication safety enhancement in railway signalling systems

H.-J. Jo, J.-G. Hwang, B.-H. Kim, K.-M. Lee & Y.-K. Kim
Train Control & Communication Research Division,
Korea Railroad Research Institute (KRRI), South Korea

Abstract

Safety-critical systems related to the railway communications are currently undergoing changes. Mechanical and electro-mechanical devices are being replaced by programmable electronics that are often controlled remotely via communication networks. Therefore designers and operators now not only have to contend with component failures and user errors, but also with the possibility that malicious entities are seeking to disrupt the services provided by their systems. Recognizing the safety-critical nature of the types of communications required in rail control operations, the communications infrastructure will be required to meet a number of safety requirements such as system faults, user errors and the robustness in the presence of malicious attackers who are willing to take determined action to interfere with the correct operation of a system. This paper discusses the safety strategies employed in the railway communications and proposes a security mechanism for the Korean railway communication system. We present the developed communication safety evaluation tool based on the proposed security mechanism and also evaluate its protecting capability against threats of masquerading, eavesdropping, and unauthorized message manipulation.
Keywords: railway communication, safety evaluation tool, security mechanism.

1 Introduction

As the conventional mechanical and electronic systems used in communication for railway signal control are being replaced by programmable electronic systems that can be remote-controlled through telecommunication networks,

WIT Transactions on The Built Environment, Vol 114, © 2010 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR100781

the safety of railway communication networks have been highlighted. Factors that may adversely affect safety in railway communication networks include the faults or failures of system components or software and security issues arising from conversion to an open system from closed one. In other words, the closed system uses only physically dedicated wired networks, requiring safety provisions against failures or faults. However, the open system uses networks based on wireless communication or Internet technologies, which are not physically independent, and require traditional safety measures as well as stricter security provisions against unauthorized access or intentional attacks [1–3].

With regard to the safety of the communication component in the railway control system, the EU developed European railway signalling safety standards (EN 50159-1 (for the closed system) and EN 50159-2 (for the open system), and IEC 62280-1 (for the closed system) and IEC 62280-2 (for the open system)) to provide the requirements for communication safety [4, 5]. In this study to investigate the security issues relating to data transmitted through the railway signalling communication network, the safety evaluation system for wireless communication in the railway control system is analyzed and then, approaches, requirements, and procedures for safety evaluation of wireless open systems are provided.

Further, requirements for the validation of communication safety and criteria for the determination of safety are analyzed to suggest potential factors that may pose risks to the communication networks in the railway control system and provide recommendations on a secure data link for the communication networks [6]. Moreover, this study describes the means for safety evaluation of the open system on the basis of basic design derived from analysis and discusses such means and their potential applications. In principle, those means are based on the international standards IEC 62280-2.

2 Safety evaluation system for wireless communication networks in railway control system

The open system has network control and management functions that can set (and dynamically re-set) the message routes according to the program unknown to users, through arbitrary routes consisting of more than one transmission media with the characteristics sensitive to external influences unknown to users at both ends of the system. The open transmission system is not known to the control and protection system designers and may have other users that send unknown amount of data in unknown formats. Further, there may be users that may attempt to access data sent by other users, in order to read or copy data without authorization from system administrators. Moreover, the open system may be affected by additional threats of all kinds that may pose risks to the safety-related data integrity. In addition, the transmission link of the open system consists of all items (H/W, S/W, transmission media, etc.) between more than 2 pieces of safety-related equipment connected through the transmission system.

The system reference structure is shown in Figure 1 that uses the open transmission system connecting safety-related and non-safety-related systems

with unreliable transmission systems, irrespective of what kinds of internal transmission protection approaches are employed. The safety-related transmission systems relate to the unreliable transmission system and any kind of safety requirements should not be imposed on the open transmission system. This structure is based on safety-related transmission functions and safety-related connection protection functions.

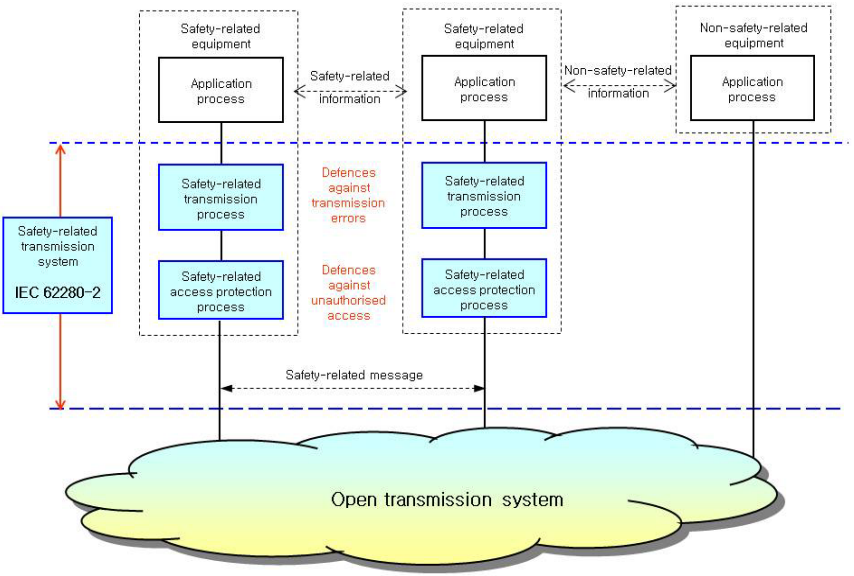

Figure 1: Structure of safety-related system using a non-trusted open transmission system.

Confirmation of functional and technical safety regarding the safety-related transmission function should follow the provisions described in IEC 62280-2. However, any kinds of safety requirements are not imposed on unreliable transmission systems, but the safety procedures and safety encryption that operate inside the safety-related equipment are employed for the safety aspects. As a result, the safety-related message expression models on the transmission media are obtained as shown in Figure 2.

In order to evaluate the safety of open communication networks, the hazard cases encountered in the networks and external environments, relationship with threats, and provisions for defense are summarized in Table 1. Especially, in Table 1, the security factors that have to be considered in the open transmission networks are added to summarizing the hazard cases encountered in the closed transmission networks. In other words, the disrupters and intruders are added as hazard factors to the identification of hazard cases in external environments. Hazard cases that may be caused by disrupters include the taping of

communication lines, damage to or destruction of hardware, and unauthorized modifications to software. Hazard cases that may be caused by intruders include picking-up of channels and unauthorized transmission of messages.

Table 1: Hazard cases, threats and defenses based on an open transmission system.

Hazardous events	Threats						
	Repetition	Deletion	Insertion	Resequencing	Corruption	Delay	Masquerade
HW systematic failure	x	x	x	x	x	x	x[1)]
SW systematic failure	x	x	x	x	x	x	x[1)]
Cross-talk		x	x		x		x[1)]
Wires breaking		x			x	x	
Antennas misalignment		x			x		
Cabling errors		x	x		x	x	x[1)]
HW random failures	x	x	x	x	x	x	x[1)]
HW ageing	x	x	x	x	x	x	x[1)]
Use of not calibrated instruments	x	x	x	x	x	x	x[1)]
Use of not suited instruments	x	x	x	x	x	x	x[1)]
Incorrect HW replacement	x	x	x	x	x	x	x[1)]
Fading effects		x		x	x	x	
EMI		x			x	x	
Human mistakes	x	x	x	x	x	x	x[1)]
Thermal noise		x			x		
Magnetic storm		x			x	x	
Fire		x			x	x	
Earthquake		x			x	x	
Lightning		x			x	x	
Overloading of transmission system		x				x	
Wires tapping	x	x	x	x	x	x	x[1)]
HW damage or breaking		x			x	x	
Not authorized SW modifications	x	x	x	x	x	x	x[2)]
Transmission of not authorized messages	x		x				x[2)]
Monitoring of channels[3)]							
Defenses	-Using sequence # -Time stamp	-Using sequence #	-Using sequence # -Source & destination identifiers -Feedback message -Identification procedure	-Using sequence # -Time stamp	-Using safety code - Using cryptographic techniques	-Time stamp -Timeout	-Feedback message -Identification procedure -Using cryptographic techniques

1) In this case, a correct message is delivered to the wrong receiver due, for instance, to a misrouting; a possible countermeasure is the specification of the sender address.
2) In this case, the message is fraudulent from the beginning; a strong defence is needed, for example the use of a key.
3) It makes sense that there is no threat for the hazardous event "monitoring of channels"; the secrecy, in fact, is a system requirement: it has to do with the particular application

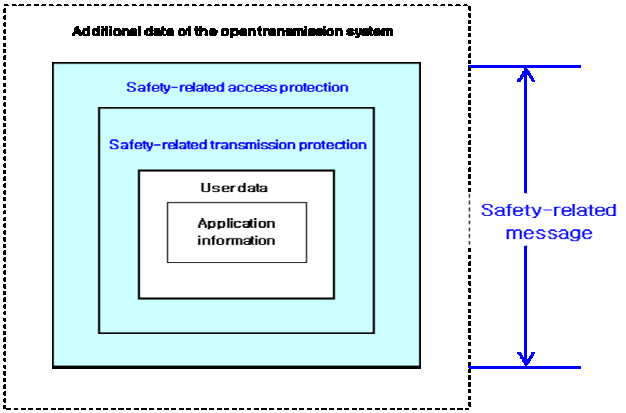

Figure 2: Model of a safety-related message.

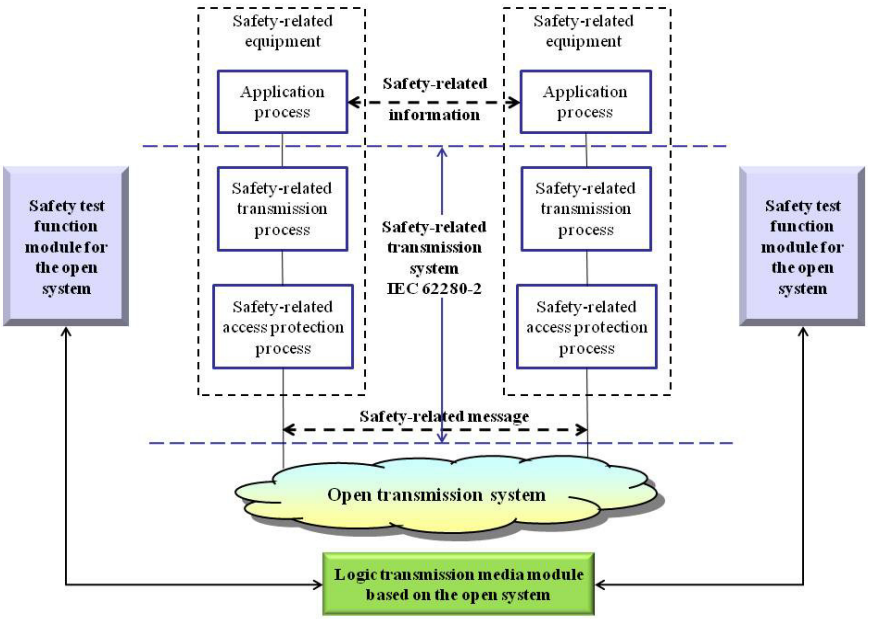

Figure 3: Total structure of testing tool for safety evaluation in the open transmission system.

3 Means for validation and determination of communication safety of railway control system

As shown in Figure 3, the basic structure for the realization of a means for safety evaluation of the open system consists of two modules. With regard to the

safety-related transmission function (IEC 62280-2), it consists of a safety test function module for the open system and a logic transmission media module based on the open system replacing the transmission media based on unreliable open transmission system.

The safety test function module for the open system consists of a sending component and a reception component and communication is realized through the underlying logic transmission media module based on the open system. Figure 4 shows the safety test function module for the open system. This module (sending component) is the open-type safety function simulation and consists of

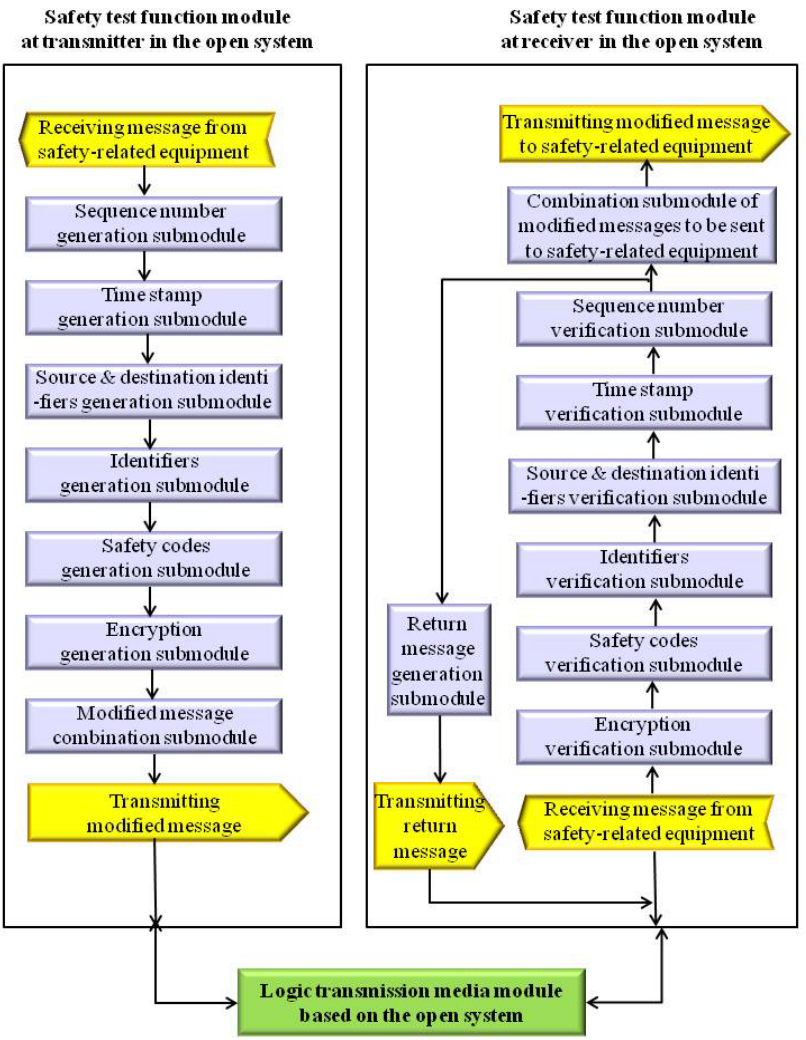

Figure 4: Safety test function module for the open transmission system.

the following seven functional submodules; “sequence number generation submodule”, “time stamp generation submodule”, “source and destination identifiers generation submodule”, “identifiers generation submodule”, “safety codes generation submodule”, “encryption generation submodule”, and “modified message combination submodule”.

The “sequence number generation submodule” generates the sequence numbers to prevent various threats, such as repetition, deletion, insertion, or sequence rearrangement, in the open-type transmission. The “time stamp generation submodule” generates the time stamps for generation of messages to prepare for various threats, such as repetition, sequence rearrangement, and delay. The “source and destination identifiers generation submodule” generates the identifiers for both source and destination to prepare for insertion threats. The “identifiers generation submodule” generates the identifiers for data sources to prevent insertion and falsity threats. The “safety codes generation submodule” generates the safety codes to prevent damage threats. The “encryption generation submodule” generates encryption to prepare for falsity threats. Finally, the “modified message combination submodule” collects data created by the above submodules and combines them to make a modified message. Such combined messages are sent to the underlying logic transmission media module based on the open system.

Table 2: Program structure of testing tool for safety transmission and validation in the open system(JAVA).

Type	Program	Total Program Structure File & Folder	Inner File & Folder	Function
Open type	Testing Tool for Safety Transmission & Validation in the Open System (JAVA)	-\datainfo.java	.	Structure file of simulation tool for safety verification in the open transmission system
		-\project2.java	.	Main source file of testing tool for safety transmission & validation in the open system
		-\project2.exe	.	Executing file of testing tool for safety transmission & validation in the open system
		-\datainfo.class -\project2.class -\project2.jar -\project2.jsmooth -\manifest.txt	.	Remaining related files of testing tool for safety transmission & validation in the open system

Meanwhile, the safety test function module for the open system (receipt component) is the open-type safety function simulation and consists of the following eight functional submodules; “encryption verification submodule”, “safety codes verification submodule”, “identifiers verification submodule”, “source and destination identifiers verification submodule”, “time stamp verification submodule”, “sequence number verification submodule”, “return message generation submodule”, and “submodule for combination of modified messages to be sent to safety-related equipment”.

The program structure of actual testing tool for the safety transmission and verification in the open system is composed of JAVA programming languages like Table 2. Each developed program module is summarized as Table 2, that is, total program structure file & folder, inner file & folder, and functions. The program explanations for simulation tool are as followings. “project2.exe” is executive file and “project2.java” is methods and program involving GUI(Graphic User Interface) related simulations. “datainfo.java” includes methods for structure and structure approach. The specific contents of each program module are like followings.

1) datainfo.java
   The structure is made up of ‘frame start(1byte)’, ‘data length(1byte)’, ‘message type(1byte)’, ‘source identifier(1byte)’, ‘received identifier(1byte)’, ‘data sequence number(1byte)’, ‘time stamp(1byte)’, ‘data(40byte)’, ‘MD5(16byte)’, ‘error-detection CRC-16(2byte)’ and ‘frame end(1byte)’. MD5 calculates source identifier, received identifier, data sequence number, time stamp and data. CRC-16 calculates the remaining things except frame start and end. 3DES calculates all things including CRC-16.

2) project1.java
   - crc16Tab[] : crc-16 table for calculating crc-16
   - crc16Check : returning crc-16 for incoming byte[], byte number
   - generate_others : generating the remaining things except data and CRC for structures of transmitted/received part
   - generate_data_word : generating transmitted 40byte data randomly(the type of random small alphabet)
   - generate_random_data_error : generating the modifications of random position for data
   - go : methods for GUI
   - actionPerformed : methods for GUI
   - md5Check : generating md5 code for incoming byte[]
   - generate_3des_key() : generating keys for 3des
   - Encrypt_3des : 3des encrypt
   - Decrypt_3des : 3des decrypt
   - simulation: methods for simulation

The total operation of the simulation tool executes firstly inputting the number of simulation running and operating simulation for the number by using ‘for sentence’. And then after making transmitted messages by

'generate_data_word' and 'generate_others', Hazard cases of 25 kinds are decided randomly from mixing various types. We can choose randomly the number from '1' to '100' for each hazard case, the selected hazard case is generated if the number is more than '90'. Also the possible threats for hazard cases are able to be selected randomly, and the selected probability is tend to high if some threats occur simultaneously at hazard conditions. We determine randomly the number from '1' to '100' for each threat, and use the number like following contents for each error.

- Corruption: Case of the number less than '15'
- Delay: Case of non-selecting above mentioned threats & less than '20'
- Repetition: Case of non-selecting above mentioned threats & less than '20'
- Deletion: Case of non-selecting above mentioned threats & less than '20'
- Resequence: Case of non-selecting above mentioned threats & less than '20'
- Insertion: Case of non-selecting above mentioned threats & less than '50'
- Masquerade: Case of non-selecting above mentioned threats & less than '80'
- Normality: Case of non-selecting all threats

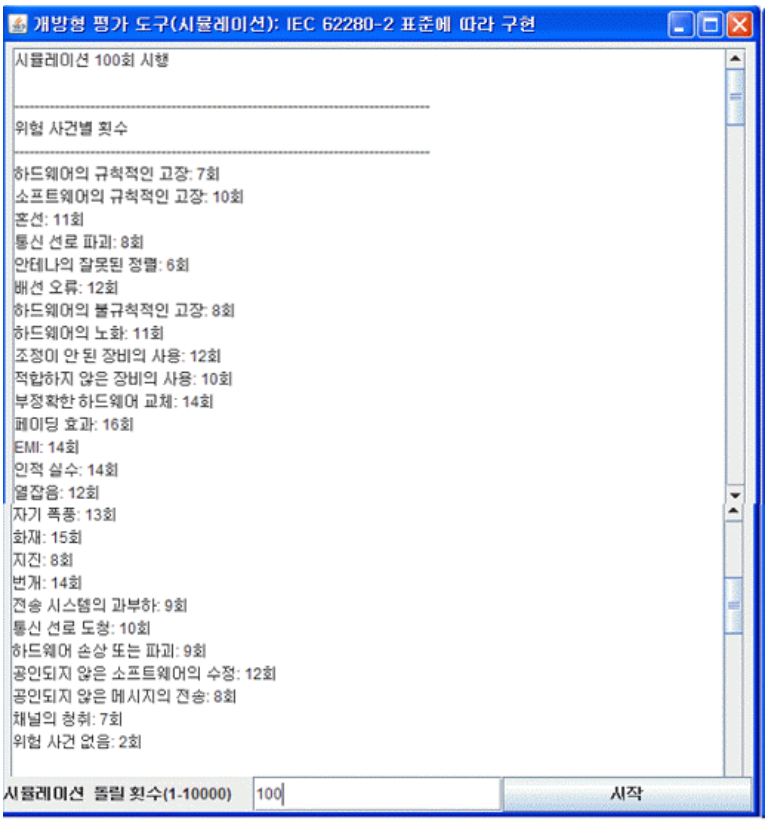

Figure 5: The screen of frequencies at total hazard cases in the validation tool of open transmission systems.

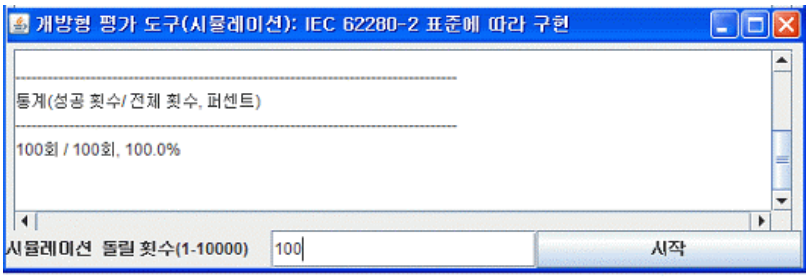

Figure 6: The screen for success number of the developed validation tool in open transmission systems.

This developed tool can show statistical data and inspect whether or not it is continuously checking threats for the inputted number. The operating total procedure of the simulating tool is expressed at the screen like Figure 5. As shown in Figure 5, there are generated frequencies by the program execution as hazard cases. The percentage and number of safety transmission and verification for a total hazard frequency can be presented as the screen of Figure 6.

4 Conclusion

Existing railway communication systems are based on the closed communication networks characterized by expensive costs for installation and difficult maintenance and repair. Owing to the lack of alternative communication methods, those systems result in a delayed introduction of flexible railway control systems. However, new communication technologies, such as wireless communication and TCP/IP protocol, are able to provide various railway communication services with lower costs for installation of infrastructures relating to the open-type communication technology. From the economic perspective, these new technologies are promising. However, the open communication systems have safety and security problems. Change into the open-type, remote-controlled railway control system is increasing. Such a trend in transmission or communication-based railway control (CBTC) leads to concerns over the safety and security aspects. It is not possible to determine the costs for such broadcast communication systems from the safety perspectives and use of the open communication networks with CBTC is strongly required for more application efforts.

The safety is a combination of the system design and the environment where the system is used. The railway control application environments are considerably different from the current basic structure and operation environments. In the closed communication networks, the safety-critical systems can be designed with the assumption that errors and failures are key risk factors to one-to-one communication links. However, the open communication networks require stable operation even when malicious and intentional attacks are increased. In conclusion, in order to ensure the safety of the railway

communication networks from more complex and various risk factors, measures for safety and security are required to prepare for threats from both perspectives of the closed and open communication networks.

References

[1] Winther R. and Johnsen O., Gran B. A.(2001), "Security Assessments of Safety Critical Systems Using HAZOPs," Proceedings of 20th International Conference on Computer Safety, Reliability and Security, SAFECOMP, Lecture Notes in Computer Science, Vol. 2187, pp. 14-24

[2] Knight J. C.(2002), "Safety Critical Systems: Challenges and Directions," Proceedings of the 24th International Conference on Software Engineering, pp. 547-550

[3] Eames D. P. and Moffett J.(1999), "The Integration of Safety and Security Requirements," Proceedings of 18th International Conference on Computer Safety, Reliability and Security, SAFECOMP, Lecture Notes in Computer Science, Vol. 1698, pp. 468-481

[4] IEC 62280-1(2002), "Safety-related communication in closed transmission systems"

[5] IEC 62280-2(2002), "Safety-related communication in open transmission systems"

[6] Jong-Gyu Hwang, Hyun-Jeong Jo, Yong-Ki Yoon, Yong-Kyu Kim(2006), "Safety Characteristics Analysis of Korean Std. Protocol for Railway Signalling according to IEC 62280," Autumn Conference of Korean Society for Railway 2006, pp. 863-869