STUDY FOR THE COMPATIBILITY OF BOTH CYBERSECURITY AND FUNCTIONAL SAFETY STANDARDS FOR RAILWAY SIGNALLING APPLICATIONS

JUN YOSHINAGA
National Traffic Safety and Environment Laboratory, Japan

ABSTRACT
A new railway sector technical specification for the cybersecurity of railway applications was issued in July 2021 as CENELEC/TS 50701. Until now, the concept of development and design of railway applications related to safety have been based on conformity with functional safety standards such as IEC 62278, IEC 62279, and so on. In this paper, we discuss the new issues caused by the scope overlap of functional safety standards and the scope of CLC/TS and by the difference between the lifecycle span of CLC/TS and the functional safety standards argued from the configuration of some typical railway signalling applications. And it is described that CLC/TS requirements raise some new issues that may need some configuration reformation not only the separation of processing programs and its data and data preparation tools kits (this is required by IEC 62279) but also it might need to make some configuration changes by manufacturer and its management method changes by infrastructure managers. In addition, we propose a reasonable validation measure based on functional safety and CLC/TS when railway applications have changed such as creating a preliminary plan to achieve satisfying both viewing points at the same time.
Keywords: cybersecurity, CLC/TS 50701, functional safety, operation phase, vulnerability.

1 INTRODUCTION

With the development of technologies such as railway digitalisation and driverless operation, safety and cybersecurity risk tolerance are becoming more necessary. In 2021, CENELEC issued technical specifications of cybersecurity for railway applications. Cybersecurity threats may increase gradually.

Since technological progress is too rapid in cybersecurity than safety technology, it is essential to pay close attention to cybersecurity information in other industries in order to maintain the performance of railway products.

In this paper, we focus on vulnerabilities which had hidden behind the railway signalling system countermeasures though sometimes suddenly arising from the characteristics of CLC/TS short-term life cycle during the operation phase on the basis of some configuration of recent railway signalling systems. And we argue our proposal against vulnerabilities.

2 METHOD

The methodologies and know-how to achieve the safety of functional safety standards, general information can be referred to from the existing signalling systems which have already developed and operating now. Based on these information, our evaluation experiences, and researching CLC/TS articles, we identify issues related to compatibility between functional safety and cybersecurity and consider appropriate measures to ensure both compatibility.

WIT Transactions on The Built Environment, Vol 213, © 2022 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR220031

3 FUNCTIONAL SAFETY STANDARDS AND CYBERSECURITY STANDARD

3.1 Functional safety standards for railway sector

The aim of functional safety standards is to archive functional safety required for the railway product [1], [2].

In functional safety standards, they assumed that the hazard sources are random failures not cybersecurity risks. Whether or not the target product can achieve safety is determined by risk assessment, and the factors to be examined are:

1. frequency of occurrence of some risk; and
2. its impact (seriousness).

It is common to investigate these factors rate from existing similar products and use them as input of safety risk assessment, and these are known information to some extent, and their values tend to be stable.

The achieved safety is expressed by SIL (safety integrity level). In the case of railway signalling products, it is common to achieve the highest level of SIL (SIL4) because it is important for railway safety.

3.2 CLC/TS requirement

Concerning CLC/TS and IEC 62443(cybersecurity for industrial automation and control system), a design method which called “security design” is applied to a target system [3].

In the security design, the required security levels are classified into SL (security level) 1 to SL4 according to the assumed security risk. SL1 assumes an accidental attack, and SL4 assumes an attack using advanced technology. SL0 is also defined, but it is not discussed here because it is a “No protection system” and is not used for safety equipment.

In IEC 62443-3-3 and CLC/TS, the target system is classified into “zone” and “conduit” from the viewpoint of cybersecurity.

There are some examples of Likelihood evaluation factors in CLC/TS, but the impact is calculated based on the evaluation indicators of “exposure(EXP)” and “vulnerability(VUL)” on a scale of 3 to 5 degrees (see 6.3.2 of CLC/TS)) is mentioned. It is also characteristic that vulnerabilities and expertise are liable to fluctuate depending on the situation.

3.3 Study of differences between safety and cybersecurity risk

There are many differences, of course, but I would like to raise some issues regarding maintaining the cybersecurity and safety functionality of the railway product during the operation phase.

First, the evaluation scales stability shown in Fig. 1. Because using the scale of EXP and VUL is one of methods in CLC/TS, other scales are possible. In any case, these scale values are change rapidly as technology advances or security incidents occur, and so on.

Second, cybersecurity and safety factors sometimes overlap, but CLC/TS requires the separation of the two. In the case of a system that considers cybersecurity from the beginning, it is supposed to evaluate how cybersecurity threats adversely affect the safety of the system.

However, many functional safety standards-based systems currently in operation are usually designed in a mixed manner, as described in Section 4.1 below. At that time for updates to apply a patch of security risks, it may be sometimes difficult to identify an impact in the view of safety.

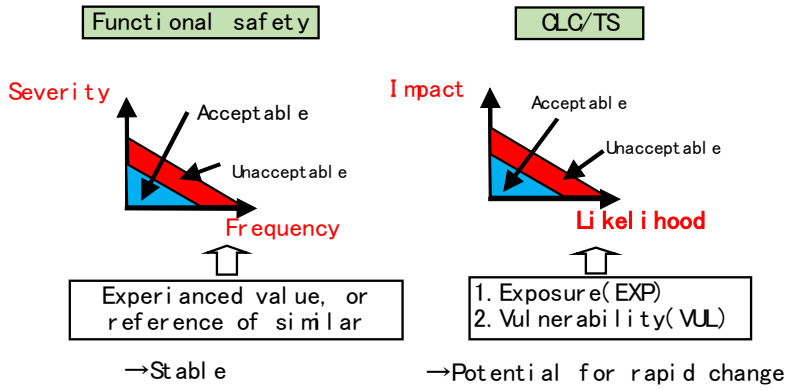

Figure 1: Comparison about evaluation scales.

The third point is that although SIL is examined for the target product in functional safety standards, the CL of cybersecurity risk is not applied to each product but is required for the zone as one group. The target CL is achieved as a whole zone, the vulnerability of one device may or may not be cybersecurity risk.

4 STUDY OF COMPATIBILITY ISSUES

4.1 General network structure of signalling system

Fig. 2 shows a recent typical network configuration of general railway signalling systems. As shown in Fig. 1, the network is mainly constructed from three networks. It is considered that these networks correspond to the zone mentioned in CLC/TS [3].

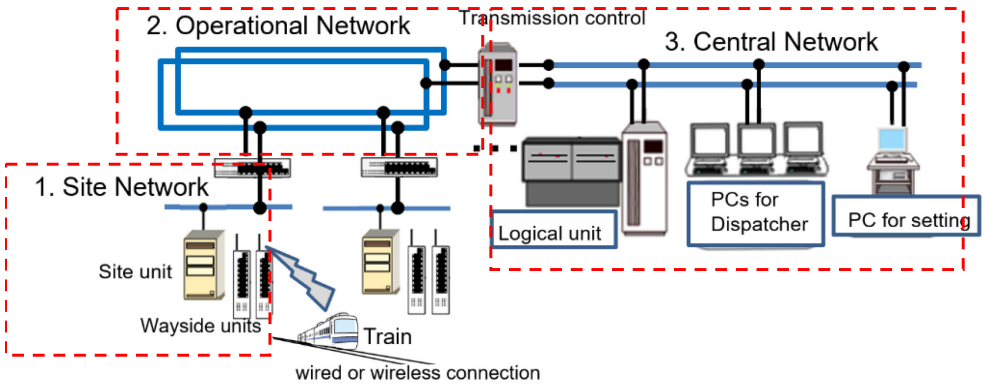

Figure 2: Typical signalling system network structure.

The “1. Site Network” in that figure is the on-site network. Generally, it is installed at each interlocking station separately. The “3. Central Network” is like OCC, and “2. Operational Network” lies along a railway wayside and connecting other networks.

Currently, most of railway lines are using connections between trains and wayside equipment via track circuits, but the number of systems using a wireless connection is increasing.

When using wireless, there is also a network between a train and on-site equipment. In this case, more strong safety measures are generally taken based on IEC 62280 (one of functional safety standard for information and communication) or IEEE 1474.1 than a wired connection.

Although not shown in the figure, security measures such as locking buildings doors and granting system usage rights are also taken in networks other than along the railway lines. Therefore, physical access to the network is considered to be extremely difficult.

4.2 Adopted measures of current signalling system

Since railway products have sometimes decades of life cycle, CLC/TS also stipulates recommendations for legacy systems (Annex B Handling legacy systems) until cybersecurity considerations are widespread.

Table 1 shows CLC/FS description. The mid column in the table shows corresponding measures that can find in the actual signalling product design and deployed materials [4]–[6]. In addition, the applicable provisions of the functional safety standard are described in the right column. These items shown here are main ones, many measures have actually been taken.

Table 1: Examples of measures adopted for products based on functional safety standards.

	Measures for legacy system described in CLC/TS Annex B	Typical measures adopted in signalling products	Related terms of the functional safety standards
1	Closed network (B.4.4)	• Not use open network	• IEC 62280 7.3.7 • IEC 62425 B.4.6, etc.
2	Network segmentation/ restricted data flow (B.4.5)	• Checking right of access to system • Components segmentation • Data encryption, technical sophistication, etc.	• IEC 62425 B.4.6 • IEC 62425 B.3.2 • IEC 62280 C.2
3	Redundant communication (B.4.9)	• Providing fault tolerance	• IEC 62425 3.1.38
4	Security gateway (B.4.10)	• Protection against unauthorized access • Choice and use of safety codes and cryptographic techniques	• IEC 62425 B.4.6 • IEC 62280 C.2

Concerning hazardous mistakes, measures have been taken for some kinds of handling mistakes. As shown in Table 2, countermeasures are taken assuming in current SIL4 of functional safety signalling systems such as wrong machine installation with mistakes, etc. Although these are not measures that directly assume cybersecurity risks, they are also considered to function as security risk measures.

Table 2: Examples of hazard assumptions of current signalling systems for cybersecurity.

Estimating hazards	Example of countermeasures
Wrong handling by human error	To void wrong data
Unexpected system configuration	Rejecting data of illegal equipment
Illegal data receiving	To void To design adopting high confidential connection

From these present conditions, it can be said that measures for cybersecurity threats have actually been taken even for existing signalling system.

Therefore, even if some devices in the zone become vulnerable for cybersecurity threats, it is considered that cybersecurity risks can be protected due to these strong countermeasures. And such cybersecurity accident has not occurred in Japan.

4.3 Possibility of vulnerability

Although strong measures have been taken in railway signalling system, it has been reported that the number of APT attacks is increasing [7], one day a vulnerability may be exploited.

Even in a railway system, it is common that general-purpose software and general-purpose communication equipment are partially used in a non-safety function mainly.

General-purpose products are considered to have a higher risk of being subject to zero-day attacks after vulnerability information is revealed because they are used more widely [8]. We assume a case where the vulnerabilities associated with such general-purpose equipment become a problem.

However, it is unlikely that it will interfere with safety as described above, but there may be some risk to be out of operation. For example, it is possible that a combination of these events will lead to vulnerabilities.

Fig. 3 is not actual system but only imaginary situation. Thought it shows that a device that is temporarily connected as tool for maintenance is equipped with a Wi-Fi connection that is never use normally.

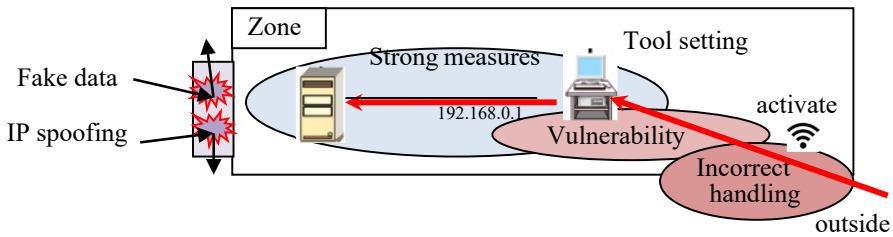

Figure 3: Concept of unauthorized access due to two causes.

It does not pose a threat to safety immediately, though it is not desirable to be able to access it from outside by incorrect handling. We would like to consider measures to prevent such vulnerabilities from being exploited.

Many of the products currently in use have strong countermeasures, so there is a concern that they will continue to be used with these vulnerabilities, so we would like to consider this countermeasure.

4.4 Our proposal of vulnerability evaluation method

The issue of vulnerability Section 4.3 mentioned occurred in the operation phase of the railway product life cycle. Vulnerabilities were sometimes rapidly changed as a result of being received from various channels such as security incidents from worldwide.

This kind of vulnerability may be temporary until measures until patching security holes are taken.

On the other hand, the measures that shown in Table 1 (specifically, functions such as passwords and keys) are defined by the signalling system manufacturer or integrator for secure design, the reduction of this vulnerability also affects the usability of the product. It is thought that the nature is different from the former vulnerability and later because the former vulnerability is considered to be more than a temporary effect and it has the potential to recover.

To manage vulnerability factor more simply in operation phase, our propose is to divide into two scales, like temporary vulnerability and system vulnerability.

We think that the proposed scaling has the following advantages than not separated.

1. After receiving cybersecurity information from the manufacturer of general-purpose products, it is possible to record that there is a problem with the vulnerability all at once, and it is possible to take prompt measures. Table 3 shows to change Temporary Vulnerability of Unit A immediately.
2. Since the current state of vulnerabilities is quantified, it is possible to compare vulnerabilities with similar systems and examine the order of countermeasures within the system (IEC62443 states that the simultaneous update function is desirable). The current use of railway products is considered to be extremely limited).

Table 3: Example of updating a vulnerability revealed in a general-purpose product.

	Unit A	Main unit B	…	Zone total (weakest value)
System vulnerability (stable factor)	1	1	…	1
Temporary vulnerability (variable factor)	1→3	1	…	3
Total vulnerability (by multiple)	1→3	1	…	3

4.5 Measures for incorrect handling in operation phase

Next, we will consider how to deal with human handling incorrectness. Most vulnerabilities occur after deployment product to the user (operation phase) and are not considered to be the first responsibility of the manufacturer and integrator. Therefore, we think that a mechanism that allows users to evaluate their own current situation is necessary.

In the functional safety standard, if a security risk due to the handling of the user is assumed at the product development stage, the user (IM, RU) should comply by notifying the user as a product handling rule books (SRAC, user manual, etc.). Therefore, it is not certain that user manages in the best condition or not.

4.5.1 Ideal solution

ISMS (ISO/IEC 27001) has control measures. It is desirable to evaluate this control measure and the following (1)–(4) view point (in addition, this is one of analysis methods for ISMS control measures) of deficiencies as Table 4, though it seems difficult to list all the devices using in the system that fall under the control measure especially legacy system. That is described 3.3 second point above.

1. Physical (stolen, lost);
2. Unauthorized access;
3. Loss of availability (disaster, breakdown);
4. Mistakes (operational mistakes, rule violations, omission of security measures).

Table 4: Desirable GAP analysis method based on ISMS.

ISMS control measures	Detailed control measures	Concerned equipment of system	View (1)	View (2)	View (3)	View (4)
A11.1.2 Management of room enter/exit checking	Item a: Restriction for visitor move	AR01, AR01a, AR02e …	1. … 2. … 3. … 4. …	1. … 2. … 3. … 4. …	1. … 2. … 3. … 4. …	1. … 2. … 3. … 4. …
	Item b:	…				
	….	…				

4.5.2 Suggestion of solution

If the railway system gradually becomes unprotected over time, a mechanism to prompt detection and optimization might effective.

The GAP analysis method is known for evaluating the difference between the ideal state and the actual state. It is possible to weigh the questions and survey results for the influential factors and evaluate the degree of impact when the event occurs.

1. Key questions about cybersecurity handling

To list up all assets is difficult mentioned above, then it is conceivable that the user performs periodical self-check by answering to the relevant key questions. This requires the cooperation of the manufacturer or integrator as shown in Fig. 4.

2. Evaluation of vulnerabilities and threats

Vulnerability values (five levels from 1 to 5) are assigned with reference to Table 5. This is to make it easier to answer and to see tendency.

This advantage is it is not required specialised knowledge, and it is easy to check current situation visibly.

4.6 Necessity of safety evaluation

In the functional safety standards, to validate modified system is described in its the maintenance plan, however cybersecurity updates are frequent as shown in Fig. 5.

If the impact range can be identified and modification like patch for cyber security, it is reasonable to plan by limiting the test range.

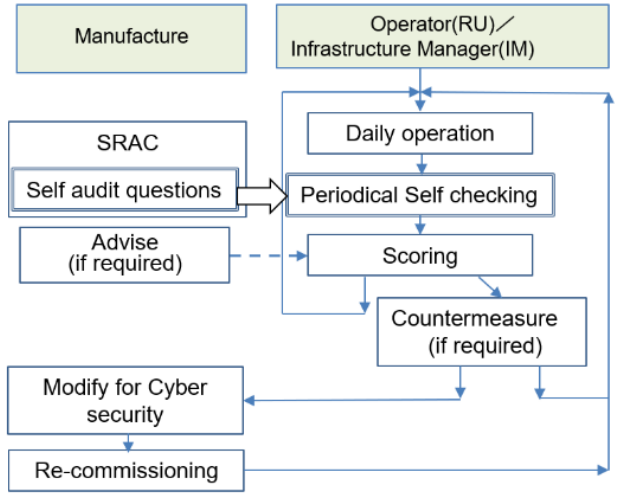

Figure 4: Proposal of a scheme that provides key questions making by manufacturer or integrator.

Table 5: An example of answer options for signalling system user.

Answer option		Weight	Explanation
Total execution	Regulated	1	Requirements are regulated and conducted surely
	Clearly	2	Requirements are not regulated but conducted definitely
Partial execution	Partial	3	Partially conducted for requirements
	Depend on person	4	Implemented irregularly for requirements
	Few	5	It has not been implemented at all
Void	Not required	–	Determined that it does not need to be implemented

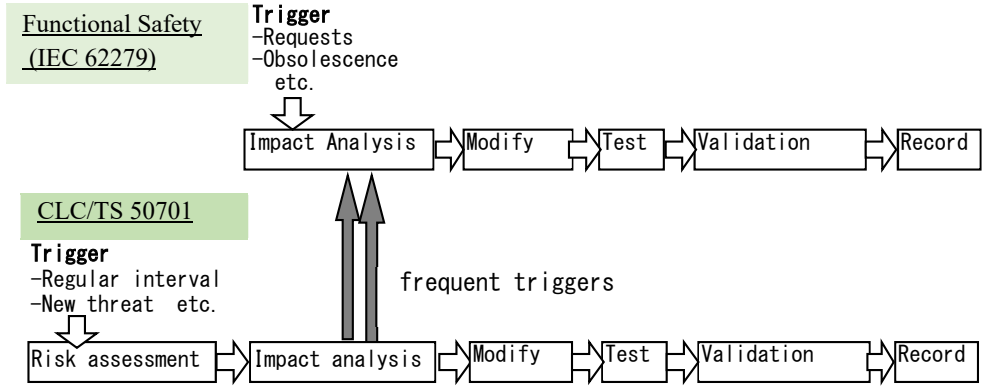

Figure 5: Modification procedure of software in operation phase.

5 CONCLUSION

In this paper, we discussed the differences between functional safety standards and CENELEC/TS 50701. CLC/TS has a concept to assess each zone against cybersecurity threats, we argued evaluation scales of CLC/TS has rapidly changed described by the configuration of a typical signalling system.

In order to match the characteristics, we proposed to manage vulnerabilities separately into two parameters. And proposed a method based on GPA analysis that makes it easy for product users to aware the current situation of their handling management regarding handling.

Regarding the direction of research, we would like to demonstrate the advantages of the proposed method and to improve a question database based on ISMS controls.

REFERENCES

[1] IEC 62425, Ed. 1.0 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, September 2007.
[2] IEC 62279, Ed.2.0 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems, June 2015.
[3] European Union Agency for Cybersecurity, Zoning and Conduits for Railways, February 2022.
[4] Baba, Y., Radio train control system (ATACS). *JR East Technical Review*, **3**, 2003.
[5] Kurita, A., Radio communication network for train control of SPARCS (safety-infrastructure), STECH/1C11 RADIO, 2015.
[6] Nakashima, K., New CBTC System for smart operation latest developments for safe and reliable railways. *Hitachi Review*, **67**(7), 2018.
[7] National Institute of Standards and Technology (NIST), Information security. NIST Special Publication 800-137, p. B-1, 2011.
[8] ENISA threat landscape 2021, April 2020 to mid-July 2021, October 2021.