A practical report of CBTC security analysis

Shunsuke YATABE[1], Masaki OTA[1]

[1] West Japan Railway Company, Technical R&D dept., Railway Operations HQ. Osaka, Japan
Corresponding Author: Shunsuke YATABE (syunsuke-yatabe@westjr.co.jp)

Abstract

West Japan Railway Company did security analysis from 2013 to 2016 for, “Wireless ATC system” (WATC), a CBTC system which will be introduced in Wakayama Line till 2024. Since the authorized security risk assessment methodology has not existed in the railway industry still now, we applied "EVITA” which is for the security assessment framework used in the automobile industry. However, in applying this methodology, mainly two issues exist as below originating from the difference between the automobile industry and the railway industry.

(1) Clear identification of the place of the definition of the security functions in the railway system lifecycle in terms of IEC 62278 (so called “*RAMS standard*”)
(2) Clear definition of the socially tolerable risk level of security

In this paper, we report the details of their differences and their solutions.

Keywords: IT security, Security Analysis, Security Life Cycle, tolerable risk level.

1. Introduction

Recently, information technology is being applied for the improvement of efficiency not only in the field of management and maintenance but also in the field directly related to safety of signaling system. As a matter of concern of the application, security problems like “artificial” threats, as masquerade attack by malicious attackers (hereinafter "security problem") should be handled in particular to CBTC because of the involvement of human lives.

For almost all current CBTC systems, it is not so serious problem still now: they uses 2.4GHz or higher band for wireless transmission with short radio range, so their security is relatively strong because its rich transmission capacity allows to implement many security methods as encryption methods and their short radio range allows to make physical protections of railroad side effective. Therefore, it is regarded that IT security is a future problem in railway industry, in particular, in Europe.

However, this is not necessarily applicable in Japan, which means that IT security is a present problem. On the occasion of the development of the “Wireless ATC system” (WATC) which is equivalent to ATACS, JR East’s *Advanced Train Administration and Communications System,* and ERTMS level 3 in JR West, 400MHz band is an only choice for wireless transmission because of the governmental radio wave regulation. Its relatively poor transmission capacity cannot be accepted strong security methods and its long radio range requires to address a wide range of threats. Thus, an assessment process to forecast artificial threads and to implement effective security functions which works without rich system resources is necessary. And it is a matter of present urgency because the WATC security protection functions will be introduced in JR West Wakayama Line before 2024. In addition, as a near-future topic, it is highly plausible that the ground IP network of WATC will soon be suggested to connect to not only safety-related networks but also non-safety related networks for the purpose of labor-saving of maintenance work such as the online updating of databases. Since the system lifecycle is planned to be 20 years, this kind of risks, though such online maintenance is not applied soon, should be kept in mind now. Thus, a practical methodology of IT security analysis taking the actual workplaces into consideration in railway has been discussed.

As a result of the discussion of the way of the establishment of the methodology for the railway industry, "EVITA” which is for the security assessment framework in the automobile industry, including its risk matrix is applied [1], because the authorized security risk assessment methodology does not exist in the railway industry still now. However, in applying EVITA, mainly two issues exist as below, originated from the difference between the automobile industry and the railway industry.

(1) Clear identification of the place of the definition of the security functions in the railway system lifecycle

This issue can be said to come from the difference of the lifecycle between railway systems and that of automobile. Some researchers insist that the definition of the safety function in the railway industry, including the safety-related transmission function against the accidental threats, should be done before the security analysis against the artificial threats, others insist that the simultaneous evaluation of the safety and the security function should be theoretically ideal to reduce the costs.

(2) Clear definition of the socially tolerable risk level of security

This issue can be said to come from an unexpected internal attacker who has not been subjected for the dedicated communication but should be subjected for the public communication and the maintenance workers management.

While defining security mitigation measures of the wireless transmission system has no methodological difficulty because the target of technical countermeasures can be limited against external attackers, the ground IP network, which is expected to substitute for public communication, has some difficulty because the complex circumstance such as many stakeholders, including maintenance workers, and potential internal attackers, which is expected to increase in number in the future, could give influence on the definition of suitable tolerance risk level for IP network.

Therefore, this paper describes the practical ways to solve issues both (1) and (2) by reflecting our practice of security analysis and security function definition of WATC addressed from 2013 to 2017.

2. Preliminaries

2.1 Outline of WATC system

WATC is a sort of CBTC, Communication Based Train Control system, developed by JR-West, which conforms to JIS-E3801 (Japanese Industrial Standard: Train control system using radio communication / Japan Radio Train Control system: JRTC) and is based on the ATACS of JR East [1].

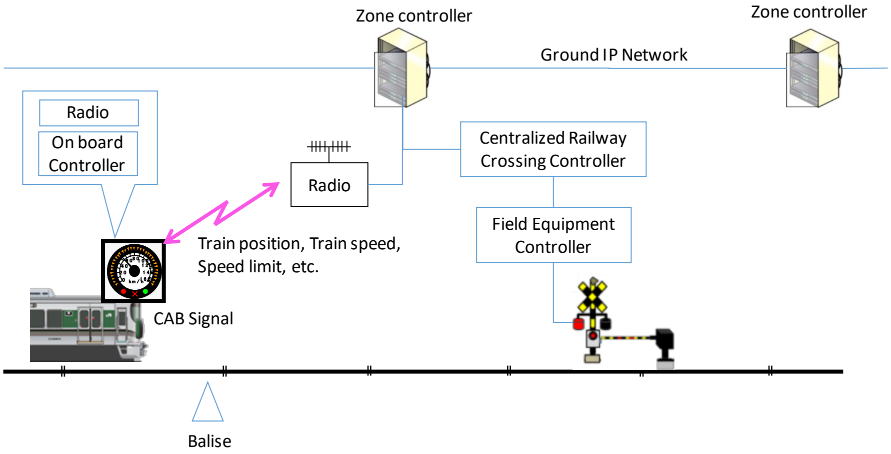
Zone controller
Zone controller
Ground IP Network
Radio
On board Controller
Radio
Centralized Railway Crossing Controller
Field Equipment Controller
Train position, Train speed, Speed limit, etc.
CAB Signal
Balise

Figure1. Outline of JRTC-W

WATC has various controllers and communication devices:

- “Zone Controller” manages interlocking and distance between trains,
- “Field Equipment Controller” connects ordinary equipment via relay,
- “On board Controller” prevents the violation of train signals and shuts out speeding,
- “Centralized Railway Crossing Controller” insures railway crossing safety.

Brief specifications of JRTC-W is shown as below:

Table 1 WATC specification

Specifications	Details
Radio Specifications	Frequency: 400MHz Band Duplex: Full Duplex with 2 frequency channels Modulation: PI/4 Shift QPSK Bandwidth: 5.8kHz Controllable trains: up to 12 on one base station Frequency repetition:4 or 5 channel repetition
Safety-related transmission functions (IEC62280)	ID, Time-out, Sequence number, Safety code, Cryptographic technique

2.2 The Security analysis flow

The IT security analysis requires us to clarify the model of the wireless communication first, to identify the threats systematically and exhaustively secondly, and to find the attacks which is realized to be the potential threats thirdly. The risk of the threat is estimated from the evaluation of the attack potential and that of the severity of the result by the attack fourthly. Finally, the risk reduction method is decided. The following diagram shows the process of the analysis [1]:

Table 2 The security analysis flow

steps	details
1. Clarifying the model of the wireless transmission system:	A model in which the safety-related transmission functions are implemented is established. (But any security function has not been defined.)
2. Identifying potential threats over the wireless transmission system	The following points are systematically identified by using the attack tree method [2]: ● all threats, ● their consequence (like "*Derailment*") and severity (like "*many people could be injured"*) "Attack objectives" should correlate to the Hazardous Events in "Hazard log" in the safety analysis of the RAMS phase 3.
3. Identifying attack methods and assets	All attack methods which represent concrete attack methods like "*replay-attack*" is systematically identified. The analysis is on the basis of basic information of the transmission functions, the use-case of the system and so-called "wireless message code format" which shows what information is transmitted through the wireless transmission zone. Effective attacks consist of two ways with respect to attacker's knowledge on the code format: ● to interrupt the wireless transmission without any knowledge of the code format (e.g. by jamming), ● malicious change of the message in accordance with the code format. And the final result of the decomposition of attack methods consists of "assets" which are simple and non-divisible actions like "*emplacement information of the train which is sent by wireless communication*".
4. Assessing the attack potential	The attack potential, and the risk of the threat from the rating and the severity in conformity to ISO/IEC 15408 (CC CEM) are assessed.
5. Deciding risk reduction methods	Risk reduction methods to reduce risks to below the tolerable level are decided. These methods are evaluated their sufficiency by experts in the committee. The detailed explanation of this step is to be omitted intentionally due to the confidentiality of risk reduction methods.

3. Discussions and analysis on two problems

The methodology and the result of our analysis of WATC was qualified by the experts' committee named "WATC System Evaluation Committee" including IT security experts as a result of the assessment and the audit in terms of the security between 2013 and 2017. During the security analysis process, two issues explained in section 1 are regarded as a matter of concern in the committee.

3.1 Clear identification of the place of the definition of the security functions in the railway system lifecycle

In the committee, we interviewed the committee members of suppliers. As a result of the interview, the application of the simultaneous evaluation of the safety and the security function on the development of the signaling system including WATC can be said to be difficult because the signaling system has enough safety function.

As for the safety function, the safety analysis concerns only accidental threats, like thermal-noise or HW random errors. As for 7 kinds of threats of IEC62280, only 6 threats (repetition, deletion, insertion, re-sequencing, corruption, delay) are objects of this analysis. This analysis for whole the system has been done in the RAMS phase 3, and the result has been recorded in the hazard log. The safety-related transmission functions like safety-code are implemented on demand from the risk analysis based on this safety analysis and they can be said to be sufficient for accidental, non-artificial threats as a result of risk analysis.

As for the security function, the security analysis is a relatively new issue. This concerns intentional, artificial, malicious threats, which are out of scope of risk analysis of RAMS 3rd phase, including masquerade of IEC62280:thus all kinds of threats are considered here. According to the Japanese suppliers, designing the security functions is done after the apportionment of the overall Safety requirements for the system to designate sub-systems, components and external facilities. The security functions are added to the system with safety functions on the basis of the list of information, so called *the code format*, sent by the transmission system. Therefore we concluded that this analysis should be placed in the RAMS phase 5, in which the detail of apportion has been decided, by using the result of the safety analysis at the phase 3 (See the figure 1).

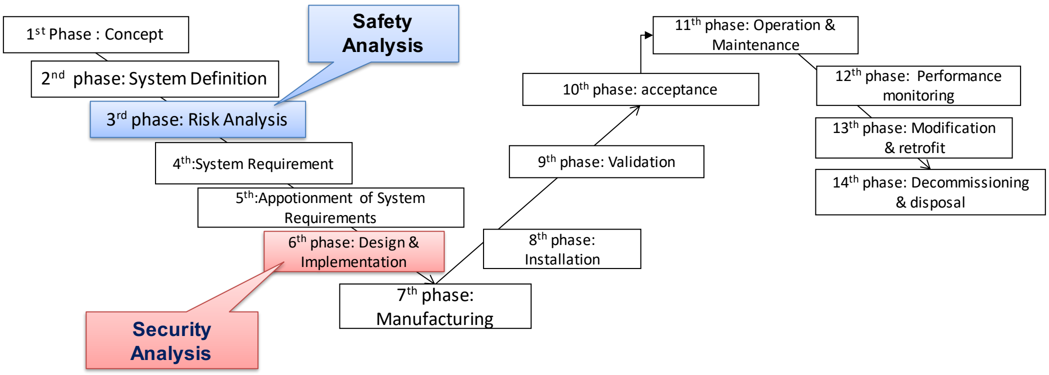
1st Phase : Concept
2nd phase: System Definition
3rd phase: Risk Analysis
Safety Analysis
4th:System Requirement
5th:Appotionment of System Requirements
6th phase: Design & Implementation
Security Analysis
7th phase: Manufacturing
8th phase: Installation
9th phase: Validation
10th phase: acceptance
11th phase: Operation & Maintenance
12th phase: Performance monitoring
13th phase: Modification & retrofit
14th phase: Decommissioning & disposal

Figure 1 RAMS System Life cycle and system-wide safety and security analysis phases

This, setting security analysis at 6th phase seems to be based on a thought that security functions are sub-functions of safety functions. It can be said to be true for the meantime because almost all equipment, at least at the System Function Specification level, has been already designed before security functions become actual issues, therefore we add security functions to the equipment. But from now on, since security is becoming more important, it should depend on a trend in the society whether security functions should be designed with the same importance and the same priority to the safety functions.

3.2 Clear definition of the socially tolerable risk level of security

We assessed the risk of each asset by using the risk matrix of EVITA [2] (see Table 3): its input consists of two values, the rate of the aspects of the attack potential and the degree of the severity of the corresponding hazardous event (*Severity ID*).

Table 3 The risk matrix of EVITA

		Severity ID				
		4 No injuries	3 Light / moderate injuries	2 Severe injuries	1 Fatal injuries	0 Fatal for multiple vehicles
Attack potential ID	1 Basic	0	3	4	5	6
	2 Enhanced Basic	0	2	3	4	5
	3 Moderate	0	1	2	3	4
	4High	0	0	1	2	3
	5Beyond high	0	0	0	1	2

We assess the attack potential in conformity to ISO/IEC 15408 (CC CEM). We apply the analysis method of EVITA [2] which is used for security analysis of automotive on-board network to rate the aspects of the potential attack. The evaluation is determined by 7 parameters: elapsed time, expertise, knowledge of the system, window of opportunity, equipment. We note that the method and the metrics of EVITA is also applied to the security analysis of the ground network among zone controllers of the category 2.

The severity of the threat is estimated from that of the corresponding hazardous event. As already noted, every threat corresponds to some Hazardous event in (2), and each hazardous event is assigned to its severity in the safety analysis. We assign these values as those of the severity of the threats.

In the risk analysis of the wireless transmission system implemented in 2014 and the ground IP networks implemented in 2015, the residual risk tolerance level was set at less than 3 out of 7(0-6) risk assessment levels in the table. Almost all risks can be reduced less than 3 by risk mitigation measures. There are some risks in Ground IP network whose risk values are still over 3 as below:

- RAM-related risks: these are all relatively minor (Risk Value 3). Typical examples of this class are the destruction of equipment, that of power supply, and the cut of signaling cables which make train stop by WATC. We cannot exclude the both possibilities of an external and an internal attacker.

- Labor-saving of maintenance work related risks (Risk Value 4): these risks are not regarded as a threat today. They are threats on so-called *online maintenance*, i.e. remote configuration changes, or remote software updates. This is a future problem because online maintenance has not been applied because of being under consideration to take such security risks now.

- Encryption key distribution-related risks (Risk Value 4): a new risk reduction facility was established on the distribution paths of the encryption key.

In this paper, we focus on RAM-related risks because labor-saving of maintenance work related risks depends on the company's security principle, and encryption key distribution-related risks is purely technical problem.

We set the border line the risk value 2. As a result of our analysis, the application of EVITA reveals a difficulty because the railway industry which is a mass transit is generally said to have only two kinds of security risks "little damage" (risk values less than 2) or "many casualties appear" (risk value larger than 4) while the automobile industry which uses EVITA contains an intermediate value representing dangerous phenomenon called "accident that a few people are injured" etc. in its risk matrix. Instead, the destruction of equipment/facilities and the cut of signaling cables etc, are turned out to be assigned as the intermediate values (risk value 2, 3) as a result of risk value calculation. The analysis cannot exclude the possibility of internal attackers.

This RAM-related risks as the destruction of equipment/facilities are not new but known threats even today. At present, the RAM-related risks of external attacker is reduced by periodical patrols etc. and those of internal attackers are accepted with the following reservations which monitor and manage potential internal attackers:

- Pre-approval of the workplan,
- Taking a record of the work and thereby securing the traceability after the misconduct

For this reason, at the committee in 2016, it was determined that, according to the convention of Japanese railway operators, these risks are accepted “conditionally” under the certain conditions on maintenance and operation.

This is one of the biggest differences between automobile and railway. Unlike stand-alone automobiles, the interaction between the ground equipment and the equipment of on-vehicle is a major factor in railway, especially in CBTC. These maintenance-related factors have not been analyzed in the framework of EVITA, therefore they should have been accounted by means of a research project similar to EVITA but containing the detailed security evaluation of the railway maintenance phase.

4. Conclusions

We reported two practical topics related to the security of a CBTC system which were discussed for the design and the implementation of “Wireless ATC system” (WATC) in Wakayama Line. Since the authorized security risk assessment methodology has not existed in the railway industry still now, we applied "EVITA” which is for the security assessment framework in the automobile industry.
We found the following:

(1) Since the railway industry is organized along the line of the V-model of IEC62278, the clear identification of the place of the definition of the security functions in the railway system lifecycle should be necessary. Current Japanese railway RAMS lifecycle fits the claim that the security analysis should be done in 6th Phase, but this needs to be modified continuously as technology advances.

(2) Unlike stand-alone automobiles, the interaction between the ground equipment and the equipment of on-vehicle is a major factor for system operation in railway, especially in CBTC. These aforementioned maintenance-related factors of the ground equipment have not been analyzed in the framework of EVITA, therefore these factors should have been accounted in security analysis of the railway. As a result of our analysis, these RAM-related risks correspond to risk value 3 that they can be accepted conditionally.

Our result, the methodology and know-how mentioned above, can be applied not only to WATC but widely to the CBTC system all over the world.

Acknowledgment

We would like to thank all the member of WATC System Evaluation Committee between 2013 and 2017 for their helpful comments and discussions.

References

[1] Takashi Mori, Shunsuke Yatabe, Daisuke Souma, Kenji Taguchi, Hideki Nishihara, Hidenori Kuwakado, “Security Evaluation for Communication Based Train Control System Using Attack Tree Method,” The Proceedings of International Symposium on Seed-up and Service Technology for Railway and Maglev Systems: STECH 2015 .

[2] EVITA, Deliverable D2.3: Security requirements for automotive on-board networks based on dar-side scenarios (2009).

[3] IEC 62278 / EN 50126 Railway applications - The specification and demonstration of Reliability, Availability Maintainability and Safety (RAMS), 2002.