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

The content of this talk

We report a practical topic related to the security of a CBTC system discussed for the design and the implementation of “Wireless ATC system” (WATC)* in *Wakayama Line.*

- We applied “EVITA” which is for the security assessment framework used in the automobile industry.
- Mainly two issues exist as below originating from the difference between the automobile industry and the railway industry.
  1. Clear identification of the phase of the definition of the security functions in the railway system lifecycle in terms of IEC 62278,
  2. Clear definition of the socially tolerable risk level of security.

We discuss them.

*“Wireless ATC system” (WATC) is a sort of CBTC equivalent to JR East’s *Advanced Train Administration and Communications System* (ATACS), and ERTMS level 3 in JR West.

The contents

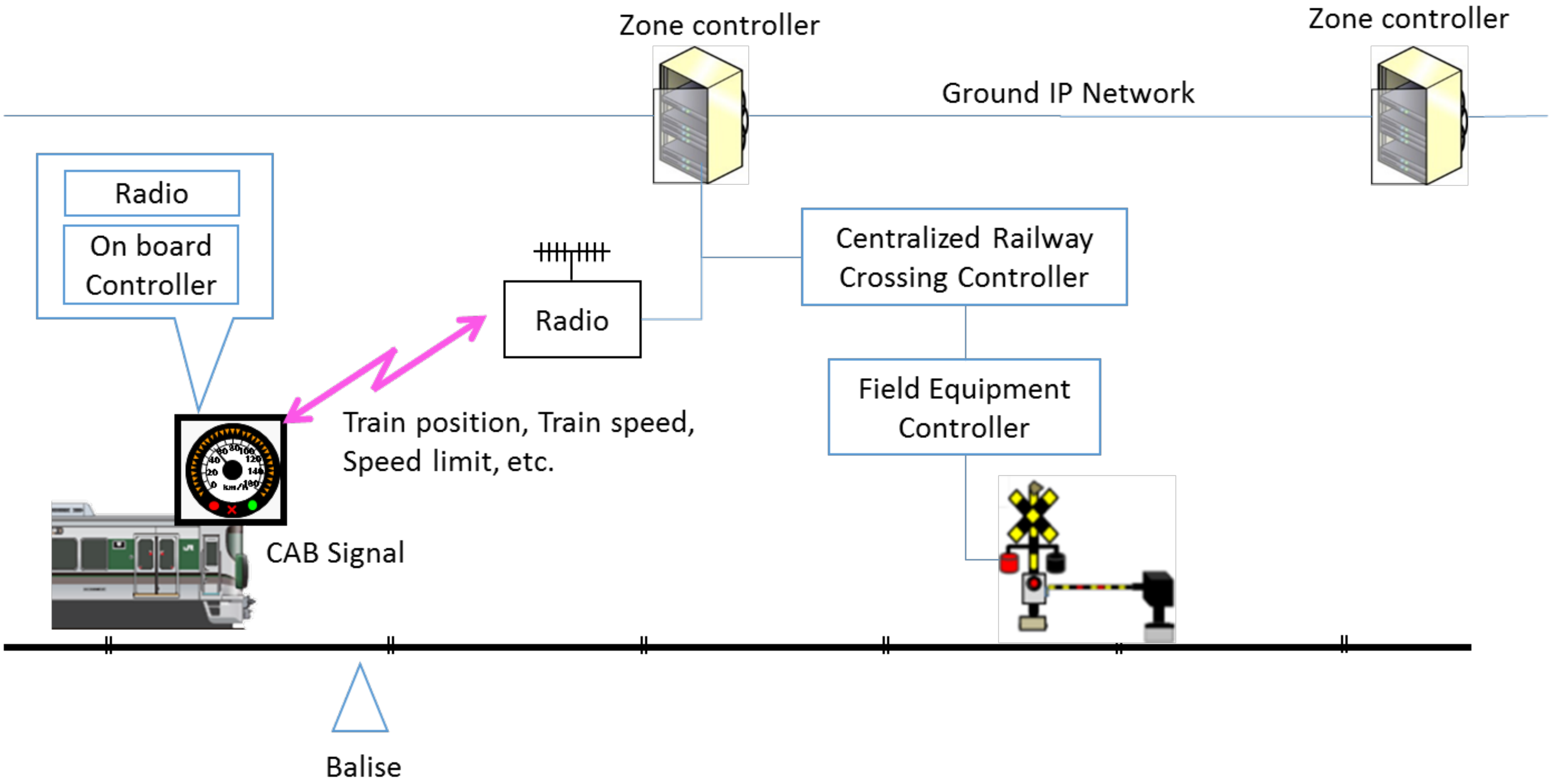
Background: Introducing the *Wireless ATC system*

1. Identifying the phase of the definition of the security function

2. Defining the socially tolerable risk level of security.

3. Consequence

Background: Introducing the *Wireless ATC system*


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

WATC security protection functions will be introduced in JR West *Wakayama Line* before the starting the operation in 2024.

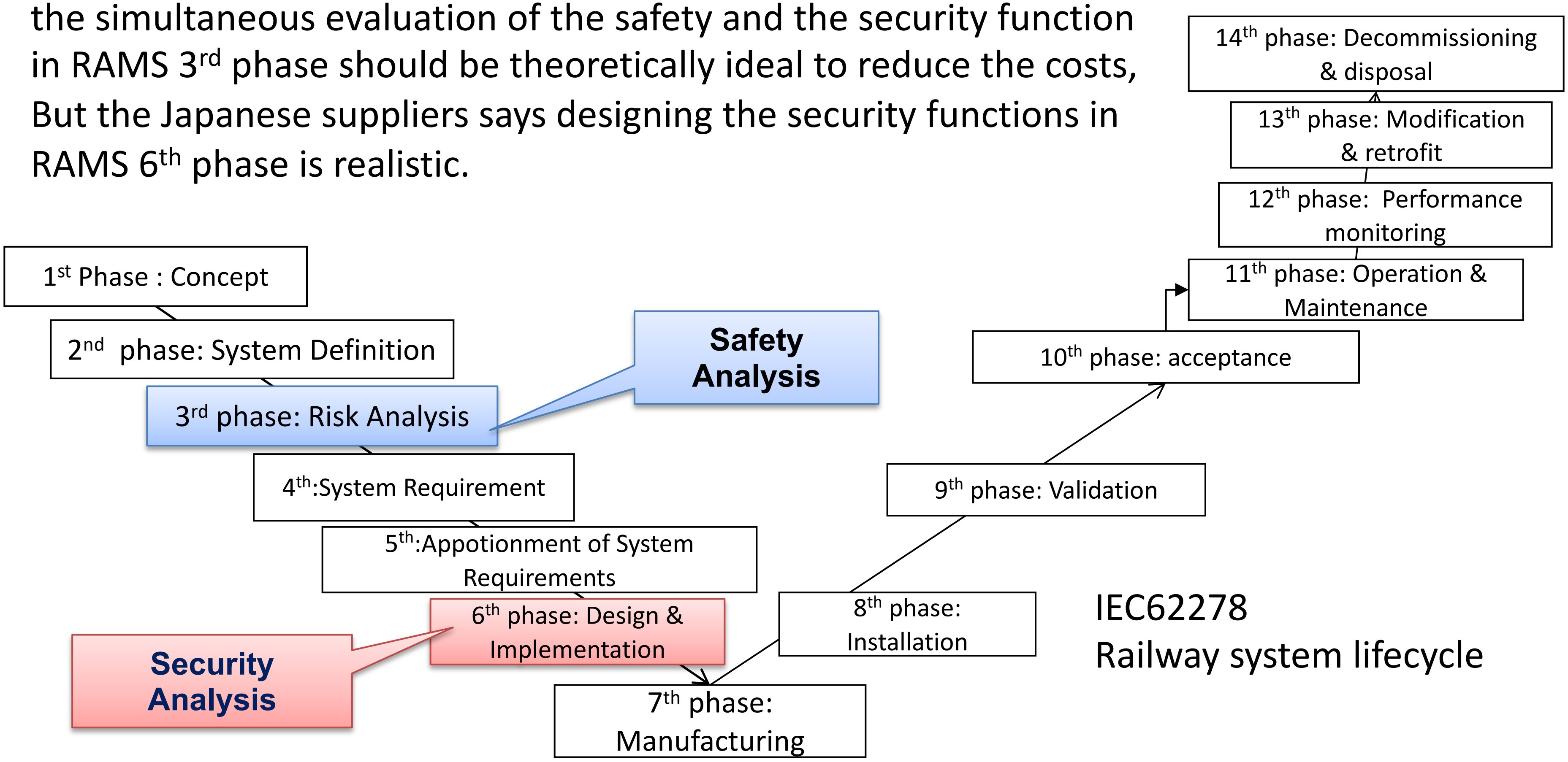
- 400MHz band wireless transmission (relatively weak security protection) ,
- Ground IP network (the risks for connecting to non-safety related networks should be kept in mind now).

1. CLEAR IDENTIFICATION OF THE PHASE OF THE DEFINITION OF THE SECURITY FUNCTION

Clear identification of the phase of the definition of the security function

The gap between the safety analysis and the security analysis

- the simultaneous evaluation of the safety and the security function in RAMS 3rd phase should be theoretically ideal to reduce the costs,
- But the Japanese suppliers says designing the security functions in RAMS 6th phase is realistic.



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

IEC62278
Railway system lifecycle

We decided ....

- we concluded the security analysis should be placed in the RAMS phase 6, by using the result of the safety analysis at the phase 3 from practical reason,

2. CLEAR DEFINITION OF THE SOCIALLY TOLERABLE RISK LEVEL OF SECURITY.

The socially tolerable risk level of security

- The risk analysis is done by using the attack tree method.
- The risk evaluation is carried by out applying the risk evaluation method of *EVITA*, in conformity to ISO/IEC 15408 (CC CEM).

EVITA's application

- Applied for automotive on-board network to rate the aspects of the potential attack.

EVITA's *major* premise

- the system is stand-alone,

Question:

Can we think the socially tolerable risk level of security of railway system is the same as that of automobile?

The serious residual risks

Before talking about the tolerable risk level, let's see what kind of residual risks we have…

- The risk tolerance level had been set at less than 3 out of 7(0-6)
- Almost all risks can be reduced less than 3 by risk mitigation measures except some Ground IP network risks as follows

Target	Risk level	Dangerous zone in the Route	Potential attackers on the blacklist	Major risk	Major protection methods for masquerading *
The Encryption key for wireless transmission system	4	• Ground IP network	• External attacker • Internal attacker	Stolen	• Encryption
The database information (Labor-saving of maintenance work related issues in near future)	4	• Ground IP network	• External attacker • Internal attacker	Rewriting the database information	• Authentication

*For simplicity, we only introduce protection methods related to the masquerading attack.

…and borderline residual risks (related to Availability)

There are some risks in Ground IP network whose risk values are still over 3:

Trget	Risk Level	Dangerous zone in the Route	Potential attackers on the blacklist	Major risk
Ground equipment, facilities, etc. (these are related to mainly Availability)	3	• Ground network	• External attacker • Internal attacker	Physical destruction (Equipment, power supply, the cut of signaling cables , etc.)

These Availability-related risks as the destruction of equipment / facilities are known threats even today.

Can Tolerable risk level be over 3?

Present risk reduction methods for availability-related risks

	external attackers	internal attackers
The risk reduction methods	periodical patrols	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, it was determined that, according to the convention of Japanese railway operators, these level 3 risks are accepted “conditionally” under the certain conditions on maintenance and operation.

3. CONSEQUENCE

Consequence

1. Traditionally the safety was the first concern of designing railway systems, and the designing the security function should be seamlessly embedded to the railway lifecycle.
2. Quite contrary to 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.

Therefore these factors should have been accounted in security analysis of the railway. (we need an appropriate security model including them, in particular maintenance related issues)