The Scenario based EMP Risk Analysis for RF-CBTC

Dong-Min Kim, Min-Seok Yoon
National Security Research Institute (NSR)
1559, Yuseong-daero, Yuseong-gu, Daejeon, 34044
Republic of Korea
supperdm@nsr.re.kr

Abstract— As intentional electromagnetic interference (IEMI) sources are developed, the threat of electromagnetic pulse (EMP) to national infrastructure is increasing. Therefore, the risk analysis for national infrastructure is becoming inevitable. However, there are several limitations for analyzing the vulnerability of the EMP. This paper introduces one of the methods to investigate the EMP susceptibility of radio frequency communication based train control (RF-CBTC) system.

Keywords- EMP, IEMI, RF-CBTC

I. INTRODUCTION

Many researchers had studied the EMP attacks in regard of the electronic equipment and device such as computers and cell phones [1]. But, it is hard to find a definitive solution for national infrastructure. Although there is a common EMP threat analysis method, there are drawbacks in applying the process to the national infrastructure. In this research, we mainly focus on the railway system (RF-CBTC) among many other critical national infrastructures. There was a previous study conducted by the United States committee in 2008. However, this report just addressed the EMP susceptibility level of the railway system without a risk analysis procedure [2]. Thus, we suggest the effective method to overcome the limitation of the previous researches for analysis of the RF-CBTC system.

II. General EMP risk analysis of national infrastructure

The general EMP risk analysis is divided into four stages . First, the environment of the national infrastructure that requires protection should be investigated. Second, the threat level which is transmitted to the equipment under test needs to be obtained. To predict the electric field, there are some ways such as the EM-simulation and numerical calculation. Third, the vulnerability test of a target device is performed and the susceptibility level is found. At last, by comparing the results of the threat level and susceptibility level, the EMP threat of national infrastructure is predicted. On the basis of this estimate, the approximate protective level can be confirmed

III. Limitation of general EMP risk analysis

The nuclear electromagnetic pulse threat level is specified at about 50kV/m, but the level of threat to IEMI is difficult to define. Because the types of IEMI sources are diverse and the predicted levels are different depending on the location of the perpetrator. Accordingly, it is necessary

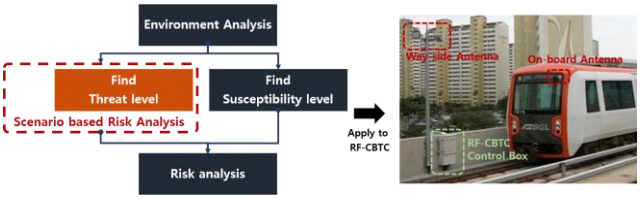

Figure 1. Proposed EMP risk analysis for RF-CBTC

to analyze the risk taking into account the scenarios which should be reflected by the background of each national infrastructure. In addition, the target system, perpetrator's position, and kinds of EMP source are essential factors included in the scenario.

IV. Proposed threat level analysis for RF-CBTC

The threat level analysis based on the scenarios can complement the limits of the general EMP risk methods. We have created a number of threat scenarios considering the domestic RF-CBTC environment to find the threat level. The important factors that are reflected in the scenarios are shown in Table 1. The conditions for the train to operate must be considered first.

In addition to these factors, by anticipating the points that are vulnerable to EMP, the kinds of IEMI source for the facility can be determined. If we choose the wayside radio unit with the antenna as the target device, there are two paths that can be attacked by EMP. The first possible way is back-boor coupling such as AC power cable coupling. Even though surge protection device is located inside the radio unit, it may not block the pulse. The second possible way is front-door coupling. For the most of the RF-CBTC that transmits train control information using the 2.4GHz ISM band, the wayside antenna is used. If EMP passes through the wayside antenna, there is a high possibility of communication interruption and low noise amplifier module destruction. As a result, in the first case, there is a high probability that damped sinusoidal or ultra-wide band sources will be used in EMP attack, and in the second case, high power microwave sources are likely to be used.

TABLE I. Elements used for threat scenario

#1	Train operation conditions
#2	Distance between each wayside radio unit
#3	Number of access points simultaneously connected to the train
#4	Configuration of radio unit network
#5	Number of on-board antenna

REFERENCES

[1] Jongwon Lee (2017). "Malfunction of Electronic Equipment by Repetitive Ultra-Wideband Pulse", Asian High-Power Electromagnetics Symposium 2017, Bangalore, India
[2] U.S. EMP Commission. (2008). "Report of the Commission to Assess the threat to the United States from Electromagnetic Pulse(EMP) Attack", USA, pp.1-185