국제표준기반 철도차량 사이버보안 적용 사례 분석

A Case Analysis of International Standard-Based Cybersecurity Application for Rolling Stock

김동현*†

Donghyun Kim*†

초 록 철도차량의 고도화로 마이크로프로세서 기반 제어와 이더넷(Ethernet) 네트워크로 구성됨에 따라 사이버보안에 대한 수요도 증가하고 있다. 일찍이 해외에서는 유럽을 중심으로 사이버보안 국제표준인 IEC 62443 시리즈를 철도차량 시스템 전반에 적용하고 있다. 본 논문에서는 IEC 62443 위험관리 방법을 해외 프로젝트에 적용된 사례를 기반으로 설명한다. 먼저 위험평가 과정에 활용되는 환경, 자산, 위협분석 항목을 소개한다. 이후 노출도(Exposure) 및 취약점(Vulnerability) Rating을 토대로 사이버보안 발생가능성(Likelihood)을 측정하는 방법론과 위험평가 및 사이버보안 기술 요구사항 사례를 소개한다.

주요어 : 철도 사이버보안, IEC 62443, 사이버보안 위험평가

1. 서 론

철도차량의 마이크로프로세서 기반 열차 제어, 이더넷(Ethernet) 기반의 네트워크 연결성이 증가함에 따라 철도 사이버보안에 대한 수요도 증가하고 있다. 해외에서는 유럽을 중심으로 IEC 62443 시리즈가 사이버보안 산업규격으로 정의되고 국제표준으로 채택되어 통용되고 있다.

IEC 62443 시리즈는 사이버보안 적용방안으로 사이버보안 관리 체계, 위험관리 및 사이버보안 기술 요구사항 등을 명세하고 있다. 이 중 위험관리 표준인 IEC 62443-3-2는 위험평가 이후 산출된 위협에 완화조치를 적용하고 최종 검증까지의 과정으로 구성된다. 본 논문에서는 IEC 62443-3-2 표준 위험관리 방법 및 사이버보안 기술 요구사항 사례를 소개한다.

† 교신저자: 현대로템주식회사 SE
(donghyun.kim@hyundai-rotem.co.kr)
* 현대로템주식회사 시스템엔지니어링팀

2. 본 론

2.1 사이버보안 환경 및 시스템 정의

2.1.1 환경 분석

환경 분석은 운영 및 유지보수 상황 가정을 토대로 진행한다. Table 1은 환경 분석을 위한 사례이며, 철도차량 사이버보안 위협 식별을 위한 참고자료로 활용된다.

Table 1 Environment Assumption Case

Environment Assumption / Confirmed	
Operation	Each Owner is responsible for cybersecurity In Trackside/Radio/On Ground systems or networks
	Natural event such as climatic phenomenon, flood and environmental disturbance are analyzed and addressed as part of RAMS, EMC and Fire management.
Maintenance	Maintenance mobile device has cybersecurity features. 1) Deny any unauthorized USB 2) Block unnecessary physical and service ports. 3) Block Wi-Fi Function and Any unnecessary application such as game.

2.1.2 자산 분석

철도차량 공급범위 내, 관리 자산에 대해 분석한다. 이때, 이해관계자와 (1) 인터페이스, (2) OS 유/무, (3)물리적 위치, (4) 기능, (5) 저장/유휴/전송 데이터 등을 최소한으로 식별한다. 자산 분석 결과는 이후 취약점 분석을 위해 사용된다.

2.1.3 위협 분석

모든 이해관계자와 위협 목록을 확정한다. 통용되는 철도차량의 위협 목록은 (1) IEC 62443 (2) TS 50701:2021 Section 6 (3) ISO 27005 (4) NIST SP 800-53 등이 있다.

2.2 위험평가

앞서 2.1절의 사이버보안 환경 및 시스템 정의를 토대로 철도차량의 사이버보안 위험관리를 수행해야 한다. 사이버보안 위험관리를 위해 위험평가 및 보안 요구사항 수준을 도출해내야 한다.

2.2.1 위험 매트리스 결정

사이버보안 위험 평가를 위해서는 Likelihood와 Impact를 측정해야 하며, TS50701의 방법론을 활용하면 Likelihood를 다음과 같이 측정 할 수 있다.

Table 2 Likelihood Based on TS 50701[1]

Rating	Exposure	Vulnerability
1	Highly restricted logical or physical access for attacker	— Successful attack is only possible for a small group of attackers with high hacking skills
2	Restricted logical or physical access for attacker	— Successful attack is feasible for an attacker with average hacking skills
3	Easy logical or physical access for attacker	— Successful attack is easy to perform, even for an unskilled attacker

Likelihood = 노출도 + 취약점 -1

Impact 및 위험 매트리스는 운영사의 위험매트리스를 협의하여 사용하는 것이 일반적이다.

2.2.2 위험평가 및 요구사항 도출

위험 매트리스를 결정한 후에는 위험평가를 통해 취약점 및 위협시나리오 별 위험도를 산정하고 완화조치를 위한 보안 요구사항을 도출한다.

Table 3 Risk Assessment Case

Risk ID	Asset	Vulnerabilities	Threat Scenario
RID-1	Passenger Wi-Fi system	Gateway for passenger Wi-Fi system do not block unauthorized external access.	Attacker could internal access from passenger Wi-Fi network.
RID-2	Passenger Wi-Fi system	Wi-Fi service use weak protocol such as WPA or WPA2	Attacker could sniff passenger data through weak protocol

Table 4 Derived Requirements Case

Risk ID	Risk Rating	Mitigate measure	IEC 62443 control measure
RID-1	Medium	Passenger Wi-Fi network shall be segregated from Train network. Gateway for passenger Wi-Fi shall include firewall to block anomaly traffic. Gateway for passenger Wi-Fi shall be installed in locked panel.	CR (Component Requirement) 5.1 Network Segmentation CR 5.2 Zone boundary protection CR 7.7 least functionality CR 3.11 physical resistance
RID-2	Medium	Passenger Wi-Fi service shall use protocol. Transmission for passenger data shall be encrypted with industrial practice algorithm	NDR (Network Device Requirement) 1.6 Wireless access Management CR 4.3 Use of cryptography

Table 3 및 Table 4와 같이 각각의 취약점과 위협시나리오에 대해 영향도와 위험수준을 결정하고 그것에 맞는 완화조치, 통제항목을 요구사항으로 할당하여 사이버보안의 위험수준을 감소시키는 것이 위험평가의 주된 목적이다.

3. 결 론

철도차량 및 하부장치의 보안 수준 및

요구사항은 철도 운영사의 위험평가 결과를 기반하여 이루어지며, 철도차량의 사이버보안을 보장하기위한 활동의 일환이다. 철도 운영환경 및 기타 제반사항을 충분하게 반영하여, 현실적이고 실용적인 보안수준을 수립해 나가야 한다.

참고문헌

[1] CLC/TS 50701 Railway applications – Cybersecurity (2021)

[2] IEC 62443 series Industrial automation and control systems (2018)