

Global Report

유럽철도산업연맹의 철도분야 사이버보안에 관한 비전

1. 도입
2. 추진경과
3. 유럽 철도분야에의 도전(단기, 중기, 장기)
4. 핵심 메시지 및 권고사항
5. 결론

1. 도입

유럽철도산업연맹 사이버보안 워킹 그룹에서 개발된 본 문서는 유럽의 철도시스템에 예상되는 사이버보안 문제를 평가하고 단기, 중기, 장기로 나누어 목표와 우선적 해결사항을 제시함으로써, 유럽연합 공공 기관과 다른 철도 이해관계자들이 사이버보안 문제에 추가적인 관심을 기울일 기반을 제공할 것이다.

2. 추진경과

유럽연합 내에서는 사이버보안 문제를 다루기 위해 몇 가지 이니셔티브가 시작되었다. 네트워크 및 정보 보안(NIS, Network and Information Security) Directive 2016/1148, 사이버보안법(Cybersecurity Act) 2019/881 그리고 유럽연합 일반 데이터 보호 규정(EU General Data Protection Regulation) 2016/679 은 더욱 일관성 있고 조화된 사이버보안 관리체계를 위한 가장 보편적인 조치이다.

유럽연합의 [Digital Single Market Strategy]는 사이버보안관련 법제화를 진행할 때 조화된 프로세스와 솔루션을 만들도록 하고 있으며, 사이버보안 솔루션이 시작되고 실행되는 속도는 민간과 공공 모두와 밀접히 협력하여 사이버범죄에 대응하기 위해 새로운 기술과 서비스를 신속하고 광범위하게 진행되도록 해야 한다고 규정하고 있다.

조화로운 체계를 만들기 위해 필요한 몇 가지 조치들은 다음과 같다.

- 1) 유럽전기표준화위원회(CENELEC)를 통한 유럽연합 차원의 표준화 진행
- 2) 철도분야와의 협력
- 3) 연구개발 및 기술혁신(R&D&I, Research & Development & Innovation)
- 4) 최신 트렌드(슈퍼컴퓨팅, 양자 컴퓨팅, 인공지능 기술 등)에 대한 모니터링

3. 유럽 철도분야에의 도전(단기, 중기, 장기)

3-1. 단기 도전(1~3년)

ㄱ. CENELEC TC 9X WG 26 내에서의 기술사양 완성

모든 이해관계자들이 이 기술사양의 완성을 위해 상당한 리소스를 투자하여, 기술사양 [CLC/TS 50 701]을 2021년 초까지 완성하는 것이 목표이다.

ㄴ. 법률규정 프로세스에 대한 명료화 시작

기술사양 [CLC/TS 50 701]은 인증의 기본이며, 시간제약 때문에 이와 병행하여 법률규정 프로세스도 업데이트되고 조화되어야 한다.

ㄷ. CENELEC 표준화와 유럽연합 연구개발 및 기술혁신(R&D&I) 프로젝트의 컨버전스 필요

ㄹ. 정보공유 및 분석센터(ISAC, Information Sharing and Analysis Centre)의 설립

이 이니셔티브는 유럽연합집행위원회와 유럽연합 사이버보안국(ENISA)으로부터 제기된 것이다.

ㅁ. 유럽연합 철도교통관리시스템(ERTMS, European Rail Traffic Management System) 기술사양 개발을 위해 설립된 [UNISIG]이 차세대 열차제어 및 신호시스템(CCS, Control command and signalling) 상호호환성 기술사양(TSI, Technical Specification for Interoperability)을 개발할 때 사이버보안을 고려

ㅂ. 신규 및 기존 상호호환성 기술사양(TSI)에 사이버보안 문제를 적절하게 규정

3-2. 중기 도전(4~6년)

ㄱ. CENELEC 기술사양(CLC/TS)을 프로젝트 차원에서 적용

ㄴ. [CLC/TS 50 701]을 향후 유럽연합 표준(EN Standard, CENELEC Standard)으로 개발

ㄷ. 전체 공급체인에의 적용

ㄹ. 양자-보안(Quantum-Security)과 암호화 민첩성(Crypto-Agility) 기술적용 검토

양자 기술의 발전이 급속도로 진행되고 그 위험이 증가함에 따라, 철도산업계는 양자 컴퓨팅 기술에 대응하는 양자-보안 문제에 유의하여 준비해야 하며, 철도관련 장치와 시스템에 암호화 민첩성 기술 적용을 검토해야 한다.

ㄴ. 멀티모달 및 인터모달 보호기술의 개발

최근의 항공, 철도 그리고 도로의 멀티모달 모빌리티 상황에서, 개별적인 사이버보안 방식이 전체적으로 통합적 관점에서 조화가 이루어져야 한다.

3-3. 장기 도전(7~9년)

ㄱ. 프로젝트가 아닌 프로세스 차원에서의 인증

ㄴ. 차세대 시스템을 위해, 전체 제품 수명주기의 보장

ㄷ. 국제 표준의 개발

4. 핵심 메시지 및 권고사항

사이버보안 문제에 대한 완벽한 협력을 위해, 유럽철도산업연맹은 표준화와 연구개발 그리고 기술혁신 활동에서 모든 필요한 이해관계자들과의 협력적인 접근이 되어야한다고 믿으며 아래와 같이 관련기관에게 제안한다.

1) 유럽연합집행위원회 정보통신국(DG CONNECT)에게

유럽연합 회원국에게 유럽연합 차원의 사이버보안 규정인 [NIS Directive] 적용을 일관되게 적용하도록 조화가 필요하며, 추가적인 규정화 활동이 진행되기 전에 법률규정 프레임워크의 상세 수준과 IT 기술개발 간의 밸런싱이 고려되어야 한다.

2) 유럽연합집행위원회의 타 부처에게

현재 진행 중인 [Shift2Rail] 프로젝트가 [Horizon Europe] 차원으로 확대되도록 철도연구에 더 많은 자금 지원이 필요하다.

3) 유럽연합 사이버보안국(ENISA)에게

철도분야를 사이버보안 전략에 포함시키고, 관련 솔루션이나 정책을 개발할 때 유럽철도산업연맹과의 협력이 필요하다.

4) CENELEC TC 9X 워킹그룹에게

철도분야에 IEC 62443(산업자동화 및 제어시스템 보안, Security for industrial automation and control systems) 적용을 위해, 기술사양 TS 50 701을 종결하고 발행해 주기를 바란다.

5. 결론

본 문서에서는 철도분야의 사이버보안 도전적 요소들이 단기, 중기, 장기로 구분되어 분석되었다. 철도분야에서의 첫 번째 단계는 곧 사용하게 될 유럽전기표준화위원회(CENELEC) 기술사양(Technical Specification)을 명확하고 강력하게 만드는 것이다. 본 문서는 새로운 기술개발과 요구에 의해 정기적으로 업데이트될 예정이다.

<원문제목> UNIFE Vision on Cyber-Security in Railways

<원문출처> UNIFE