

Global Report

철도 사이버보안에 대한 유럽철도산업연합의 입장

1. 유럽철도산업연합(UNIFE)에 대하여
2. 도입
3. 추진경과
4. 유럽 철도분야를 위한 도전
5. 핵심 메시지와 권고사항

1. 유럽철도산업연합(UNIFE)에 대하여

- 1992년부터 브뤼셀에 기반을 둔 유럽철도산업연합(UNIFE, Association of the European Rail Industry)은 유럽연합과 세계 차원에서 유럽의 철도 조달산업계를 대표하는 연합조직이다. 회원으로는 철도차량(지역철도, 도시철도, 트램, 화차 등)과 철도신호 그리고 인프라시설용 장치를 설계, 엔지니어링 및 제작하는 중소기업부터 대형 기업까지 약 100개 이상의 기업이 참여하고 있다. 또한, 11개 유럽연합의 국가 철도산업 연합체와 협력하고 있다.
- 경제성장과 산업계의 리더십에서 핵심적인 역할을 하는 철도 공급산업 : 4십만 개의 일자리를 공급하고 연간 470억 유로의 판매실적을 유지하며 계속적으로 환경적으로 우수한 제품제작을 늘리고 전 세계에 판매하는 유럽의 철도차량 제작회사와 철도용 장치 조달회사들은 유럽연합 산업계의 경쟁력과 지속가능성 유지에 핵심적 역할을 한다.
- 유럽연합 그린딜(Green Deal)의 핵심요소인 철도 : 유럽연합 그린딜은 2050년까지 기후중립을 지향하는 유럽의 진로이다. 현재 유럽의 모든 배출량의 거의 1/4를 담당하고 있는 교통분야의 탈탄소화 없이는 이 목표 달성은 불가능할 것이다. 철도는 교통분야에서 예외로 취급되는 바, 지난 20년간 점차적으로 탄소발자국을 감소시켜 왔고 에너지 효율성을 개선시켜 왔다. 이용할 수 있는 가장 지속가능한 대중교통 수단으로서 철도는, 가장 기후친화적인 방식으로 모든 지역을 연결하려는 희망을 현실화시키려는 유럽연합의 계획에 매우 핵심적인 요소임에 틀림없다.

2. 도입

- 유럽철도산업연합(UNIFE)이 수립한 사이버보안에 대한 비전은 유럽의 철도시스템의 모든 자산에 디지털 혁신을 계속적으로 통합시키기 위한 유럽 철도 조달산업계의 도전과제에 대한 평가를 나타내는 것이다. 또한, 이번 조사는 단기, 중기 그리고 장기적 기준으로 우선추진사항과 목표를 설정한 것이다. 유럽연합의 관련기관과 다른 철도 이해관계자들과 더욱 협력하기 위한 일련의 권고사항도 제안하고 있다.

3. 추진경과

3-1. 사이버보안 : 유럽 철도 공급산업계를 위한 우선 추진사항

- 유럽 철도 조달산업계는 안전하고 신뢰성 있는 철도와 도시철도 대중교통을 유지하기 위해서 사이버 위협을 완화시키는 것이 매우 중요하다고 인식하고 있다. 이 사이버위협은 복잡한 상호의존성과 예전에 설치된 인프라시설 요소를 감안할 때 작은 위협이 아니다. 사이버보안은 이러한 모빌리티 시스템을 효과적으로 적용하고 연결된 디지털 환경과 완벽하게 조화시키기 위해서는 핵심적인 필요조건이다. 간선철도와 도시철도 시스템 양쪽 모두를 통합하고 운영상의 연속성 기준을 유지하는 것은 모든 분야에서 공유해야 할 목표이다.
- 사이버보안 위협은 국경을 넘어서는 문제이며, 한 나라의 핵심 인프라시설에 대한 사이버 공격은 유럽연합 전체에 쉽게 영향을 미친다. 결과적으로, 회원국들은 자신의 통치구역 내에서 사이버보안 조치를 수행할 수 있고 정보교환을 통해 다른 회원국의 해당기관과 협력할 수 있는 강력한 정부기관을 보유해야 한다. 이것은 사회에서 정상적이고 활동에 방해받지 않아야 하는 아주 중요한 분야에서는 특히 중대한 문제이다. 철도는 필수적인 승객과 화물을 수송하는 것과 관련된 위험과 원격통신 네트워크에 매우 의존하는 방대한 시스템 때문에 매우 중요한 분야로 인식되고 있다.

3-2. 정책과 규정 프레임워크

- 만약 사이버보안 관련 법률이 개정되거나 신설될 경우에, 유럽연합 디지털 싱글마켓 전략(EU Digital Single Market Strategy) 수립이 프로세스와 솔루션을 조화시킬 것으로 예상된다.

- 그런데, 철도분야는 모든 운영상황에서 사이버보안과 관련된 프로세스에 대한 깊은 이해가 필요한 복잡한 규정적 프레임워크에 직면하게 된다. 더욱이, 디지털화는 철도교통을 변환시켰는데 특히, 운영 측면, 인프라시설 측면 그리고 대중교통 측면에서 뚜렷한 전환을 이루어 내었다. 또한, 상호호환성의 실현을 촉진시키는 중이다. 그러므로 사이버보안 요구조건의 실행은 철도분야의 디지털적 성능 향상과 보안을 위해서는 기본적인 것이다.
- 유럽연합 차원에서, 사이버보안 정책과 법률적 프레임워크는 정상적인 페이스로 변화 중이며 유럽 전체 차원에서 더욱 일관성 있고 조화로운 사이버보안 관리 문제를 해결하기 위해 몇 개의 이니셔티브가 시작되었다. 이러한 이니셔티브 중에서 가장 우선적인 것은 [일반 데이터 보호 규정](GDPR, General Data Protection Regulation), [사이버보안 법](Cybersecurity Act) 그리고 [유럽연합 사이버보안 전략](EU Cybersecurity Strategy)이다. 가장 중요한 것 중의 하나인 마지막 문서는 [네트워크 및 정보 보안 규칙](NIS2, Network and Information Security Directive) 개정판과 [핵심 시설의 복원성 규정](Resilience of Critical Entities Directive)으로 구성되어 있다. 이러한 요구조건은 철도의 특정한 규정적 범주에 적용되는데 예를 들어, [유럽철도교통관리시스템](ERTMS, European Railway Traffic Management System)의 탄력성 향상과 2022년까지 [상호호환성을 위한 기술 규정](TSIs) 개정안 내에서 데이터와 메시지 교환을 위한 [화물/여객 서비스를 위한 텔레매틱스 적용](TAF/TAP, telematics applications for freight and passenger services) 규정의 추가적인 도입과 같은 특정한 활동이 해당된다.
- 모든 신규 사이버보안 정책과 규정 제안은 [신규 법률적 프레임워크](New Legislative Framework)를 구성하게 되는데, 이것은 국가적 차원에서 실행될 때 도전적인 문제가 될 수 있고 스케줄과 규정에 일치시키기 위해 복잡해질 수 있으며 조화로운 프로세스를 만들기 위해 긍정적으로 기여할 것이다.

3-3. 유럽 철도 공급산업계가 직면하는 사이버보안 도전

- 정책과 규정 프레임워크에 추가로, 사이버보안 문제는 기업들이 정보통신기술(ICT, Information and Communication Technology) 제품과 서비스를 책임져야 하는 책임성 문제도 제기될 가능성이 있다. 왜냐하면, 그것들의 복원성은 가치사슬을 따라 모든 이해관계자와 관련이 있기 때문이다.
- 사이버보안 솔루션이 도입되고 시행되는 속도는 민간과 공공 모두의 리소스에 밀접하게 관련되어 있다. 이 솔루션들은 공공기관에서부터 민간 기업까지 모든 유럽의 이해관계자들이 사이버 범죄를 예방하거나 싸울 수 있도록 신기술과 서비스를 신속하고 광범위하게 적용하기 위해 할당되는 것이다.
- 현재, 모든 탈탄소화 프로젝트는 스마트 디지털화 전략과 연결되어 있다. 사이버보안에 소요되는 비용은 디지털화된 매우 중요한 인프라시설을 보호하기 위한 투자의 일부로 간주되어야 한다.
- 사이버보안 환경이 끊임없이 진화하고 있다는 사실은 잘 이해되고 있다. 현재의 사이버-복원성(cyber-resiliency) 수준은 전체 시스템에서 개별적으로 아주 중요한 비즈니스 자산, 위협의 범위 그리고 이용 가능한 사이버 능력의 성숙도 측면에 대한 총합이다. 이러한 모든 것이 운영, 관리 및 실행적 목적을 위해 취해지는 조치와 커스터마이징된 사이버보안 인식을 통합하도록 고려되고 이끌어져야 한다.
- 유럽의 철도분야 내에서 사이버보안의 조화를 위한 견고한 기준선을 제정하기 위해서는 여러 가지 방법이 존재한다.

<1> 유럽전기표준화위원회(CENELEC, Committee European de Normalization Electrotechnique)를 통한 유럽연합 차원의 표준화 : 유럽전기표준화위원회(CENELEC)의 위원회 중의 하나인 [CENELEC TC 9X]는 워킹그룹 26(Working Group 26)에게 기술사양(CLC/TS 50 701) 발간의 임무를 부여했고 2021년 7월에 발간되었다. 이 기술사양은 광범위하게 수용되어 있는 국제전기기술위원회(IEC, International Electrotechnical Commission) [IEC 62443] 표준 즉, [산업용 자동화 및 제어시스템 보안](Security for industrial automation and control systems) 표준을 철도분야에 적용한 것이다. [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS

50701:2021 철도분야 - 사이버보안)는 철도분야에서 핵심적인 시금석이 될 것이다. 왜냐하면, 이 표준은 철도차량, 신호 그리고 인프라시설을 포함한 모든 서브시스템에 적용가능하기 때문이다.

<2> 유럽연합 차원에서의 법률 프레임워크 : 유럽은 유럽연합의 디지털 변화에 아주 중요한 신기술을 규정하는 입법화 작업에 우선순위를 두었다. 몇 가지 규정화 이니셔티브가 네트워크화가 가능한 제품과 서비스 보호를 위한 노력의 초석으로 이미 사이버보안에 초점을 두고 있다. 규정의 일관성을 보장하는 것이 [네트워크 및 정보 보안 규정](NIS2, Network and Information Security Directive) 개정판의 핵심 목표가 되어야하며 특히, 그 범위의 확장을 지향해야 한다. 동시에 진행되고 있는 법률화 제안은 집합적으로 사이버보안 복원성을 만들면서 회원국 사이에서 파편화되는 상황을 막는 것이 목표이다. 그런데, 수평적이고 수직적인 법률적 도구들은 충분하게 조화되어야하고 규정의 중점은 되도록 피해야 한다. 이 목표의 달성을 위해, 관련된 [네트워크 및 정보 보안 규정](NIS2)의 영역과 특정 분야의 법률화 작업 간에 충분한 협력이 반드시 강조되어야 한다.

<3> 철도분야 내부에서의 협력 : 유럽철도산업연합(UNIFE)은 유럽 철도 조달산업계의 사이버보안 비전의 보고자로서 중요한 역할을 하고 있으며, 사이버보안 워킹그룹 활동을 통해 기업 간의 대화도 촉진하고 있다. 추가로, 2019년 초 유럽연합집행위원회 산하 [통신 네트워크, 콘텐츠 및 기술국](DG CONNECT, Directorate-General for Communications Networks, Content and Technology)과 [모빌리티 및 교통국](DG MOVE, Directorate-General for Mobility and Transport)이 철도분야의 디지털화 우선순위를 논의하기 위해 공동으로 조직한 [디지털 철도 라운드 테이블](Digitisation Rail Roundtable)을 쫓아, 유럽철도산업연합(UNIFE)은 철도분야 전체에 걸쳐 전문가들을 참여시킨 사이버보안 작업 흐름을 조직했다. 유럽연합과 국가 차원 모두에서 진행 중인 철도분야 사이버보안 법률화 이니셔티브, 현재의 표준화와 규정의 환경 그리고 연구 및 기술혁신(R&I, Research & Innovation) 활동에 대한 분석을 시작으로, 이 집단적인 노력은 유럽연합집행위원회에 4가지 핵심 권고사항을 제출하는 성과를 도출했다. 철도분야 전체에 걸친 그리고 유럽연합 기관과 함께 하는 협력은 유럽의 철도분야를 보호하기 위해 학습한 교훈들이 반영된 동질의 결과를 이루어내는데 핵심적인 문제이다.

<4> 연구와 기술혁신(R&I, Research & Innovation) : [Horizon Europe] 프로젝트 산하의 미래 서브프로젝트와 미래 [유럽 철도 민관합동 연구](ER JU, Europe's Rail Joint Undertaking)를 포함하여 유럽연합이 자금을 지원하는 연구와 기술혁신(R&I) 프로젝트에의 참여를 통한 횡단협력의 진행 : 과거 그리고 현재 진행 중인 철도 연구와 기술혁신(R&I) 프로젝트들이 이미 철도 사이버보안 요소를 다루고 있다는 것을 밝히는 것이 중요하다. 예를 들어, [Roll2Rail], [CONNECTA] 그리고 [X2Rail] 프로젝트와 같은 [S2R JU](Shift2Rail Joint Undertaking) 프로젝트들은 열차제어모니터링 시스템(TCMS, Train Control and Monitoring Systems)과 사이버보안에 관련된 연구를 완료했다. 또한, [4SECU Rail] 프로젝트는 철도분야를 위해 [사이버 보안사건 대응팀](CSIRT, Cyber Security Incident Response Team) 모델을 개발하여 성공적인 결과를 내고 있다. 이러한 모든 사례와 이니셔티브들은 우리의 집단적 보안을 위한 협력 연구와 기술혁신(R&I) 프로젝트의 중요성을 보여준다. 사이버 위협이 계속적으로 일어나는 것을 고려할 때, 비슷한 횡단 협력이 [Horizon Europe] 프로젝트 산하의 미래 프로젝트와 미래의 [유럽 철도 민관합동 연구](ER JU)의 형태로 생겨날 것으로 예상된다.

<5> 가장 최신의 트렌드에 대한 모니터링 : 철도는 유럽 철도시스템의 사이버보안에 영향을 미칠 수 있는 예측과 협력을 보장하기 위해 슈퍼컴퓨팅, 암호해독 기술, 양자 컴퓨팅, 블록체인 그리고 인공지능과 같은 핵심 분야의 중요한 기술적 발전에 대한 인식을 계속 진행해야 한다.

<6> 철도분야의 고유한 특수성 - 기존의 시스템 : 철도분야는 사이버 공격의 위험성을 증가시키는 디지털 전환이 진행되고 있기 때문에, 철도 이해관계자들은 운영적 요구, 비즈니스 경쟁력, 새로운 기술과 사이버보안의 적용 등의 균형을 맞추는 필요가 있다. 철도분야의 규정적 복잡성은 철도시스템 내의 운영기술(OT, Operational Technologies)을 빨리 쇠퇴시키거나 구식이 되도록 만드는

데, 그 이유는 개념 파악을 진행할 때는 안전한 접근법으로 고려되는 것에 기반을 두지만 일단 사용되는 기술이 전체를 커버하게 되면 쉽게 바이패스되는 경향이 있기 때문이다. 이것은 도입되는 운영기술(OT) 시스템을 최신의 사이버보안 요구조건에 일치시키는 작업을 어렵게 만든다. 더욱이, 이 시스템들의 다른 위치(보통 정거장에서 네트워크 전체에 걸쳐, 궤도를 따라서, 온 나라 전체에 걸쳐서 그리고 철도차량과 차량탑재 온보드 시스템 내와 같은 이동형 자산 등의 서로 다른 위치에 존재함)는 포괄적인 사이버보안 제어를 어렵게 만든다. 새로운 철도 규정을 도입할 때 사이버보안을 고려하는 것은 요구사항에 대한 더욱 일관된 검토를 가능케 한다.

4. 유럽 철도분야를 위한 도전

4-1. 1년~3년 내 높은 우선순위를 가진 단기적인 도전

① 표준화와 규정 문제

- 유럽전기표준화위원회(CENELEC) [CENELEC TC 9X] 워킹그룹 26(Working Group 26)이 개발한 기술 사양(CLC/TS 50 701)이 철도분야를 위한 인증제도로 고려되어야 한다.
- [사이버보안법](Cybersecurity Act) 2019/881을 근거로 설립된 [유럽연합 사이버보안국](ENISA, European Union Agency for Cybersecurity)은 유럽의 기술(정보통신) 제품, 프로세스 그리고 서비스를 위한 사이버보안 인증 프레임워크 개발을 위임받았다. 제품, 서비스 또는 프로세스의 사용계획과 관련된 위험수준에 기반을 두고, 하나 또는 여러 개의 보증수준(기본, 중요 또는 높음)을 규정하는 각각의 계획이 진행될 것이다. 제안된 프레임워크는 (일부 경우에) 사물인터넷(IoT, internet of things) 내부로 플러그인이 가능하도록 유럽연합 시장 내에서 또는 유럽연합 시장을 위해 제작된 제품과 연결된 제품이 설계단계부터 사이버보안 조치를 담고 개발되거나 ‘설계에 의한 보안(security by design)’ 개념을 사용하여 창조되도록 보장할 것이다. 필요하다면, 철도분야는 인증에 부합할 수 있는 아주 중요한 특정 정보통신기술 서비스, 시스템 또는 제품에 동의하거나 보안과 관련된 인증을 해 주는 인증 형식에 대해 동의를 해야 할 것이다.
- 철도분야 내부에서, [CENELEC TC 9X] 워킹그룹 26(WG 26)은 신호, 철도차량 그리고 고정 시설물을 포괄하는 [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안) 표준을 개발했다. 이 신규 [CLC/TS 50701]는 철도 정보통신기술 제품과 서비스 그리고 프로세스를 위한 동질의 인증제도 창조를 위한 기초 역할을 해야 한다.
- 이것이 단기적인 장애물을 없애는 가장 유력한 방법이다. 철도분야 전체적으로 단일한 방식으로 사이버보안을 다루기 위한 기술 사양(TS, Technical Specification)이 이러한 요구를 만족시킬 수 있을 것이다. 그리고 이 기술 사양은 기존에 존재하는 산업용 사이버보안 표준(예를 들어, IEC 62443)에 기반을 두어야 한다.
- [CLC/TS]는 기업들에게 전체적으로 수용되어야 한다. 처음에는 프로젝트 단위로 시행될 것이지만, 장기적인 목표는 리스크에 기반을 둔 접근법이 잠재적인 위협을 알려주는 것을 포함한 프로세스 자체가 인증받는 상태를 지향한다. 기술 사양(TS)을 적용하고 관련 데이터가 수집되며 서류화되어야 할 뿐 아니라 프로젝트를 [CLC/TS]에 점차적으로 적용시키는 로드맵도 수립되어야 한다.
- 최종적으로, 일단 표준이 준비되면 인증기관이 필요한지 여부가 결정되어야 한다. 그 경우에는, 안전 승인 프로세스와의 관계가 조정되어야 할 것이다. 이 안전 승인 프로세스는 4차 철도 패키지(4th Railway Package)의 [Technical Pillar] 때문에 개별 국가기관에서 유럽연합 철도국(ERA, European Union Agency for Railways)으로 이전된 바 있다. 이것은 안전과 보안의 서로 다른 필요조건을 만족시키는 조화롭고 적절하며 잘 정리된 접근이 되어야 한다.

- [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안) 내에서 철도 이해관계자들의 인식 향상
 - 위 섹션에서 언급한 것처럼, 철도분야의 특수한 도전은 단기적으로 해소시키고 동일한 출발지점에 서야 한다. 이것을 적절하게 해소하기 위해, 유럽연합의 모든 철도 이해관계자들이 [CLC/TS 50701]에 규정된 최소한의 기준에 대한 인식 확대가 특히 중요하다. 이것을 통해, 유럽 철도분야는 철도 네트워크를 따라 같은 방식으로 이 표준을 알고 정확하게 적용할 수 있을 것이다.
 - 이것은 모든 철도산업을 고려하는 수평적인 접근법으로 뿐만 아니라 철도분야의 사이버보안에 기여하는 모든 직원들을 책임지는 수직적인 접근법으로도 진행되어야 한다.
 - 이를 달성하기 위해, 철도분야 내에서 이 접근법을 고려하고 그것을 최소한의 사이버보안 필요조건 세트를 모으기 위한 일반적인 프레임워크를 제공하기 위한 워크숍과 교육훈련이 진행되어야 한다.

- [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)을 세계적인 표준으로 이전시키고 독려
 - 위에 언급된 유럽전기표준화위원회(CENELEC) [CLC/TS]는 이에 기반을 둔 세계적인 표준으로 만들기 위해 국제전기기술위원회(IEC, International Electrotechnical Commission)로 이전시킬 필요가 있다. 이 프로세스는 6년 정도 소요될 것이다.
 - 만약 이 작업이 완료되면, 경쟁력과 효율성이 증대되어 시장 접근이 원활해지고 무역비용을 절감하며 계약적 합의를 단순화시키고 품질이 향상될 것이다.

- 유럽전기표준화위원회(CENELEC) 표준화 작업과 유럽연합 연구와 기술혁신(R&I) 프로젝트의 융합(예를 들어, 미래의 철도 민관협력 사업, [Horizon Europe] 등)
 - 유럽의 철도 민관협력 사업(Rail Joint Undertaking)과 같이 [Horizon Europe] 내에서 유럽전기표준화위원회(CENELEC)와 유럽연합 연구와 기술혁신(R&I) 이니셔티브와의 협력이 필요할 것이다. 유럽연합 연구와 기술혁신(R&I) 이니셔티브에 의해 이루어진 성과는 나중에 새로운 유럽표준 개발에 사용될 수 있을 것이다. 표준화 활동 과정에서 확인된 잠재적인 이슈는 새로운 철도 연구과제 개발에 도움이 될 것이다. 이 협력은 강력하게 진행되어야 한다.

- 유럽철도산업연합(UNIFE)은 차기 [제어명령 및 신호](CCS, Control Command and Signalling) 상호호환성 기술기준(TSI, Technical Specifications for Interoperability) 준비에 사이버보안을 위치시키고 신규 및 기존 상호호환성 기술기준(TSI)에서 적절하게 해소되도록 보장해야 한다.
 - [제어명령 및 신호](CCS) 상호호환성 기술기준(TSI)과 관련하여, 유럽철도산업연합(UNIFE)은 신호산업연합(UNISIG, Union of Signalling Industry)을 통해 [Shift2Rail Innovation Programme 2] 및 시스템을 취급하는 유럽연합 철도국(ERA) 코디네이션 그룹과 협력하여 미래의 유럽철도교통관리시스템(ERTMS, European Rail Traffic Management System) 개발에 적극적으로 참여하고 있다. 가장 중요한 이행과제는 열차자동운전(ATO, Automatic Train Operations), 레벨 3의 유럽철도교통관리시스템(ERTMS), 미래 철도 모바일 통신시스템(FRMCS, Future Railway Mobile Communication System)과 사이버보안 문제이다. 후자와 관련하여, 핵심 목표는 유럽이 가장 경제적인 방식으로 의존하고 있는 신호 및 통신시스템에 가해지는 어떠한 중요한 위협에 대응하는 최적의 보호수준을 확보하는 것이다.
 - 특히, 수정된 [제어명령 및 신호 상호호환성 기술기준](CCS TSI) 2022 하에서, 유럽연합 철도국(ERA)과 철도분야 조직 모두는 현재의 유럽철도교통관리시스템(ERTMS) 사양에 의해 제공되는 보호수준을 평가하고 5G에 기반을 둔 미래 철도 모바일 통신시스템(FRMCS)과 같은 게임 체인저가 되는 중요기술과 관련된 추가적인 요구조건에 맞게 그것들을 준비해야 한다.
 - 추가로, 사이버보안은 [제어명령 및 신호](CCS) 및 [화물 및 여객서비스를 위한 텔레매틱스 적

용](TAF/TAP, Telematics Applications for Freight/Passenger Services) 상호호환성 기술기준(TSI)에 대한 신규 및 개정안의 개발과정에서 적절하게 규정되어야 한다. 유럽철도산업연합(UNIFE)은 아래의 미래의 보안 디자인과 적용될 비용 기준에 찬성한다. 즉, 데이터 통합의 강력한 보호(안전), 이용가능성(availability, 운영 성과)과 비밀유지성(confidentiality)이 그것이다. 상호호환성, 하위호환성(backward compatibility, 장기적인 이전) 그리고 표준기술의 사용은 유지보수성과 업그레이드의 원활성을 보장할 것이다. 반대로, 시스템 간의 상호의존성과 불필요한 복잡성은 피해야 한다. 또한, 실행, (재)인증을 위한 운영 그리고 승인비용도 낮게 유지되어야 한다.

② 법률적, 정책적 프레임워크

- 새로운 법률적 프레임워크 내의 일관성
 - 디지털화의 증가 그리고 그로 인한 사이버보안 수준의 격상이라는 현상을 통해 유럽이 직면하고 있는 기회와 도전을 만족시키기 위해 정치적, 법률적 프레임워크가 급속도로 변하고 있다. 위에 언급한 것처럼, 정책과 법률적 프레임워크 내에서 고려되고 있는 사이버보안을 다루는 몇 가지 법률 이니셔티브가 진행되고 있다.
 - 비록 위의 법률적 이니셔티브가 합법적인 사이버보안 문제를 다룬다고 할지라도, 그것들은 유럽의 철도 이해관계자들을 위한 요구조건에 혼란을 주거나 중복되는 규정상의 파편화가 발생하지 않도록 조화될 필요가 있다. 잘 조화가 이루어진 새로운 규정 프레임워크 내에서, 네트워크화가 가능한 제품의 수평적 사이버보안 법제화의 도입은 사이버보안 향상에 매우 효과적이고 많은 이익이 될 것이다.

③ 철도 이해관계자 간의 협력

- 모든 철도 이해관계자들 간의 우수한 협력체계 구축과 [정보공유 및 분석센터](ISAC, Information Sharing and Analysis Centre) 설립
 - 사이버보안은 국경이 없고 사이버공격도 마찬가지이다. 모든 철도 이해관계자들은 유럽연합 내부에서 그리고 글로벌 차원에서 모두 우리 분야에 영향을 미치는 가장 최신의 위협에 보조를 맞추기 위해 협력할 필요가 있다.
 - [정보공유 및 분석센터](ISAC) 이니셔티브는 유럽연합집행위원회와 유럽연합 사이버보안국(ENISA)이 주창한 것이다. 이러한 플랫폼을 통해, [유럽철도-정보공유 및 분석센터](ER-ISAC)는 유럽연합의 모든 회원국 철도 이해관계자들에게 개방되어 있다. 유럽철도산업연합(UNIFE)은 [유럽철도-정보공유 및 분석센터](ER-ISAC)의 활동을 지원하고 있으며, 철도 생태계 내에서 전혀 다른 요소 간에 정보교환을 향상시키기 위해 개발되고 긍정적인 대화가 유지하기를 원한다. 그럼에도 불구하고, 인프라시설 관리자, 철도 운영기관 그리고 철도 조달산업계 등 철도분야의 특정 영역을 포함한 새로운 필수 조직(essential entities)과 중요 조직(important entities) 카테고리에 관련된 [네트워크 및 정보 보안 규칙](NIS2, Network and Information Security Directive)의 제안내용에 대해서는 협력과 정보공유가 반드시 필요하다.
 - 이러한 플랫폼의 목표는 특히, 매우 중요한 인프라시설과 관련된 사이버위협에 대한 정보수집의 핵심 자원을 제공하는 것이다. 또한, 근본원인, 사고 그리고 증가하는 위협에 대해 민간분야와 공공분야 사이에 상호 정보가 교환되도록 해야 하며, 경험, 우수사례, 지식 그리고 분석결과에 대한 원활한 공유를 이루어야 한다. 밀접한 협력에 기반을 둔 이러한 구조는 철도분야의 사이버보안 준비와 인식을 개선하는데 핵심적인 사항이다.

④ 철도 조달산업계에 걸친 사이버보안

- 유럽연합과 개별국가 차원에서의 일반적인 접근법을 통해 적절한 철도 조달 사이버보안의 보장
 - 공급망 데이터의 통합과 제품 안전을 보장하기 위해, 유럽 철도 조달산업은 모든 요소들이 목표를 공유하고 효과적이고 조화로운 보안조치를 수행할 때 진실로 안전하며 이것이 글로벌 경제의

보안에 이바지하는 것이다.

- 새로운 강제적인 조치들이 신 사이버보안 규정 프레임워크(New Cybersecurity Regulatory Framework)에 의해 만들어졌다. 그것들 중에는, [네트워크 및 정보 보안 규칙](NIS2) 제안에 따라 공급망 보안 평가를 수행하기 위해 몇 가지 요구사항 도입을 강제하며, 공급망 전체에 걸친 정확한 보안 평가를 요구하고 있다. 이러한 평가는 리스크에 기반을 두고 비차별적인 것으로, 회원국 간에 조화로운 접근을 통해 경쟁력있고 조화로운 하나의 시장을 가능케 하기 때문에 매우 중요한 것이다.
- [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)에 기술된 것처럼, 프로세스의 도입과 함께 전체 철도공급망을 보호하는 것이 중요하다. 철도 조달기업들이 사이버보안 평가에 참여하고 안전한 제품과 서브시스템을 어떻게 창조할 것인지를 알게 될 때, 보안 목표의 실행은 가능하다.
- 동일한 접근법을 통해 철도공급망 전체에 걸쳐 정확한 사이버보안 수준을 보장하는 것이다. 개별 기업들이 사이버보안 프레임워크 필요조건을 만족시키기 위해 필요한 자원과 비용은 얼마 되지 않을 것이다.
- 유럽철도산업연합(UNIFE) 회원들은 완성된 철도시스템 내에서 보안사양과 프로세스를 도입하는데 이바지할 수 있다. 그런데, 이러한 기준은 종종 수직적인 접근법과 함께 출발한다. 결국, 공동의 리스크 평가 프레임워크를 가지기 위해서는 철도분야 전체의 협력이 필요하다.

⑤ 연구와 기술혁신

- 사이버보안에 대한 연구 및 기술혁신을 위한 투자의 증가
 - 사이버위협은 계속 증가하고 급속도로 발전하고 있지만, 아직까지 새롭고 효과적인 사이버방어 기술의 성장은 더딘 것이 현실이다. 사이버범죄가 심오한 공격기술을 계속 배치하고 있고 예측하기 힘든 힘과 리소스 그리고 글로벌 차원으로 사이버범죄를 진행하기 때문에, 위협과 방어 방법 간의 차이가 더 넓어지고 있다.
 - 이러한 상황에 대응하여, 신속하게 혁신적인 사이버수비 개념을 도입하기 위해 ‘시장 출시’(time to market)를 단축시킬 필요가 있다.
 - 나날이 증가하는 사이버위협에 대항하는 적합형 방법과 전략이 가장 최신의 사이버보안을 능가하는 방식으로 개발되어야 하고 이러한 사이버위협을 예측할 수 있어야 한다. 결국, 다른 유럽의 철도 이해관계자 간에 협력적인 연구를 통해 새로운 수비방식의 전략 개발을 지원하기 위한 연구와 기술혁신 사업에 더 많은 투자가 필요하다. 이러한 경쟁력을 확보하기 위해서는, 미래의 유럽 철도 민관협력 연구(Europe’s Rail Joint Undertaking)와 [Horizon Europe]이 핵심적인 도구가 될 것이다.

⑥ 철도분야 내에서 사이버보안의 특이성

- 사이버보안의 하나의 축으로 암호기법(cryptography)을 고려하라
 - 암호기법은 비밀유지성, 통합 그리고 인증을 보장하는데 중요한 역할을 한다. 예를 들어, 백도어(‘Backdoor’란 인증자와 비인증 사용자 모두 정상적인 보안 조치 접근이 가능하고 높은 수준의 사용자 액세스 권한 획득이 가능함을 의미함)로 암호를 약화시키는 것은 불안정한 시스템을 만드는 매우 위험한 방식이다. 단대단 암호화(end-to-end encryption, 데이터 통신에서 발신 측에서 데이터를 암호화하고 수신지에서 부호화하는 방식) 방식에 더불어, 우리는 적절한 암호화 코드 서명 메커니즘과 관련 평가 인프라시설을 보유하기를 권고한다. 추가로, 양자내성(postquantum) 디지털 서명과 제품에서의 암호화 민첩성(crypto agility)을 위해 필요한 예상되는 신규 표준의 신속한 보급을 준비하는 것이 중요하다.
- 기존 철도시스템은 적절한 리스크 수용 평가가 필요할 것이다.

- 유럽 철도분야는 많은 기존시스템을 관리하고 있다. 일부는 새로운 법률적 프레임워크(New Legislative Framework)에 의하면 구식으로 설계된 것이다. 예를 들어, 일부 신호 및 철도차량은 수명주기가 몇 십 년으로 계산되는 것으로 분류되고 있다. 새로운 사이버보안 조치에 일치하기 위해서는, 기존시스템에 대한 적절한 리스크 수용 제도와 평가가 필요하다.
 - 이것은 보완적인 대응조치의 하나인 공격 보호 시스템과 같은 프로그램의 추가 설치로 결론이 날 수도 있다. 이러한 시스템을 개조하는 것은 높은 수준의 투자가 필요할 것이다.
 - 또한, 이러한 기존시스템을 위해 다른 종류의 인증제도를 만들 가능성도 있다. 이것은 최소한의 취약성 평가(vulnerability assessment) 수용을 통해 시행될 수 있을 것이다.
 - 신제품과 서비스를 위해, [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)에 수립된 것처럼 사이버보안과 대응조치를 포함하는 수명주기 관리가 계획되고 신규 시스템에 대한 예측이 가능해야 할 것이다.
- 허용된 패치 관리를 통해, 안전한 환경에서 철도 유지관리의 개선
- 시스템 전체 수명주기에서 인정할만한 사이버보안 수준을 유지하는데 필요한 조직적, 기술적 방법은 우리 분야에 매우 보편적이다. 철도에서의 조직적, 기술적 시스템은 종종 설치될 때 안전을 보장하는데 사용되는 파라메타에 기반을 두고 있지만, 시스템이 가진 긴 시간의 수명주기 때문에 사이버보안 관점에서는 구식이 되거나 낡은 것이 되었다.
 - 사이버위협이 급속도로 증가함에 따라, 시스템은 단기적으로도 더 이상 안전하지 않을 수 있다. 이러한 시스템들은 정확한 패치 관리시스템을 신속하게 설치함으로써 명확하게 안전이 보장되어야 한다. 이것은 철도분야에는 도전적인 일로, 아무리 중요한 어떠한 변화라고 할지라도 적용될 경우에는 반드시 분석되고 인증이 필요하기 때문이다. 이것은 철도 안전에 변화를 줄 수 있는 영향을 분석하는데 필요한 시간을 확보해야 하므로 어려운 일이다.
 - 중요한 핵심적인 문제는 이러한 시스템의 안전을 방해하지 않는 안전한 조건에서 신속하고 정련된 유지관리를 가능하게 만드는 패치 관리시스템을 성공적으로 규정하는 것이다.

4-2. 4~6년내의 중기적인 도전

- 양자 보안(Quantum-Secure) 및 암호화 민첩성(Crypto-Agility)
- 양자 기술이 더욱 심오해짐에 따라, 이 기술은 점차 보안과 공공의 핵심 암호 패러다임에 대한 위협을 증가시킬 것이다. 만약 충분한 대형 양자 컴퓨터가 만들어진다면, 그것은 기존의 인프라 시설과 네트워크를 보강하는 특정 공공 핵심 암호('Cryptography'는 정보를 읽고 프로세싱할 수 있도록 의도된 사람들에게만 이용이 가능하도록 코드 사용을 통해 정보와 통신을 보호하는 방식이다.)와 비대칭형 암호화('Asymmetric cryptography'는 암호화의 두 번째 형태이다. 이것은 데이터가 다른 통신 파트너들 사이에서 자주 교환되는 데이터가 있는 매우 크고 계속 확장되는 환경에서 사용효율성이 높다.)를 파괴할 수 있을 것이다.
 - 유럽 철도 공급산업은 대용량의 양자 컴퓨터를 이용할 준비가 되기 전까지 그들의 정보통신 인프라시설을 '양자-보안'(Quantum-Secure) 상태로 준비할 필요가 있다. 데이터를 보호하는 것은 단기적으로는 기존의 고전적인 컴퓨터와 재암호 데이터에 포스트-양자 암호(Post-Quantum Cryptography) 즉, 양자에 대응하는 알고리즘(quantum resistant algorithms)을 도입하는 것과 관련된다.
- 멀티모달 모빌리티를 보호하는 기술의 개발
- 디지털화는 멀티모달 교통을 이루기 위한 추진체로 세팅되어, 그 안에서 항공, 철도, 도로 그리고 해상을 이용한 이동은 통합될 것이다. 이것에는 서로 다른 정보통신 시스템과 운영기술 시스템의 통합과 각자가 가진 사이버보안 방법의 조화가 필요할 것이다. 오늘날, [V2X] 기술과 5G 통신기술을 적용하여 지속가능하고 스마트한 멀티모달 교통을 제공하기 위해 [S2R JU](Shift2Rail Joint Undertaking) 프로젝트 내에서 이러한 주제에 대한 연구가 진행 중이다. 이 연구는 미래의 유럽

연합 민관합동 연구(ER JU) 내에서 계속되어야 할 것이다.

- 규정과 표준화 관점에서, 서로 다른 교통수단과 운영기술 시스템은 자체의 표준과 인증을 가지고 있다. 그런데, 이러한 운영기술 시스템을 운영하는데 필요한 정보통신 시스템이나 클라우드 제공 기업은 우리가 멀티모달 능력을 향상시킴에 따라 융합이 필요할 것이다. 이러한 시나리오 상에서, 모든 시스템이 [네트워크 및 정보 보안 규칙](NIS2, Network and Information Security Directive) 제안과 잘 조화된 법률적인 프레임워크 아래에서 커버되는 것이 필수적이다.
- 강력한 사이버보안 표준 기준을 철도에 적용되는 모든 신기술에 포함 - 가까운 미래에 더욱 안정적인 시스템 구축
 - 우리가 디지털 혁명을 계속 진행함에 따라, 새 세대의 파괴적인 기술이 새로운 전환의 길을 만들었다. 가장 영향력 있는 떠오르는 기술 중의 일부는 인공지능(Artificial Intelligence), 스마트 유지관리(Smart Maintenance), 사물인터넷(IoT) 그리고 디지털 트윈(Digital Twins) 기술이다. 여러 가지 기술 중에서 이 기술들은 철도분야에서 미래를 위해 준비된 운영기술 제공을 약속하고 있다. 이러한 기술들은 엄청난 양의 데이터가 필요하고 강력한 사이버보안 기준을 충족해야 한다. 특히, 인공지능 기술이 철도분야 전반에 적용됨에 따라, 전체적인 보안을 향상시킬 수 있는 지렛대 역할을 할 수도 있다. 이것은 예측할 수 없고 매우 심오한 사이버공격의 위협이 상존하는 현재의 상황에서 특히 중요하다. 계속적으로 진화하는 인텔리전트 악성코드(malware)의 위협에 대항하여, 인간의 조심보다는 인텔리전트 보안이 더 효과적인 해답이 될 것이다.
 - 블록체인(Blockchain) 기술이 발전하고 있는 바, 이 기술의 근본적인 특성은 암호와 분산된 데이터 스토리지를 통해 제공하는 보안성이다. 기업들이 그들의 미션을 수행하는데 핵심적으로 중요한 프로세스를 이 디지털 장부(digital ledger)에 안전하게 이동시킬 수 있고 필요한 계산을 수행하며 수시로 데이터를 업데이트할 수 있기 때문에, 이 기술은 클라우드 인프라시설에 전환을 가져올 수 있다.
 - 견고하고 강력한 사이버보안 기준과 [일반 데이터 보호 규정](GDPR, General Data Protection Regulation)에 일치하는 이러한 신기술을 포함한 새로운 혁신적인 기술은 시스템의 보호 수준을 업그레이드함으로써 사이버보안을 향상시키는 것이 목표이다.

4-3. 다음의 우선순위를 위해 모니터링되어야 하는 6년 이상의 장기적인 도전

- 프로젝트가 아닌 프로세스의 인증(Authorisation)
 - 규정과 관련된 프로세스를 수립하는 첫 번째 단계에서, 프로젝트가 [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)를 사용하여 인증되는 것은 필요불가결한 것이다. 그런데, 일단 철도 제작회사, 인프라시설 관리자 그리고 철도 운영기관이 몇 번의 인증절차를 진행하게 되면, 각각의 프로젝트를 개별적으로 인증하기 보다는 산업 개발 절차들에 대한 인증을 시행하는 것이 더 효과적인 방식이 될 것이다.
- 차세대 시스템을 위해, 전체 제품의 수명주기 전체를 안전하게 보호
 - 철도개발이 가진 긴 수명주기 때문에, 최초 프로젝트에 이용된 규정 프로세스가 진행 중인 프로젝트에 적용될 것이다. 장기적으로, 모든 프로젝트들은 초기부터 [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안) 방식을 사용하여 개발되어야 할 것이다.
- 사이버보안 대응을 크게 개선하기 위해, 해당분야를 넘어서는 협력의 증대
 - 사이버위협이 더 복잡해짐에 따라, 사이버보안을 위해서는 글로벌 협력이 더욱더 중요해질 것이다. 분야를 넘나드는 협력 프레임워크 특히, 다른 핵심적인 인프라시설 분야 간에 협력이 매우 적절한 것이다. 위협과 리스크, 취약성 그리고 성공적인 이전 전략에 대한 지식의 공유는 글로벌

차원에서 이해와 분석을 진행하는데 매우 중요할 것이다.

- 다른 분야 간에 강력한 협력관계를 구축하는 것이 사이버보안에 관련된 도전에 대응하는 유럽의 능력을 키우게 할 것이다.

5. 핵심 메시지와 권고사항

유럽철도산업연합(UNIFE)은, 유럽의 사이버보안 경기장에서 완벽한 협력에 도달하기 위해서는 표준화, 연구와 기술혁신 그리고 사이버위협 공유 활동에 모든 철도 이해관계자들이 포함되는 협력적인 접근법이 있어야 한다고 믿고 있다. 이 목표를 달성하기 위해, 유럽철도산업연합(UNIFE)은 다음과 같이 요청한다.

<1> 유럽연합집행위원회에게

- ※ 연구 및 기술혁신국(DG RTD, Directorate-General for Research and Innovation), 통신 네트워크, 콘텐츠 및 기술국(DG CONNECT, Directorate-General for Communications Networks, Content and Technology), 모빌리티 및 교통국(DG MOVE, Directorate-General for Mobility and Transport)
- [네트워크 및 정보 보안 규칙](NIS 2)의 핵심목표인 규정적인 일관성을 보장하기 위해, 사이버보안에 대한 예상되는 범위의 확장과 그에 동반하여 발생하는 법률적 제안을 허용해야 한다. 수평적이며 분야에 전반적으로 적용되는 법률적 수단이 충분히 제공되어야 하며 규정의 중첩은 피해야 한다. [네트워크 및 정보 보안 규칙](NIS 2)은 범위 내에 있는 모든 이해관계자에게 적용되는 명확한 판단기준을 포함해야 한다. 이것은 회원국들이 의무적인 이행을 강제할 수 있어야 하므로 애매모호함을 피하는 것이 아주 중요하다.
- 사이버보안은 나날이 발전하는 위협을 따라잡기 위해서 지속적인 기술혁신이 필요하기 때문에, 사이버보안이 적절하게 해결될 수 있도록 철도 연구와 기술혁신에 유럽연합의 더 많은 자금지원이 할당되어야 한다. 이것은 미래의 유럽 철도 민관합동 연구(Europe's Rail Joint Undertaking)를 위해 특히 중요하다. 프로그램은 모든 사이버보안 우선해결사항을 해소해야 하고 [Shift2Rail] 프로젝트와 다른 유럽의 철도연구 프로젝트에서 시작된 연구를 계속 진행해야 한다.
- 유럽연합 사이버보안국(ENISA)에 적절한 예산을 할당하여, 이 조직이 아주 중요한 인프라시설의 보호를 지원하는데 중요한 역할을 할 수 있도록 해야 한다.

<2> 유럽연합 사이버보안국(ENISA)에게

- 철도를 사이버보안 전략에서 계속 고려해야 한다.
- [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)에 기반을 둔 철도용 인증제도를 만들어서, 유럽 철도분야 전체에서 사이버보안 실행시 서로 다른 기준을 적용하는 것을 피해야 한다.
- 시민들을 위해 안전하고 복원력있는 중요한 인프라시설을 창조하여 해당 인프라시설에 우려되는 사이버 및 물리적인 리스크를 이해하고 관리를 진행 중인 유럽연합의 노력을 이끌고 있는 중요한 이해관계기관을 더 지원해야 한다.

<3> 유럽연합집행위원회(통신 네트워크, 콘텐츠 및 기술국, DG CONNECT)와 유럽연합 사이버보안국(ENISA)에게

- [네트워크 및 정보 보안 규칙](NIS 2) 제안은 특정 제품과 서비스에 대해 공급망 전체를 통해 보안 평가 시행을 위한 필요조건을 많이 도입하고 있다. 그러므로 유럽연합 회원국 전체적으로 협력적인 접근법을 유지하고 경쟁력 있고 조화로운 단일시장을 보장하기 위해, 이러한 평가들이 리스크에 기반을 두고 비차별적이어야 함은 매우 중요하다. 목표로 설정된 철도분야 기업들은 이러한 리스크

평가에 참여해야 하며, 이것은 그들의 전문적인 능력이 복잡한 철도 공급 프로세스를 성공적으로 고려하는데 기초가 되기 때문이다.

<4> 유럽연합 철도국(ERA, European Union Agency for Railways)과 유럽연합 사이버보안국(ENISA)에게
- 철도분야에 사이버보안 강화를 위한 협력을 지속해야 한다.

<5> 유럽표준화위원회(CEN, European Committee for Standardization)와 유럽전기표준화위원회(CENELEC, European Committee for Electrotechnical Standardization)에게
- 특히 새로운 [CLC/TS 50701:2021 Railway applications – Cybersecurity](CLC/TS 50701:2021 철도분야 – 사이버보안)을 통해, 철도 이해관계자들이 사이버보안에 대한 인식을 높일 수 있도록 지원해야 한다.

<원문제목> UNIFE Position Paper on Cybersecurity in Railways

<원문출처> <https://www.unife.org>