Cybersecurity Risk Management in Rail and Transit Systems.

철도 및 교통 시스템의 사이버 보안 리스크 관리

www.tuv.com

TÜVRheinland®
Precisely Right.

철도 및 교통 시스템의 사이버 보안 위험

철도와 대중교통 시스템의 OT(Operational Technology) 및 컨트롤 네트워크의 사이버 보안 관련 사고가 증가하고 있습니다. 사이버 공격으로 인해 노선이 중단되고 승객의 개인 정보가 유출된 사례가 보고되고 있으며, 이는 증가하는 사이버 보안 규정 요구사항을 준수할 수 있는 운영자의 역량뿐만 아니라 수익성에도 영향을 미치고 있습니다.

철도 및 교통 시스템 전반에 걸쳐 디지털화가 진행되면서 더 많은 장비와 시스템이 상호 연결됨에 따라 관련 사이버 보안 위험이 증가합니다. 기존의 IT 보안 위험 모델은 사무실이나 상업 환경에서 사용되는 것과는 다를 수 있으므로 디지털 철도의 특수한 특성을 이해하지 못하는 경우가 많으며, 이는 철도의 안전에도 영향을 미칠 수 있습니다. 특정 안전 설계 요구사항을 충족하는 교통 시스템이 사이버 공격으로 인해 손상될 수 있습니다.

사이버 보안 리스크는 어떻게 평가됩니까?

TÜV 라인란드의 전문가는 디지털 철도 사이버 보안을 이해하는 데 도움이 되는 효과적인 방법으로 귀사와 협력합니다. 귀사의 상황에 가장 적합한 산업 표준을 바탕으로 신속하게 사이버 보안 평가를 수행합니다. TÜV 라인란드는 학습 기회를 극대화하고 비즈니스 및 운영의 핵심 부분이 프로세스에 참여할 수 있도록 조사 결과를 논의할 수 있는 협업 워크숍 방식으로 진행합니다.

사이버 보안 리스크를 평가하는 이유는 무엇입니까?

- 필수 안전 및 사이버 보안 리스크를 이해하기 위한 규제 또는 법적 요구사항이 있습니다.
- 경영진은 사이버 보안 문제가 비즈니스에 어떤 영향을 미칠 수 있는지 우려합니다.
- 투자자와 주주는 시스템이 잠재적인 사이버 보안 문제를 관리할 수 있으며, 새로운 투자가 보호될 것이라는 확신이 필요합니다.

TÜV 라인란드의 OT 및 산업 보안 전문가가 운영 환경의 요구사항에 따라 포괄적인 맞춤형 서비스 포트폴리오는 제공합니다. IEC 62443에 따른 사이버 보안 프로세스/제품 인증 및 리스크 평가를 제공하며, 조직이 사이버 보안에 대해 더욱 잘 이해할 수 있도록 도와드립니다.

TÜV 라인란드와의 협력

TÜV 라인란드는 150년 이상 쌓아온 경험과 전문성, 각 분야의 전문가들로 구성된 글로벌 네트워크를 통해 안전, 보안, 데이터 개인정보 보호 및 인프라의 복잡한 문제를 해결하고, 시장에 대한 깊은 이해를 바탕으로 안전하고 신뢰할 수 있는 철도시스템 개발과 철도 프로젝트 성공을 위해 철도 라이프 사이클의 전 과정을 함께 합니다.

산업 보안 서비스 포트폴리오

산업 보안 위험 평가
운영 기술과 산업 보안 위험을 이해하고 있습니까?.

OT 아키텍처 검토
산업 기술 설계 및 아키텍처가 안전하며, 사이버 보안 표준 및 규정을 준수합니까?

OT 시스템 침투 테스트
운영 기술 취약성 평가 및 침투 테스트를 수행해야 합니까?

OT 정책, 프로세스 및 절차 검토
정책, 프로세스 및 절차가 산업 및 운영 기술 시스템의 고유한 사이버 보안 및 규제 요구 사항을 준수하고 있습니까?

OT 시스템 사고 대응 및 복구
기존 운영 기술 사고 대응 및 복구 계획이 마련되어 있습니까?

OT 시스템 보안 모니터링
OT 네트워크 및 시스템에서 무슨 일이 일어나고 있는지 알고 계십니까?

철도 및 교통 산업을 위한 OT 서비스
전반적인 철도 및 교통 시스템의 운영 기술과 산업 보안 위험을 이해하고 있습니까?

TÜV 라인란드 코리아
서울시 영등포구 문래로 28길 25
세미콜론 문래 N타워 2층
Tel: 02-860-9860
Fax: 02-860-9862
E-mail: info@kor.tuv.com

www.tuv.com

철도 홈페이지

TÜVRheinland®
Precisely Right.