AI EDGE LABS

RAILWAY CYBER SECURITY

Railways Under Cyber Attack

The Honey Train Project, a virtual rail transport model that quantifies cyber attack aggressiveness, was hit by 2.7M cyber attacks in 6 weeks.

86% of 1,000 devices supplied to San Francisco's Rapid Transit system contained hidden backdoors and a persistent ping sending data to a foreign nation hostile to America.

22% of railway survey respondents report experiencing a cybersecurity incident with more than 1,000 records breached, over $10,000 in losses, and operating system shutdowns.

82% of survey IT professionals in the railway industry have suffered a disruptive event (downtime or data loss).

Railways Cybersecurity Landscape

The global railway cybersecurity market will reach $16.72B by 2028.

Research predicts that a successful attack on a locomotive's control systems can result in over 100 deaths from a single hacked train.

The U.S. economy would lose over $2B per day in the event of a nationwide shutdown of rails.

Cybersecurity Preparedness in Railway

47% audit their cybersecurity programs annually.

43% do not believe they have the resources needed for cybersecurity preparedness.

41% provide annual cybersecurity staff training.

36% do not have a disaster recovery plan.

42% don't have an incident response plan.

53% do not have an operations continuity plan.

58% do not have a business continuity plan.

60% actually have a cybersecurity preparedness plan.

How AI Can Advance Security in Railway

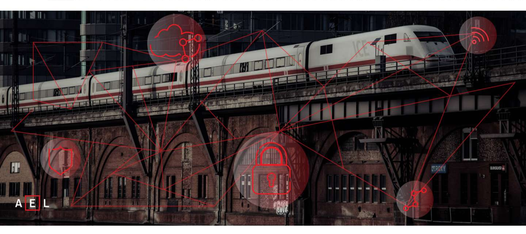
90% of accidents on EU transportation are caused by human errors, meaning systems based on AI used in autonomous transportation can significantly improve road safety.

80% of incidents can be forecasted thanks to AI applications such as predictive analytics and maintenance.

41,7% growth of AI-powered video analytics in railway and public transport networks.

30% reduction of train switches incidents thanks to predictive analytics and maintenance according to SNCF.

50% of increase in efficiency, cost savings, and time savings as a result of MTR Corporation of Hong Kong using AI to automate engineering scheduling to adhere to maintenance rules, regulations, and guidelines in a secured environment.



AI EdgeLabs is a robust, enterprise-grade, and AI-based platform that brings advanced network visibility, early threat detection, and automated incident response and remediation vital for the railway industry. Enriched with Deep Reinforcement Learning, our platform is smart and impressively accurate in detecting threats before they even have a chance to cause harm.

On Gateways, AI EdgeLabs sensors can secure connectivity to the ships and operate as a smart firewalling solution. Edge Sensors can deliver very high quality detections using Reinforcement Learning algorithms.

PROTECT YOUR EDGE & IOT ENVIRONMENT

AI EDGE LABS