Cybersecure railway switch heating: Kaspersky collaboration with Russian Railways

kaspersky

KasperskyOS

JSC NIIAS

"'SMART. Switch heating' is an important step towards the digital railroad of the future. This smart system helps automate railway infrastructure processes and significantly improve their reliability and efficiency. We are proud to be part of this groundbreaking project with Kaspersky IoT Infrastructure Security, one of the first KasperskyOS-based solutions for transport infrastructure that protects systems from cyberattacks and keeps them running smoothly. We continue to develop technologies for highly automated and self-driving vehicles."

Grigory Sizov,
Head of KasperskyOS Business Unit

Russian Railways (RZhD) are trying to find more cost-effective ways for utilizing the railway equipment resources of its Central Infrastructure Directorate (branch of JSC RZhD). To reduce electricity costs, JSC NIIAS, a leading industry institute of JSC Russian Railways, developed a cutting-edge project called **"SMART. Railway Switch Heating".** It optimizes electrical heating of railway switches through process automation and autonomous adaptation to environmental parameters.

This type of project could not have been created without integrated cybersecurity. A successful attack on "SMART. Railway Switch Heating" could not only disrupt system operations but also threaten the information security and physical security of the infrastructure. Kaspersky technologies helped protect this project at all levels. One of these technologies is a specialized KasperskyOS-based solution called Kaspersky IoT Infrastructure Security, which ensures that the internet of things is secure and functional.

Challenge

Electrical heating of railway switches throughout most of JSC RZhD network is managed manually.

The existing switch heating system has the following flaws:

- Runs excessively without accounting for real-time dangers of icing or precipitation.
- Untimely shutdown.

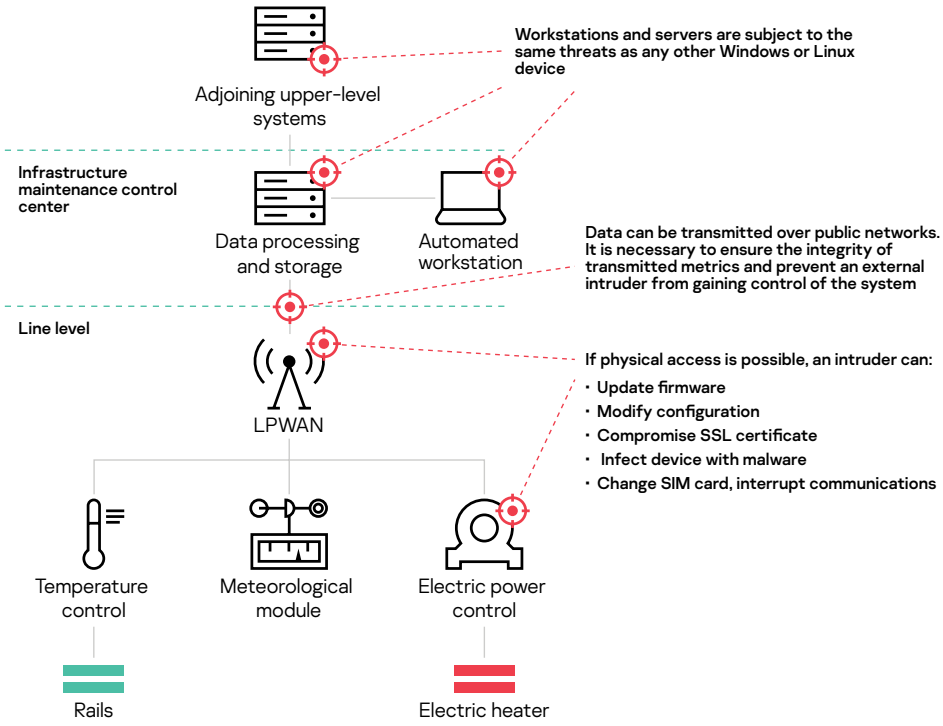
"SMART. Railway Switch Heating" will help resolve these problems through adaptive control based on the monitoring of the temperature of rails, weather conditions and the state of electrical devices. Automated online processing of these parameters will help optimize heating operations, and Kaspersky solutions provide comprehensive protection of the infrastructure and prevent cybercriminals from exploiting its vulnerabilities.

"Modern railways are a complex technological system with increased information security requirements. The use of Kaspersky's advanced cybersecurity technologies makes it possible to accelerate the implementation of innovations at JSC Russian Railways that provide new levels of quality, speed and safety in railway transportation."

Ilya Nikolaev,
Head of the Center for Telecommunication Systems and Industrial Internet at JSC NIIAS — Rostov branch

Importance of cybersecurity

Expanding automation and digitizing the infrastructure of Russian Railways significantly increases the risks of cyberattacks being launched against its facilities. Data transfer channels, cloud platforms and IoT devices attract the most attention from cybercriminals.



Threat vectors for railway heating systems

Internal threats

Unauthorized connections to the "SMART. Railway Switch Heating" system may lead to malware infection of an automated workstation and, consequently, cause a disruption in its operations. For example, cybercriminals might attempt the following:

- Manipulate the weather control module (WCM), electrical control module (ECM), rail temperature control module (RTCM), and the LPWAN communication module (CM) to breach the integrity of transmitted data.
- Disable the "SMART. Railway Switch Heating" system or its individual components.

External threats

Digital infrastructures connected to the internet are especially prone to attacks from the outside. The "SMART. Railway Switch Heating" system is most vulnerable to the following threats:

- Compromise that results in incapacitation of the system or its individual components.
- Remote manipulation of the WCM, ECM, RTCM and CM in order to breach the integrity of transmitted data.
- Capture and modification of information transmitted over public networks.

Problems (threats) that arise during administration and operational maintenance of the system

- Difficulty monitoring the IoT infrastructure (lack of a complete picture in real time)
- Delayed response to information security incidents (late detection/notification of the problem)
- Complexity of management and operational maintenance (lack of a unified system for management, reporting and incident response)

Impacts of cyberattacks launched against the "SMART. Railway Switch Heating" system

- Loss of the capability to monitor the IoT infrastructure (and incorrect data received from the ECM, RTCM and WCM)
- Disrupted operations of the WCM, ECM, RTCM and CM
  - Loss of control
  - Incorrect data received from the ECM, RTCM, and WCM; inappropriate control input
  - Failure of the railway switch electrical heating system

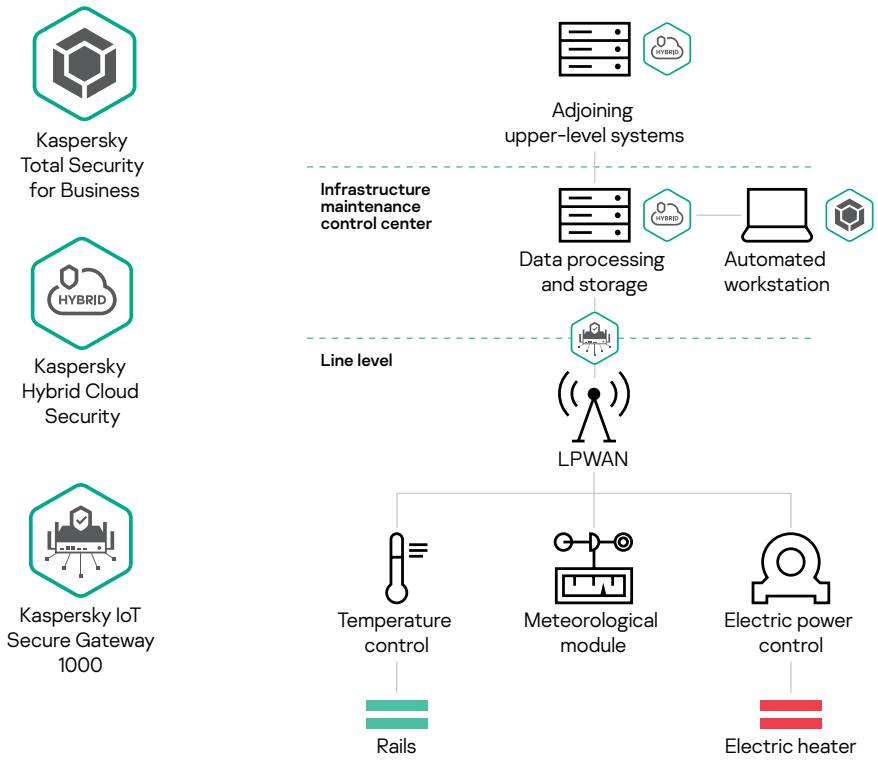
Existing problems handling information security incidents

- Inability to detect dangerous manipulation prior to its obvious negative effects (physical damage)
- Slow response to information security incidents
- Lack of a unified system for managing and responding to information security incidents
- Lack of information security incident reporting

Solution

Cybersecurity of the railway switch heating system requires an integrated approach at all levels of the architecture:

Levels	Threat vectors	Kaspersky products and solutions
Management level (information storage and processing module)	Antivirus protection	Kaspersky Hybrid Cloud Security Kaspersky Total Security for Business
Data transmission channel	Protection of data transferred to the cloud via traffic encryption (TLS-MQTT) Protection against external threats (Firewall/IPS)	Kaspersky IoT Secure Gateway 1000
	DDoS (channel unavailability)	Kaspersky DDoS Protection
Endpoint level	Detection of unauthorized devices Prevention of unauthorized interactions (Firewall) Protection of the gateway against hacking: · Verification of the gateway firmware when booting (Secure Boot) · Verification of updates (Secure Update) · Prevention of unauthorized interactions at the operating system level (Cyber Immune KasperskyOS)	Kaspersky IoT Secure Gateway 1000



Kaspersky's comprehensive approach to the cyber protection of "SMART. Railway Switch Heating"

Protection tools

Kaspersky IoT Secure Gateway (KISG) 1000 is a hardware and software system based on the KasperskyOS operating system. It has Cyber Immunity, innate protection against the overwhelming majority of cyberattacks which means it will perform its critical functions even in an aggressive environment. The gateway protects data, generates security events in the IoT infrastructure, enables management of connected devices via the MQTT protocol over TLS, and helps build secure systems for the internet of things. Centralized administration of KISG 1000 events is via the Kaspersky Security Center platform.

Kaspersky Hybrid Cloud Security is a solution for protecting virtual machines and systems (local ones as well as the ones residing at data centers or in public clouds).

Kaspersky Total Security for Business is a solution for protecting endpoint devices (workstations and servers) and other nodes of an enterprise network (mail servers, internet gateways).

Result

Solutions developed by Kaspersky ensured the cybersecurity of the "SMART. Railway Switch Heating" system at all levels, and made the system transparent and manageable.

Attack vector	Potential threat	Protection method
Cloud	DDoS (system unavailability)	Kaspersky DDoS Protection (service)
	Compromise (hacking, gaining access, modifying configurations, data spoofing/leakage)	Kaspersky Hybrid Cloud Security
Data transmission channel	Compromise (Man-in-the-middle, gaining access to data and substituting it)	Traffic encryption (MQTT) ensures that the connection and data transfer are secure (Kaspersky IoT Secure Gateway 1000)
	DDoS (channel inaccessibility)	Kaspersky DDoS Protection
Gateway	Gateway compromise — network or local attack/physical access (hacking, gaining access, modifying software configurations, data spoofing/leakage)	IDS/IPS, Secure Boot, Secure Update; inability to perform unauthorized actions or manipulate critical functions of the system (Kaspersky IoT Secure Gateway 1000 and KasperskyOS technologies)
Internal IoT network (inside breach)	Breach of the structural integrity of the network (new unauthorized connections to the network)	Network Discovery — detection of a breach and notification about the connection of an unauthorized device/user (Kaspersky IoT Secure Gateway 1000)
Cloud platform (external breach)	Disclosure and compromise of the "SMART. Railway Switch Heating" system	Kaspersky Hybrid Cloud Security

System administration and operational maintenance processes	Difficulty of monitoring the IoT infrastructure and prolonged response time to information security incidents (inability to detect dangerous manipulation until physical damage is already apparent; lack of a full picture in real time; late detection/ notification of the problem)	Multitude of notification capabilities: sending security events to Kaspersky Security Center, cloud platforms, SIEM systems; push notifications to devices
	Security system management and operational maintenance (lack of a unified system for management, reporting, and incident response)	Unified cybersecurity management system with a centralized system for reporting, logging, and notifications (Kaspersky Security Center)

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe.

The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Kaspersky also advances the development of Cyber Immune solutions based on its own operating system, KasperskyOS. Such solutions are innately secure against the overwhelming majority of cyberthreats, both known and unknown.

Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them.

The Joint Stock Company Russian Railways is a modern transport and logistics complex of strategic importance for Russia. The company is the most important link in the unified economic system of the country and ensures the uninterrupted economic activity of industrial enterprises and affordable cargo and passenger transportation for millions of citizens.

Russian Research and Design Institute for Information Technology, Signalling and Telecommunications in Railway Transportation (JSC NIIAS) is a subsidiary of JSC Russian Railways. It develops and implements advanced digital solutions for railway transport. The main activities of the Institute include integrated intelligent control systems, automation and diagnostics, unmanned rolling stock, robotization of technical equipment, and cybersecurity.

KasperskyOS

Kaspersky
IoT Infrastructure
Security

Learn more on os.kaspersky.com

www.kaspersky.com