Kaspersky OT Cybersecurity

Vertical offering
for power system and grid
operators, power plants
and utilities

kaspersky

Industry summary

The Power & Utilities industry is crucial to society, playing a central role in driving economic growth, enhancing quality of life and supporting technological advancements. Electricity is an essential resource, powering a number of key areas including:

- Residential use and smart cities (street lighting, HVAC, etc.)
- Transportation (EV, charging)
- Manufacturing

The industry plays an important role in achieving net-zero emissions in line with the goals of the Paris Agreement (UN). The industry supports electrification across other industries and drives the transition to renewable energy.

The industry trend towards clean energy demands robust, efficient smart grids.

~x2

worldwide investment in clean energy compared to fossil fuels[1]

[1] World Energy Investment 2024, report by IEA

Digitalization objectives

Digitalization is an enabler of the industry's sustainability goals, with digital solutions supporting the strategic goals of industry players:

- Improve asset security and efficiency
- Drive global decarbonization and electrification
- Accelerate the deployment of renewable energy infrastructure
- Ensure safe working conditions

Main digital solution use cases in the industry

- Internet of Energy (IoE) devices
  Enable wide-area automation for real-time monitoring and control of grid operations
- Energy Cloud
  Real-time analytics, scalable infrastructure, remote management and integration of new technologies
- Electrical digital twins
  Grid mode simulation, predictive insights, real-time monitoring and diagnostics of equipment
- ML & AI driven smart grid
  Optimization, predictive maintenance and condition monitoring
- Robotization
  Robotic and aerial plant inspections, vegetation management

As digitalization transforms the industry, operations will inevitably face security challenges.

Ppower systems will need extended communication and automation capabilities that are secure, reliable and effective.

2.3 p.p.

Decrease in the number of ICS computers in the Energy sector on which malicious objects were blocked in Q1 2025 (compared to Q1 2024)[2]

[2] Threat landscape for industrial automation systems report by ICS CERT

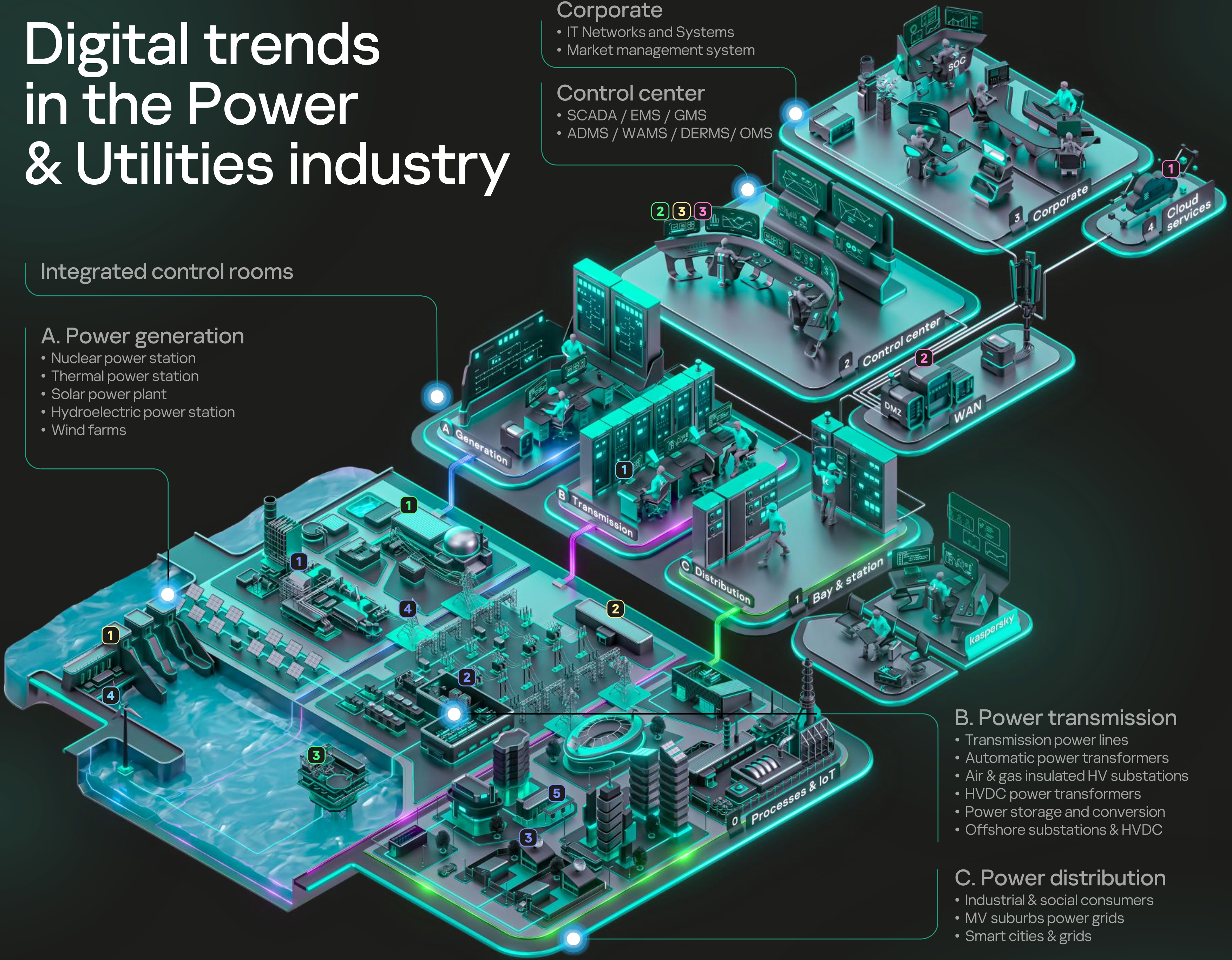
Digital trends in the Power & Utilities industry

Corporate
- IT Networks and Systems
- Market management system

Control center
- SCADA / EMS / GMS
- ADMS / WAMS / DERMS / OMS

Integrated control rooms

A. Power generation
- Nuclear power station
- Thermal power station
- Solar power plant
- Hydroelectric power station
- Wind farms



B. Power transmission
- Transmission power lines
- Automatic power transformers
- Air & gas insulated HV substations
- HVDC power transformers
- Power storage and conversion
- Offshore substations & HVDC

C. Power distribution
- Industrial & social consumers
- MV suburbs power grids
- Smart cities & grids

IoE
1. Smart energy ad heat metering
2. Monitoring of the condition of primary equipment
3. Managing distributed energy resources (DER)
4. Monitoring of transmission and distribution (T&D) line condition
5. Monitoring charging stations and connected vehicles

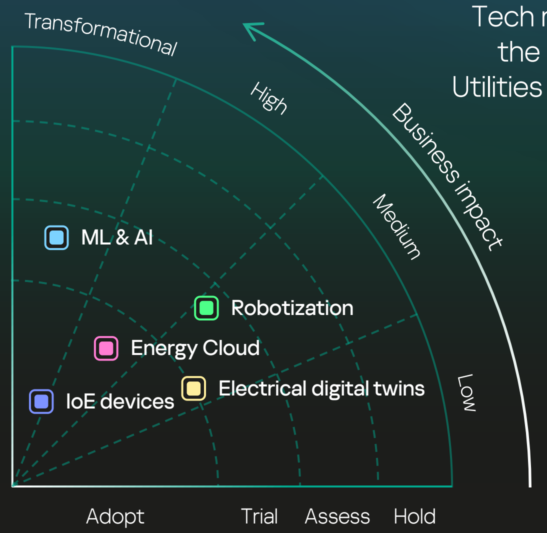
Energy Cloud
1. Predictive analysis in supply using weather forecasts and other data
2. WANs enabling real-time communication between OT systems systems, sensors and grid control centers
3. Network Information Systems (NIS) providing distribution grid operators with routes and grid topology

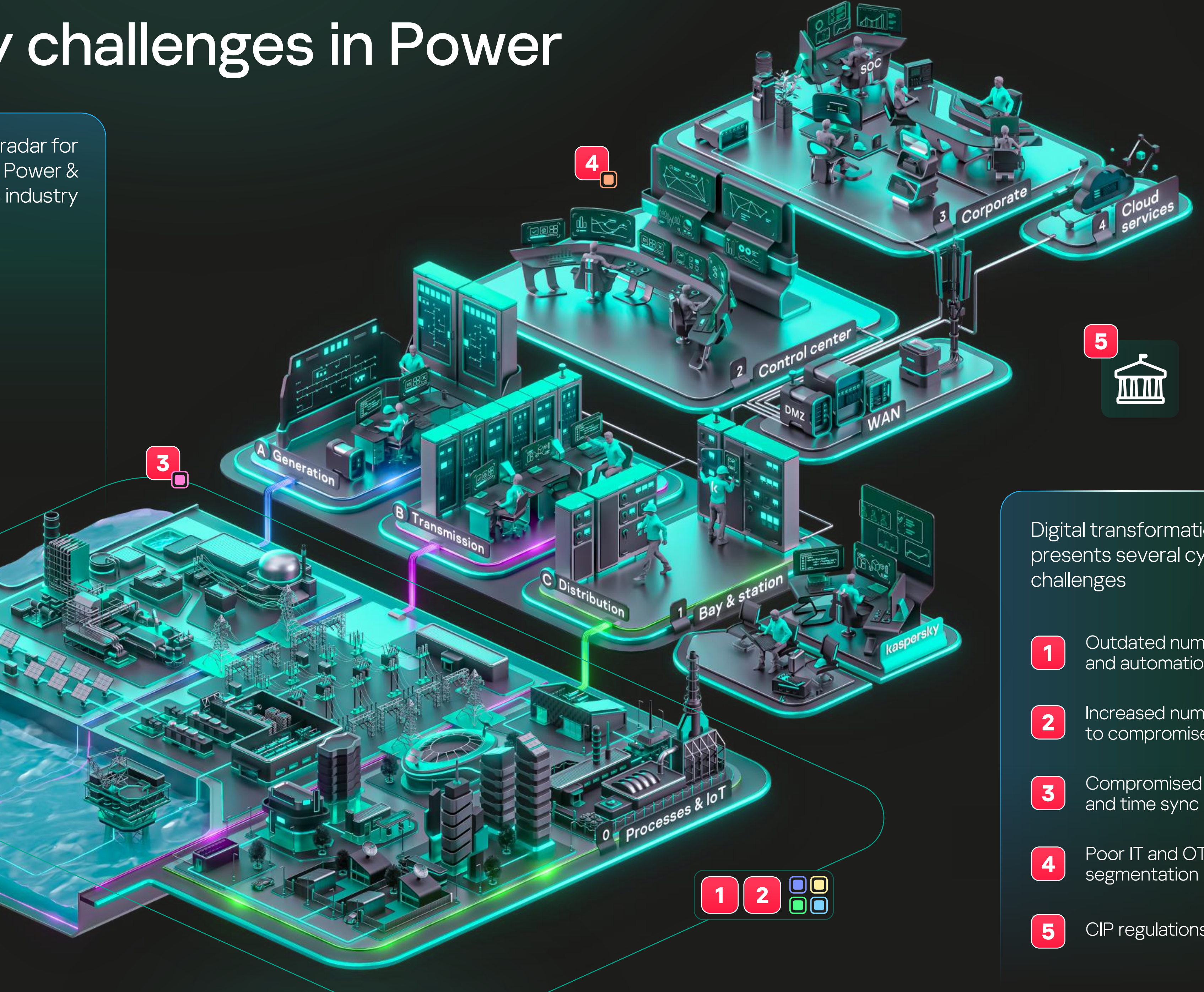
Electrical digital twins
1. Asset performance management with equipment monitoring and root-cause analysis
2. Mapping risk clusters to visualise areas with concentrated risks and avoid cascading failure
3. Energy storage simulation for optimizing supply plans and peak load analysis

ML & AI
1. Grid balancing by dynamically adjusting power flows, minimizing losses and preventing overloading
2. Reactive power optimization and voltage control to avoid brownouts
3. Analysis of smart metering infrastructure data for better commercialization and peak demand flattening
4. Predicting weather patterns to adjust blade positions

Robotization
1. Sensor-integrated drones for aerial surveys
2. Automatization of inspection activities to identify potential issues (e.g. hot spots, leaks, power lines, etc.)
3. Underwater inspection of offshore wind farms

Cybersecurity challenges in Power



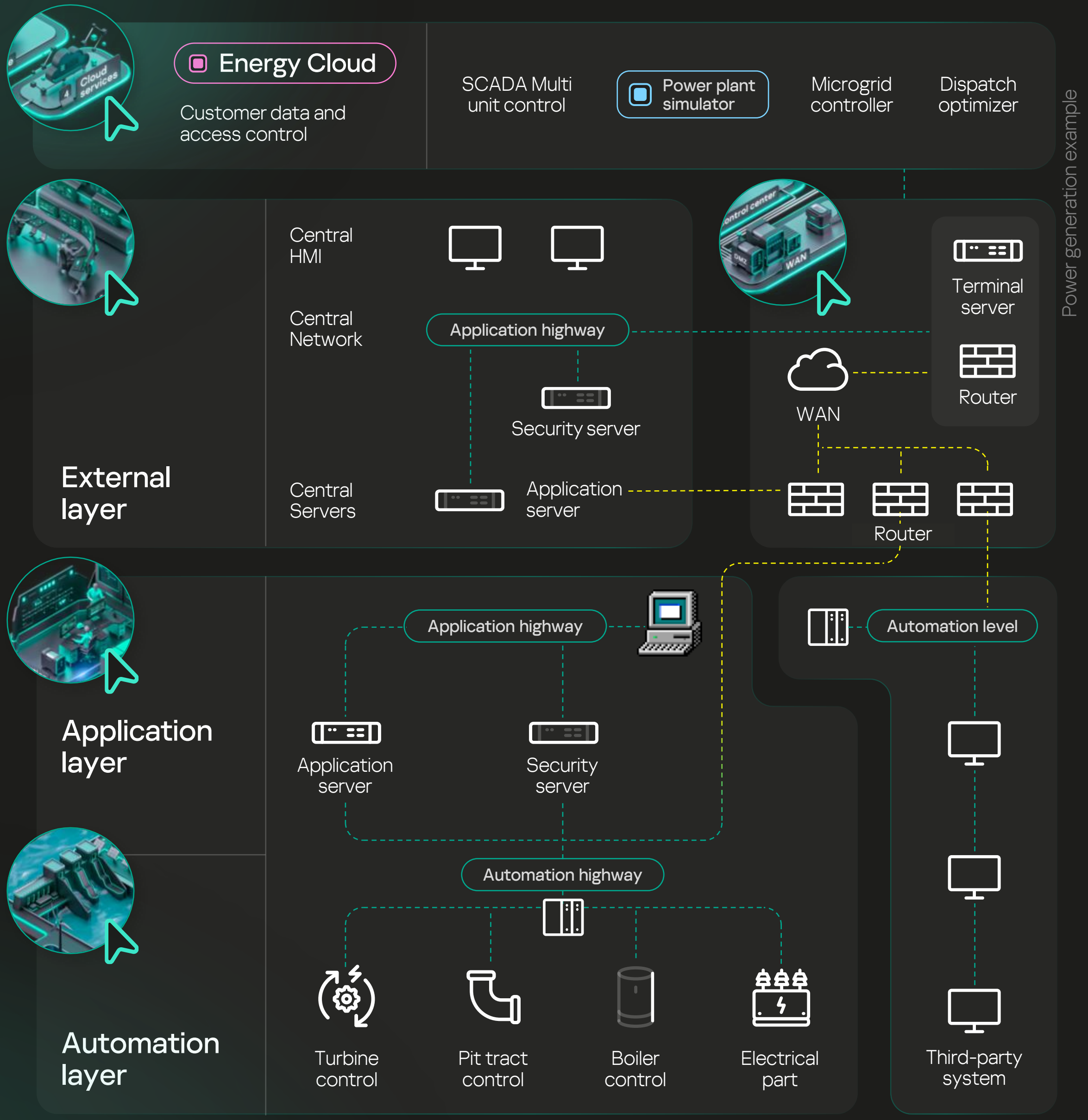


Digital transformation in the industry presents several cybersecurity challenges

1. Outdated numerical relays and automation
2. Increased number of nodes to compromise
3. Compromised remote access and time sync
4. Poor IT and OT network segmentation
5. CIP regulations

Outdated numerical relays and automation

▣ Energy Cloud ▣ ML & AI



▣ Energy Cloud

Customer data and access control

SCADA Multi unit control

▣ Power plant simulator

Microgrid controller

Dispatch optimizer

Power generation example

External layer

Central HMI

Central Network

Application highway

Security server

Central Servers

Application server

Terminal server

WAN

Router

Router

Application layer

Application highway

Application server

Security server

Automation level

Automation highway

Automation layer

Turbine control

Pit tract control

Boiler control

Electrical part

Third-party system

Integrating outdated systems with modern technologies like ML, AI and cloud presents several key challenges.
Compatibility issues can occur when older systems struggle to interface with newer technologies. Limited interoperability may disrupt operations and reduce the efficiency gains offered by modern solutions. In particular, legacy systems often cannot communicate effectively with cloud platforms or AI-driven automation tools.

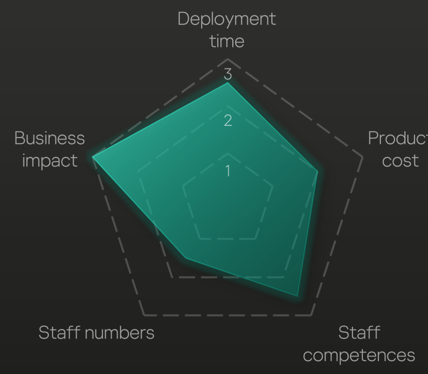
Legacy hardware currently accounts for

>1/3

of organisations' total power consumption[1]

[1] Daisy Corporate Services Study

Solution characteristics



How Kaspersky helps

Kaspersky Industrial CyberSecurity

- Continuous monitoring of industrial networks for vulnerabilities
- Endpoint detection and response
- Regular security audits

Kaspersky Machine Learning for Anomaly Detection

- Predicts failures in aging relay systems using machine learning
- Detects cyberthreats targeting outdated relays

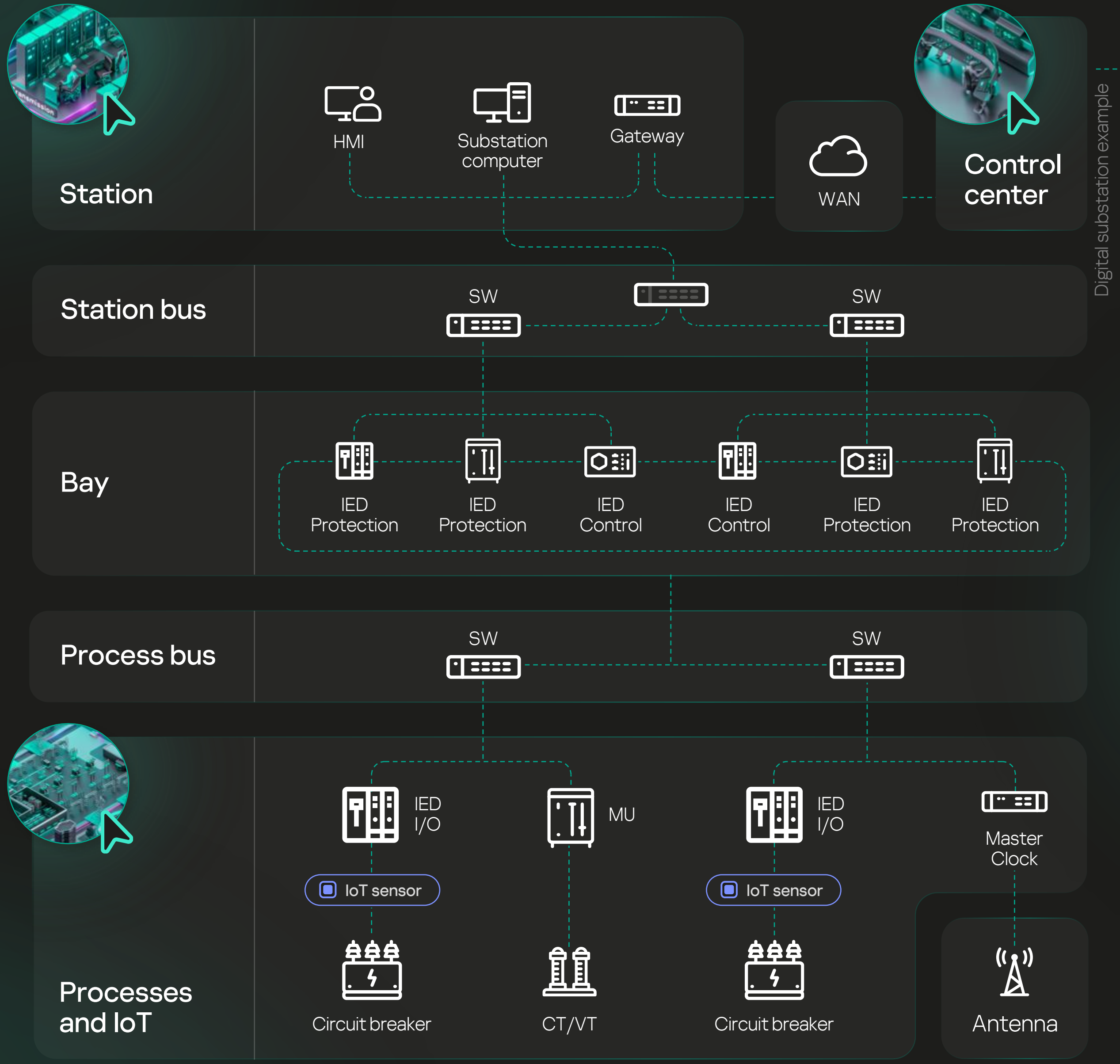
Ecosystem of supporting services

Kaspersky ICS Threat Intelligence

- Comprehensive analysis to identify and evaluate the exposure to risk and the security levels of industrial network infrastructures

Increased number of nodes to compromise

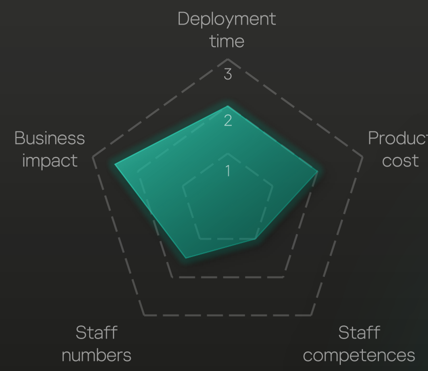
IoE



Integrating robotics and IoT into substations creates more entry points for cyberattacks as each unsecured device is a potential target.

Managing and patching diverse connected devices is challenging, and a single breach can cascade across systems, risking widespread disruption.

Solution characteristics



How Kaspersky helps

Kaspersky Industrial CyberSecurity

- Network visibility and network anomaly detection
- DPI of industrial communications with machine-learning capabilities
- Detailed system audit

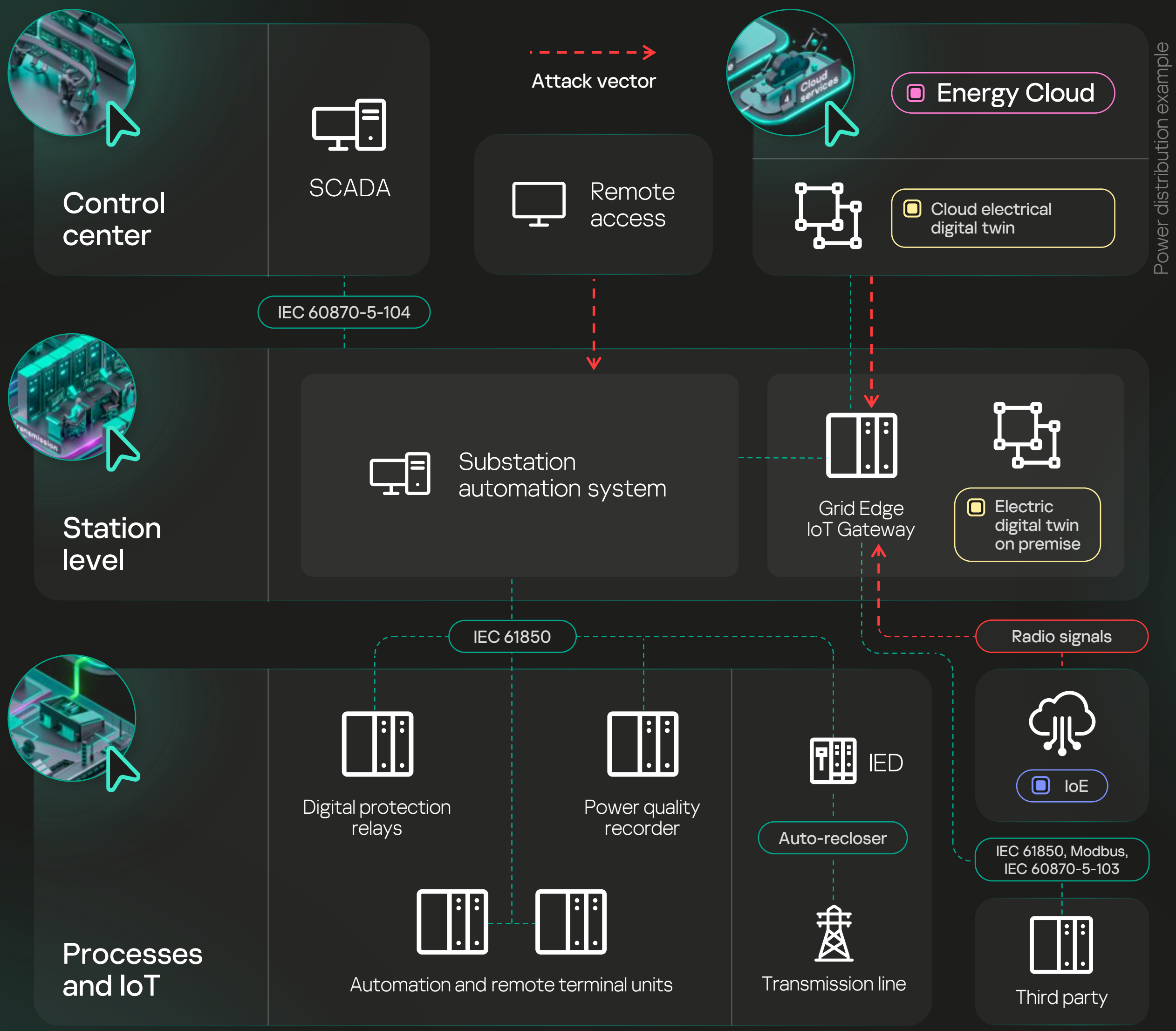
Ecosystem of supporting services

Kaspersky Managed Detection and Response

- Threat hunting and incident investigation
- Security monitoring

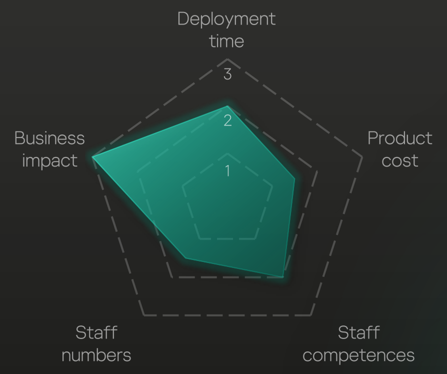
Compromised connections and time sync

▣ IoE ▣ Energy Cloud ▣ Electrical digital twins



Integrating technologies like IoE, digital twins and cloud services into power substations increases the risk of cyberattacks due to compromised connections, which may allow unauthorized access to SCADA systems and control networks. In addition, maintaining precise time synchronization for protection relays and phasor measurement units is critical as any errors can lead to faulty operation of grid devices

Solution characteristics



How Kaspersky helps

Kaspersky Next XDR Expert

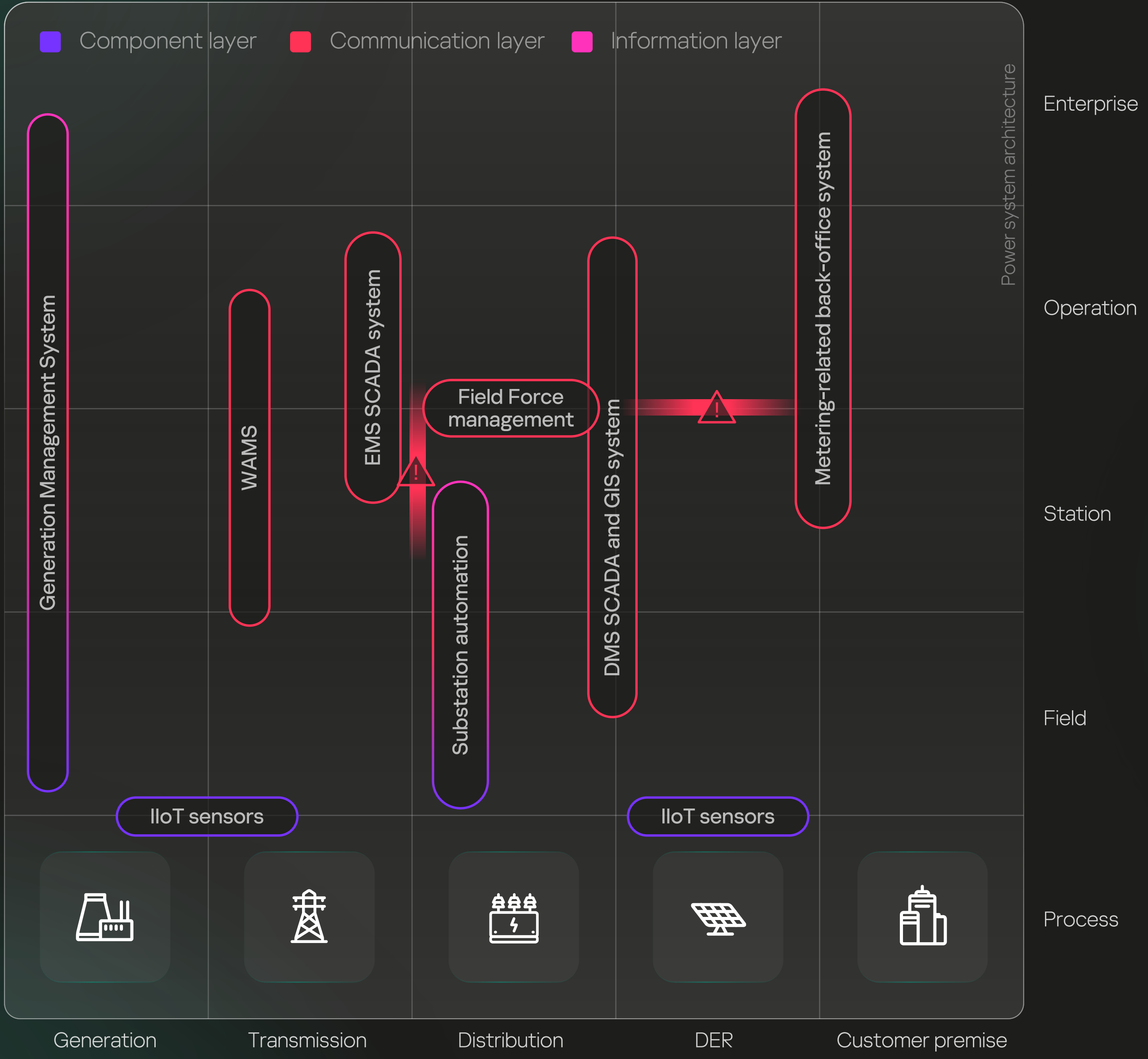
- Robust protection of physical and virtual endpoints
- End-to-end coverage across complex infrastructures

Kaspersky Thin Client

- Remote connection and engineering by staff and contractors
- Centralized monitoring and management of all thin client infrastructure events

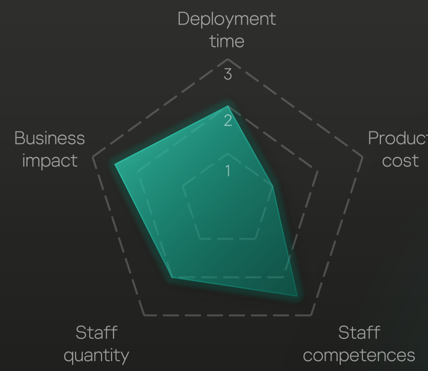
Poor IT and OT network segmentation

IoE



Inadequate network segmentation in power grids, particularly with integration of digital twins, can lead to significant security vulnerabilities. When these networks are not properly segmented, the interconnected nature of digital twins can increase the risk of cyber-attacks spreading from IT systems to critical OT infrastructure. This can disrupt power distribution and cause widespread outages

Solution characteristics



How Kaspersky helps

Kaspersky Industrial CyberSecurity

- Network traffic analysis to identify anomalies and threats
- Endpoint protection, detection and response
- Network segmentation and usage compliance

Kaspersky SD-WAN

- Real-time monitoring of distributed network
- Network visibility
- Unified network security and management

Ecosystem of supporting services

Kaspersky ICS Security Assessment

- Identifies security flaws in network architecture
- Provides actionable recommendations for remediation
- Internal penetration testing

CIP regulations

Cybersecurity regulations for the power and utilities sector vary globally but share a common goal: enhancing resilience, protecting critical infrastructure and ensuring service continuity. Many countries have implemented regulations to ensure that electricity providers and grid operators adopt robust cybersecurity practices, conduct regular vulnerability assessments and adhere to standardized incident response protocols.

Global

- ISA/IEC 62443
- IEC 62351 (IEC 61850 TR)
- ISO/IEC 27019
- IEEE 1547.3-2023, C37.240, 1686
- IAEA Nuclear Security Series No. 17-T

Indonesia

- PR 47/2023 National Cyber Security Strategy and Cyber Crisis Management
- BSSN Reg. 1/2024 Cyber Incident Management
- BSSN Reg. 2/2024 Cyber Crisis Management

Egypt

- ENRRA Technical Guidelines for Nuclear Facility Cybersecurity

UAE

- National Cybersecurity Strategy
- DESC Critical Information Infrastructure (CII) Protection Framework
- NESA CIIP Policy

Turkey

- NDK Cyber Security Plan for Nuclear Power Plants
- BTK CIPR Regulation
- Cybersecurity Law No. 7545

Thailand

- NCSA B.E. 2566
- NCSA B.E. 2562
- NCSA B.E. 2564

Saudi Arabia

- OT Cybersecurity Controls OTCC-1:2022
- Essential Cybersecurity Controls ECC-1:2018

Brazil

- National Cybersecurity Strategy (E-Ciber)
- ANEEL Resolution No. 964/2021
- ANEEL PRODIST Module 8

South Africa

- Critical Infrastructure Protection Act
- NNR RG-0014 Guidance
- National Cybersecurity Policy Framework

India

- CEA Cyber Security Guidelines and regulations
- NCIIPC Guidelines
- CERT-In Directions
- AERB Safety Codes and Guidelines

China

- GB/T 44462.1-2024
- GB/T 36572-2018
- GB 42250-2022
- GB/T 36627-2018

Malaysia

- NACSA CNII regulations
- CyberSecurity Malaysia guidelines (MyVAC)
- Suruhanjaya Tenaga Cybersecurity Rules

Europe

- NIS2 Directive
- CER Directive
- ENISA Guidelines
- Network Code on Cybersecurity for Cross-Border Electricity Flows

USA

- NERC CIP
- NIST CSF
- NRC Regulatory Guide

France

- National Cybersecurity Strategy
- ANSSI Cybersecurity Framework for ICS
- Critical Information Infrastructure Protection Law

Germany

- IT-Sicherheitsgesetz 2.0
- Energiewirtschaftsgesetz
- BSI KritisV / BDEW- B3S

Netherlands

- The Netherlands Cybersecurity Strategy (NLCS)
- Network and Information Systems Security Act (WBNI)
- NSCS Guide to Cyber Security Measures

Spain

- The National Security Framework
- CNPI Royal Decree 704/2011
- CCN-STIC Security Guides

UK

- Nuclear Industries Security Regulations (NISR)
- NCSC CAF
- NCSC OT Guidance
- Cyber Security for IACS (OG86)

How Kaspersky helps

Kaspersky Industrial CyberSecurity

Kaspersky solutions safeguard power plants, substations, grids and other power system elements to maintain the continuity of critical industrial and utility operations with a 'defense in depth' approach.

Solutions for power grids compliant with **ISA/IEC 62443, NIS2, SOC 2 Type2, ISO/IEC 27001, GB 42250-2022**

IEC AICPA SOC TÜV AUSTRIA

Compatibility tested:

Schneider Electric, CHINT, Valmet, SIEMENS, ProSoft Systems, EKRA

>150

systems from 50+ vendors

Kaspersky Security Awareness and Expert Training

Empower employees with essential cybersafety skills, complying with the requirements of the NIS2 Directive

Read more about NIS2 Directive and our product compliance

Cyber resilience with the Kaspersky OT ecosystem

Inventory and assess

Expertise

Network Asset Discovery

- Identify all hardware and software assets within the OT infrastructure
- Create a detailed inventory to plan your cybersecurity strategy

Endpoint Inventory

- Catalog hardware and software components
- Maintain an up-to-date inventory to identify critical assets and vulnerabilities

Policy Development

- Develop comprehensive policies and procedures.
- Use hazard and impact analysis to set cybersecurity levels and identify required controls.

Essential security

Technology

OS Hardening

- Securely configure systems and regularly apply patches and updates
- Implement additional controls
- Exploit prevention and removable devices check

Application Control

- Restrict unauthorized applications to maintain system integrity

Endpoint Protection

- Implement anti-malware solutions to secure devices within ICS and OT environments.

Advanced threat detection, audits and compliance

Knowledge+Technology+Expertise

Network Visibility

- Monitor network traffic to detect anomalies and understand attack patterns.

Threat and Anomaly Detection

- Use machine learning and DPI to identify network intrusions and anomalies
- Use EDR technology to monitor OT host telemetry

Security Audits

- Conduct regular vulnerability scans and compliance audits.

Configuration Control

- Maintain detailed system audits and control configurations.

Compliance Management

- Ensure adherence to regulatory requirements and industry standards.

Network segmentation

Knowledge+Technology+Expertise

Intrusion Prevention

- Enhance advanced threat detection to prevention capabilities by integrating with existing network equipment.

Restricted Data Flow

- Use SD-WAN and VLANs to optimize segmentation and data flow
- Enforce security controls even in remote and smaller locations.

IIoT Controls

- Implement security controls visibility with advanced secure by design gateways and protocols for IoT devices

Remote Access

- Utilize thin clients and secure gateways for controlled remote access

Mature security operations

Knowledge+Technology+Expertise

Industrial SOC Threat Intelligence

- Use real-time threat intelligence to protect against malware, phishing, vulnerabilities, and exploits

SOC Consulting

- Engage experts to enhance your SOC's ability to handle sophisticated threats.

Converged IT-OT Detection and Response

- Integrate IT and OT security for unified threat detection and response

Managed Protection

- Use managed detection and response services for continuous monitoring and expert incident handling

Fault tolerance and readiness

Technology

Expert Training

- Provide specialized cybersecurity training for staff to handle and mitigate faults effectively

Awareness Training

- Conduct regular training sessions to increase overall fault tolerance and readiness among all employees

Asset Performance Analysis

- Utilize tools and methodologies to analyze asset performance, ensuring reliability and identifying potential failures

Learn more about Kaspersky's approach to comprehensive cybersecurity at all levels

Kaspersky’s Power & Utilities track record

10+
years
of active experience in the sector

80+
projects
completed in nuclear, thermal, hydraulic and other energy sectors, including renewables

40+
Power & Utilities companies
already protected by Kaspersky

60,000+
licenses
Issued to customers

Kaspersky OT CyberSecurity provides comprehensive protection for the industrial infrastructure of power companies at all levels

Why Power & Utilities companies choose Kaspersky

Supports compliance and compatibility

- Solutions tested for compatibility with products from the largest vendors
- Provides robust cybersecurity measures that are compliant with multiple regulatory standards

Building scalable architecture

- Enhances transparency across ICS, taking the specific needs of power grid companies into account
- Supports legacy and contemporary systems, ensuring that all components of the ICS are protected

Integrates into a robust ecosystem

- Single-vendor solution offering comprehensive protection through a unified ecosystem
- Integrates corporate and industrial environments into a unified, secure infrastructure with end-to-end security

Successful case studies from Power & Utilities industry

In the last decade alone, Kaspersky has:

Delivered cybersecurity for the **world's 4th largest electricity-producing company** with a top-5 hydropower complex by installed capacity

Implemented protective solutions at the largest national electricity supplier responsible for generating **17% of the country's total electricity**

Executed an industrial infrastructure protection project for **a top-5 global renewable energy producer** with over 600 energy generation facilities

EMC

Serbia's largest energy operator

Learn more

Chose Kaspersky solutions after a thorough assessment of competitor offerings. Decisive factors for selection included the presents of a local partner and full compatibility with existing IT infrastructure.

Implemented KICS for Nodes and KICS for Networks, planning to deploy our KUMA SIEM platform.

€500 M
turnover

34
substations earmarked for KICS implementation

PacificLight

Electricity power generator and retailer

Learn more

Vulnerability assessment of their industrial networks to identify weaknesses and areas for improved security.

Simulated industry-specific attack vectors to uncover vulnerabilities, malicious activities and anomalies.

1 M
households served

10%
of total Singapore's electricity generation

Grid Company

Large power transmission company

Learn more

More than 150 servers and workstations in the Grid Company Group's process loop are protected by KICS for Nodes, while 10 KICS for Networks servers monitor key segments of the industrial network.

19239 MVA
Installed capacity

388
Substations

ROSATOM

The #1 nuclear power plant in Russia by installed capacity

Request Case Study

Implemented Kaspersky Industrial CyberSecurity to protect the infrastructure at all levels, from SCADA servers and operator workstations to programmable logic controllers (PLCs) and network equipment.

4337 MW
output

7 M
consumers

www.kaspersky.com

Manage your security with Kaspersky and become a partner

Contact us and take part in our global customer conference

Learn more

#kaspersky
#bringonthefuture