KASPERSKY lab

Kaspersky Industrial CyberSecurity: solution overview 2017

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity: solution overview 2017

Attacks on industrial systems are on the increase

Cyber-attacks on industrial control systems are not just on the increase, but have transitioned from speculative to indisputable[1]. 67% of IT/OT Security Managers perceive the current ICS cyberthreat level as critical or high, a more than 43% increase over last year's findings[2]. Business and supply chain interruption has ranked as the number one risk concern globally for the past five years; cyber-risk is the number one emerging concern[3]. For businesses operating industrial or critical infrastructure systems, the risks have never been greater. Industrial security has consequences that reach far beyond business and reputational protection. When it comes to protecting industrial systems from cyberthreats, there are specific and significant ecological, social and macro-economic considerations.

[1] PwC: Global State of Information Security 2015

[2] SANS 2016 State of ICS Security Survey

[3] Allianz Risk Barometer 2017

Operational technology vs. information technology

As defined by automation standard IEC 62443, an Industrial Control System (ICS) is a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial (technological) process.

Industrial Control Systems include but are not limited to:

- Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), Supervisory Control And Data Acquisition (SCADA) and diagnostic systems.
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operational functionality to continuous, batch, discrete, and other processes.

In more high-level terms, any industrial systems infrastructure can be broken down into two domains:

- Information Technology (IT) – systems required for managing data in the context of business goals
- Operational Technology (OT) – systems required for managing the physical, industrial processes of industrial automation.

IT security strategies tend to focus on data protection, and to follow the objectives of the 'C-I-A' model: Data Confidentiality, Integrity and Availability. However, for most OT systems, cybersecurity is not about 'data' but about the continuity of technological processes. So, in terms of the C-I-A model, 'availability' is a main focus of security strategies as applied to OT. This is what distinguishes industrial cybersecurity needs from those of other systems, meaning that the even most effective classical IT cyber-security solution is inappropriate for use on OT systems, putting the availability (and in some cases the integrity) of processes at risk.

Risks and threats

Despite a growing awareness of the prevalence of cyber-based attacks on industrial control systems, many IT security models continue to adhere to the outdated belief that physically isolating systems (through 'airgaps') and 'security by obscurity' is enough. It's not – in the era of Industry 4.0, most non-critical industrial networks are accessible via the internet[4], whether or not by choice. Extensive research by Kaspersky Lab ICS CERT, using data from the Kaspersky Security Network, indicates that industrial PCs are regularly attacked by the same generic malware that afflicts business systems (IT), including (but not limited to) well-known culprits such as trojans, viruses and worms. During the second half of 2016, Kaspersky Lab products across the globe blocked attempted attacks on 39.2% of all Kaspersky-protected computers classified as components of industrial infrastructure[5].

The 'Kido' (also known as Conficker) worm, although not industrial systems-specific, forced the shutdown of a German nuclear power plant for several days in April 2016 – not by direct penetration of the plant's control system, but through infecting the adjacent office network.

Another rising threat to the ICS is ransomware. The range and diversity of ransomware escalated massively between 2015 and early 2017. The emergence of ransomware is highly significant for the industrial sector – such infections can cause high-impact, wide-ranging damage to critical systems, making the ICS a particularly attractive potential target – as proven by several incidents of ransomware attacks hitting SCADA systems during 2016. Ransomware designed to attack industrial systems may have its own specific agenda – instead of encrypting data, the malware may set out to disrupt operations or to block access to a key asset.

As well as generic threats, industrial security must contend with ICS-specific malware and targeted attacks: Stuxnet, Havex, BlackEnergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack – the list is growing rapidly. As the Stuxnet and BlackEnergy attacks have shown, one infected USB drive or single spear-phishing email is all it takes for well-prepared attackers to bridge the air gap and penetrate an isolated network.

Many attacks targeting industrial complexes use both the corporate network and ICS to launch and propagate. During the BlackEnergy attack on the Ukrainian power grid in December 2015 that led to a severe energy shutdown, for example, hackers used several attack vectors. First, access credentials to the SCADA system were stolen from the corporate environment via a spear-phishing attack. The hackers then started turning off the power grid manually, and then planted a malicious KillDisk program that wiped or overwrote data in essential system files into the industrial network, causing the operator's machine to crash. In parallel, the utility's call center was DDoSed to prevent customers reporting the outage.

In addition to malware and targeted attacks, industrial organizations face other threats and risks targeting people, processes and technology – and underestimating these risks can have serious consequences. Kaspersky Lab develops solutions and services

[4] ICS and their online availability 2016, Kaspersky Lab

[5] Threat Landscape for Industrial Automation Systems for H2 2016, Kaspersky Lab ICS CERT

to help our customers tackle and manage not only malware and targeted attacks but also many other cyber-incidents and risk factors, such as:

- Mistakes by SCADA operators or contractors (3rd parties)
- Fraudulent actions
- Cyber-sabotage
- Compliance issues
- Lack of awareness and hard data for forensic investigation

The need for specialized industrial cybersecurity

Only cybersecurity vendors who understand the differences between industrial enterprises and data-oriented enterprises can deliver solutions that meet the unique security needs of industrial control systems and infrastructure. Forrester Research advises industrial organizations selecting a security vendor to "Look for specialized industry expertise." Forrester goes on to identify Kaspersky Lab as one of the few vendors with genuine specialist expertise in this sector.

Kaspersky Lab: trusted industrial cybersecurity provider

A recognized leader in cybersecurity and industrial protection[6], Kaspersky Lab is continually researching and developing solutions that do more to address constantly evolving threats to industrial and critical infrastructures. From operations management to the ICS level and beyond, Kaspersky Lab is playing a leading role in helping industry, regulators and government agencies globally to anticipate changes in the threat landscape and to defend against attacks.

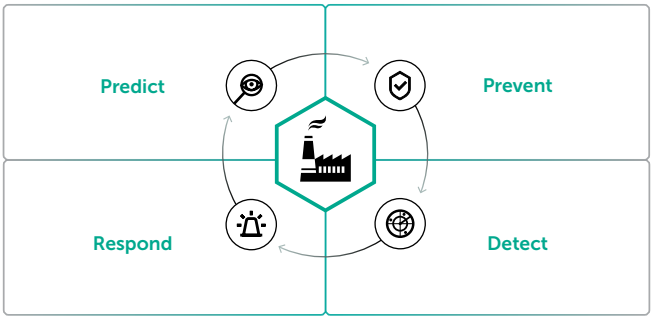
A trusted security provider and partner to leading industrial organizations who have relied for many years on our anti-malware protection, Kaspersky Lab collaborates with well-recognized industrial automation vendors and organizations, including Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium and others, to establish compatibility, specialized procedures and co-operation frameworks which protect industrial environments from existing and emerging threats, including highly targeted attacks.

Kaspersky Lab has developed a portfolio of specialized solutions to address specific industrial cybersecurity market needs – Kaspersky Industrial CyberSecurity (KICS). These solutions provide effective security from cyberthreats at all ICS layers – including SCADA servers, HMI, engineering workstations, PLCs

[6] Gartner Market Guide for Operational Technology Security, 2016

and industrial network connections – without impacting on operational continuity and the consistency of technological processes.

In keeping with Kaspersky Lab's overall multi-layered security strategy, Kaspersky Industrial CyberSecurity delivers a combination of protection methodologies. Taking a holistic approach to industrial cybersecurity – from predicting potential attack vectors, through specialized industrial prevention and detection technologies, to responding proactively to a cyber-incident – is the ultimate guarantee of your organization's uninterrupted and safe functioning.



The Adaptive Security Architecture

Kaspersky Industrial CyberSecurity: services

Our suite of services forms an important part of the KICS portfolio – we provide the full cycle of security services, from industrial cybersecurity assessment to incident response.

Knowledge (education and intelligence)

- **Training:** Kaspersky Lab offers training courses designed for both IT/OT security experts and ICS operators and engineers. During training, participants gain an insight into relevant cyberthreats, their developmental trends and the most effective methods to protect against them. Courses also enable security professionals to further develop their skills in specific areas, including ICS Penetration Testing and Digital Forensics.

- **Awareness Programs:** To increase awareness of relevant industrial cybersecurity issues, as well as fostering the skills needed to address and resolve them, Kaspersky Lab offers training 'games' for security managers and engineers. For example, Kaspersky Industrial Protection Simulation (KIPS)

simulates real-world cyberattacks on industrial automation systems, demonstrating the main issues associated with industrial cybersecurity provision.

- **Intelligence Reporting:** Up-to-date threat intelligence reports are prepared for you by our dedicated ICS Cyber-Emergency Response Team.

Expert services

- **Cybersecurity Assessment:** For organizations concerned about the potential operational impact of IT/OT security, Kaspersky Lab provides minimally invasive industrial cybersecurity assessment. A crucial first step in establishing security requirements within the context of operational needs, this can also provide significant insight into cybersecurity levels, even without further deployment of protection technologies.

- **Solution Integration:** If an organization's industrial control systems have a unique architecture or are based on custom hardware and software components not widely used in the industry, Kaspersky Lab can adapt recommended cybersecurity tools to work with these systems. This service incorporates support for unique software and hardware systems, including proprietary SCADA, PLCs, and industrial communication protocols.

- **Incident Investigation:** In the event of a cybersecurity incident, our experts will collect and analyze data, reconstruct the incident timeline, determine possible sources and motivation, and develop a remediation Plan. In addition, Kaspersky Lab offers a malware analysis service – within its framework, Kaspersky Lab experts will categorize any malware sample provided, analyze its functions and behavior, and develop recommendations and a plan for its removal from your systems and for rolling back any malicious actions.

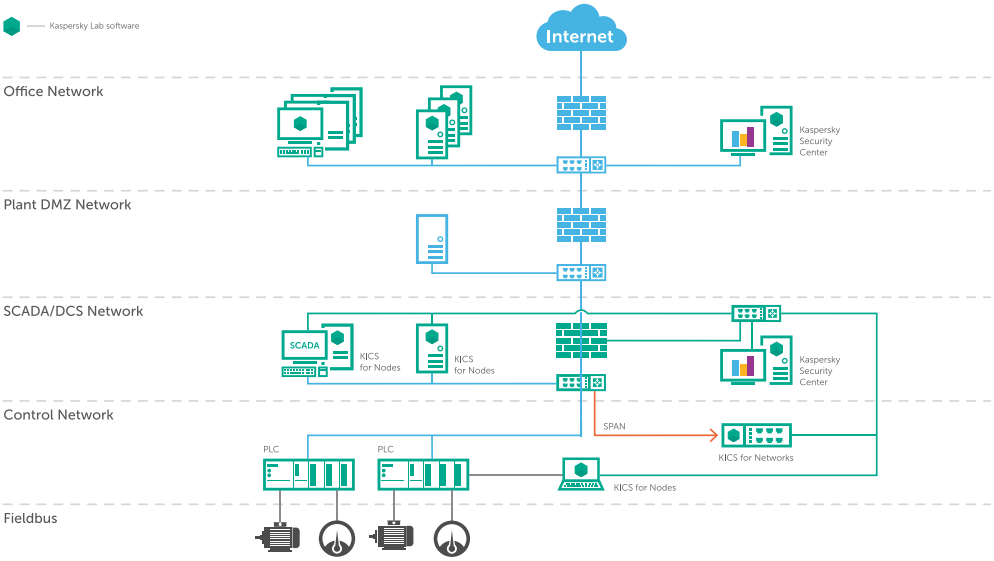
Kaspersky Industrial CyberSecurity: centralized security management

Kaspersky Security Center

To ensure the highest levels of protection from all attack vectors, security on the industrial floor should operate at both node and network levels. To ensure optimal control, ease of management and visibility, KICS – like all Kaspersky Lab protection technologies – is controlled via a single management console, Kaspersky Security Center, enabling:

- Centralized management of security policies - the ability to set different protection settings for different nodes and groups.
- Facilitated testing of updates before roll-out onto the network, ensuring full process integrity.
- Role-based access aligned with security policies and urgent actions.

Kaspersky Security Center ensures ease of control and visibility not only for industrial layers at multiple sites, but across the surrounding business floors, as illustrated below.



Kaspersky Security Gateway

KICS can also send event-related data to other systems, such as SIEMs, MESs and Business Intelligence solutions. All detected events and anomalies are reported to 3rd party systems – including SIEM, mail, syslog servers and network management systems – through CEF 2.0, LEEF and Syslog protocols. As well as helping detect, counter and investigate cyber-attacks, detailed industrial network monitoring supports predictive maintenance.

Integration with Human-Machine Interfaces (HMIs)

The solution can send security notifications directly to HMIs, providing industrial floor workers with specific information for immediate reaction to and escalation of the cyber-incident.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes was designed to specifically address threats at operator level in ICS environments. It secures ICS/SCADA servers, HMIs and engineering workstations from the various types of cyberthreat that can result from human factors, generic malware, targeted attacks or sabotage. KICS for Nodes is compatible with both the software and hardware components of industrial automation systems, such as SCADA, PLC, and DCS.

Threats and risks factors	Kaspersky Lab technologies
Unauthorized software execution	Whitelisting; prevention or detection-only (registration rather than blocking) modes
Malware	Advanced anti-malware signature-based detection engines; Cloud based detection engine, which uses Kaspersky Lab public cloud (KSN) or private cloud (KPSN)
Cryptors, including ransomware	Anti-cryptor
Network attacks	Host-based firewall
Unauthorized device connection	Device control
Unauthorized wireless connections	Wi-Fi network control
PLC programs spoof	PLC integrity check
ICS specifics — airgaps; false positives for ICS software/process, etc.	Trusted updates, which tested with software of leading industrial vendors; certification of product by leading industrial automation vendors.

Application whitelisting

The relatively static nature of ICS endpoint configurations means integrity control measures are significantly more effective than in dynamic, corporate networks. Integrity control technologies featured in KICS for Nodes include:

- Control of application installation and start-up according to whitelisting (best practice for industrial control networks) or blacklisting policies.
- Control of application access to operating system resources: files, folders, system registry etc.
- Control of all types of executable running in Windows environments, including .exe, .dll, .ocx, drivers, ActiveX, scripts, command line interpreters and kernel-mode drivers.

- Updating of application reputation data.
- Pre-defined and customer-defined application categories to manage controlled application lists.
- Fine-tuning of application controls for different users.
- Prevention or detection-only modes: blocking any application that isn't whitelisted or, in 'watching' mode, allowing applications which aren't whitelisted to run, but registering this activity in Kaspersky Security Center, where it can be assessed.

Device control

Management of access to removable devices, peripherals and system busses, based on device category, family and specific device ID.

- Support for both whitelisting and blacklisting approaches.
- Granular, per-computer, per-user policy assignment to a single user/computer or group of users/computers.
- Prevention or detection-only mode.

Host-based firewall

Set-up and enforcement of network access policies for protected nodes such as servers, HMIs or workstations. Key functionality includes:

- Control of access over restricted ports and networks.
- Detection and blocking of network attacks launched from internal sources, such as contractor laptops, which may introduce malware that attempts to scan and infect the host as soon as it joins the industrial network.

Wi-Fi network control

This enables the monitoring of any attempt to connect to unauthorized Wi-Fi networks. The Wi-Fi Control task is based on Default Deny technology, which implies automatically blocking connections to any Wi-Fi network 'not allowed' in the task settings.

PLC integrity check

This enables additional control over PLC configurations via periodical checks against a selected, Kaspersky Lab-secured server. The resulting checksums are compared against saved 'Etalon' values, and any deviations are reported.

Advanced anti-malware protection

Kaspersky Lab's best-in-class proactive malware detection and prevention technologies are adapted and re-designed to meet heavy resource consumption and system availability requirements. Our advanced anti-malware protection is designed to work effectively even in static or rarely updated environments. Kaspersky Lab's anti-malware covers the full spectrum of technologies, including:

- Signature based malware detection.
- On-access and on-demand detection.
- In-memory (resident) detection.
- Ransomware detection via special Anti-Cryptor technology.
- Kaspersky Security Network (KSN) and Kaspersky Private Security Network (KPSN), enabling the ultimate malware detection service.

Trusted updates

To ensure Kaspersky Lab security updates have no impact on the availability of the protected system, compatibility checks are performed prior to both database/component releases and process control system software/configuration updates. Potential resource consumption issues can be addressed through a number of different scenarios:

- Kaspersky Lab performs database update compatibility tests with SCADA vendor software on the Kaspersky Lab test bed.
- Your SCADA vendor performs compatibility checks.
- Kaspersky Lab checks security database updates for you: SCADA, workstation, server and HMI images are integrated into Kaspersky Lab's test bed.
- Kaspersky Lab security updates are tested on your site and automated via Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Lab's network level security solution operates at the industrial communication protocol (Modbus, IEC stack, ISO, etc) layer, analyzing industrial traffic for anomalies via advanced DPI (Deep Packet inspection) technology. Network integrity control and IDS capabilities are also provided.

Threats and risks factors	Kaspersky Lab technologies
Appearance of unauthorized network devices on industrial network	Network Integrity Control detects new / unknown devices
Appearance of unauthorized communications on industrial network	Network Integrity Control monitors communications between known/unknown devices
Malicious PLC commands by: • Operator or 3rd party (e.g. contractor) in error • Insider (fraud actions) • Attacker / Malware	Industrial DPI analyzes communications to and from PLCs and control of the commands and parameter values of the technological process.
Network attacks	An Advanced Intrusion Detection System identifies all known network attack patterns, including the exploitation of vulnerabilities in industrial software and hardware
Lack of data for investigation and forensics	Forensics tools: monitoring and safe logging of suspicious industrial network events and detected attacks

Non-intrusive industrial network traffic inspection

KICS for Networks delivers passive network traffic monitoring of anomalies and network security while remaining invisible to potential attackers. Installation is as simple as enabling/configuring port mirroring; easy integration of the software/virtual or hardware appliance into existing industrial network equipment is achieved via the SPAN port of the existing switch or TAP device. KICS for Networks has a modular architecture – sensors can be deployed separately from a central control unit.

Industrial DPI for anomaly detection

KICS for Networks supplies industrial users with a trusted platform for monitoring process control command flow and telemetry data, enabling, among other things:

- Detection of any command which would reconfigure a PLC or change the PLC state.
- Control parameter changes in technology processes.
- Protection against outside threats while mitigating the risk of 'advanced' insider interference from engineers, SCADA operators or other internal staff with direct access to systems.

Machine Learning

Our industrial DPI can not only be configured by a standard rule-based approach – it can also detect anomalies inside industrial processes via a powerful LSTM-based forecasting model. Machine learning capability brings industrial anomaly detection to a new level, making incident discovery possible in the most complex and frequently reconfigured industrial networks.

Network integrity control for security and assets inventory

KICS for Networks enables the identification of all Ethernet connected network assets – including SCADA servers, HMIs, engineering workstations, PLCs, IEDs and RTUs. All new or unknown devices and their communications are detected automatically. This gives security teams the capacity to develop their own reliable, secure network asset inventory, rather than using potentially vulnerable OT/IT asset management tools which are highly targeted by attackers.

Forensic tools

Kaspersky Lab's solution gives industrial users a safe logging system, which provides tools for data analysis and digital forensics. The system also prevents any changes to ICS logs.

Additional services for Kaspersky Industrial CyberSecurity

Kaspersky Security Network

Kaspersky Security Network (KSN) is a cloud-based, complex distributed architecture dedicated to gathering and analyzing security threat intelligence from millions of nodes worldwide. KSN not only detects and blocks the newest threats and zero-day attacks, but also helps locate and blacklist online attack sources, providing reputational data for websites and applications.

All Kaspersky Lab corporate solutions, including industrial solutions, can be connected to KSN if required. Key benefits include:

- Superior detection rates.
- Reduced reaction times – traditional signature-based responses take hours: KSN responds in about 40 seconds.
- Lower false positive rates.
- Reduced resource consumption for on-premise security solutions.

Kaspersky Private Security Network (KPSN)

For organizations that have very specific data privacy concerns, Kaspersky Lab has developed the Kaspersky Private Security Network option. It provides almost all the advantages of KSN, but without sending any information whatsoever outside the network.

KPSN can be deployed within any organization's own data center, where in-house IT specialists retain complete control over it. Local KPSN installations can help meet country-specific compliance requirements or other industry-specific legislation.

Key KPSN functions:

- File and URL reputation services: MD5 hashes for files, regular expressions for URLs and malware behavior patterns are centrally stored, categorized and rapidly deployed to client
- Record Management System (RMS): Sometimes security software makes mistakes and incorrectly categorizes files or URLs as trusted/not trusted. RMS acts as a 'false positives' deterrent, rectifying errors as well as continuously analyzing to improve quality
- Cloud-based intelligence and information.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and the consistency of technological process.

Learn more at
www.kaspersky.com/ics

All about ICS cybersecurity:
https://ics-cert.kaspersky.com
Cyber Threats News: www.securelist.com

#truecybersecurity

www.kaspersky.com

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize