

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 indisputable¹. 67% of IT/OT security managers perceive the current ICS cyber-threat to be critical or high, a more than 43% increase over 2015 findings².

During the 2015 fiscal year, ICS-CERT responded to 295 reported cyber-incidents involving critical infrastructure in the United States — a more than 20% increase over 2014³.

Supply chain and business interruption has ranked as the number one risk concern globally for the past three years; cyber-risk is the number one emerging concern⁴.

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 cyber-threats, there are specific and significant ecological, social and macro-economic considerations.

Operational technology vs. information technology

Industrial Control System (ICS) is a term used collectively to describe automated systems that control industrial production. The term ICS covers a broad spetrum of computers, proprietary control devices and network architectures used to control industrial processes across a wide range of industries. An ICS typically includes SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems) and PLCs (Programmable Logic Controllers).

In terms of organizational systems, these can be broken down into two categories:

- Information Technology (IT) systems required for general business purposes
- Operational Technology (OT) systems required for industrial automation purposes.

Many IT security strategies are focused on data protection and rely on the concept of the 'C-I-A' model: data **Confidentiality**, **Integrity** and **Availability**. Most OT systems prioritize continuity above all else; protection is not about 'data' but about 'process': **Availability**, **Integrity** and **Confidentiality**, in that order. This is what distinguishes industrial cybersecurity needs — the highest quality security solution is effectively useless if it puts the availability (and in some cases the integrity) of processes at risk.



¹ PwC: Global State of Information Security 2015

² SANS 2016 State of ICS Security Survey

³ ICS-CERT Monitor, November — December 2015

⁴ Allianz Risk Barometer 2015

RISKS AND THREATS

Despite growing awareness 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 available via the Internet 5 , whether or not by choice.

Extensive research by Kaspersky Lab, using data from the Kaspersky Security Network, indicates that majority of industrial PCs are infected with the same generic malware afflicting business systems (IT), including (but not limited to) well-known culprits such as Trojans viruses, worms, Potentially Unwanted and dangerous Programs (PUPs) and other exploits targeting vulnerabilities in the Windows operating system.

The Kido (also known as Conficker) worm, although not industry-specific, has not only been found in critical medical equipment, but is suspected to have been a 'door-kicker' for high-profile attacks on industrial targets. Kido is capable of completely overloading networks and bringing vital processes to a halt. Traditional industrial security techniques fail address these threats adequately: an 'air-gap' or 'security through obscurity' strategy doesn't address the reality that smart grid systems and cloud-based SCADA mean that Industrial Control Systems are coming more and more to resemble consumer PCs⁶.

Another rising threat to the ICS is ransomware. The range and diversity of ransomware's escalated massively between 2015 and early 2016. The emergence of ransomware is highly significant for the industrial sector — such infections may cause high-impact, wide-ranging damage to systems, making the ICS a particularly attractive potential target. Ransomware designed to attack industrial systems may have its own specific agenda — instead of encrypting files, 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 targeted attacks and ICS-specific malware: Stuxnet, Citadel, Energetic Bear/Havex, Miancha, BlackEnergy, Irongate, PLC Blaster — the list is growing rapidly. As the Stuxnet and Black Energy 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 industrial-specific attacks 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 severe energy shutdown, for example, hackers used several attack vectors. First, access credentials to the SCADA system was stolen from the corporate environment via a spear-phishing attack. The hackers then started turning off the power grid manually, and then planting a malicious KillDisk program that wiped or overwrote data in essential system files into industrial network, causing the operator's machine to crash. In parallel, the utility's call center was DDoSed to prevent customers reporting the outage.

⁶ EU Agency for Network and Information Security (ENISA): 'Can we learn from SCADA security incidents?'



⁵ ICS and their online availability 2016, Kaspersky Lab

In addition to malware and targeted attacks, industrial organizations face other threats and risks targeting people, process and technology — and underestimating these risks can also have serious consequences. Kaspersky Lab has developed a comprehensive portfolio of technologies, solutions and services to help our customers tackle and manage many of these risks, such as:

- Mistakes by SCADA operators or contractors (3rd parties)
- · Fraudulent actions
- Cyber sabotage
- Compliance
- Lack of awareness and hard data for incident forensics
- · Lack of incident reporting

The need for specialized industrial cybersecurity

Only cybersecurity vendors who understand the differences between industrial systems and standard, business-oriented enterprises can deliver solutions that meet the unique security needs of industrial control systems and infrastructure. For rester Research advises industrial organizations selecting security vendors to "Look for specialized industry expertise?." For rester goes on to identify Kaspersky Lab as one of the few vendors offering specialized industrial cybersecurity solutions who have genuine expertise in the sector.

⁷ Forrester Research: S&R Pros Can No Longer Ignore Threats to Critical Infrastructure, by Rick Holland



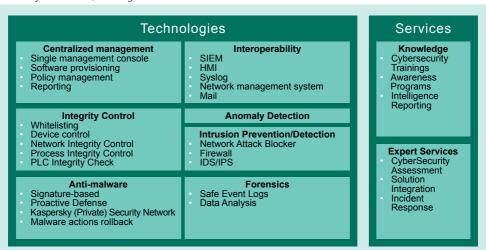
KASPERSKY LAB: TRUSTED INDUSTRIAL CYBERSECURITY PROVIDER

A recognized leader in cybersecurity and industrial protection⁸, Kaspersky Lab is continually researching and developing solutions that do more to address the constantly evolving threats to industrial and critical infrastructures. From operations management to the SCADA level and beyond, into a future where secure operating environments will be a reality, 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 leading industrial automation vendors and organizations, including Emerson, SAP, Siemens, Industrial Internet Consortium and others to establish compatibility, specialized procedures and co-operation frameworks that protect industrial environments from existing and emerging threats, including APTs and highly targeted attacks.

Kaspersky Lab is developing a portfolio of specialized solutions to address specific industrial cybersecurity market needs — Kaspersky Industrial CyberSecurity. These solutions provide effective security at all industrial layers — including SCADA servers, HMI panels, workstations, PLCs and network connections — from cyber-threats, without impacting on operational continuity and consistency of the technological process.

In keeping with Kaspersky Lab's overall multi-layered security strategy, Kaspersky Industrial CyberSecurity delivers a combination of protection types. In addition to the technologies and services that support every stage of the security cycle, Kaspersky Industrial CyberSecurity delivers protection in support of integrity control, intrusion prevention and detection, anti-malware and anomaly detection, among others.





KASPERSKY INDUSTRIAL CYBERSECURITY: SERVICES

Our suite of services form an important part of the Kaspersky Industrial CyberSecurity portfolio - we provide the full cycle of security services, from industrial cybersecurity assessment to incident response.

Knowledge (education and intelligence)

CyberSecurity Training: Kaspersky Lab offers training courses designed for both IT/OT security experts and ICS operators and engineers. During training, attendees gain an insight into relevant cyber-threats, trends in their development and effective methods for protecting against them.

Awareness Programs: To increase awareness of relevant industrial cybersecurity issues, along with developing 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 cyber-attacks on industrial automation systems, demonstrating the main issues associated with providing of industrial cybersecurity.

Intelligence Reporting: Up-to-date security intelligence reports prepared by leading cybersecurity experts, tailored to industrial customer specifics.

Expert Services

CyberSecurity Assessment: For organizations concerned about the potential operational impact of IT/OT security, Kaspersky Lab provides a minimally invasive pre-installation 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, without any further deployment of protection technologies.

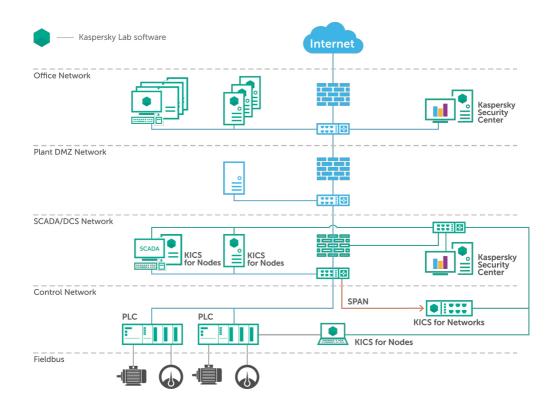
Solution Integration: If a customer's industrial control systems have a unique architecture or are based on custom hardware and software components not widely used in the industry, Kaspersky Lab can adapt recommended cybersecurity tools to work with these systems. The service includes support for unique software and hardware systems, including SCADA and PLCs, and their industrial network 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 plan to provide remediation. 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

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, Kaspersky Industrial CyberSecurity — like all Kaspersky Lab protection technologies — is controlled via a single management console, Kaspersky Security Center. This centralized management capability ensures ease of control and visibility not only of the industrial layers at multiple sites, but across the surrounding business floors too, as below image illustrates.





KASPERSKY INDUSTRIAL CYBERSECURITY FOR NODES

Kaspersky Industrial CyberSecurity for Nodes was designed to specifically address threats within ICS/SCADA environments. It works at the ICS/SCADA server, Human-Machine Interface and engineering workstation layers to deliver optimal security from various cyber-threats caused by human factor, generic malware, targeted attacks or sabotage. It's compatible with both the software and hardware components of industrial automation systems, such as SCADA, PCS, and DCS.

| Threats and Risks factors | Kaspersky Lab Technologies |
|--|---|
| Unauthorized software execution | Whitelisting; prevention or detection-only modes (not |
| | blocking but registering) |
| | Advanced Anti-Malware: signature-based and proactive; |
| Malware, including 0-days | Automatic Exploit Prevention and Kaspersky (Private) |
| | Security Network (KPSN) |
| Network attacks | Host-based Firewall and Network Attack Blocker |
| Unauthorized device connection | Device Control |
| Software vulnerabilities | Vulnerability Assessment |
| PLC programs spoof | PLC Integrity Check |
| ICS specifics — airgaps; false positives | Trusted Updates; KPSN; certification by leading ICS |
| for ICS software/process, etc. | vendors; cooperation on whitelists. |

Software and hardware integrity control

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 Kaspersky Industrial CyberSecurity for Nodes include:

Application Start-up Control and Application Privilege Control

Among other things, Application Control mechanisms enable:

- 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 a Windows environment, including: exe, dll, ocx, drivers, ActiveX, scripts, command line interpreters and kernel-mode drivers
- · Update 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 that aren't whitelisted to run but registering this activity at the Kaspersky Security Center, where it can be assessed.



Device Access Control

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

- Support for both white-and-blacklist 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 and network attack blocker

Set-up and enforcement of network access policy for protected nodes such as servers, HMIs or workstations. Key functionalities include:

- · Control access over restricted ports and networks
- Detect and block 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

Automatic exploit prevention

This enables an isolation layer to protect SCADA processes from malicious memory injections or modifications, such as exploit payloads.

PLC integrity check

Enable additional control over PLC configuration via periodical checks against a selected, Kaspersky Lab-secured server or workstations. The resulting checksums are compared against saved "Etalon" values, and 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, heuristics and behaviour-based malware detection
- On-access and on-demand detection
- In-memory (resident) detection
- · Rootkit detection
- 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 both to database/component releases and to 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 in 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.

Vulnerability assessment

Passive vulnerability assessment capability: detection and information on software vulnerabilities with zero disruption of technology processes.

Centralized deployment, management and control

Kaspersky Industrial CyberSecurity for Nodes is deployed and managed via a centralized console, 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 into network, ensuring full process integrity
- Role-based access aligned with security policies and urgent actions.



KASPERSKY INDUSTRIAL CYBERSECURITY FOR NETWORKS

Kaspersky Lab's network level security solution operates at the process control abstraction layer, analyzing and inspecting the sources of traffic while providing integrity control for both industrial network and industrial control processes. An integrated stack of complementary technologies form an efficient anomaly detection engine.

| Threats and Risks factors | Kaspersky Lab Technologies |
|---|--|
| Appearance of unauthorized network | Network Integrity Control detects new / unknown |
| devices on industrial network | devices |
| Appearance of unauthorized | Network Integrity Control monitors communications |
| communications on industrial | between known/unknown devices |
| network | |
| Malicious PLC commands by: | |
| Operator or 3rd party | Monitoring of communications to and from PLCs |
| (e.g. contractor) in error | and control of the commands and parameter values |
| • Insider (fraud actions) | of the technological process. |
| Attacker / Malware | |
| Lack of data for operators on cyber- | Alerts the operator (via HMI integration) to malicious |
| security incidents | or suspicious technological process parameter changes. |
| Lack of data for investigation | Forensics tools: monitoring and safe logging |
| and forensics. | of industrial network events. |

Passive industrial network traffic inspection, effective security monitoring

Kaspersky Industrial CyberSecurity for Networks delivers passive network traffic analyses of anomalies while remaining invisible to potential attackers. Installation is as simple as enabling/configuring port mirroring; easy integration into existing industrial infrastructure is achieved via the SPAN port of the existing switch or TAP device.



Hierarchical architecture, single point of control

Network traffic sensors passively connected to the controlled network segment via the SPAN port or TAP device are managed via a single control unit that provides the following functionality:

- Retrieve and store event data from all sensors use data for incident response and investigation/ forensics
- Report all detected events and anomalies to 3rd party systems including to SIEM, mail, syslog servers and network management systems through SNMP protocol
- · Monitor overall systems health
- Managed via Kaspersky Security Center or local interface.

Trusted industrial process control monitoring

Kaspersky Lab's solution 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, including STOP, PAUSE, change PLC program, change PLC firmware
- Control of technology process parameters and algorithms
- 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.

Network integrity and asset visibility

Kaspersky Industrial CyberSecurity for networks enables the identification of all Ethernet connected network assets — including SCADA servers, HMI, engineering workstations, PLCs 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.

Forensics

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



ADDITIONAL SERVICES FOR KASPERSKY INDUSTRIAL CYBERSECURITY PRODUCTS: 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.



Learn more about Industrial CyberSecurity at: www.kaspersky.com/ics

© 2016 Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.