Cybersecurity for Electric Power Infrastructure

www.kaspersky.com/ics
#truecybersecurity

Contents

Cybersecurity for Electric Power Infrastructure

A modern electrical power system is a complex technical facility, unique in terms of its scale and importance for human life. Given the physical characteristics of electrical energy and the typical high speed of electrical processes, controlling the operation of such a facility is a complex task from both an organizational and technical point of view – which is why devices designed for the emergency protection of power equipment and automation appeared at the same time as the power industry began. The requirements for these devices, their design and functionality have evolved alongside the electrical power systems they protect, in response to growing consumer and operation demands.

Today's Protection, Automation and Control System (PACS) is a complex set of interrelated information systems covering all areas of electric power facility operation. The rapid development of computing and communication technologies has changed the protection and automation systems of electric power components. In addition, new control features integrated into modern protection and automation systems change the construction principles of power supply network facilities.

Improving quality of control is one of the main tasks of future electric power development and transition to Smart Grid systems. Control systems therefore play a key role in the generation, transportation and distribution of electricity.

Today PACS are highly integrated and use digital communication technologies based on open international standards, such as IEC 60870, IEC 61850 and IEC 61970. The integration of separate subsystems enhanced the capabilities of protection and control systems, making them more intelligent and efficient to use. In addition, common standards significantly reduced the cost of integration and provided a higher level of functional reliability.

A modern system for control and protection of power facility includes different types of information subsystems, such as:

- hardware and software appliances for automated dispatching control
- automatic control for maintenance of electric power system operation modes
- protection systems
- automatic emergency protection systems
- process control systems
- automated electric power metering systems
- electricity quality control systems

Vulnerability of Electric Power Facility Pacs When Faced with Information Security Threats

The high level of openness and integration of electric power systems, combined with the pervasiveness of IT and Internet technologies in daily life, has raised new challenges for the electric power sector. Modern automated protection and control systems for electric power facilities are integrated distributed computing systems, which communicate through open protocols. In such systems, cybersecurity is low priority, because electric power control systems had been constructed as isolated solutions. However, for modern control systems, which are globally integrated and connected with corporate services, cybersecurity risks are very high.

In the IEC 62351 "Power systems management and associated information exchange – Data and communications security" standard, the following issues of information security at electric power facilities and their causes are emphasized:

Open Communications

Open and unprotected communication lines between protection and control system components, as well as between power infrastructure facilities:

- **Lack of Identity Verification**
  Weak or no authentication of interacting agents: for example, a random network device on the technological network can send incorrect or malicious control commands to a top level system that, in turn, could cause a dispatching operator to execute invalid actions

- **Open Standards and Open Data Transmission**
  The data transmission protocols used are based on publicly available, open, and well-documented standards. Free implementations of protocols and their source code, together with tools for analysis and emulation are publicly available. Data transmitted in such networks is usually open for capturing, reading, modification and replay, simplifying access and threat execution for potential intruders

- **High Level of Network Communications**
  The high levels of communication between IEC 60807-5-10x and IEC 61850 MMS protocols are a normal aspect of their operation. But these open communications can also facilitate simple denial of service attacks on technological infrastructure devices (for example, dispatching center process control system, or protection terminals) via the mass sending of invalid data packets

- **Connections to Public Networks**
  The corporate and technological networks of a modern industrial facility may have multiple interconnections at almost every hierarchy level of control system, which increases the risk of unauthorized external access to technological equipment

Lack of Cybersecurity Awareness Among Employees

A limited number of technical personnel maintain large numbers of devices that are often distributed on a territory and function without permanent monitoring. On-site personnel often lack even a basic knowledge of cybersecurity:

- **Privileged Remote Access From An Untrusted Network**
  For easy maintenance and convenience, technical staff often enable full-privilege access to remote facility equipment. Such access is often organized unofficially and insecurely, for example, from corporate workstations with Internet access

- **Lack of Password Protection and User Control Policies**
  A large number of devices maintained by a limited number of personnel makes it difficult to organize and maintain device access policies, including password protection and user control policies. As a result, technological devices are often operated with default passwords, simplifying unauthorized access

- **Outdated Software**
  IED software is almost never updated during its lifecycle on technological facility. Known software bugs are not eliminated unless they directly affect industrial processes

- **Maintenance from Unsafe Workstations**
  Portable workstations (notebooks) used in the course of technological infrastructure maintenance are often also used as regular corporate workstations as well as “test lab” equipment for software testing or for personal needs

- **Lack of Regular Configuration and Software Control**
  Device configuration and software verification checks are performed manually and irregularly, not more often than once a year

Security Requirements are Not Followed

Information Security requirements are rarely considered in the device or software design and development processes for technological infrastructures.

- **Weak Resistance To Hacking**
  Developers do not usually consider the vulnerability of their code to targeted attacks or illegitimate actions on technological infrastructure and its elements. This means resistance to device hacking is generally weak

- **Invalid or Insufficient Network Security Settings**
  Invalid settings of network segmentation and access control between network segments in the technological network, Absence of specific network design solutions in PACS implementation projects is a typical problem. For this reason, the quality of network infrastructure setup usually depends on the skills and qualifications of the installation team

- **Absence of Data Protection When Transmitted via Open Channels**
  There is a lack or absence of secure means for data transfer over open communication lines

- **Absence of Role-Based Access Control**
  Absence of role-based access controls can enable incorrect access permissions to devices, allowing users access that does not correspond to their official duties

- **Absence of Application Startup Control Solutions**
  The absence of compatible solutions to protect computer systems from unauthorized application startup often leaves systems unprotected from the launch of unauthorized software in industrial environments. General tools for application startup control are often incompatible or ineffective with industrial systems (incompatibility with technological software, insufficient resources on specific technological systems, etc.)

- **Absence or Insufficiency of Security Event Registration Tool**
  There are no specific monitoring and cybersecurity event registration tools within process control systems, or their functionality is insufficient to provide the correct interpretation of a situation

Complexities of Contractor Access Control

The use of contracting organizations for certain types of maintenance work is common. Consequently, it is extremely important to provide only temporary access to a limited amount of equipment that has no influence on other system components. Cancellation of access on completion of the work is vital.

Long Lifetime of Vulnerable Components

The lifetime of devices and protection and control systems is 20-30 years; insecure systems installed today will only be replaced in a couple of decades or so. Partial upgrade is usually extremely difficult as soon as secure solutions (for example, those using encryption) are often incompatible with standard vulnerable solutions.

In addition to the technical issues listed above, there are also important organizational issues. Firstly, the lack of guides defining actions to be taken when suspicious activity is detected within automated systems. Secondly, the lack of documents and practices relating to the investigation of disturbances in technological environments including malicious influence on control systems through information technologies. For example, due to their age, some reference documents for the investigation and classification of technological disturbances do not even consider cybersecurity incidents as a possible cause of malfunction. If such an incident even takes place, the real causes will not be revealed. As a result, the appropriate measures will not be taken and the incident may reoccur.

The above shows that there are is obviously several systemic problems:

- Modern electric power systems for protection and power equipment control are not isolated and not closed systems
- Protection, automation and control systems do not have sufficient built-in cybersecurity functions
- From organizational and technical points of view, detection of negative influence is extremely difficult under the present conditions
- There is an absence of clear guidelines on how to respond when attacks are detected

Technical Solutions for Cyber-Security Threat Prevention, Detection and Mitigation

The IEC 62351 “Power systems management and associated information exchange - Data and communications security” standard describes in detail the possible tools for complex information security provision at electric power facilities. However, most of the proposed solutions can only be implemented with a complete replacement of automation devices as soon as they require format and communication protocol procedure modifications.

Even though a full implementation of IEC 62351 looks like a distant prospect under the circumstances, part of the requirements can be fulfilled and applied to modern systems.

Kaspersky Industrial CyberSecurity (KICS) is a holistic solution for industrial infrastructures that fulfills these requirements.

The solution consists of two components:

- KICS for Nodes – a component for industrial network endpoint protection (such as engineering stations, operator stations, SCADA servers)
- KICS for Networks – a component for industrial network monitoring with network integrity checking and deep application protocol inspection capabilities (IEC 60870-5-104, IEC 61850, etc. for electric power infrastructures)

KICS for Nodes

KICS for Nodes is a specialized product for industrial systems. As a computer software application, it is designed to protect technological servers, engineering and operator workstations as well as HMI running OS Windows.

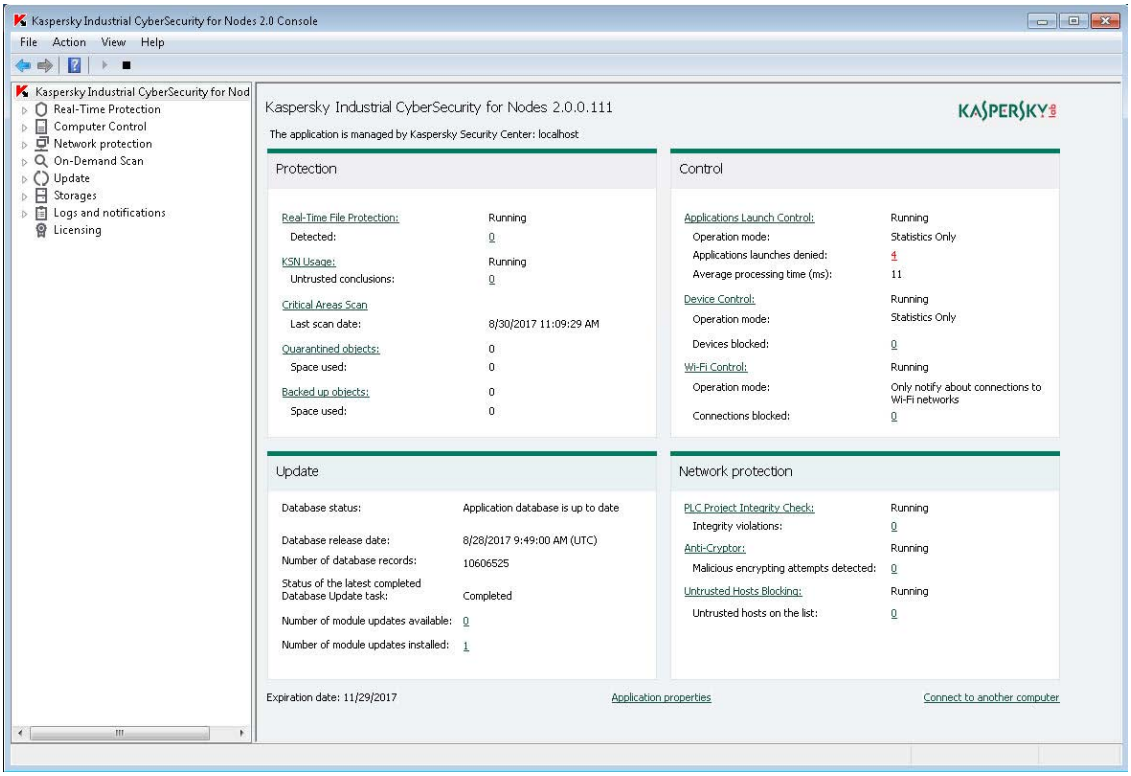

Image #1. KICS for Nodes local interface

The main solution functionalities:

- Application whitelisting (Application startup control) – blocks all applications from launching except those that are explicitly allowed. The protection component provides test mode to support easy setup and debugging at deployment stage
- Device control – allows administrators to define and specify which devices can be connected to protected industrial hosts. The technology provides opportunities to protect industrial systems from unauthorized device connections. The technology supports masks for easy administration and bulk device operation
- Wi-Fi network control – enables the monitoring of any attempt to connect to unauthorized Wi-Fi networks
- Malicious software detection (including ransomware) – combines signature and heuristic protection methods to protect Windows workstations against known, unknown and advanced threats. Special Anti-Cryptor technology allows to prevent ransomware attacks
- Host-based firewall – provides abilities to limit network connections to industrial hosts
- PLC integrity check – enables additional control over controller configuration via periodical checks of any changes in projects

KICS for Nodes can be centrally managed after integration into a security infrastructure control system based on Kaspersky Security Center, making it possible to perform the following functions:

- Centralized management and security policy control – feature allows configuration of security settings for both individual devices and groups
- Centralized update of antivirus databases on protected network nodes (even if the technological network is not connected to the Internet) – that helps to support a high security level due to the update of security agents from a single control server within the technological network. Updates can be downloaded to the control server directly from the Internet from a retransmission node (installed on the IT network or DMZ), or transferred to the control server by an administrator via USB devices
- Testing of new updates before distribution – allows updates to be checked for compatibility with industrial software prior to distribution on industrial hosts
- Role-based model for separate policy management and actions with the security agent – eliminates the possibility of unauthorized security policy changes on the control server, as well as preventing protection disabling or endpoint solution setting changes
- Centralized collection of endpoint security events data of enables comprehensive information security data analysis based on registered events, while identifying the exact causes of incidents and facilitating mitigation planning

It should be noted that operation of KICS for Nodes is based on approaches that, by default, do not impact on industrial processes.

KICS for Networks

KICS for Networks is a specialized software solution for industrial network monitoring. The solution can identify anomalies and register important information events taken from industrial network traffic without interfering on industrial process.

The main solution functions are:

1. Network integrity monitoring:

- Self-training mode that allows detection and registration of all available LAN nodes and communications between them – this data can be used as a reference point and for change tracking
- IP and MAC address-based detection and registration of new network devices connected to the controlled segments of the technological network
- Detection and registration of new network communications between nodes based on the following attributes: sender node address, recipient node address, network protocol, port, number of allowed connections, etc.

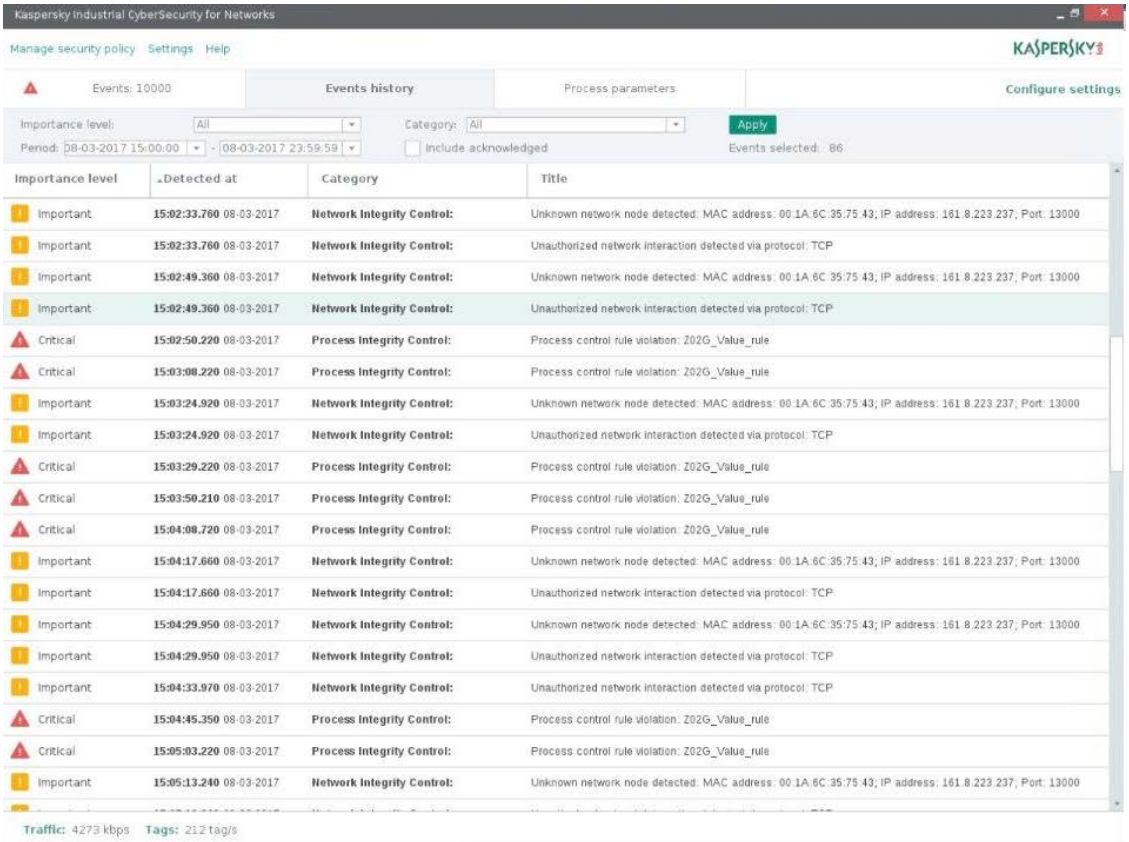

Image #2. KICS for Networks local interface

2. Deep packet inspection:

- Review, analysis and registration of important messages of technological protocols according to configuration:
  - Detection of device management commands (for example, switching On/Off) via industrial network protocols (IEC 61850, IEC 60870-5-104)
  - Detection of commands to change protection and control system operation parameters (for example, set-point group switch) via industrial network protocols (IEC 61850, IEC 60870-5-104)
  - Detection of IED control and parameterization attempts with service software via controlled network segment
- General telemetering message monitoring

3. Events storage:

- KICS for Networks system provides storage of detected events in an internal secure database
- The information is limited by storage period and the limit of archive size. An example of the solution shown in Img #3 illustrates one potential deployment scenario for KICS for Networks and KICS for Nodes deployment scenarios

KICS for Nodes and KICS for Networks: An Example of Deployment at a Modern Electrical Power Substation

A secured protection and control system includes two LAN segments of ring topology. The first segment of the electrical power substation is the station bus (according to IEC 61850), which provides communications between IEDs. In addition, substation bus, substation controllers and telemetering gateways are used for informational interaction with higher levels of dispatching control. The LAN segment provides access to the protection and control system equipment by means of engineering software. Service access can be provided both locally and remotely. Local service access is provided using a notebook connected directly to IEDs or to the station bus LAN. Service access can also be performed from a remote workstation. Prompt communications between network nodes during stable operation are conducted according to protocol IEC 61850 MMS.

Service communications regarding the parameterization of protection and control system devices are provided under the internal application protocols of the equipment manufacturer.

The physical LAN segment of the bus is a ring network, formed by two connected switches. All devices are connected to the switches as double attached nodes (DAN). Therefore, there is no single point of failure on the segment that provides a higher level of network reliability. The IEDs are equipped with built-in switches and combined in chains. The ends of chains are connected to the ring network switches; therefore, traffic between the devices of one chain is not transmitted via ring network switches. Ring topology network control is executed using the RSTP. The network switch is included to provide remote service access to the industrial network through a VPN.

The second segment – operator network segment – is also represented by a ring network topology designed for operator workstations and process control system server's interaction.

Interaction with Network Control Center and System Operator is provided directly through a substation controller connected to the automation system (See Img #3). Exchange is performed through protocol IEC 60870-5-104.

KICS for Networks installation is required in each of the selected network segments, to provide complete monitoring of the technological network infrastructure. Thus, three KICS for Networks servers should be installed for the stated diagram: one for the station bus segment, one for the operator network segment and one for the communication line to higher levels of control. To connect KICS for Networks servers to the infrastructure, switching equipment reconfiguration is required to forward all SPAN traffic of each network segment to the corresponding server.

The KICS for Networks server is connected to the SPAN ports of network switches. This configuration provides opportunities to receive industrial traffic only, without impacting on the industrial process. KICS for Networks processes industrial traffic and detects suspicious events. The data associated with registered events is encrypted and securely stored. In addition, events are transmitted via encrypted channel to Kaspersky Security Center, providing security specialists with a final list of detected events.

KICS for Nodes software has to be installed on each industrial host, to protect computer infrastructure running Windows OS. KICS for Nodes also sends detected events to the Kaspersky Security Center server. The industrial hosts should contain an additional network interface to connect to control network segment.

All control network communications are encrypted. In the event of control network failure, KICS for Networks and KICS for Nodes components will continue their operation in standalone mode. Collected data will be transmitted to Kaspersky Security Center when the network segment operation is restored.

KICS supports integration with SIEM systems. Kaspersky Security Center organizes an encrypted channel with the SIEM system and transfers configured events into the SIEM (HP ArcSite, IBM QRadar and others through Syslog format). Notifications can also be sent using email and SMS.

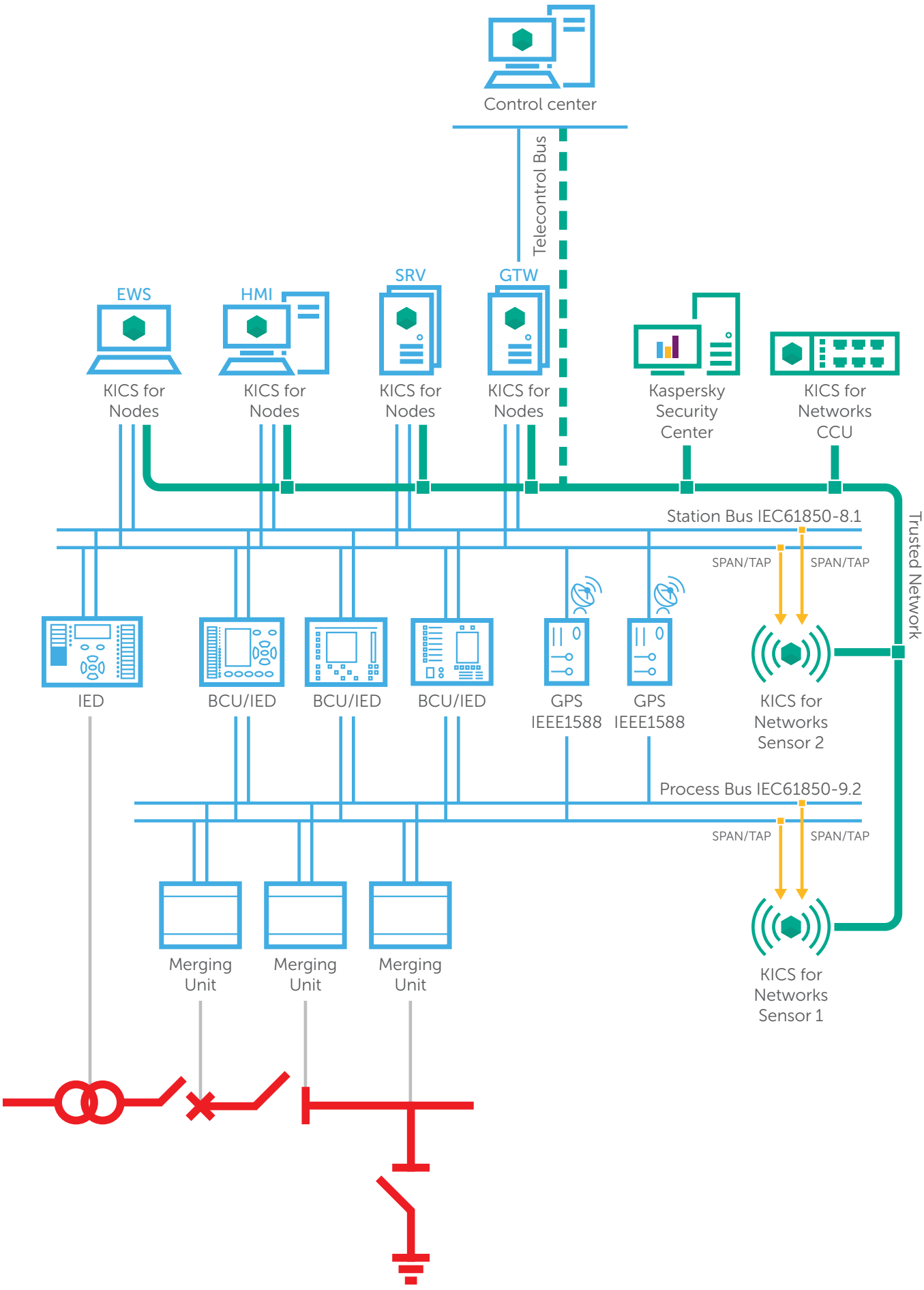

Image #3: Kaspersky Industrial CyberSecurity components deployment

Terms and Definitions

CD – Computing Device. A technical facility capable of executing data processing according to predefined program logic.

CSPS – CyberSecurity Protection System. An automated system designed to provide cybersecurity to the protected facility.

IED – Intelligent Electronic Device. A special microprocessor-based multipurpose computing facility with broad digital communication capabilities.

Industrial cybersecurity – State of protection that provides availability, integrity and confidentiality of industrial process on IT/OT level.

LAN – Local Area Network. A computer network covering a fixed set of network units connected via locally managed media and grouped according to the limited area location principle.

PACS – Protection, Automation & Control System. A collective term meaning a complex of automatic and automated control systems of different purposes, installed at the facility.

PCS – Process Control System. A human-machine system based on industrial automation and telecommunication facilities providing comprehensive on-site automatic and automated process control on the controlled facility and allowing remote control execution from a remote dispatching center.

Protection System – a complex of IEDs designed for the prompt detection and disconnection of damaged segments of controlled electric power system to guarantee stable system performance.

SCL – Substation Configuration Language. Language and representation format specified by IEC 61850-6 for configuration of electrical substation devices. It contains resources for the representation of a device information model, data sets and communication services. Based on XML language.

Smart Grid – a new-generation electric power system based on the multi-agent principle of organization and control over its operation and development in order to make effective use of all resources (natural, social and production, as well as human). This system provides secure, qualitative and efficient power supply for consumers due to flexible interaction of all its subjects (all types of generation, electric power networks and consumers) based on modern technologies and a unified intelligent hierarchical control system.

SPAN – Switched Port Analyzer. A network switch port used to collect mirrored network traffic from selected ports of the managed switch for the purpose of analysis.

Station Bus – fast and highly reliable computer network that provides data transmission via intelligent devices that implement process functions (cell level), as well as device, hardware and software complexes that implement general substation functions (substation level), for example, SCADA, telemechanic gateway, etc. In some cases, a station bus may provide horizontal communications between cell-level devices. To prevent electromagnetic interference with communications, station busses are often made with a fiber-optic data transfer medium.

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