SIEMENS
Ingenuity for life

White Paper

How to safeguard sophisticated operational technology for targeted, highly dangerous cyber threats

To protect critical infrastructure from advanced cyber threats, defense-in-depth strategies need to be augmented by an early warning system designed specifically for industrial networks and associated operational technology – the Siemens RUGGEDCOM-SNOK intrusion detection system.

Authors

Davinder Harcharan
Siemens Industry Inc.

Siv Hilde Houmb, Ph.D.
Secure-NOK AS

Erlend A. Engum
Secure-NOK AS

usa.siemens.com/ruggedcom

Growing cyber threats amidst target-rich critical infrastructure

Automation using advanced industrial control systems (ICSs) has brought modern production to the point where "things are making things" and doing so in the greater context of ubiquitous connectivity, popularly known as the Internet of Things (IoT). But for all the associated benefits of better operating visibility, lower costs, and bigger profits, these developments also have their downsides. Namely, they have provided fertile grounds for the emergence of serious cyber threats against critical infrastructure. And, unfortunately, those threats are ever increasing in their frequency and sophistication, taking advantage of the growing trend of integrating enterprise IT networks with networks linking ICSs and operating technology (OT).

After all, industries such as energy, power generation, communications, transportation and the many others that are considered part of critical infrastructure make rich targets for threat actors of all kinds. Years ago, most were rogue individuals, but today their ranks include individuals who are more educated and professional, possibly part of criminal gangs or terrorist organizations. As such, they have the skills and means that can amplify their abilities to penetrate even the strongest cyber defenses.

Break-in to beat all. To illustrate, consider the 2016 penetration of the U.S. National Security Agency (NSA), which is arguably the world's most advanced electronic surveillance operation. Hackers stole many of its tools and code, offering them for sale on the so-called Dark Web for nearly $700 million.[1] Then, a year later, the consequences of the NSA break-in appeared when WannaCry ransomware attacked an estimated 230,000 Windows PCs worldwide, disrupting operations of Britain's National Health Service and other big-name enterprises elsewhere. It's reported that the culprits behind that virus used an NSA tool in that attack.[2]

Not all cyber attacks may seek to disrupt operations, however. Some aim to steal data or intellectual property, like what happened in the NSA hack. Such acts of theft or industrial espionage can affect the integrity of critical infrastructure operations, not to mention the competitiveness of private enterprise. The impacts of these intrusions can be quite costly, too, and occur months or years before detection. Advanced persistent threats, for example, can hide out in networks long before their activation to give their owners time to see if they have been detected. If not, the malware can then quietly do its work while applications, systems, and networks seem to operate normally.

More protection needed. Siemens and cybersecurity professionals consider a layered, defense-in-depth approach to be a best practice, one that Siemens, Secure-NOK, and the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) all support. This layering approach can help alleviate the pitfalls of employing incomplete point solutions for cybersecurity by preventing a single point of failure.

The Siemens SNOK intrusion detection system (IDS) features a RUGGEDCOM switch and Secure-NOK's sophisticated yet unobtrusive SNOK intrusion detection technology. It adds another security mechanism to complement the conventional defense-in-depth model. Once deployed, it's an early warning system designed specifically to protect ICS networks and OT, while taking into account specific OT network characteristics and requirements.

Figure 1 illustrates a complete defense-in-depth model that can provide hardened protection for ICS networks and OT. The Siemens SNOK cybersecurity solution focuses on enhancing system integrity in addition to standard system hardening procedures. In combination, it provides better visibility on the network and its elements as a whole to identify threat vectors and anomalies.

This paper will help readers understand what those requirements are and how they differ from those in enterprise IT environments. They will also learn how the Siemens SNOK cybersecurity solution, featuring a RUGGEDCOM Layer 2/3 managed switch and vigilant yet non-intrusive software from Secure-NOK, can detect anomalies in ICS and OT behaviors to contain threats before damage is done or to limit its spread. To be absolutely clear, the Siemens SNOK solution is designed to provide the function of attack detection within the defense-in-depth model and is specifically designed for the unique needs of ICS networks and OT.

Finally, this paper aims to bridge the cybersecurity knowledge gap between IT and OT professionals, so they can work more effectively as a team to provide the protection their organizations need against threat actors seeking to exploit that gap. Whereas IT professionals tend to have computer science backgrounds, OT professionals come from process and industrial engineering backgrounds. The combination of these two perspectives can go a long way in fighting cyber threats as a single, formidable force for keeping hackers at bay.

[1] "Who Hacked the NSA?" by Ian Graber-Stiehl. Popular Science magazine. August 22, 2016.

[2] "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history" by Chris Graham, The Telegraph, May 20, 2017.

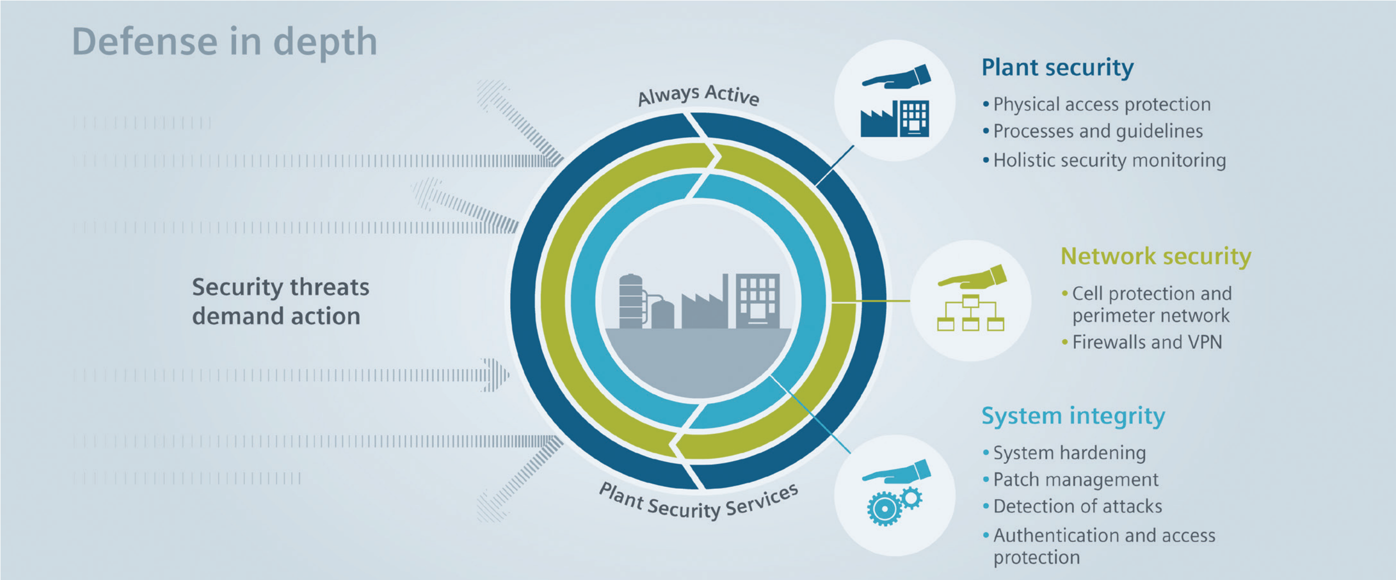
Defense in depth
Security threats demand action
Always Active
Plant Security Services
Plant security
• Physical access protection
• Processes and guidelines
• Holistic security monitoring
Network security
• Cell protection and perimeter network
• Firewalls and VPN
System integrity
• System hardening
• Patch management
• Detection of attacks
• Authentication and access protection

Figure 1. Defense-in-depth for ICS networks and the OT systems those networks support, with the Siemens SNOK IDS solution providing an early warning system for detecting attacks to strengthen system integrity.

Industrial automation trends that open new cyber vulnerabilities

Ironically, many of industry's innovations in automation and controls have created new cyber vulnerabilities. For example, for years, industry has been using Ethernet to link ICS networks to higher-level enterprise IT networks, so management can gain better views across all of their operations. Ethernet is also being used to connect the supervisory control and data acquisition (SCADA) networks running field devices. While this far-reaching integration has enabled better automation and control across both process and discrete manufacturing industries, it has also opened new doors for hackers and malware to exploit.

That's because Ethernet is a standards-based communications protocol – the world's most widely used – that can enable hackers to find plenty of ways to penetrate its safeguards. What's more, many controllers and human-machine interfaces (HMIs) have web browsers to enable remote monitoring and control of plant operation via laptops, tablets, and even smartphones. While this innovation has plenty of upsides, it also provides many more avenues for malware and attackers to penetrate OT systems.

Next on the list of growing vulnerabilities is the IoT and its fast-growing subset the Industrial IoT (IIoT). These describe a much vaster scale of interworking between traditional enterprise IT devices – desktops, servers, storage, and switches – plus the addition of machines, buildings and other infrastructure embedded with sensors, actuators and controllers. Many of the non-traditional, IP-enabled devices that are linking to the IoT, even simple devices such as home and office electronic thermostats, are contributing to what some call, in effect, an infinite attack surface because those devices lack the necessary safeguards to prevent intrusions.

Although Siemens designs, engineers and builds exceedingly strong cybersecurity safeguards into all of the industrial components in its Totally Integrated Automation (TIA) portfolio, many third-party devices do not have those safeguards built-in. This latter fact exposes their users to attack vectors that they are likely unaware of. For critical infrastructure industries especially, this means that even someone wearing a smart watch or carrying a simple cell phone could unwittingly compromise the security of an ICS network, even an air-gapped one, as Israeli researchers have found.[3]

In addition, open-source operating systems and software are greatly expanding the attack surface of critical infrastructure and industry. If these platforms are not well-maintained, monitored, or updated when weaknesses are exposed, hackers will have additional vectors for attack.

Of course, one of the most common ways to penetrate ICSs and OT networks has nothing to do with Internet connectivity. It involves internal saboteurs – disgruntled employees or ones paid to plug in removable media (e.g., a flash drive) with malware to a connected device with a USB port. Also vulnerable are employees or contractors, who might connect to the ICS network with laptops or other devices to perform maintenance work, upgrades or even diagnostic health checks, but not know their service equipment is already infected with malware.

[3] "Clever Attack Uses the Sound of a Computer's Fan to Steal Data," by Kim Zetter, Wired. June 6, 2016.

Cybersecurity: Industrial OT networks and enterprise IT networks compared

Enterprise IT professionals have plenty to worry about in defending against cyber attacks on non-industrial networks that link users in front- and back-offices with each other and with file servers, data centers, cloud-based resources, and the Internet. This connectivity supports email, web-based collaboration tools and voice communications, plus applications and various company databases, such as enterprise resource planning (ERP), customer relationship management (CRM) tools and so forth. Should malware, data theft, and corrupted data or devices occur, user productivity and even a company's transactional capabilities could be seriously disrupted.

But for all that's at stake in the enterprise IT environment, their networks differ from industrial ICS and OT networks in one profound and vital way: ***people are rarely, if ever, hurt or worse should IT networks get breached and disrupted.*** This is one of the biggest differences between enterprise network security and industrial network security. If a hacker penetrates an industrial network and disrupts critical processes or controls, especially automated life safety protections, serious consequences could occur. A catastrophic incident could cause hundreds, even thousands, of casualties.

That's why the ICS-CERT works hard to reduce risks associated with critical infrastructure-related cybersecurity incidents and mitigation measures. Both Siemens and Secure-NOK are tuned into ICS-CERT proceedings and the activities of private-sector committees, taking part in many relevant ones.

For example, Siemens took part in a NIST National Cybersecurity Center of Excellence (NCCoE) study that was conducted to develop its *NIST Cybersecurity Practice Guide SP 1800-7*, *Situational Awareness* handbook. And Secure-NOK participated in another NCCoE study that assessed anomaly behavior-detection solutions for use in the manufacturing industry and will be published in a similar practice guide.

More IT-OT differences. ICS networks differ from enterprise IT networks in other important ways, too, as Table 1 shows. First, ICS networks include lower-level supervisory control and data acquisition (SCADA) systems that operate at the machine level on factory floors. These ICS and SCADA networks are often linked to enterprise networks, which have external-facing vulnerabilities that can open doors for hackers. Wireless SCADA systems, often operating from remote locations using public IP addresses, are also vulnerable to attack, accessible via their wireless media, which include cellular, 900MHz radio, satellite and microwave.

In addition to what's listed in Table 1, industrial networks must often operate 24x7, in real- or near-real time and require 99.9% uptime or better (99.99 or 99.999% in the case of public communication networks). In contrast, enterprise IT networks typically operate on a best-effort basis (so a break in one part of the network forces routers to send data packets down alternate paths) and be available during "business hours." Point is, the disruption risks of a security breach in an ICS or SCADA network can be much greater than for an enterprise IT network. What's more, upgrades to anti-virus applications and other conventional IT safeguards, such as firewalls, can be disruptive to the real-time, 24x7 operating requirements of ICS and SCADA networks.

At the same time, the integration of a company's legacy plant systems with its enterprise systems by interconnecting industrial and corporate networks can be complex. And that's not to mention the frequent need to provide network access to external third parties, such as OEMs of plant machines, via the public Internet. Not only does external connectivity create vulnerabilities, but the integration also introduces ambiguity within companies as to which group – enterprise IT or process/industrial engineering teams – owns responsibility for overall cybersecurity.

Another set of security issues with industrial networks involves their evolution from early patchworks of electrical relays or antiquated microprocessor controllers and manually monitored indicator lights, trips and breakers. While those legacy systems might work well enough to operate relatively simple processes even today, they likely lack proper security controls.

Nonetheless, they may well be connected to modern distributed control systems (DCSs) that feature the latest programmable logic controllers (PLCs). The latter are mini-computers using Windows or Linux and are connected over industrial Ethernet to human-machine interfaces (HMIs). In turn, these HMIs are often accessible anywhere in the world via PCs or touchscreen tablets and smartphones – by legitimate plant operators or by hackers exploiting the vulnerabilities in the connections between old and new systems.

Table 1. Enterprise IT networks vs. industrial IT networks: security issues compared (Sources: *1. NIST: Guide to ICS Security and 2. ICS-CERT)*

Category	Information Technology (IT)	Operational Technology (OT)
Risk management requirements	Data confidentiality and integrity is paramount.	Human safety is paramount, followed by protection of the process.
Time-critical interaction	Less critical emergency interaction.	Response to human and other emergency interaction is critical.
Communications	Standard communications protocol.	Many proprietary and standard communication protocols.
Managed support	Allow for diversified support styles.	Support via a single OEM vendor for their machine.
Component lifetime	3-5 years	15–20 years, usually same vendor over time. Product end-of-life phases can create security vulnerabilities.
Access to components	Local and easily accessed.	Can be isolated, remote, and require extensive physical effort to access.
Anti-virus and mobile code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based.	Memory requirements can impact control systems. Organizations can only protect legacy systems with after-market solutions. Usually requires "exclusion" folders to avoid programs quarantining critical files.
Patch management	Easily defined, enterprisewide, remote, and automated.	Long timeline to successful patch installation. OEM-specific. May interfere with ICS functionality. Asset owners must define acceptable operational risks.
Testing and audit methods	Use modern methods. Systems usually resilient and robust to handle assessment methods.	Tune-testing to the system. Modern methods may be inappropriate. Equipment may be susceptible to failure during testing.
Change management	Regular and scheduled, aligned with minimum-use periods (e.g., nights and weekends).	Strategic scheduling, a critical process due to potential production impacts.
Asset classification	Common and performed annually with results driving expenditures.	Only performed when obligated. Accurate inventories are uncommon for non-vital assets. Disconnects between asset values and appropriate security countermeasures.
Incident response and forensics	Easily developed and deployed. Some regulatory requirements. Can be embedded in the technology.	Focused on system resumption activities. Forensics procedures tend to be immature beyond event re-creation. Requires good IT/ICS relationships.
Physical and environmental security	Can range from poor (e.g., office systems) to excellent (e.g., critical IT operations systems).	Usually excellent for critical areas, but maturity varies for site facilities based on criticality and organizational culture.
Secure systems development	Integral part of the development process.	Historically not an integral part of OT development processes. OT vendors are maturing, but more slowly than IT vendors. Core ICS solutions are difficult to retrofit with advanced security solutions.
Security compliance	Definitive regulatory oversight, depending on vertical sector (e.g., healthcare, financial services).	Definitive regulatory oversight, depending on vertical sector (e.g., critical infrastructure).

How ICS/OT network intrusions can occur despite defense-in-depth strategies

Figure 2 shows how a modern industrial plant can divide its common control system architectures into zones with clear boundaries to support multiple cyber-defense layers.

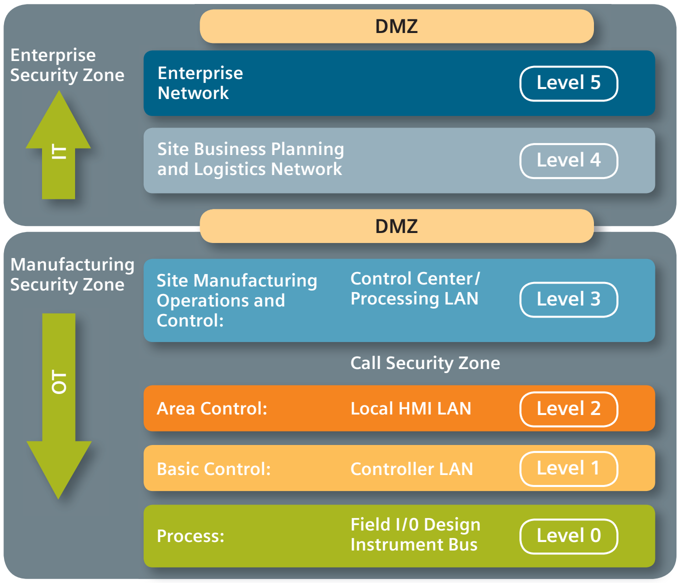
DMZ
Enterprise Security Zone
IT
Enterprise Network
Level 5
Site Business Planning and Logistics Network
Level 4
DMZ
Manufacturing Security Zone
OT
Site Manufacturing Operations and Control:
Control Center/ Processing LAN
Level 3
Call Security Zone
Area Control:
Local HMI LAN
Level 2
Basic Control:
Controller LAN
Level 1
Process:
Field I/0 Design Instrument Bus
Level 0

Figure 2. Zone segmentation of business and ICS architectures (Source: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016).

However, even with clear network segmentation and defense-in-depth models deployed, attacks on the ICS and OT networks of critical infrastructure and industrial plants can be quite sophisticated even on devices that are not directly Internet facing. Examples are the programmable logic controllers (PLCs) that provide ICSs with their operating intelligence. Siemens and Secure-NOK highly recommend the use of defense-in-depth approaches such as zone segmentation as illustrated in Figure 2. However, these countermeasures, without the inclusion of the capability to detect attacks, have their limits as no less than the ICS-CERT acknowledges:

> *"Defense-in-Depth measures do not and cannot protect all vulnerabilities and weaknesses in an ICS environment. They are applied, primarily, to slow down an attacker enough to allow IT and OT personnel to detect and respond to ongoing threats, or to make the effort on the attacker's side so cumbersome that they decide to put their effort toward easier prey."*

Combatting "low-and-slow" cyber attacks. The most insidious cyber threats to the ICSs and OT of critical infrastructure and industry at large are advanced persistent threats (APTs), also known as "low-and-slow" attacks. These are hard to detect before an attack fully executes, because they operate under the radar of most conventional IT cybersecurity tools.

Without disrupting network or ICS operations, an APT will execute a series of small events that may not constitute an actual cyber attack, but these events could still be anomalous and indicate malevolent intent. Examples include the appearance of new, copycat or forked processes or forked memory usage that occur outside of normal and prior observed ICS or network behaviors.

Early-warning system: The Siemens SNOK cybersecurity solution

To combat these kinds of sophisticated threats, Siemens and Secure-NOK have developed a unique network intrusion-detection system (IDS) – the SNOK^{TM} a non-intrusive, anomaly-based, intrusion detection software technology that is hosted on the Siemens RUGGEDCOM RX15xx Multi-Service Platform.

The latter is a utility-grade Layer 2 and 3 switch and router, engineered with built-in security enhancements, such as Layer 2 MAC filtering, Layer 3 security protocols like IPSec, and a zone-based firewall. As its name implies, the switch is rugged-rated for use in harsh, demanding industrial environments. Ruggedization isn't an add-on, but is engineered and built into the device. It is hot-swappable and has universal power supply (UPS) options, both to maximize uptime.

The Siemens RUGGEDCOM RX15xx offers a set of modular WAN, serial, and switching options with routing and management features. This allows for hassle-free upgrades in the field, and the flexibility to adapt to changing network architectures.

Operating from that hardware is the SNOK software. Its technology provides an early-warning network monitoring and sophisticated intrusion detection capabilities to identify and isolate cyber threats that may be undetectable by conventional IT security tools. It then provides early and actionable alerts to help incident response (IR) to be managed by both IT and OT teams, depending on their IR protocols and respective responsibilities. In effect, SNOK adds critical, extra hardening to the defense-in-depth cybersecurity umbrella already protecting ICS networks and any enterprise IT networks to which they're connected.

How it works. The SNOK application operates quietly behind the scenes, using the four components illustrated below to alert system owners of intrusions that traditional IT security tools might miss: Monitoring; Detection; Risk Assessment; and Response.

Monitoring
Detection
Risk Accessment
Response

Figure 3. Four components of SNOK application.

First, SNOK software agents are deployed deep into an ICS network to continuously monitor network traffic as well as endpoints in the network. These are small, non-intrusive software applets, less than 1,000 kilobytes in size. The agents collect deep, low-level information to set a baseline of normal network behavior. The information is passed to SNOK analyzers that can identify anomalous behavior patterns in the network or any of its endpoints. These patterns can indicate a low-and-slow APT or other cyber threat before an actual attack and disruption can occur. SNOK then alerts a compromised ICS network's operators to the attack. It also provides sufficient data to help them make informed decisions about an effective response and corrective action.

Examples of SNOK-detectable anomalies include:

- Host baseline alerts (install base/processes, CPU, RAM)
- Abnormal traffic patterns and volume
- New IP connections and removable media insertions
- Detection of changes in PLC memory blocks

Plug-and-play installation. The Siemens SNOK IDS solution differentiates itself by running on the RX15xx Application Processing Engine (APE) module. The APE is an x86-based computer designed to occupy a single-line, module slot in a Siemens RUGGEDCOM RX15xx appliance. The APE can host a variety of x86-based operating systems and has connectivity to devices or networks that are connected to regular Ethernet and serial ports on the RX15xx device.

This solution is compatible with new and legacy ICS networks, designed to operate in SCADA environments with plug-and-play simplicity. It requires no changes in the existing network topology or existing hardware. Uniquely, the SNOK platform has an extremely small footprint with virtually no operational load or other impacts on the ICS or SCADA networks. And because the SNOK software is signature-free (i.e., doesn't require a database of known malware profiles), it also doesn't require updates like antivirus software applications do.

The Siemens SNOK IDS powered by the RUGGEDCOM 15xx appliance and SNOK software can be flexibly deployed across critical infrastructure and other industries to meet a wide range of requirements. Here are four scenarios that will cover most use cases:

- **Single-site plant deployments:** For complex plants, such as refineries and petrochemical complexes, with hundred sub-nets.
- **Distributed deployments:** For infrastructure spanning long distances, such as long-haul transport routes, such as oil pipelines, electrical transmission facilities, and wide-area telecommunication networks.
- **Hierarchal, multisite deployments:** For aggregating IDS monitoring and detection across multiple sites, rolling up logs, incidents, and alerts to a single security operations center.
- **Hardening of PLC systems and networks:** For all industrial automation systems and networks, to provide an additional protective security mechanism and more holistic security approach.

An immediate, cost-effective way to improve industrial defense-in-depth security

The growing sophistication and frequency of cyber threats will pose ever greater dangers to the world's critical infrastructure and industry at large. A defense-in-depth approach, that includes a security mechanism providing early-warning detection tailored to the industrial infrastructure, is an essential component of the solution recommended by Siemens and Secure-NOK. It must be able to identify and contain advanced persistent threats and other malware endangering ICS and OT networks, while also respecting the operating demands of ICS and OT networks.

That's why Siemens and Secure-NOK developed an IDS that is unique in the world and features the RUGGEDCOM 15xx security appliance and the SNOK anomaly-based, intrusion detection software technology. It's designed specifically for the real-time operational requirements of ICS and OT networks without adding any operational load or other impacts to them. As enterprise IT security professionals and the world's OT process and industrial engineers team up to fight cyber threats more effectively than ever, the Siemens SNOK IDS solution can add a powerful new tool to their defensive arsenal to keep critical infrastructure and industry assets safe from attack, espionage, and sabotage for years to come.

A White Paper issued by: Siemens.

Security information
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity

Siemens Industry, Inc. 2018.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center.

Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/ruggedcom

Order No.: RCWP-CYSNK-0118
Printed in U.S.A.