Today, industries such as electric power, oil & gas, transportation and many more are becoming increasingly digital, automated and interconnected. This makes them vulnerable to cyber-attacks; once a concern exclusive to IT infrastructure. Siemens SNOK Intrusion Detection System (IDS) features a RUGGEDCOM switch and Secure-NOK™ intrusion detection technology. It adds a layer of detection capabilities, allowing an asset owner real-time insight into the security status of the industrial network. This complements the several layers of conventional protection mechanisms in the Defense in Depth model, preventing cyber attacks from affecting the industrial process. Once deployed, Siemens SNOK IDS is an early warning system designed specifically to protect ICS networks and OT, while taking into account specific OT network characteristics and requirements.
The concept of the Defense in Depth model applied to improve cybersecurity is meant to defend a system using several independent methods in layers. Such layers may include everything from segregated networks separated by access control mechanisms, to protection of each of the endpoints. For Defense in Depth to be efficient over time, it is vital to monitor and detect any security breach of a layer or defense mechanism.

SNOK software, operating on RUGGEDCOM hardware, provides 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. This is achieved through four components illustrated below: monitoring, detection, risk assessment and response. In effect, SNOK adds a critical detection layer to the Defense in Depth cybersecurity umbrella already protecting ICS networks, and any enterprise IT networks to which they’re connected. This allows for monitoring and detecting intrusions that traditional IT security tools might miss.

The following SNOK products are available with RUGGEDCOM switches:

- **SNOK Network Intrusion Detection System (NIDS)** monitors the network to detect intrusions. NIDS comes in basic, small, medium and large deployments, depending on size of the network.
- **SNOK Cybersecurity Monitoring System** monitors both the network and end points (hosts) to detect intrusions. This solution comes in small and large deployments depending on size of network and number of hosts to be monitored.
- **SNOK Enterprise Solution for monitoring of multiple sites from control centers**. Includes SNOK Cybersecurity Monitoring System (CSM) as standard.

Siemens SNOK IDS solution differentiates itself by running on the RUGGEDCOM APE – a utility-grade computing platform that plugs directly into any member of the RUGGEDCOM RX1500 family. RUGGEDCOM 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 any 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 SNOK software is signature-free (i.e. it doesn’t require a database of known malware profiles), it also doesn’t require updates like antivirus software applications do.
Siemens SNOK IDS powered by the RUGGEDCOM 15xx device 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 hundreds of sub-nets.

- **Distributed deployments:** For infrastructure spanning long distances, such as long-haul transport routes, oil pipelines, electrical transmission facilities, and wide-area telecommunication networks.

- **Hierarchal, multisite deployments:** For aggregating IDS monitoring and detection across multiple sites, roll 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 layer and more holistic security approach.

The embedded ROX II (Rugged Operating System on Linux) combines Layer 2 switching functions, Layer 3 routing functions, along with advanced cybersecurity features and comprehensive networking functions to provide a full array of intelligent functionality for high network availability and manageability. Coupled with the ruggedness and durability that is designed in from the onset, the RUGGEDCOM RX1500 is ideal for creating mission-critical, real-time, control applications where high reliability and availability is of paramount importance.

All RUGGEDCOM products are backed by a five year warranty and unsurpassed technical support.
About Secure NOK

Secure-NOK AS is a Norwegian industrial cybersecurity company with headquarters in Hamar, Norway and offices in Houston, TX (US). The company was established in 2010 and is comprised of an international team with extensive experience in controls and automation systems cybersecurity, including SCADA and embedded systems.

Secure-NOK operates in a number of industrial cybersecurity market segments, including Power Utilities, Oil & Gas Installations, Transportation Systems, Critical Manufacturing and Aviation.

About the SNOK Solution

The company’s core technology, SNOK, monitors Industrial Automation and Control Systems (IACS) from the inside to detect cyber-attacks. Secure-NOK’s unique approach combines network and endpoint monitoring with anomaly behavior detection. This reduces blind spots in the infrastructure and enables detection of known as well as unknown cyber-attacks at an early stage. Through its core technology, Secure-NOK enables well-informed security decisions by providing asset owners and operators with early warnings of cybersecurity events.

Further information is available on the Internet at www.securenok.com