WHITE PAPER

Protecting PCS 7 distributed control systems against cyberattacks

January 2024

SECURENOK®

Contact Us

secure@securenok.com

- Luramyeveien 25A, 4326 Sandnes, Norway
- Gaustadalléen 21, 0349 Oslo, Norway

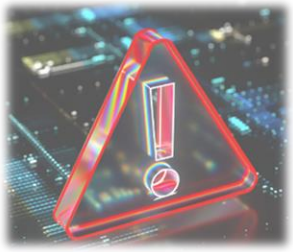
Distributed control systems used in critical industrial processes must be secured against cyber-attacks

Distributed Control Systems (DCS) are computerized systems used to control industrial processes. DCSs are particularly popular in complex, sometimes large-scale processing facilities with high reliability demands. Typically, such facilities also have strict safety requirements.

Many of the critical services we take for granted – provision of clean drinking water, generation of electrical power, district heating to our homes and workplaces, production and refining of oil & gas products – are controlled by distributed control systems (DCS).

The Siemens PCS 7 is one of the most popular DCS and has been available for decades. PCS7 systems are found in numerous facilities all over the world and are frequently deployed in newbuild projects. Due to the critical nature of the industrial processes controlled by DCS, it is imperative that they are secured against cyber-attacks. Siemens PCS 7 is no exception and today's threat situation makes this truer than ever.

Today's threat situation and regulatory response



Owners of critical infrastructure and industrial facilities must be aware ***that they could become the next victim of a targeted cyber-attack***. Some threat actors capable of carrying out such attacks, are highly advanced and well-funded nation state groups. If successful, they could bring a facility's operations to a grinding halt. Or worse.

Other threat actors include organized criminals determined to take valuable systems hostage. ***These groups are financially motivated - typically through the collection of ransom***. They are extremely well organized and supported by a wide range of illegal services on the dark web offering hacking, databases of stolen passwords, malware and so forth. Such services also benefit traditionally less resourceful threat actors such as opportunistic criminals and hacktivists and this makes their capabilities significantly more potent.

Successful cyberattacks on critical infrastructure are not only devastating for the owner but may also impact society in general. To respond to an increasingly dangerous threat landscape, ***authorities are taking explicit legislative measures***. The EU, for example, proposed the Network and Information Security Directive (NIS) in 2016, which was implemented throughout the member states by 2018. The NIS directive introduced requirements concerning cyber risk management and cyberattack incidence response for providers of critical services. In 2023, the EU proposed the NIS2 Directive, a stricter and more comprehensive version of its predecessor, which will be implemented by October 2024.

Norway is implementing NIS 1 with the Digital Security Act which has been approved by Parliament and is expected to come into force shortly. In the near future, the Digital Security Act is expected to be extended to meet the requirements of NIS2.

How to secure OT systems such as the PCS 7?

Industrial automation and control systems are often referred to as ***Operational Technology (OT*)**. In a sense, securing an OT system is not significantly different from securing any other digital system. The general cybersecurity principles of IT apply equally to OT systems as both must be protected and monitored, and, should an attack occur, plans for response and recovery efforts must be prepared and well-rehearsed. This is set out as the five main functions in the popular NIST Cybersecurity Framework: “Identify, Protect, Detect, Respond, Recover”.

In a crucially different sense, though, ***OT systems such as the Siemens PCS 7 require a tailored approach.*** The security measures, including technology, processes and procedures must be designed for the specific cybersecurity needs of both the OT equipment and its environment. Equally important, the security technology, processes and procedures must be tolerated by the very same environment and under no circumstance disturb the industrial process.

The building blocks of the Siemens PCS 7 system are the Automation Systems based on Siemens own **Simatic S7 400 Programmable Logic Controllers (PLCs).** PLCs are the dependable, tried and tested, workhorses of any automation task. However, ***OT equipment such as PLCs, are designed to operate in a trusted environment without the need for authentication and encryption of communication***. In security terms, the PLC can be said to be naïve and gullible, and certainly not fit to withstand cyberattacks.

For these reasons, protecting PLCs should follow best practices by adopting a “defense-in-depth“ approach. This is the underlying philosophy implemented by consensus standards for cybersecurity such as IEC 62443 and the NIST Cybersecurity Framework. It involves building several layers of protection or security barriers surrounding the systems. The primary function of these barriers is to slow down attackers long enough to allow security and operational personnel to detect and respond before they can cause harm. Or to make attackers direct their efforts toward easier prey. ***A facility should never rely on a single security barrier*** such as a firewall. Protection should also include access control as well as hardening and monitoring mechanisms that can be deployed in the PLC environment.

The Secure-NOK SNOK solution is tailored to monitor OT systems

The SNOK solution from Secure-NOK is tailored to protecting OT systems. SNOK comprises several modules using data from three different types of sensors. This provides comprehensive visibility of the behavior of the PCS 7 system and is ***designed to complement a defense-in-depth protection strategy.***

SNOK
Cybersecurity Monitoring System

The SNOK Network Intrusion Detection System (NIDS) module implements passive sensors designed to monitor traffic passing through a network router or switch. Sensors are deployed on separate lightweight hardware in the OT infrastructure alongside network equipment with port mirror/SPAN port capabilities. The more sensors that are used, the better the visibility of the OT network. The network sensor will self-learn the normal behavior of the network and detect unauthorized or abnormal activity.

SNOK® Network Intrusion Detection System (NIDS)

Detection of anomalies in network traffic.

Below are some examples of what the SNOK NIDS can provide:

- An Asset Inventory showing information about internal units communicating via the router or switch.
- Unknown nodes and IP addresses appearing on the network.
- Changes in protocol use and traffic patterns. For example, connection attempts to PLCs from new parts of the network.
- Any communication, both attempted and successful, to and from external addresses.

The SNOK Endpoint Monitoring module consists of host sensors installed on Windows and Linux units in the OT environment. The sensors record a wide range of information about host endpoints such as engineering PCs and HMIs. Such units are also used for direct control of PLCs and are crucial for the operation of most facilities. Consequently, they are also attractive targets for threat actors. SNOK Endpoint sensors are lightweight software agents that are non-intrusive and require very little resource from the host. The sensors are available for the most up-to-date versions of Windows and Linux as well as for older versions, including legacy systems.

SNOK® Endpoint Monitoring

Detection of anomalies in behavior of Windows and Linux endpoints.

Examples of the information registered by SNOK host sensors are:

- New processes started, signed or unsigned.
- USB stick insertions, authorized or unauthorized.
- Changes to the endpoint's firewall settings.
- Unexpected change in resource usage by the endpoint.
- Changes in network traffic to and from the endpoint.
- New user log in, including failed log ins.

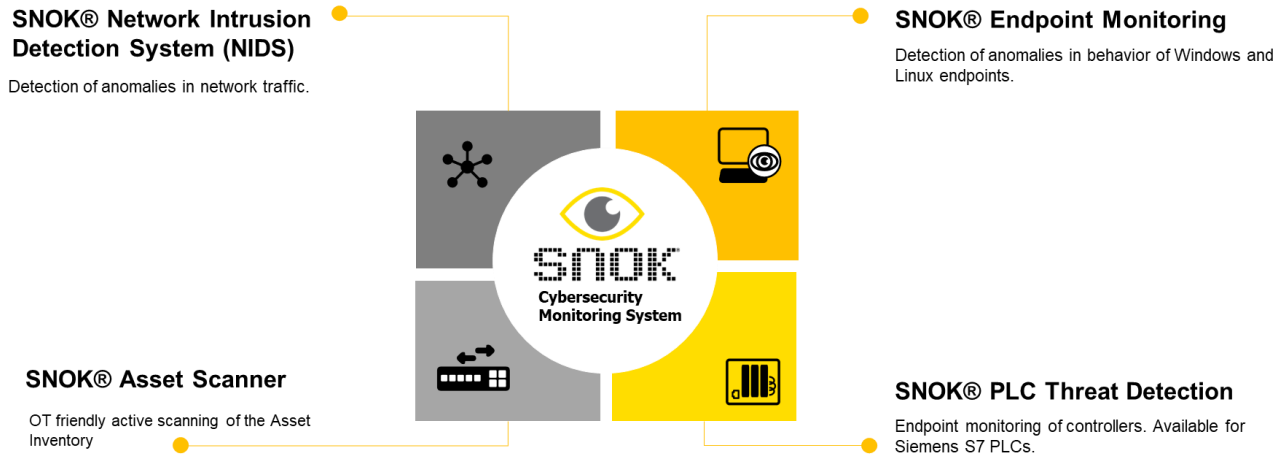
Third and finally, the **SNOK PLC Threat Detection module** consists of sensors for monitoring Siemens S7 400 and 300 PLCs directly. This sensor was developed by Secure-NOK as early as primo 2016 and has recently seen a strong increase in interest from asset owners. The PLC sensors run on separate hardware and uses the PLCs own language to request information.

SNOK® PLC Threat Detection

Endpoint monitoring of controllers. Available for Siemens S7 PLCs.

The SNOK PLC threat detection module analyzes this information to detect changes which could indicate that the PLC has been altered or otherwise manipulated. These include:

- Changes in the PLCs properties
- Runtime changes.
- Changes to the memory blocks of the PLC – for example due to reprogramming.



SNOK Product Modules

Tuning SNOK to monitor local conditions for each OT environment

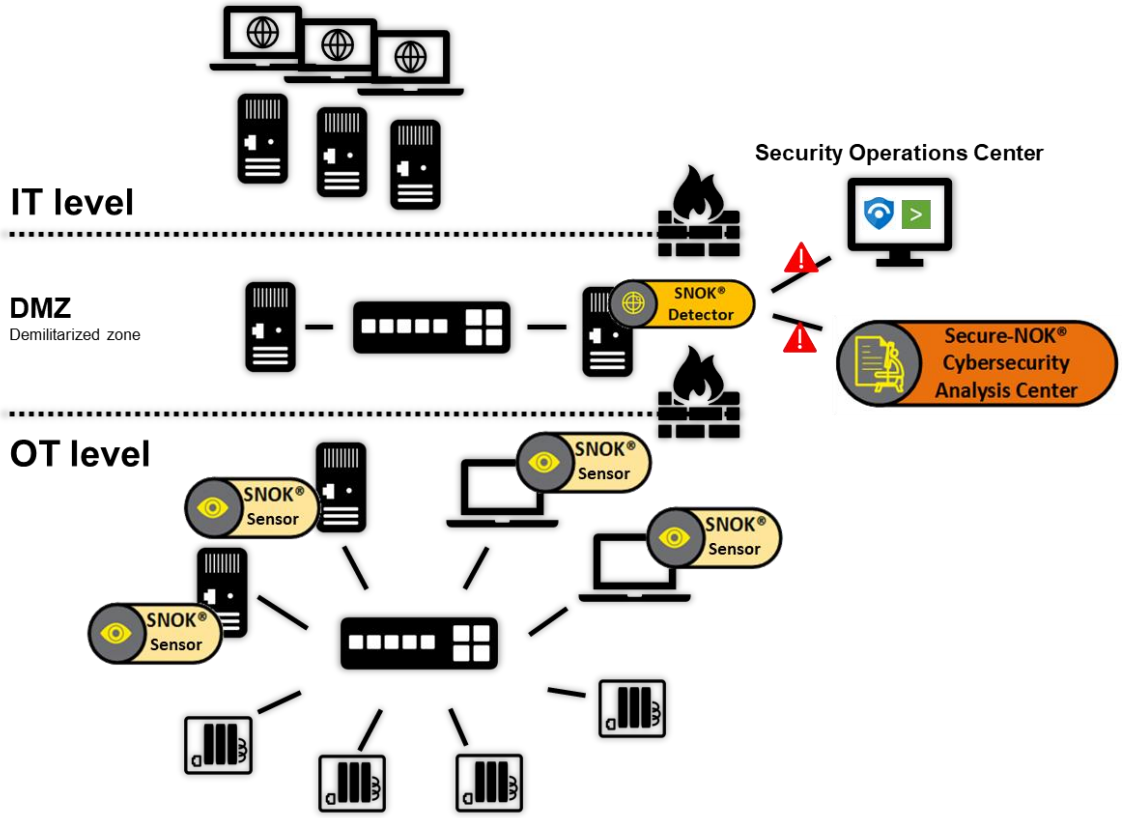
The three sensor types – the Network, Host, and PLC sensors – all funnel data to the SNOK Detector where it is analyzed. Anomalies in the sensor data will create detected events and, if sufficiently grave, raise alarms.

The security analyses carried out by all SNOK modules are based on a tailored, behavioral baseline and a configurable ruleset. The baseline is produced by recording sensor data from the facility for a set time period. During this period the SNOK Detector learns the characteristic behavior of the facility so that subsequent deviations from the baseline will create detected events. The configurable ruleset allows the user to adjust which of these events should be considered within normal variations and which are against policy and should produce an alarm. This allows SNOK to adapt to the local conditions of each individual OT environment and its sub-environments.

Handling of alarms

SNOK alarms can be viewed and handled in several different ways. The user interface is primarily designed for operational and technical personnel responsible for the OT system. Secure-NOK's Cybersecurity Analysis Center offers services to help system owners to analyze, interpret and respond to alarms.

Many organizations have a dedicated team to monitor and respond to cyber threats across its assets and systems. Traditionally, such teams are trained within IT security and focus on protecting IT systems. These teams are commonly referred to as Security Operations Centers (SOCs) and can be staffed by in-house personnel, delivered as a managed service by a third party or a hybrid of the two. SNOK alarms can be forwarded to all common systems used by SOCs and ***Secure-NOK's Cybersecurity Analysis Center offers support in responding to alerts from OT environments monitored by SNOK***. This support includes developing alarm handling rules and preparing workbooks for presenting and analyzing SNOK alarms in the most common tools such as Splunk and Microsoft Sentinel.



Flexible deployment options

Each SNOK module can be deployed standalone or in combination with other SNOK modules. This provides flexibility when using SNOK to monitor a PCS 7 system regardless of the network infrastructure surrounding it. The SNOK sensors of various types can be selected to meet the needs of the PCS 7 infrastructure – both in existing industrial installations and in completely new projects.

Deploying network monitoring to observe traffic to and from PLCs is one way of keeping an eye on their behavior. However, many existing PCS 7 networks are built using switches that lack the port mirror capabilities necessary to support network monitoring. ***Upgrading the network infrastructure in a large facility would require a significant investment.*** With the flexibility offered by SNOK, the SNOK PLC Threat detection module can still be deployed to monitor the PLCs as it does not depend on mirrored traffic. SNOK Endpoint Detection sensors can also be deployed to monitor other units in the network as well as the traffic to and from these units.

OT cyber-attack scenarios – and how they can be detected by SNOK

OT systems are usually shielded from direct internet exposure, and this makes attacks on such systems less frequent when compared to IT systems. Even so, there are still several attack vectors that intruders may use to target OT environments. Two common examples are:

- the surface of OT system towards internet exposed services elsewhere in the infrastructure,
- remote access solutions used for providing operators, technicians and vendors with system maintenance and control capabilities.

In addition, the possibility of having a malicious insider, either knowing or unwitting, must also be taken into account.

Critical functions should be protected by several security barriers. If attackers have managed to breach an organization's first layer of defense, their next step is likely to be ***lateral movement within the infrastructure*** to reach the OT environment and achieve deeper access. In this phase, SNOK will detect unexpected events. Some of the alarms generated by the SNOK network sensors may be quite subtle and could be interpreted as legitimate activities such as system maintenance. In an actual attack, however, the attack steps will leave a trail of detected anomalous events. For example: new addresses, protocols or disturbance of OT devices. This should gain the attention of Security Operations personnel, allowing them to match observed behavior against known legitimate activity going on at the current time.

Critical functions should be protected by several security barriers. These must be monitored to detect breaches at an early stage.

To disturb, disrupt or otherwise impact an OT system, the attacker needs to gain a foothold in the infrastructure. One way of achieving that is to ***compromise endpoints providing key functionality within the OT system***. These could be operator stations/HMIs, engineering stations or other units authorized to communicate with the industrial controllers. These devices are likely to be already equipped with the capabilities that the attackers need and are usually under a less strict security regime than IT equipment. With SNOK endpoint sensors installed on such units, alarms will be raised following events such as a new user log in, the use or installation of new programs, new processes or traffic to or from the unit. Insider activity such as the insertion of a USB memory stick, will also trigger an alarm.

The PLCs in a PCS 7 DCS are critical to the safe operation of the system. A SNOK PLC sensor is able to closely monitor the PLC itself so that manipulation attempts can be detected***. It should certainly be a goal to detect an attacker before they are in this position, however this is not always possible.*** The PLC network could be of an unmanaged type where network sensors cannot be deployed without comprehensive network upgrades. Insider attackers could have direct physical access to PLCs. Sophisticated attackers could steal vendor credentials and compromise access to remote maintenance solutions. In such cases, the SNOK PLC sensor will detect and warn of events affecting the PLC itself, for example reprogramming attempts.

Although great effort should be spent on protecting critical OT infrastructure such as a PCS 7 DCS, each security protection, barrier or measure can always be compromised, and threat actors can find a way around them. "*The concept of Defense-in-Depth says a system must* ***detect and alert an***

organization of an intrusion early on *so they can take defensive action before critical assets are breached.[1]"*

The SNOK Cybersecurity Monitoring system is flexible and has several types of sensors that can be deployed in a way that leaves as few blind spots in the PCS 7 system and its environment as possible. This provides system owners with the opportunity to respond to threats before attackers can achieve their desired impact.

[1] CISA Recommended Practice - Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

ABOUT SECURE-NOK™

Secure-NOK™ is a cybersecurity specialist company for Industrial Automation and Control Systems. We provide solutions that detect cyber-attacks such as espionage, sabotage, malware and other harmful cybersecurity events in industrial installations.

The company was established in 2010 and is headquartered in Sandnes, Norway with offices in Oslo. Secure-NOK™ is comprised of an international team with extensive experience in controls and automation systems cybersecurity.

SECURE-NOK™ Technology AS
Luramyrveien 25A
4313, Sandnes, Norway

SECURE-NOK™ AS
Gaustadalléen 21
0349 Oslo, Norway

secure@securenok.com

www.securenok.com