ARC VIEW

OCTOBER 28, 2021

# SIMATIC PCS neo: Redefining Cybersecurity

By Thomas Menze

## Keywords

Cybersecurity, Siemens, SIMATIC PCS neo, IEC 62443, Defense in Depth, DCS

## Summary

With the introduction of SIMATIC PCS neo, Siemens aims to set new standards in process automation by offering an innovative, web-based process control system. As a completely new system software, Siemens had the chance to build in key features right out of the box. These include global, web-based collaboration in engineering and operations, an intuitive user interface with all relevant information available from a single workbench, and significantly, cybersecurity embedded deeply in the system DNA.

*SIMATIC PCS neo takes into account best practices of industrial cybersecurity and embeds them deeply in the system DNA.*

## Rethinking Process Automation Engineering

SIMATIC PCS neo users can take advantage of an intuitive graphical user interface (GUI) through which applications can be accessed with just a few clicks. The SIMATIC PCS neo Workbench allows easy switching between the Engineering and Monitoring & Control views. The object-oriented data model increases efficiency and quality throughout the entire plant life cycle.

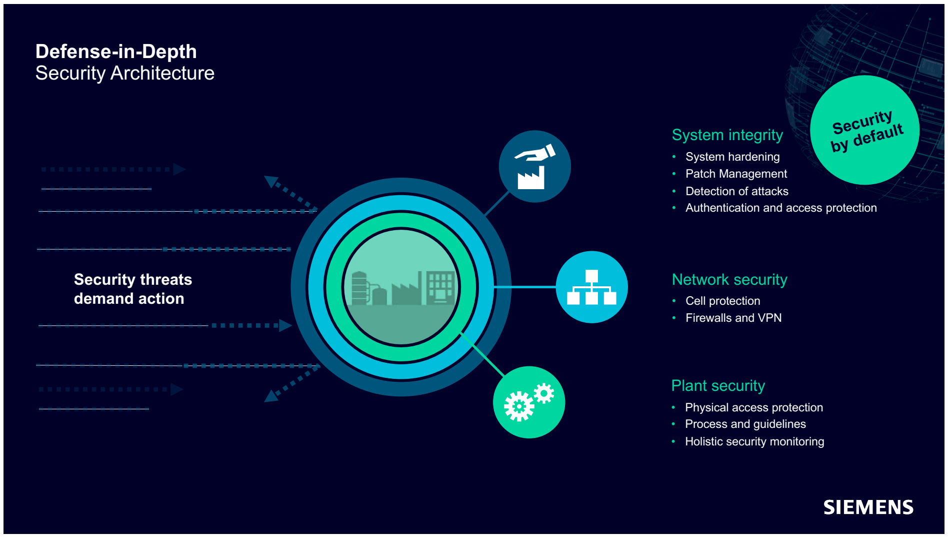
Although SIMATIC PCS neo was designed as a web-based system, users can also access software and system updates offline, i.e. without direct access to the internet, so the system can be easily kept up to date, even in critical plant areas.

## Cybersecurity Right from the Start

To protect against cyber-attacks at industrial plants, security and detection must be applied at multiple levels at the same time. In addition to built-in security features, SIMATIC PCS neo adopts the "defense-in-depth" approach, a comprehensive protection strategy based on recommendations from IEC 62443, the global standard for security and industrial automation.

## Defense-in-Depth

Defense-in-depth addresses plant security, network security, and system integrity. Implementing a variety of security measures in these areas makes it more difficult for attackers to breach a system. It is important to recognize that once plant network and security system strategies are implemented at startup, they cannot be forgotten. Organizations must constantly update their cybersecurity strategies throughout the entire service life of their plants.



**The SIMATIC PCS neo Architecture Enables Physical Access Protection to Be Realized in an Optimal Way**

SIMATIC PCS neo's server-client architecture with web-based access makes it possible to protect physical access to critical data and systems. Critical components like servers and controllers are in separate, locked control cabinets and physically accessible lean clients do not contain any sensitive data. Access by employees to the system components can be limited to specific users.

## System Integrity

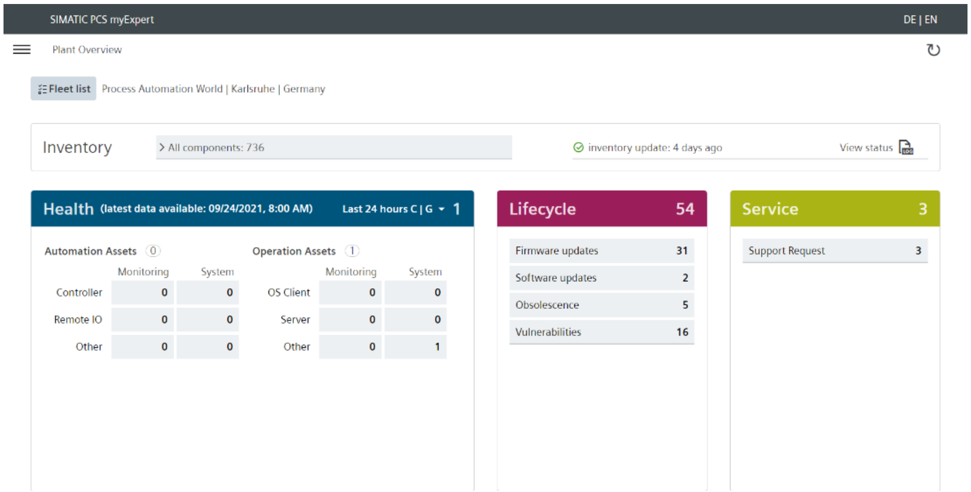
The integrated „security by default“ of SIMATIC PCS neo ensures that functions are securely preconfigured according to the Charter of Trust, principles 3. This means that the essential cybersecurity measures were deeply integrated into the system concept right from the start.

SIMATIC PCS neo system integrity ensures that any undetected changes to the automation process are discovered. Authentication and access protection are integrated system functions, and the management is simple and practical, allowing employee rights to be transferred to workplace requirements. Further system hardening is ensured by system modularity. The keyword "least functionality" guarantees that only the required software functionality is installed in the first place. The integrity of the entire system is monitored by digital signatures. This ensures that only unmodified Siemens software is used on the system. These measures reduce the exposure for cyber-attacks right from the start, so that the system can be operated securely.

Sophisticated patch management ensures system integrity throughout the lifecycle. A central overview of the patch status allows discrepancies to be identified immediately. Different software maintenance packages provide updates and system upgrades; these include Basic, Dynamic and Premium packages.

## SIMATIC PCS myExpert

An essential part of the software maintenance packages is the function SIMATIC PCS myExpert. This service allows access to the Siemens expert network, which provides reliable help with all questions about SIMATIC PCS neo, including proactive notifications of vulnerabilities in individual installations.



Process Automation World | Karlsruhe | Germany

Inventory: > All components: 736 — inventory update: 4 days ago

Health (latest data available: 09/24/2021, 8:00 AM) — Last 24 hours C | G — 1

| Automation Assets (0) | Monitoring | System | Operation Assets (1) | Monitoring | System |
|---|---|---|---|---|---|
| Controller | 0 | 0 | OS Client | 0 | 0 |
| Remote IO | 0 | 0 | Server | 0 | 0 |
| Other | 0 | 0 | Other | 0 | 1 |

| Lifecycle | 54 |
|---|---|
| Firmware updates | 31 |
| Software updates | 2 |
| Obsolescence | 5 |
| Vulnerabilities | 16 |

| Service | 3 |
|---|---|
| Support Request | 3 |

SIMATIC PCS myExpert is part of the Software Maintenance Packages

## Network Security

Similar to the access protection described above, network security is also enhanced. Network cells can be best configured and protected by firewalls and virtual private networks (VPN). SIMATIC PCS neo was designed from the beginning to work in separate network cells, so the communication between the network cells, i.e. between servers and clients, is encrypted using HTTPS. The use of certificates is integrated into the HTTPS communication.

*The integrated „security by default" of SIMATIC PCS neo ensures that functions are securely preconfigured.*

Different firewall layers ensure access rights in the network. In this way, the access rights of users to certain network areas can also be limited.

- The front firewall secures communication with the office network.
- A DMZ allows secure service and support for the plant enviroment. This ensures a controlled and monitored data exchange with the process control network.
- Each host is equipped with a Windows firewall configured by SIMATIC PCS neo.

## Plant Security

Industrial security cannot be put into effect by technical measures alone. Instead, it has to be actively applied in all relevant company units as a continuous process. Physical protection of the critical components is enabled by giving only the right employees access to the relevant systems. Access to components containing sensitive information can be configured accordingly.

### Certificate Management

SIMATIC PCS neo is equipped with certificate management right from the start, which makes certificate enrollment, renewal or revocation available to the plant administrator. In addition, a central overview provides all details about the status of the certificates in the plant. The user is free to choose whether to use the certificate authority (CA) integrated in SIMATIC PCS neo or an externally provided Microsoft-based certification authority that is in the responsibility of the customer's IT.

### Data Protection/User Management

SIMATIC PCS neo is GDPR-compliant (General Data Protection Regulation, the European Union's data protection law). The creation and maintenance of users and passwords is in the hands and responsibility of the customer (users created remain in the system).

"Security by default" is also fulfilled for user management and is set up during the initial plant installation, i.e. no pre-configured users and passwords are part of SIMATIC PCS neo. If necessary, existing users from the customer's existing IT environment can be mapped into the OT user administration of SIMATIC PCS neo.

### Off/Online Operation

All system components can be operated offline as well as online. This means that the system can be operated on-premise or online.

## Conclusion

Process control systems have long lifecycles that match the industrial processes they control and monitor. Features are added as new demands and challenges arise, but a completely new system creates a rare window of opportunity to integrate these features while opening a fresh new path for future development.

With the development of SIMATIC PCS neo, Siemens was able to break with the past and, at the same time, create a bridge to the future. With a fresh start, the new DCS deeply integrates key features like cybersecurity that over the years have been "bolted on" to existing systems. Looking ahead, Siemens studied the way future process engineers expect to interact with DCSes and created a system that supports global collaboration in engineering and operations, and an intuitive, web-based user interface that makes all relevant information available from a single workbench.

Integrating cybersecurity deeply within the system DNA of the DCS was possible by starting with a clean slate. These means that key function are securely preconfigured (security by default) according to Charter of Trust principles and IEC 62443, reducing the DCS's exposure to attack and enabling a plant to be operated securely right from the start.

SIMATIC PCS neo’s security concepts are in accordance with the Charter of Trust in many fields. These aspects PCS neo also supports operators in patch management and attack detection. A central overview of the current patch level is used to display variations so that they can be installed from a central location.

*For further information or to provide feedback on this article, please contact your account manager or the author at* tmenze@arcweb.com. *ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.*