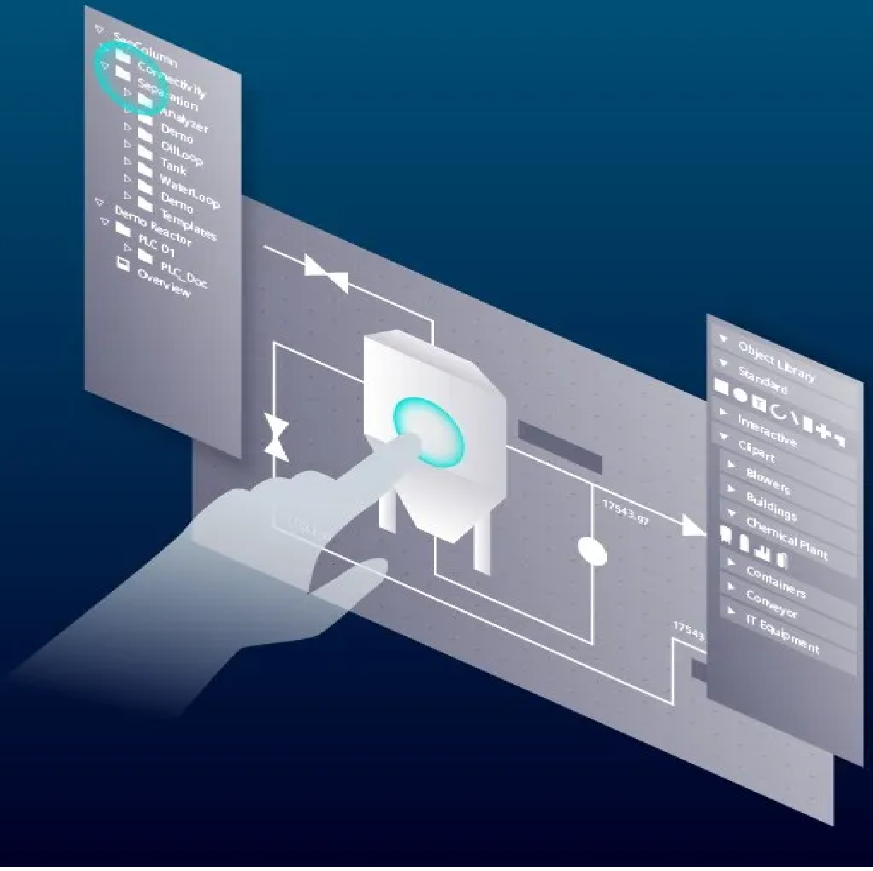
SIEMENS



The **Future** of **Process** **Automation**

Web-Based Process Control Becomes Reality

The process industry operates in a complex environment, and the requirements for its control technology are correspondingly demanding; an intelligent response to this challenge is a web-based process control system with object-oriented data management.

Process industry companies that have not embarked on their digital transformation journey risk being left behind. The history of process control has marked a progression from manual control to pneumatic, and eventually to distributed control systems (DCS). Technological advances such as browsers, networking, the Internet, cellular communications, and the Industrial Internet of Things (IIoT) have set the stage for web-based process control. The result is a more flexible, easily managed control system with built-in security based on ISA/IEC 62443 industrial cybersecurity standard.

HTML5 and web-based process control

HTML5 is a language for writing web applications, designed to operate without requiring additional software or plugins. Maintaining consistency with other web applications, it is a non-proprietary universal standard that operates across many platforms such as tablets, laptops, smartphones, smart TVs, and so on. Its goals are to improve the language with support for multimedia and other newer features; to keep the language easily readable by humans, and consistently understood by computers and devices such as web browsers, parsers, and the like; and to be backward-compatible with older software.

HTML5 includes detailed processing models to encourage more interoperable implementations; it extends, improves, and rationalizes the markup available for documents; and introduces markup and application programming interfaces (APIs) for complex web applications. For the same reasons, HTML5 also is a candidate for cross-platform mobile applications because it includes features designed with low-powered devices in mind.

When applied to process control, access to the control system engineering and operations environment is gained through an HTML5-compliant web browser such as Google Chrome or Microsoft Edge. It should be noted that HTML5 is an open standard that's not specific to control systems.

HTML5 web-based process control does not require an Internet connection. That does not mean the control system is running in the cloud; it can work on a local network not connected to the Internet. It uses web technologies based on HTML5 for communication between servers and web clients.

Siemens has embraced web-based process control with the introduction of the SIMATIC PCS neo process control system with object-oriented data management. The PCS neo platform incorporates open technologies to improve organizational collaboration and business performance. PCS neo is a future-proof platform that integrates and supports current, evolving, and future standards including module type package (MTP) and OPC UA.

Benefits of web-based process control

While HTML5 is a strong point for SIMATIC PCS neo as the first fully web-based DCS, it is not the only strong point. For example, pre-installation on devices is not necessary to run PCS neo due to Siemens zero-installation client approach.

The PCS neo client doesn't need as many resources as were required by non-web-based control systems because the project information is stored on servers. This helps reduce the overall system cost. For a large plant, typically only a few higher cost servers are required. Companies can save money with lower-powered machines for clients. PCS neo client requirements simply include Windows 10 Enterprise and Google Chrome.

The zero-installation client approach requires no software or licenses to be installed on workstations. All licenses are centrally installed and maintained at the server level, which simplifies system upgrades. It also means faster system setup as well as on-demand scalability. As projects scale, more engineers can be added as resources become available to expedite project timelines. Operator stations can be easily added as needed.

In addition, the zero-installation client approach means fewer requirements for workstations. Users have the flexibility to use devices that best meet their needs, whether it's a PC with quad monitors in the control room, a laptop at home or in the office, or a tablet in the field.

There is less need for dedicated specific-use workstations such as engineering, operations, and maintenance based on installed software licenses. The same workstation can be used for engineering and operations if the user has the required access rights.

PCS neo is the first fully web-based DCS on the market, from engineering to monitoring and control. It should be re-emphasized that web-based does not mean Internet-based. While remote access to the plant is a highlight of PCS neo, it is not necessary, as it also runs as designed on a closed network.

Remote access allows users to pull in the right engineering resources regardless of where they're located in the world. It allows operations to operate the plant from any location—even access the plant from home. Remote access has eliminated the need for installation on the client, and it reduces infrastructure and travel costs. Using web-technologies with HTML5 gives maximum flexibility and security for distributed collaboration in engineering and operation as well as remote access via a terminal server in the demilitarized zone (DMZ) with corresponding security standards.

The PCS neo web-based process control system provides a consistent, end-to-end workbench for all tasks and an intuitive graphical user interface (GUI) for usability on fixed and portable devices. This provides operating personnel with information to make real-time decisions in their daily work based on rapid analysis of process information as well as immediate collaboration with engineering to collaboratively and quickly diagnosis and fix production issues.

The intuitive GUI screen automatically fits to the current monitor size. Quad segmentation can be set up on a single monitor, which means less money spent on equipment. In addition, users can change the current view by zooming in or out to see process displays and faceplates more clearly, which provides better visibility than non-web-based process control systems. The intuitive GUI also features better button size if needed for touchscreens. Users will find that shortcuts from other HTML5 applications are familiar.

Web-based process control remains safe and secure

Siemens considered built-in security a priority for PCS neo. It uses its integrated security mechanisms as well as allows users to configure project-specific adaptations. Secure and fast data access is made possible using the latest cybersecurity technologies coupled with site-administered role-based access management. Web-based process control systems conform to industry standards as an integral part of defense-in-depth strategies to achieve multiple layers of protection of manufacturing plants including:

- Physical and organizational security measures
- Users' intellectual property and know-how protected against unauthorized access
- Network segmentation, protection of access points, and communication security—HTTPS, VPN, and certificates
- User management and role-based access
- Patch management
- Malware detection
- TÜV certification of secure product life cycle process, based on IEC 62443-4-1
- TÜV certification for network and system security, based on IEC 62443-3-3
- TÜV certification for IACS service providers, based on IEC 62443-2-4
- Compliant with current IACS security standards
- Secure web connection.

Physical access protection and monitoring means critical data stored on hardware can be separately protected by physical restrictions. By using web clients in a web-based architecture, users can protect critical components in a separate cabinet room with the highest access protection. Access protection refers to:

- Facilities and buildings
- Control and equipment rooms
- Cabinets
- DCS devices (controller, input/output [I/O] system, power supplies, etc.) and PCs
- Network components (switches, router, wireless, Wi-Fi), and local area network (LAN) ports
- Cables and wiring.

PCS neo is designed to operate in separated network cells through multiple firewall layers. The front firewall controls and restricts data exchange with the office network. The perimeter network, or DMZ, allows service and support access to the plant with controlled and restricted data exchange with the process control network. On every host, a Windows firewall is automatically configured by PCS neo.

PCS neo's system hardening helps reduce security risks by eliminating potential vulnerabilities. Web-based process control patch management provides an overview about missing patches in the plant. The integrated central patch management with the administration console allows security vulnerability repair. Windows server update services (WSUS) is used for installation and management of Microsoft updates with a compatibility test for SIMATIC PCS neo.

Early attack detection allows the system to take countermeasures and reduce the potential damage. PCS neo is compatible with antivirus software, and additional protection is provided with support of optional systems like security information and event monitoring (SIEM), intrusion detection system (IDS), and intrusion prevention system (IPS). Authentication and access protection provides control, overview, and easy administration of access to the system. Users and applications have only as many rights as they require for their tasks (least privilege).

PCS neo uses a Microsoft Windows domain as a system environment and a certificate authority. This can be a standalone domain just for the DCS, or it can integrate to the corporate domain, allowing operators to log on to the DCS with the same credentials they do for their corporate email. Between domains and certificate usage, Siemens is not only validating the users who access the system, but the end devices as well. This is adhering to the defense-in-depth strategy that PCS neo employs out of the box.

Software is installed only on servers and licenses are centrally managed by the administration console. No DCS software or licenses are required on client stations. If a user accesses the plant remotely from a laptop or mobile device and accidentally loses this station, there is no plant data on this device. Plant data is only on the servers, which are at the site, locked in a control cabinet—safe and secure.

Access control is critical. Users want to give all users of the system the right amount of access. Not more, and not less. Once an engineer or operator opens PCS neo, they will only get a prompt for a username and password, if the station they are on has the PCS neo certificate issued from the certificate authority. Then, the user enters their domain-specific username and password, and they are in PCS neo, with only the amount of access their account is activated for.

With PCS neo security administration, security is "built in" instead of "bolted on." Users can have integrated security with limited administration effort—a future-proof concept.

Siemens is providing PCS neo training to its partners for system administration to ensure a secure installation and recommendations, as well as providing documentation on security setups and best practices.

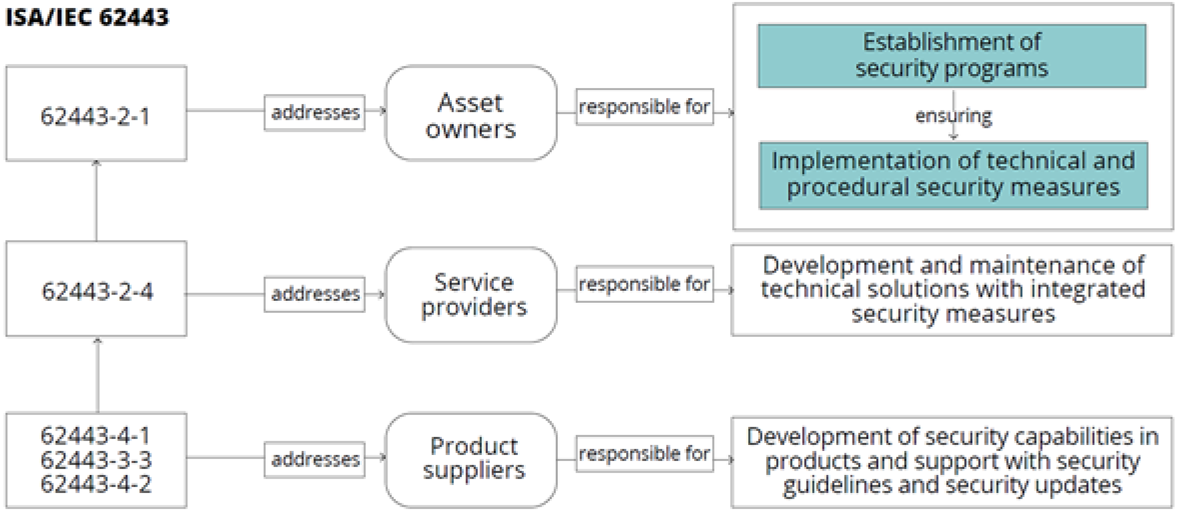
Web-based process control is one way for process industry users to get ahead, and not get left behind on their digital transformation journey.

Ensuring Cyber Secure Web-Based Control Systems

Although SIMATICS PCS neo is a web-based control system, web-based does not mean Internet-based. It can run as designed on a closed network and has been designed from the start to be compliant with current Industrial Automation and Control System (IACS) security standards, including the ISA/IEC 62443 series of standards.

Many organizations have established policies and procedures governing cybersecurity of their corporate IT sys tems based on ISO/IEC 27001/2. Securing industrial operational technology (OT) systems, however, require another approach. ISA/IEC 62443 series of cybersecurity standards are purpose-built for securing OT systems. When used in combination with ISO/IEC 27001/2, they ensure that organizations maintain conformance with ISO/IEC 27001/2 through common approaches wherever feasible, while applying different approaches for IT vs. OT where needed.

While some continue to debate about whether to use ISO/IEC 27001/2 or ISA/IEC 62443 for securing OT infrastructure, the right approach is to use both. Pierre Kobes, who has worked for more than 40 years for SIEMENS AG with responsibility for Standards, Regulations, and Certifications, participated in the development of most of the documents for ISA/IEC 62443. He has been involved in multiple projects to implement the standard within Siemens and continues to work in its evolution. He authored a white paper for the ISA Global Cybersecurity Alliance (ISAGCA.org). that describes how these two globally accepted standards can be used together for establishing an integrated, company-wide cybersecurity plan.


ISA/IEC 62443
62443-2-1
addresses
Asset owners
responsible for
Establishment of security programs
ensuring
Implementation of technical and procedural security measures
62443-2-4
addresses
Service providers
responsible for
Development and maintenance of technical solutions with integrated security measures
62443-4-1
62443-3-3
62443-4-2
addresses
Product suppliers
responsible for
Development of security capabilities in products and support with security guidelines and security updates

ISA/IEC 62443 addresses all entities involved in the protection of industrial operating facilities. Note: The image document refers to the most recent version of part 62443-2-1, which is not finally approved as an International Standard and may be subject to changes. Source: ISAGCA

“Asset owners rely on the design of adequate technical solutions with integrated security measures, and on security capabilities of products used in these solutions,” says Kobes. ”The ISA/IEC 62443 series provides a significant added value by addressing all other entities that support asset owners in applying a defense-in-depth approach for the protection of operating facilities against cyber threats.”

ISO/IEC 27001/2 includes five controls (class A.15) specifically about suppliers, and a number of mentions of suppliers in guidance for other controls. The ISA/IEC 62443 series supports implementation of these controls by providing specific parts of the standard with which OT suppliers in specific roles should comply. This gives the asset owner a basis for placing cybersecurity requirements on OT suppliers and potentially requiring third-party certification to relevant parts of the 62443 standards for their OT suppliers or for product purchases.

For example, says Kobes, 62443-4-1 includes requirements on product suppliers for reducing and managing vulnerabilities such as threat modelling, applying secure design principles, eliminating coding vulnerabilities by following coding guidelines, finding and eliminating vulnerabilities via testing such as fuzz testing, penetration testing and binary analysis, providing security guidelines for users, and addressing vulnerabilities discovered in the field with a process for security updates.

In addition, the ISA/IEC 62443 series includes requirements for the technical security capabilities of products used in OT infrastructures and defines Security levels (SLs) to differentiate the level of protection which can be potentially reached commensurate to the tolerable cybersecurity risks of asset owners.

PCS neo holds the following certifications related to specific parts of ISA/IEC 62443:

- TÜV certification of secure product life cycle process, based on ISA/IEC 62443-4-1
- TÜV certification for network and system security, based on ISA/IEC 62443-3-3
- TÜV certification for IACS service providers, based on ISA/IEC 62443-2-4

Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005

1-866-663-7324
info.us@siemens.com