

Security architecture and policy development

Customer FIRST cybersecurity services

Service at a glance

A successful and reliable security environment starts with a solid architecture, powerful system design, and integrated policies. You need people who understand your industry, your business, and your challenges.

Leverage the skills and experience of a seasoned, global team to ensure that you are protecting your enterprise and meeting all regulatory standards.

Minimize the risks of lost productivity, counter threats to safety, and ensure the integrity and performance of your operation's assets.

Cybersecurity basics

The modern plant is a hierarchy of networks, all interconnected to provide seamless integration of various systems, both automation and information. When it comes to developing cybersecurity for these systems, there is often a gap between the knowledge and understanding of a typical IT-oriented service provider and those that control and automate plant operations.

An understanding of the individual characteristics as well as the intricate nature of integrating control systems and enterprise networks is essential. An awareness of the impact of downtime as well as operational and maintenance restrictions not faced in other industries is of vital importance.

Security architecture and policy development

Customer FIRST cybersecurity services

Straightforward cybersecurity

Schneider Electric has over 100 years of experience in the automation industry and has systems installed in over 50,000 plants worldwide. The company is at the forefront of plant integration, with comprehensive knowledge and skill to develop and design security solutions that protect without obstructing. Schneider Electric security designs provide the maximum amount of flexibility while maintaining data integrity, and more importantly, safety. Our Security Architecture and Policy Development service provides solutions to mitigate vulnerabilities and satisfy the policy requirements identified in an assessment.

The main goals of security architecture and policy development are:

- Establish network and security designs based on established industry standards
- Determine and evaluate applicable regulatory drivers
- Create security policies with proper authorizations

Specific service elements are applied to address these goals:

- **Site Security Design** — Development of a plantwide security architecture that protects all of the interconnected systems from the field and control networks throughout the organization. Involves the selection of appropriate hardware and software components required to secure objectives, e.g., firewalls, intrusion prevention, biometrics, antivirus, etc.

- **System Security Design** — Similar to a site security design, but focusing on securing a specific system, often with specialized requirements
- **Security Policy Creation** — The development of the security policies that will govern by whom and how the various networks and systems are used and accessed
- **Procedure Creation** — The creation of the procedures that will dictate how the various networks and systems are supported, maintained, and updated
- **Compliance Evaluation** — The security and policies currently implemented are checked against a set of criteria — particularly relevant where government or industry regulations establish requirements which must be complied with.
- **Security Planning Workshop** — A planning workshop where relevant personnel participate in developing the security designs. The concerned site personnel attend to help develop the security designs and policies that need to be implemented. This allows site personnel to participate in the design phase and aids knowledge transfer.

A complete solution is offered using a combination of these elements, allowing Schneider Electric to develop a unique and customized approach.

Benefits

- Unique design perspective based on knowledge of process control and the plant environment
- Architecture for a security-focused network for the entire plant, not just part of it
- Focus on maintaining plant operations, reducing downtime, and increasing availability of data
- Experience in both control systems and security design bridges the gap between IT and control
- Proactively secure the site through designs based on intrusion prevention over simple detection
- Service organization with global reach

Security architecture and policy development

Customer FIRST cybersecurity services

Get more with Schneider Electric

Schneider Electric has a dedicated team of security specialists with expertise and experience in control systems, security, and IT to provide a portfolio of security services that are not just for Schneider Electric products. Schneider Electric is an active participant in government and industry security initiatives to ensure the most up-to-date knowledge is available to customers.

The Security Architecture and Policy Development solution is an integral component of the Schneider Electric cybersecurity portfolio. Its primary goal is to deliver customized security solutions that provide only the elements required. Schneider Electric understands that customers will be at different stages of network maturity, and can help no matter where the assets are in the lifecycle process. Our services provide a unique industry approach that focuses first and foremost on the control automation layer and then up to the corporate IT layer, facilitating a secure integration between the operations and IT networks.

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On

