Rockwell Automation

Securing Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS)

Linkage of Security and Safety in SCADA and Industrial Control Systems

Real-world security threats put the safety and operational integrity of Supervisory Control and Data Acquisition (SCADA) and other Industrial Control Systems (ICS) at risk. Ignoring security risks and discounting the need to protect against security threats may have far reaching consequences that extend beyond the value of the manufacturing equipment and proprietary information that comprises the system. These events can affect and disrupt health and safety, economic stability, national security and international, country-to-country relations.

Security incidents involving an ICS can restrict access to the system or components. They can result in a loss or disclosure of mission-critical data and information. There is also potential for incidents to affect control or result in asset and collateral damage to those affected by a particular incident.

Unintended and intentional attacks strain Safety Instrumented Systems (SIS) engineered to specifically protect people and assets from harm. As a result, security and safety design considerations in a control system are closely intertwined and prove essential to helping protect control system assets, including people, property and proprietary information.

Why secure SCADA and ICS?

Communications and reliable information exchange is core to maintaining quality production and operational vitality of a manufacturing system. Critical Infrastructure processes and critical manufacturers provide power, gas, clean water, quality food to consumers in a safe and secure manner. The safe and reliable production of products and services is critical to both the manufacturer and to the consumer.

Simply put, it is critical to secure SCADA and ICS for the following reasons:

One answer is safety.

Securing control systems is imperative in order to assure functional safety and the reliable operation of mission-critical systems. Without addressing security, there can be no integrity in the functional safety system.

The certification process of a safety system only includes the verification of the use of safety-certified products and the logic applied in that safety system. The integrity and trustworthiness of the data used throughout the safety system are essential in order to ensure operational uptime and avoid nuisance-trips that disrupt production.

Another answer is intellectual property protection.

The value of the intellectual investment and know-how designed into control systems often exceeds the value of the control system components. Custom recipes and routines, production data and proprietary algorithms are typically unique to an application and determine performance, quality, consistency, and the ability for market differentiation essential to maintaining customer loyalty. Without securing and safeguarding this information the risk of tangible loss increases.

A comprehensive Industrial Security Program that accounts for asset protection can help:

- Protect brand reputation
- Sustain customer loyalty
- Prevent counterfeiting

The last answer is uptime.

Reducing industrial security risks and maintaining safety in industrial control systems have a direct bearing on operational integrity and ultimately, bottom-line profitability. Uptime, as a measure of reliability of the control system, is affected by controllable variables. These variables include system design, employee training, company policy, operating procedures and adaptability of the infrastructure to a changing threat landscape. Appropriate management of these variables bolsters the robustness and resiliency of the system against events that can reduce operational uptime.

Industrial Security Recommendations

Industrial Control System security programs define the controls, behaviors, and expectations (of users and processes), and lays the groundwork for securing ICS assets. A well-planned, comprehensive security strategy enhances functional safety solutions, while helping safeguard key control system assets and information from disruption, damage and catastrophic loss.

Establish a Security Governance Program

Security and Governance Programs for ICS environments should take a multifaceted approach to addressing and managing the needs of these environments. This allows for the inclusion of both technical and non-technical controlling elements within the environment.

Examples of technical controlling elements:

- firewalls, routers with the appropriate layer three access control lists (ACL)

- Microsoft® Active Directory permissions and Group Policy Objects (GPO)

Examples of non-technical controlling elements:

- standard operating procedures
- environmental rules
- general policy and procedures

Develop a Security Policy, Procedures and Guidelines

Security policies are the rules for controlling user interaction with the complex control system.

Examples of relevant control system policies include:

- Physical & logical access (local and remote)
- Authorization, Authentication and Accounting
- Disaster recovery and incident response plans
- Patch management and upgrade policies
- Change and configuration management
- End-point protection of controllers & components
- Human resource management (hire/fire)

An industrial control system's intended use, and the engineering requirements for the function of that control system must be addressed when developing a security policy. Once addressed, a profile of an appropriate level of security can be characterized for the control system and audits can be conducted to evaluate its security.

Conduct Asset-Based Risk and Vulnerability Assessments

Through an objective approach, security procedures can be developed that will account for:

- Risk and threats targeting the control system
- Usability, ease of use, and system accessibility
- Necessary protections for people, assets, and key information

Develop Technical Security Controls

Mitigating and compensating controls should be developed and deployed to address the risks identified in the assessment process. Security controls can include:

- Guards, gates, and physical security measures
- Network Access Control (NAC), 802.1x, Port-security elements, RADIUS, etc.
- Active Directory and other control-system authentication stores
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Layer-3 Access Control Lists (ACL) and Unified Threat Management device policy and rules
- Windows Server Update Services (WSUS) and vendor-specific patch qualification services
- Back-up, archiving, and disaster-recovery tools
- End-point protection software

Focus on Security Lifecycle Management

Security throughout the automation lifecycle of a control system requires ongoing investment in order to protect the system from evolving threats. In managing this life-cycle, it is essential to proactively plan and implement a control system strategy that accounts for obsolescence and associated risks with aging products and systems. In addition, competency of control system operators and maintenance personnel is key to the mitigation of evolving security risks. Lifecycle management focal areas include:

- Training and continuous improvement
- Monitoring of people, process and components
- Auditing
- Maintenance, replacement, migrations

Industrial Security Support and Expertise

A robust security strategy is both broad and deep in the enhanced protection it facilitates in control system safety and operational integrity. The scope of a truly expansive industrial security solution includes the control system and its constituent products, but also the people, policies and procedures necessary to maintain a specific level of security. Expert consulting services can often help assure a more thorough and complete evaluation of security posture. Rockwell Automation's Network & Security Services group has the expertise and know-how to help address industrial security concerns in a balanced way.

For more information about Rockwell Automation's Industrial Security position and capabilities, including Network & Security Services, visit www.rockwellautomation.com/security.