IndustryWeek MachineDesign

FAQ

HOW TO PROTECT YOUR PLC CONTROL SYSTEMS FROM SECURITY THREATS

The increasing connectivity of our world is a beautiful thing. However, with this increasing connectivity also comes the potential for increased cybersecurity risk to an facility's control system.

As is true with any organization's digital transformation, it encompasses more than the implementation of technologies; it drives adoption of best-in-class behaviors and enables cultural and behavioral change within an organization, helping create and empower a digital workforce. One that has personnel focused on high-value tasks and empowered with actionable data from digital technologies and services that leads to improved decision making in daily operations.

As the potential for cyber threats continue to evolve and become more complicated to detect and respond to, the need to modernize how these threats are addressed should be every industry's top priority. Adopting a risk-based approach to cybersecurity can help identify potential vulnerabilities and make strategic decisions based on the likelihood and impact of each vulnerability.

Here are some common questions and ways to address the risks when trying to stay ahead of the emerging threats and empower a digital workforce:

What are some ways to monitor your network and detect threats?

The easier it is to monitor network activity, the faster a facility can respond once a threat is detected, which ultimately reduces the impact of the threat. Therefore, one of the most important steps in protecting your programmable logic controllers (PLC) and programmable automation controllers (PAC) control systems from security threats begins even before a threat is detected.

Using network communication port monitoring will make checking for unexpected network protocols, connections, or communications types easier. While unexpected activity on a network may not end up being a threat, it should always raise a red flag, and is always worth investigating.

Most enterprises are aware that they should implement anti-malware software on their HMI and SCADA servers, but it is just as critical to set up anti-malware software on every device that will connect to these control systems, like laptops, tablets, smartphones, or any other device that might share a network with the control systems because a compromised ancillary device may provide a hacker the perfect gateway to a system's data.

When implemented across an entire facility, a centralized anti-malware software can prevent, detect, and remove malicious software, making the monitoring process more effective and efficient.

How do you limit damage from a breach?

No matter how prepared you are, security attacks and breaches can still happen. Therefore, it is important to not just try to prevent them from occurring, but also to ensure that if they do occur, the damage is as minimal as possible.

One way to limit network damage is to have more than a single security control; implement a robust, tiered approach with security controls at many independent levels that an attacker must breach in order to truly compromise the entire system. Having the right cybersecurity defense-in-depth strategy helps avoid safety issues and plant shutdowns.

Segmenting networks into logical zones to thwart internal threats, which, while less common, often result in the most damage. Having separate zones, often described as "enhanced network segmentation," is more challenging to implement and maintain compared to traditional network segmentation; however, it is considered one of the best ways to protect control assets.

At a minimum, facilities should also ensure secure deployment with firewalls and segmentation to block unsolicited incoming traffic, as well as isolate networks to restrict data transfer to its intended locations. Use of advanced or application layer firewalls is an ideal approach to increase this capability.

Another way to limit the effects of a breach is by utilizing redundancy or including backup components in a system, so that the system can continue to function in case of a component failure or security breach.

Finally, one of the most important ways to limit the impact of a security breach is establishing effective and sound business continuity or recovery processes and policy that are practiced, so that a breach can be dealt with before its impact has the chance to spread and mitigated from future threats.

What are some other ways to reduce your attack surface area with PLCs?

Locking down all unused communication ports and turning off all unused services are simple steps to take to reduce the surface area that can be attacked.

Facilities should work with vendors who have proven certifications, such as Achilles, for PLCs and PAC systems that span the design and engineering technical security requirements for a control system. Certifications enable control system vendors to formally illustrate compliance of their control system produced with cybersecurity requirements.

Monitoring machine-to-machine communication within a facility is another critical step when striving to ensure an attack is not occurring. All communications should be done securely through protocols for industrial automation such as OPC Unified Architecture (OPC UA), which offers robust security that consists of authentication and authorization, and encryption and data integrity. By monitoring the network communications, newly opened ports or protocols being used alert you a potential threat.

What is the best way to manage PLC user authentication?

Unintentional behaviors can be one of the most critical threats to an organization. To lead change in an organization, it is important to adopt best in class behaviors and help educate your own workforce on steps to mitigate risk. For example, one of the biggest threats to security is password selection. In a world where some of the most common passwords are "password" or "123456," it cannot be stressed enough how important it is to instruct users to select strong passwords and to offer guidelines about how to do so.

Require user authentication between a client application(s) and a server to ensure that only authorized users are accessing the server. Multi-factor authentication and role-based access control are the best options if your system can support this level of security.

What is the best way to isolate the PLC network?

The biggest risk posed by remote network access is that it makes it possible for a hacker to gain deeper access to an organization from outside of it, and once they do, it becomes very challenging to prevent unplanned shutdowns, loss of control, data loss, etc.

Businesses should also audit their PLC network to locate any obscure access vectors a hacker might use, and regularly monitor the access points.

A company can implement multi-factor authentication, which requires a user to successfully present two or more pieces of evidence—or factors—to an authentication mechanism in order to be granted access to a device, application, or information.

Two-factor authentication is a commonly used subset of multi-factor authentication. This method confirms a user's claimed identity by using a combination of two of the following different factors: something they know, like a password; something they have, like a keycard or software token; or something they are, like presenting fingerprint or facial identification.