

4 Steps To Secure Your Automation System

Due to advancing technologies, automation systems utilize digital network infrastructures and if these systems are not secured properly, they can be very susceptible to hazardous risks. Maintaining a secure automation system can be achieved by using proven steps that consist of industry best practices, which are customized to meet the desired level of security required.

Security is defined as a state of being free from danger and to achieve this you must constantly be on alert to guard against potential threats. Independent third party evaluations from a specialist with in-depth integration experience provide intrinsic value. Third party experts encompass comprehensive knowledge of system interactions, data exchange, and a complete understanding of process control as well as production demands.

Here's an example. The upper management of a long-time customer was having difficulty accepting the site engineer's assessment that the control system was indeed secure. As a third party, we were asked to come in and provide an assessment to confirm the current state of the system. After the review, we identified some basic safety practices that had been overlooked through years of projects and system upgrades. After some simple corrections and adjustments, the system was validated to meet the expected security standards and was accepted by upper management.

4 Steps To Secure Your Automation System

1. Define
2. Assess
3. Implement
4. Review

The method and strategies used to secure your automation system start with defining what is in place. Next, an assessment must be completed to confirm, verify, and further identify vulnerabilities. Once all risk factors are known, the implementation phase includes the selection of the desired security level, and execution of the customized solution to meet the specific site needs. Finally, a

4 Steps To Secure Your Automation System

follow-up audit to ensure security measures are effective. Once you have defined the system assets, identified vulnerabilities, and implemented a tailored solution, then maintaining a level of security becomes a routine periodic procedure.

The steps listed below outline a proven and cost effective method to protect your automation system assets from potential threats.

1. Define Your Architecture

To manage your control system security you must be able to define the assets. A network architecture diagram will define the logical connection details to ensure that all devices are identified within the network. This includes any and all communication protocols as well as different media connections, such as third party interfaces, business network connections, wireless access points, fiber optic infrastructure, and any field I/O BUS networks. This diagram should include a unique device name and include a network address and the physical connection port to identify the actual interface connection, which will become important during the review process.

Create a cross-reference device list, essentially a Bill Of Material (BOM), that includes additional supporting information of your assets such as make, model, serial number, firmware version, physical access level, etc. The network diagram should segment the associated areas of the facility to depict the distribution of assets across the entire control system. This diagram and associated information provide a road map of your system and it is critical to fully define and understand the asset vulnerabilities.

The diagram may require multiple pages and links to additional information to clarify the associated equipment to ensure all the information is depicted thoroughly depending on the size of your system.

2. Assess Your Site

Site assessment is a critical process that requires acute attention to detail and can be very time-consuming. Typical site assessments further outline the network infrastructure and generally identifies potential action items that need to be clarified

4 Steps To Secure Your Automation System

and/or defined by the end-user. Physical accessibility to equipment is only one aspect of potential vulnerability.

This phase also includes the finalization of each element connected to the physical network and this is typically achieved by utilizing simple network scanning tools to identify all communication nodes. This investigation includes a thorough evaluation of each device in an effort to identify all vulnerabilities.

This phase can be an exhaustive search-and-find effort depending on the past installation practices, the size of the automation system, and status of existing supporting documentation. This effort should be well planned to ensure the entire existing infrastructure is completely identified and documented to ensure that all the information is accurate, as well as to ensure that the automation system production is not compromised during the investigation.

3. Implement Your Security Plan

Once the data is collected from the onsite assessment, it is compiled into a full report. This report will define all of the vulnerabilities identified in the current system and outline a list of possible recommendations to remove as much risk as possible to provide a secure automation system. Security measures typically include multiple layers of protection methods to remove as much risk as possible.

The level of risk that is assumed can only be defined by the end-user and must be balanced against the likelihood of a security breach versus the potential results. Once the final solutions are accepted, these costs can be defined, the actions planned, and the solutions can be implemented. Once chosen, the final solutions can encompass multiple layers, steps, and require extensive planning and implementation strategies.

Typically, security measures can be broken down into short-term and long-term goals. The short-term goals can potentially be put in place fairly quickly to help remove or reduce a potential vulnerability. Long-term goals can include extensive levels of solutions that require multiple phases depending on the existing practices and integration of networks. The idea is to identify the simplest and easiest

4 Steps To Secure Your Automation System

methods first while outlining additional security goals in a larger planning strategy. This may require multiple steps to appropriately reduce risk while preserving production run-time.

4. Review Your Assets

Once the vulnerabilities are identified and you have chosen the level of acceptable risk, you must define a review or audit period to successfully manage the security lifecycle. Security is something that must be maintained for continuous use. Threats and vulnerabilities can migrate, grow, and morph or adapt over a period of time due to technology, human error, or external influences. Therefore, a scheduled review of the system health activity is required to ensure new vulnerabilities are not introduced.

A thorough review or audit procedure should be defined after or during the implementation phase. The procedures should identify clear and precise steps to allow anyone with basic knowledge to complete the evaluation and determine the health of the system. Each step should have a measurable goal to achieve and ensure the integrity of your automation system is not compromised. As new tools or advancements in technology are released, the audit procedures should be updated to ensure the continual evaluation remains current. Successfully managing the security of your automation system is a continual effort, but consistent practices can ensure the integrity of your assets.

Conclusion

Security threats are continuous. To ensure your assets remain safe from harm, you must protect your livelihood by ensuring automation system vulnerabilities are identified, dealt with properly, and effectively resolved.

The most vulnerable threats to automation systems are simply overlooked or unknown to internal engineers. Third party evaluation from a specialist with in-depth knowledge and a proven assessment process can provide insurance that production systems remain safe and secure. External validation removes liability and provides management a layer of assurance that the production's assets remain secure.

4 Steps To Secure Your Automation System

Implementation of acceptable industry standards should be customized to meet the desired level of security defined by the end-user. This can be achieved through thorough analysis, implementation, and periodic audits to ensure your company meets the production requirements by protecting the automation system critical assets from harm. Our process automation experts have years of experience working with automation system security in a range of applications and can work with your team to ensure your automation process is safe, and efficient.