

How Vulnerable Is Your Industrial Control System?

Threats to the Industrial Control System (ICS) network infrastructure are at an all-time high and the level of sophistication is greater than ever before. The increased volume and sophistication of these attacks make an ICS an easy target for perpetrators because of its aging infrastructure, lack of security planning/design, and minimal focus from a corporate group to protect ICS assets.

A detailed analysis of the infrastructure and operational aspects of your business can provide great insight to your level of risk as well as identify potential countermeasures to protect key assets. This type of holistic approach should be taken to assure all aspects are considered to fully understand the actual level of risk posed to the production system. This includes the cyber and physical security, as well as the status of the system lifecycle. To help discern the exact level of risk, each element should be evaluated thoroughly to understand the design, operational, and maintenance differences to preserve the livelihood of production systems.

How We Got Here: ICS Evolution

Historically, ICS providers utilized proprietary hardware and/or software solutions, which were physically isolated from external connections. Today, ICS utilizes commercial off-the-shelf (COTS) components and standard operating systems such as Microsoft based platforms and common communication protocols. The move from proprietary systems to open technology allows for the use of third-party hardware and software components, which has helped drive the overall lifecycle costs of ICS down. In addition, the adaptation of standard common components and associated communication protocols facilitates easier connections with IT or business systems. This sharing of data from the production system to the business system can potentially provide valuable business insight with minimal effort to collect and analyze the data.

These same features that have improved the lifecycles and made connectivity a snap can expose the vulnerabilities of ICS applications which are not specifically designed with security as a primary focus. ICS providers typically publish recommended security practices which define a specific methodology to allow for connecting to external systems, but ultimately the responsibility of securing an ICS network is completely up to the end user to deploy and maintain. Securing these

How Vulnerable Is Your Industrial Control System?

networks to ensure production availability and protection from a security concern should be a comprehensive business objective defined and supported by management.

Many of the infrastructures deployed today do not follow the National Institute of Standards and Technology (NIST) standard guide to Industrial Control System Security, which is recognized by the Department of Homeland Security. The Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21), proactively coordinates, strengthens, and maintains critical infrastructure that is vital to public safety, prosperity, and overall well-being.

Why You Cannot Manage IT and ICS Infrastructure The Same Way

The IT and ICS infrastructure both utilize common networking components, but they are very different when it comes to maintenance, operation, and security management. The security goals of an IT business network and ICS network are completely different concepts, but they are based on the same principles of confidentiality, integrity, and availability.

For IT, business owners are mainly concerned about disclosure of intellectual property and confidentiality is the highest priority. Next, the integrity of the data is very important and that is followed by network availability. The ICS network has vastly different priorities due to the critical nature of production system data. The dependence upon human interface requires the availability of the system to be the highest priority for the industrial sector. The integrity of the data is also very important due to the significance of having accurate information. Then finally confidentiality is not typically a major concern for industrial networks. These differences in the system priority make the operation and security management aspects of the network drastically different.

While both systems utilize common components for infrastructure, the operation of IT and ICS networks are significantly different. Typically, IT network operations are initiated by users on an irregular basis, or as needed. The amount of traffic generated on the business network can be sporadic and unpredictable. The network components such as servers, network devices, and computers are removed or

How Vulnerable Is Your Industrial Control System?

added to support business needs. Business system communication protocols are built around this type of operation and typically do not include any type of deterministic mechanism because of the sporadic data.

On the other hand, ICS networks require a very high level of availability to support continuous and uninterrupted production system requirements. These systems are designed to deliver data at a deterministic rate to allow for predictability and repeatability. ICS communication protocols support deterministic activities that capture time-critical events. These systems are designed to allow for high availability of critical data that is time sensitive. The contrast in network operations of IT and ICS makes the implementation of security methods very different as well.

Standard IT “Fixes” May Harm ICS

IT typically deploys broad security countermeasures to help prevent cyber attacks. However, most common IT security methods can have an adverse effect on ICS networks due to their requirement of needing deterministic high-available data. An example of some standard IT security practices includes applying operating system patches, application updates, and server system upgrades. These are considered common practice in the IT world. However, on an ICS network, these actions can potentially have a very negative effect on the operations and associated components.

Other common IT practices such as domain changes, virus scanner updates, anti-malware updates, router configuration changes, port blocking strategies, etc. are all examples of actions that can be detrimental to ICS networks due to critical nature of associated software, system components, and/or delivery of data. The deployment of any such change to an ICS network or associated components must be carefully considered and should be staged on a test system to analyze performance characteristics prior to deployment on an active production system.

In addition, special consideration of security practices must be taken to ensure the ICS network operation is not impeded. Identifying the correct approach and applying the most cost-effective risk mitigation solutions are critical to support business for both IT and ICS infrastructure. The availability of ICS network

How Vulnerable Is Your Industrial Control System?

requirements makes them much more sensitive to any minor changes within the production system.

Determining An Accurate Risk Level

Failure to assimilate the actual level of risk of an ICS network is a lack of awareness and understanding of all the potential vulnerabilities. Just like IT systems, the effort required to make an ICS network cyber-ready must be a comprehensive effort recognized by management to ensure the availability of the production systems. Simply putting a firewall between the ICS and IT network is not enough protection to remove the risk considering the sophistication of modern hackers. To fully understand the actual level of risk to a production system, one must evaluate all aspects that expose vulnerabilities, such as a loss in production, environmental harm, equipment damage, and/or human safety. This can include cyber, physical, and local interface vulnerabilities that are potentially threatening from internal, external, malicious, and unintentional incidents. All aspects of the ICS lifecycle must be defined to ensure all potential hazards are considered.

Risk can be introduced through multiple vulnerabilities in ICS infrastructure such as utilizing legacy platforms, system architecture design, connectivity to external networks, wireless access points, and/or remote interface points. Generally, ICS are deployed much longer than standard IT systems, which can be contributed to costs, availability of production outages to move to a newer system, as well as a lack of knowledge of associated risk with running legacy systems.

Other factors that contribute to potential vulnerabilities are a failure to design and/or maintain a secure ICS network, which may be a result of multiple engineers responsible over a period of years without a proper security plan and procedures in place. Alternatively, it can also be a result of fast-track deployment of multiple projects, upgrades, or additions that have compromised security. To successfully manage risk you must fully define exactly what is in place, understand where you are in your ICS lifecycle, and ensure a plan is in place to maintain your production system from all possible vulnerabilities. These charters should be mandated by management to assure the livelihood of production system assets remains intact over the entire lifecycle of the system.

How Vulnerable Is Your Industrial Control System?

The Unique Threat to ICS

Threats to both IT and ICS infrastructures are continually evolving and becoming more and more difficult to prevent, detect, and mitigate. The ICS networks are challenging to secure due to the critical nature of production requirements. Therefore, the technicians and engineers that oversee the ICS infrastructure must have a more stringent, planned, and disciplined approach to deploy security methods.

Completely disconnecting the ICS network from internet connectivity still does not remove all associated risk. External threats are obvious if connected to the internet, but internal threats have even more harmful potential than external threats. This includes both inside malicious and unintentional human-error that can cause havoc on the ICS network. Threats to your production system include any and all aspects of the system's ability to display accurate run-time data continuously and uninterrupted. This includes the ability for operators to access Windows desktop functions, local login permissions, and access to system ports and/or interfaces. The effort to physically and procedurally secure the automation system can be very extensive and time-consuming. However, the only way to prevent common system failures is to remove the ability for common users to access these systems, which includes software, hardware, and physical access as well.

The lack of planning and/or procedures to fully manage both the security and lifecycle of the ICS represents the largest threats ICS critical infrastructure within the U.S. As mentioned above, security can be compromised through digital networks or physical aspects. However, operating on a legacy platform can be detrimental to the longevity of a production system. Legacy hardware, software, and support for the system can be both sparse and expensive if they are available at all.

Typically, IT systems are upgraded on a cycle of three (3) to five (5) years, whereas production systems may remain in place much longer. Due to the high availability requirements of production systems, the change-over to a new system can be risky as well. It is very likely that the new system will require re-programming and for logic to be deciphered and/or compiled to a new language. This introduces the possibility of human error and could potentially have adverse effects on the

How Vulnerable Is Your Industrial Control System?

production system.

The operator interface will most likely look and operate vastly different than the existing legacy system. Migrating from a legacy to a newer system can involve many aspects of detail logic specifications to define the safe operation, extensive testing, and operator training to fully qualify a production system. Full-scale replacement may take a period of years and include multiple complex phases to minimize the production outages. Management of an ICS lifecycle should include a comprehensive roadmap planning out all of the cut-over details to minimize the amount of risk to the production system.

What Does “Readiness” Mean?

Mitigating risk and identifying a holistic plan to protect business assets requires a comprehensive assessment that encompasses all aspects of risk to a production system.

Protection of assets should include layers of security and should not rely on a single piece of software or hardware to minimize risk. The consequences of a compromised ICS can potentially cause a loss of production, environment harm/release, damage processing equipment, and compromise personal safety. These consequences are very important and critical to manage and protect the livelihood of our businesses.

Asset protection starts with direction from upper management to identify a proactive initiative to assure the readiness of your ICS is in place to handle evolving threats. A holistic plan encompasses documented security tasks & procedures that outlines the layers of protection, mitigation procedures, and the migration plan to cover the lifecycle of the ICS. Reaction to an incident that compromises the production system should be a planned event that is clearly understood by all personnel to minimize the impact.

The migration plan should include a system roadmap to minimize the production outages and ensure a safe and reliable system during the change-over period. As threats continue to become more complex in nature it is highly recommended to

How Vulnerable Is Your Industrial Control System?

perform an audit of the protection layers annually to ensure they are not compromised. The risk factor will never be completely removed, and it is the responsibility of the asset owners to ensure the readiness of the production system by removing as much risk as possible, protecting our businesses and livelihood.