Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

SECURITY CONSIDERATIONS FOR INDUSTRIAL CONTROL SYSTEMS

JULY 2021 **ITSAP.00.050**

An industrial control system (ICS) automates and controls industrial processes (e.g. manufacturing, product handling, production, and distribution) and mechanical functions to keep processes and machinery running smoothly. An ICS may support critical infrastructure (e.g. energy and utilities, transportation, health, manufacturing, food, and water) that is essential to the ongoing safety, security, and well-being of Canadians. An ICS is the base controller for the other layers in an infrastructure (i.e. production, office, enterprise), therefore it should be secured to maintain functionality. This document introduces some ICS security threats and risks and the security measures that you can implement to protect these systems from harm.

WHAT IS AN ICS?

ICS is a general term that includes other types of control systems such as distributed control systems, supervisory control and data acquisition systems, and programmable logic controllers. An ICS uses processes and controls to achieve an industrial objective. The systems can be fully automated or can include a human in the control loop. Whether your ICS manages a simpler control system or a complex network of systems, you need to secure your ICS to protect the integrity and the availability of industrial processes.

A traditional ICS was not as interconnected with other systems and networks; it could be isolated and secured physically. These legacy devices could only be accessed remotely through a single access account for all users to manage the system through their home and other networks. This left the system vulnerable to cyber threats with no ability to monitor users.

WHAT ARE THE MAIN THREATS?

Your ICS is a high-value target for threat actors because they can cause real world effects, ranging from annoyances (e.g. turning on and off lights) to life threatening and costly events (e.g. equipment malfunctions and permanent damage). Threat actors use targeted attacks to directly compromise your organization or non-targeted attacks to spread malicious software to breach systems where possible. Some main cyber threats to your ICS include the following:

RANSOMWARE

A threat actor delivers malware through an entry point in the system (e.g. by phishing, insider threats, or targeted hacks) to restrict all functions from being accessed until a ransom is paid to the threat actor.

INSIDER THREAT

Anyone who has access to the ICS can cause harm to the system intentionally (e.g. compromise data for personal gain) or unintentionally (e.g. handle equipment inappropriately unknowingly).

DENIAL OF SERVICE (DoS) ATTACKS

A threat actor attacks your system making the services unavailable for intended users. DoS attacks can delay functions and operations, causing your organization to use more resources to restore the operations.

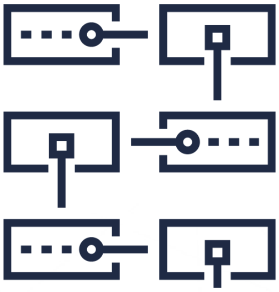
Your ICS is at a high risk of cyber threats if it is not properly secured. Areas of your ICS that are misconfigured or connected to an unpatched virtual private network (VPN) introduce more security vulnerabilities. If you have remote equipment that can access your ICS, handle it cautiously. With the recent increase in work-from-home, remote access, remote technologies have become a high-value target for threat actors. If remote equipment or peripherals are compromised (e.g. malware), threat actors can carry out further attacks on the ICS, which can lead to loss of information, damaged equipment, or life threatening incidents.

Cat. No. D97-1/00-050-2021E-PDF
ISBN 978-0-660-39674-3

WHAT ARE THE RISKS?

If your ICS is compromised, your organization could be at risk of some of the following:

- Blocked or delayed flow of information through ICS networks can disrupt ICS operations (e.g. power generation supply interruption).
- Unauthorized changes to instructions or commands can damage or disable equipment.
- Inaccurate information sent to operators can cause unauthorized changes and inappropriate actions.
- Infected ICS software can spread through your organization's network and devices.
- Malfunctioning operations can result in loss of data or profits and harm your reputation (e.g. outage at a power plant will cause a series of interruptions with all connections).



HOW DO I SECURE MY ICS?

To mitigate risks, your organization should implement the following security measures and industry best practices:

ISOLATE THE SYSTEM

Isolate the ICS from regular corporate functions. Connect it to a different network so that you can disconnect it from the Internet without disrupting other organizational activities (e.g. office and enterprise).

MANAGE ACCESS AND PRIVILEGES

Any system used to maintain and manage industrial systems must only be handled by authorized users and used for its intended purpose. Remote access to the system should be carefully weighed and considered depending on the potential risks involved (e.g. subcontractor acquires time-limited access to handle system).

Create individual accounts with multi-factor authentication (MFA) and use encryption to restrict unauthorized access to sensitive data.

TRAIN EMPLOYEES

Train employees on your security processes. Create learning exercises on different security tactics and emphasize the importance of continuous communication. Users handling the ICS should understand why certain security measures are in place so that they don't disable them.

LOG AND MONITOR

Enable logging and monitor all access and event information. If your system malfunctions or an attack occurs, audit logs capture event information (e.g. who had access, what actions were performed, what changes were made).

USE SECURITY SOFTWARE AND HARDWARE

Protect your ICS from malicious intrusions and malware infections by using anti-virus software and firewalls. Scan all removable media before connecting it to your ICS to reduce the risk of hidden malware infecting your system.

Use a VPN to protect transmitted data.

If you have the resources available, implement a unidirectional security gateway to control external cyber threats. This tool is a strong alternative to a firewall and needs to be properly configured by senior IT.

BACK UP SYSTEMS

Back up your systems and data regularly, and preferably offline. You can back up encrypted data online, but you should store it offline. Backups ensure that your systems can be quickly restored if an incident of unplanned outage occurs.

UPDATE AND REPLACE IF POSSIBLE

Update and patch your systems to fix security vulnerabilities and maintain ongoing functionality.

Replace unsupported systems and outdated parts if possible for your organization and your ICS. Because an ICS needs continuous operation, you may not be able to remove a device for firmware updates. If this is the case, your organization should assess and approve its risk tolerance and implement other security measures to enhance the security of the ICS.

LEARN MORE

For more information on ICS security, refer to the National Institute of Standards and Technology *SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security*.

Visit our website at cyber.gc.ca to find our catalogue of cyber security publications, including:

- *ITSAP.00.099 Ransomware: How to Prevent and Recover*
- *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*
- *ITSAP.10.003 Protect Your Organization from Insider Threats*
- *ITSAP.70.011 Virtualizing Your Infrastructure*
- *ITSAP.10.094 Managing and Controlling Administrative Privileges*
- *ITSAP.10.093 Offer Tailored Cyber Security Training to Your Employees*
- *ITSAP.00.057 Protect Your Organization from Malware*
- *ITSAP.40.002 Tips for Backing up Your Information*
- *ITSAP.10.096 How Updates Secure Your Device*

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**