Protect Your Operational Technology

July 2022 ITSAP.00.051

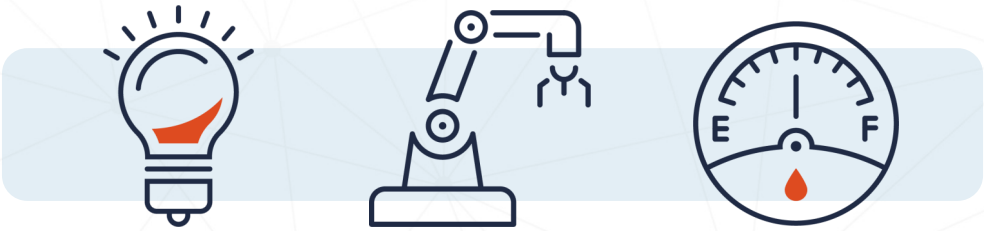
Operational technology (OT) plays an essential role in the management of Canada's critical infrastructure (CI). OT refers to hardware and software used to monitor and cause changes in processes that affect the physical world. This document offers information on the risks to OT and what security measures you can practice to reduce the risks of cyber threats.

How does OT work?

OT is used to control and automate industrial processes in many different sectors (e.g. manufacturing, resource extraction, and essential services). Traditionally, OT consisted of offline systems for industrial process control, but has now adopted data processing and communication protocols from information technology (IT) for safer and more efficient operations. OT systems are becoming more connected to IT networks and potentially the internet, increasing the likelihood of cyber related attacks.

Industrial control systems (ICS) are specialized OT that monitors and controls industrial processes. ICS can sense and change the physical state of industrial equipment to deliver the appropriate product or service.

Cyber-physical systems (CPS) are advanced OT that control and monitor physical systems using computer-based algorithms. CPS integrate computing, networking, and physical process management with CI, creating smart systems to measure and control the physical world to achieve goals.



What are the risks?

OT design prioritizes personal safety and process reliability over data security. Compromised OT systems and devices can put critical processes at risk of failure. Depending on the resources available and the strength of the attack, your OT might shut down and force processes to work in a manual mode (i.e. operating systems without automated processes). Your OT being compromised could risk:

- malfunctioning equipment and disrupting processes and deliverables
- compromising intellectual property and sensitive information (e.g. financial and customer data)
- losing revenue from disrupted processes, costly repairs, or paid ransom
- damaging organizational credibility
- compromising security measures (e.g. emergency services)
- causing major accidents and disasters (e.g. injury or loss of life)

The failure of an OT device could impact an entire industrial process and the safety of operators. Threat actors seek opportunities where they know destruction and loss of services could cause serious damage to high value systems, processes, and infrastructure.

AWARENESS SERIES

Cat. No. D97-1/00-051-2022E-PDF
ISBN 978-0-660-44026-2

What are the threats?

Cyber security threats to OT can impact Canada's CI and other important processes. Some of the main threats to OT include:

- **Remote access:** if your OT is connected to an IT network or the internet, cyber criminals can use different attack methods and take control of your OT remotely.
- **Ransomware:** a type of malware that denies a user's access to a system or data until a sum of money is paid.
- **Malware:** malicious software designed to infiltrate or damage a computer system, without the owner's consent.
- **Insider threat:** anyone who has knowledge of or access to your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm.
- **Denial of service (DoS) attacks:** activities that make services unavailable for use by legitimate users, or delay system operations and functions.

These threats can offer cyber criminals access to manipulate data in systems (e.g. change calculations or how information is displayed), presenting false information or affecting connected systems.

Some vulnerabilities to consider under your organization's control are:

- **End-of-life and out-dated systems:** devices that are no longer supported with updates.
- **Unpatched software and firmware:** leaves systems and devices vulnerable to known threats.
- **Peripherals:** external connected devices that can be used to compromise systems and networks.

Alongside these threats, cyber criminals are continuing to improve and advance their attack methods.

How to protect my OT?

Protect your OT with the following cyber security best practices:

Testing manual mode:
Test your systems and processes in manual mode. Have an incident response plan in place to ensure your systems can run to their best ability if certain OT have to be disconnected from the internet. Be prepared under imminent threat to isolate OT components and services from the internet.

Monitoring and logging:
Monitor systems and equipment using audit logs to track vulnerabilities and access points for attacks. Monitored entry points will allow you to target and isolate attacks from spreading.

Updating and patching:
Use a risk-based approach to determine what OT can and should be updated. Assessing your OT is critical to ensure updates do not affect connected systems which can impact the reliability of your OT and systems.

Isolating system processes:
Use firewalls, virtual private networks (VPN), and multi-factor authentication (MFA) on systems connected to your OT, including remote work access. Use network zoning to separate areas with sensitive OT from remote access networks to offer isolation.

Implementing the principle of least privilege:
Ensure only individuals who need access to OT are allowed. Use MFA and two-person integrity (TPI) on OT that handles sensitive equipment or information. TPI requires two authorized individuals to unlock access to restricted systems.

What if my OT becomes compromised?

If your OT and connected systems are compromised by threat actors, consider the following steps:

1. Evaluate the impact on equipment and disconnect from the internet, where necessary, to contain the spread of the attack.
2. Use your audit logs to target the attack and any connected systems and accounts that could be affected.
3. Keep impacted accounts, OT, and systems disconnected or isolated from the processes that are under control, if possible.
4. Have your IT team repair the damaged equipment and scan for lingering threats.
5. Update and patch the impacted OT with the appropriate software version to function accordingly.
6. Report the incident to the Cyber Centre and the Royal Canadian Mounted Police (RCMP) depending on the nature of the incident and its severity.

Learn more

Visit the Cyber Centre website to find related publications, including:

- *Security considerations for industrial control systems (ITSAP.00.050)*
- *Security considerations for critical infrastructure (ITSAP.10.100)*
- *Ransomware: How to prevent and recover (ITSAP.00.099)*
- *How to protect your organization from insider threats (ITSAP.10.003)*
- *Protecting your organization against denial of service attacks (ITSAP.80.100)*
- *Protect your organization from malware (ITSAP.00.057)*
- *Managing and controlling administrative privileges (ITSM.10.094)*
- *Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)*
- *Baseline security requirements for network security zoning (version 2.0) (ITSP.80.022)*
- *Preventative security tools (ITSAP.00.058)*