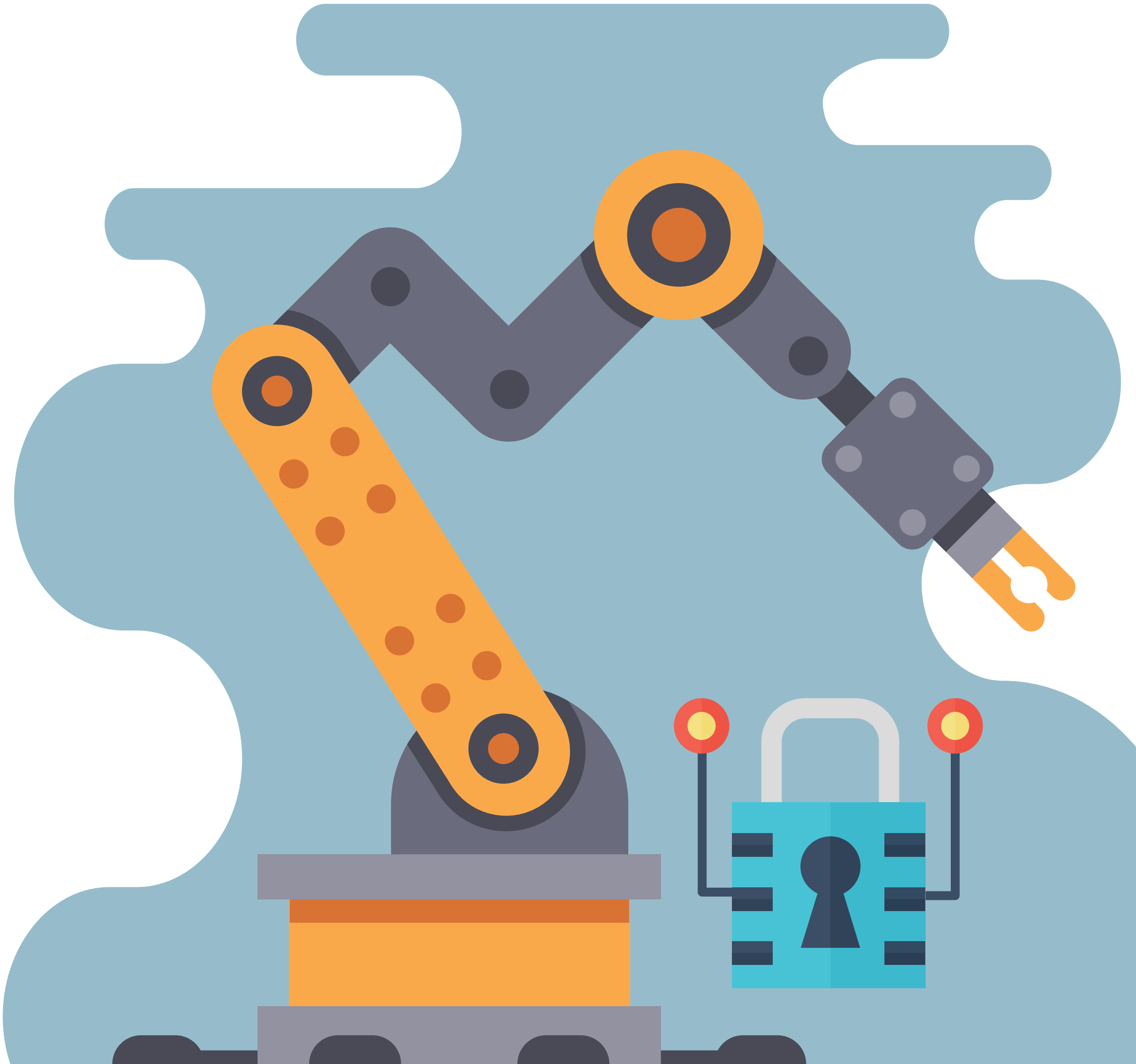
An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NCSC

NATIONAL CYBER SECURITY CENTRE

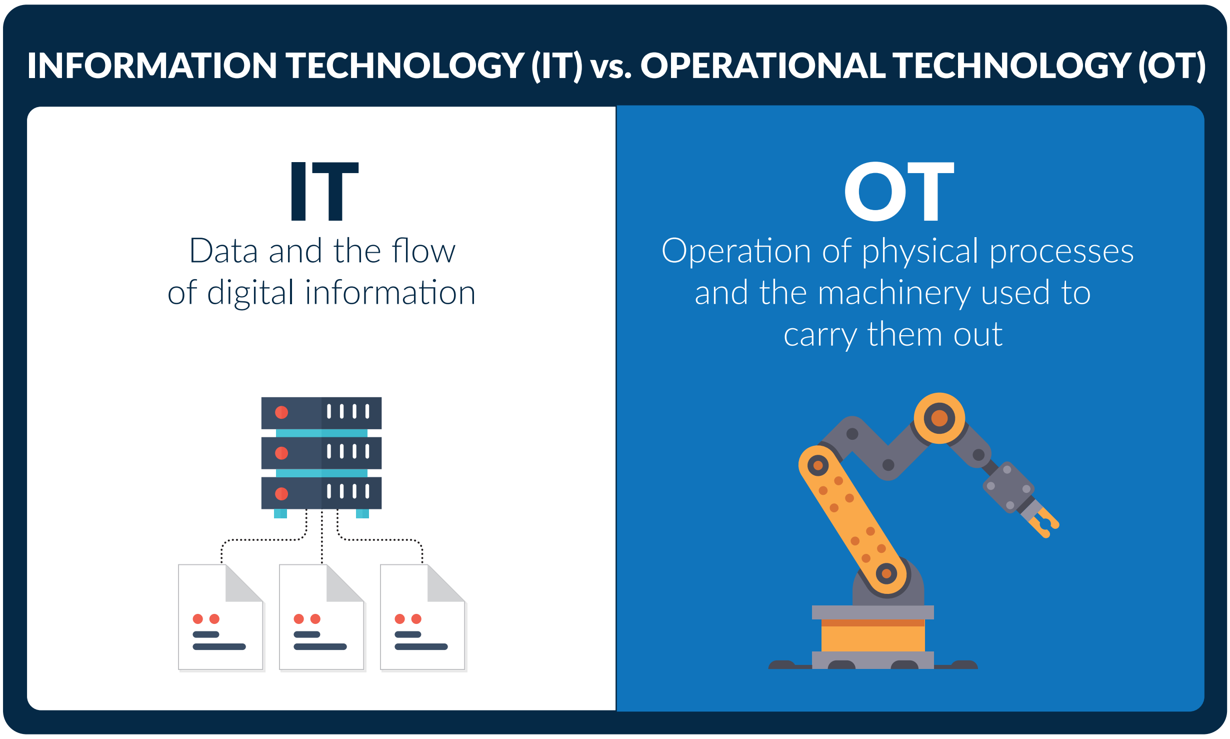
Securing Operational Technology



What is Operational Technology?

Operational Technology (OT) includes Industrial Control Systems (ICS) which includes Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) Systems.

While Information Technology (IT) deals with information, OT generally deals with machines and interacts with the physical world. IT manages the flow of digital information, such as data, while OT manages the operation of physical processes and the machinery used to carry them out.



INFORMATION TECHNOLOGY (IT) vs. OPERATIONAL TECHNOLOGY (OT)

IT

Data and the flow of digital information

OT

Operation of physical processes and the machinery used to carry them out

OT is Used to Monitor and Control Processes in:

- Electricity
- Drinking water and waste
- Oil and gas
- Transportation
- Chemical
- Pharmaceutical
- Pulp and paper
- Food and beverage
- Manufacturing industries

Given these services are vital for the functioning of our society and economy, protecting OT systems from malicious cyber activity is crucial to ensuring the safe and reliable delivery of these services.

What Are the Risks?

Attacks on industrial systems are increasing in frequency and sophistication. Not only is there intersection with threats and attack vectors aimed at IT assets, but there exists a growing number of threat actors specialising in the targeting of OT environments, including with **specialised OT malware variants** aimed at attacking industrial systems specifically. Examples of industrial system specific malware variants discovered include: Stuxnet, Havex, Black Energy 2, Industroyer/CrashOverride, HatMan/Triton/Trisys, Industroyer 2, and Pipedream/Incontroller. The latter two variants having been disclosed in April 2022 alone.[1,2] These OT specific malware variants can allow attackers to compromise, and control affected devices which could lead to serious disruption to critical services.

An additional risk stems from the increasing **convergence of IT and OT environments**. OT systems evolved first in an environment where they were “air gapped” and not connected to outside IT systems, however as part of business transformation IT systems are increasingly being connected to OT systems, allowing them to transmit data to each other. Whilst this brings with it certain business efficiencies and innovation, it can increase cybersecurity risks, exposing traditionally separated OT systems to the less secure business environment or the Internet.

Finally, much like traditional IT systems, OT systems can be severely impacted by malicious software such as **ransomware**. Even in cases where the OT system has not been infected with malware, the knock-on impacts can result in OT networks being shut down due to safety concerns over the ability to safely operate and monitor OT networks. In May 2021 in the operator of the largest fuel pipeline in the United States, Colonial Pipeline halted its pipeline operations to contain the ransomware attack to its IT operations and ensure the safety of the public. The resulting shutdown caused gas shortages and panic-buying by the public having a national level economic impact.

There are also significant challenges to OT **vulnerability & patch management** as it may be difficult to implement an automatic update routine for older OT systems, vulnerability scanning tools may impact devices, and often Original Equipment Manufacturer (OEM) patch approval may be required. As a result, the patching cycle for OT is often much longer than IT networks, leaving devices & software vulnerable for extended periods.

Given these significant risks to the security of Operational Technology, the NCSC recommend taking the following actions to protect these systems and devices.

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

[2] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Actions to Take

1 Take Risk-Based Approach ☑

a **Prioritise critical systems** by identifying your:

- Core products and services.
- Critical technical & business activities required to deliver these products and services.
- Network and information systems which underpin these activities.

2 Know Your Infrastructure ☑

a **Create and maintain an accurate asset inventory.** This should include both the hardware type and software versions. This will be a helpful reference during normal operation as well as during a potential cybersecurity incident.

b **Maintain an up-to-date network configuration diagram.** This should provide context for maintenance, system changes, or response/recovery in the event of an attack and include:

- Connections between separate OT networks and to the IT/Corporate network.
- All external connections, to the Internet or to Vendors or support partners, including private network connections. Ensure this includes secondary, dual path, backup and support or vendor connections. Not just those connections directly under the organisation's full control. Ensure, unused or disabled connections which cannot be removed are recorded and the status included (this could include various Wi-Fi adapters on equipment such as 802.11 x, Bluetooth, Bisbee, etc).

c **Use a passive scanning tool to listen to network traffic and fingerprint devices as they are found.** It is useful for creating a basic asset inventory, baseline normal network traffic patterns and map networks.

d **Know and understand all the critical elements of your system.** Involve all parts of your business information technology teams, cyber security engineers, process operators, process control specialists and functional safety engineers and other relevant stakeholders.

e **Protect documentation:** Store this sensitive information in a secure encrypted location and limit access to it. Access to key documentation should be on a need-to-know basis. Copies should be stored offline and available in the event of your system being encrypted by ransomware.

3	Segment & Isolate ☑
a	**Segment your OT network and isolate it from your corporate network using strong perimeter controls.** Assume your Corporate network, or any external network, is compromised and act accordingly.
b	**Have a secure de-militarised zone (DMZ)** between your OT network and Corporate network.
c	**Segment your OT Network,** divide your network into zones organised by groups of systems that have similar operational function and risk profile. Consider necessary traffic flows between end points, considering the protocol types within your OT network and implement segmentation accordingly.
d	**Create boundaries between zones** – Communication in and out of the zone is denied unless explicitly permitted using firewalls or access control lists. If one device, e.g., a HMI, gets compromised by ransomware, it can only affect other devices within the same zone that it is specifically allowed to communicate with.
e	**Have the highest level of trust in your Safety Zone,** followed by the OT zone and then the IT/Corporate zone.
f	Consider hardwired I/O between critical skid systems and DCS I/O.
g	The Purdue model is a helpful reference model.

4	Control Access to the Network ☑
a	**Use Multi-Factor Authentication (MFA)** – this is essential for all Remote Access and Admin Access.
b	**Use a Virtual Private Network (VPN) gateway** for remote access to the OT network, followed by a bastion host/jump box to constrain user activity to agreed policies.
c	**Apply the principle of least privilege** – only grant access to specific information/rights required to perform the role.
d	**Implement a privileged account management policy** – use a separate account for administering the OT network. Don't share passwords or other credentials between separate accounts. Never use privileged account for standard operations, browsing the Internet or reading emails.
e	**Remove/change/disable default accounts.**
f	**Review access rights regularly.**
g	**"Sheep-dip"[3] USB devices.**
h	**Enforce separation of duties** between systems wherever feasible.

[3] https://www.techopedia.com/definition/4102/sheepdip

5	Network & System Hardening	✓
a	**Turn off non-essential services,** consider application whitelisting on OT HMIs and workstations.	
b	**Limit device functionality** to strictly necessary services and software	
c	Physically and logically disable ports.	
d	**Implement firewall rules** which deny everything except for agreed critical network services.	
e	**Separate OT network from your IT/Enterprise network.**	
f	**Restrict access to the Internet or email.**	
g	**Push sensor data from higher trust zones to lower trust zones (from OT to IT).** Conduct operations such as data analytics in the low trust zone.	
h	**Apply AV** to all ICS devices that are capable of running such software	
6	Change Control & Configuration Management	✓
a	**Have a good process** to track, document, approve, test and deploy changes.	
b	**Combine change management with controls to detect changes which will be more effective** i.e., activity will be tracked against authorised configuration changes.	
c	**Update changes in support** documentation such as asset management or network configuration.	
7	Vulnerability & Patch Management	✓
a	**Know what vulnerabilities** are present on your network by comparing your asset register with known vulnerability registers. Consider signing up for an OT specific vulnerability alerting service.	
b	**Remove all unnecessary applications and software from your OT systems** – if they are present, you will have to patch them.	
c	**Engage with your original equipment manufacturer (OEM)** to ensure you get all relevant patches; find out if they have robust Supplier Bill of Materials (SBOM) and an active vulnerability program; and review all patch notes to capture all patches that have security related content relevant to your systems.	
d	**Have reliable backups** before commencing the patch process.	
e	**Confirm HASH values** of patches prior to deployment.	
f	**Test** on a set of devices after deployment to ensure all key processes are working correctly.	
g	**Use scheduled outage windows** to conduct vulnerability scans and patch hardware/software.	

8	Log Management & Analysis ☑
a	**Collect relevant security events and logs** from the multiple devices and systems used on your network particularly for systems on the edge of zones and to communicate with lower trust systems. If possible use IDS/IPS to monitor traffic.
b	**Aggregate and analyse logs** to provide evidence about the cybersecurity state and operation of your OT network which is a key objective is to detect malicious code and traffic.
c	**Collect and analyse domain name requests and attempted connections** to Internet systems from OT environments to detect malicious activity.
d	Tools such as the NCSC UK **Logging Made Easy** may assist in log collections. However larger operators should have a dedicated Security Operations Centre (SOC).
e	**Focus on monitoring:** ● North-South (ingress/egress and) and East-West OT Networks communications, for OT protocol aware technologies and safety systems. ● Look out for non-standard workstations or accounts, PLC modifications occurring outside usual maintenance window, and new connections or devices.

9	Prepare for an Incident – Respond and Recover ☑
a	**Have an effective Incident Response (IR) plan** to implement in the event of a cybersecurity incident.
b	**Review & test** your BCP/DR/Incident Response plans regularly using realistic OT scenarios. Test your plans regularly.
c	**Ensure the IR plan is OT focused** with the appropriate SOPs for operating with an affected control system.
d	**Have processes to regularly Backup critical data** e.g., the ladder logic and controller config files. This is particularly important before patching or configuration changes.
e	**Follow the 3-2-1 rule** – 3 copies of the data, using 2 different systems, 1 offline.
f	**Perform test restores** ensuring that you can recover from backup.

10	Supply Chain Risk ☑
a	**Apply the zero trust principle** i.e., only allow users onto your network for a specific activity for a specific time. Consider using one-time-passwords. Consider using endpoint inspection to verify endpoint security before granting access.
b	**Set minimum security standards for your suppliers** ensuring their access does not reduce overall network security.
c	**Review your contracts and ensure there are appropriate security clauses in place. For example:** ● Right to audit. ● Obligation on supplier to notify you if they suffer a cybersecurity incident. ● Obligation on supplier to comply with your security and change control requirements. ● Obligation on supplier to disclose their vulnerability handling policy.
d	**Implement security measures on third party access,** including for support partners and vendors, to maintain both control of the access and visibility of activities on your network.

11	Human Element ☑
a	**Train** your OT Operators, Engineers and Security Personnel to be aware of security lapses and indicators of potential compromise, and to understand their roles in incident reporting, response and recovery.
b	**Have Policies & Procedures** which outline OT security roles, acceptable use and expected controls. Make sure people are aware of these policies & procedures.
c	**Promote a culture of information sharing and dialogue** between OT & IT Security personnel, to ensure best practice is applied.

12	Continuous Improvement ☑
a	**Critically assess your cybersecurity posture on a regular basis** taking account changes in the threat landscape and relevant sectoral incidents.
b	**Identify gaps** in your security posture.
c	**Risk rate and prioritise identified gaps** to be addressed.
d	**Regularly Review** and update, if necessary, your security policies, procedures and controls

Further Reading

- NCSC site – where you will find Alerts, Advisories and Guidance documentation: https://www.ncsc.gov.ie/
- NCSC UK:
  Design Principles and Operational Technologies
- NIST Cybersecurity Framework, Critical Infrastructure Resource
- NIST Guide for Cybersecurity Event Recovery
- CISA-ICS Advisories
- CISA-ICS Alerts
- NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
- IEC 62443
- SANS paper on the Dragonfly attack
- ENISA Reports Publications
- Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)

Glossary

AV	Anti-virus
BCP	Business Continuity Plan
DCS	Distributed Control System
DMZ	De-Militarised Zone
DR	Disaster Recovery
HMI	Human Machine Interface
ICS	Industrial Control system
IR	Incident Response
IT	Information Technology
MFA	Multi-Factor Authentication
OEM	Original Equipment Manufacturer
OT	Operational Technology
PLC	Programmable Logic Controller
SBOM	Supplier Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operation Centre
SOP	Standard Operating Procedures
VPN	Virtual Private Network