Control System Defense: Know the Opponent

Summary

Operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors. These cyber actors, including advanced persistent threat (APT) groups, target OT/ICS assets to achieve political gains, economic advantages, or destructive effects. Because OT/ICS systems manage physical operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of National Critical Functions.

OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks.

Traditional approaches to securing OT/ICS do not adequately address current threats.

Traditional approaches to securing OT/ICS do not adequately address current threats to those systems. However, owners and operators who understand cyber actors' tactics, techniques, and procedures (TTPs) can use that knowledge when prioritizing hardening actions for OT/ICS.

This joint Cybersecurity Advisory, which builds on previous NSA and CISA guidance to stop malicious ICS activity and reduce OT exposure [1] [2], describes TTPs that malicious actors use to compromise OT/ICS assets. It also recommends mitigations that owners and operators can use to defend their systems. NSA and CISA encourage OT/ICS owners and operators to apply the recommendations in this CSA.

Technical Details

OT/ICS assets operate, control, and monitor industrial processes throughout U.S. critical infrastructure. Traditional ICS assets are difficult to secure due to their design for maximum availability and safety, coupled with their use of decades-old systems that often lack any recent security updates. Newer ICS assets may be able to be configured more securely, but often have an increased attack surface due to incorporating Internet or IT network connectivity to facilitate remote control and operations. The net effect of the convergence of IT and OT platforms has increased the risk of cyber exploitation of control systems. [3]

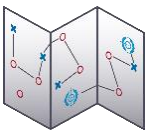
Today's cyber realm is filled with well-funded malicious cyber actors financed by nation-states, as well as less sophisticated groups, independent hackers, and insider threats. Control systems have been targeted by a variety of these malicious cyber actors in recent years to achieve political gains, economic advantages, and possibly destructive effects. [4] [5] [6] [7] [8] More recently, APT actors have also developed tools for scanning, compromising, and controlling targeted OT devices. [9]

Malicious actors' game plan for control system intrusions

Cyber actors typically follow these steps to plan and execute compromises against critical infrastructure control systems:

1. Establish intended effect and select a target.
2. Collect intelligence about the target system.
3. Develop techniques and tools to navigate and manipulate the system.
4. Gain initial access to the system.
5. Execute techniques and tools to create the intended effect.

Leveraging specific expertise and network knowledge, malicious actors—especially state-sponsored ones—can conduct these steps in a coordinated manner, sometimes concurrently and repeatedly, as illustrated by real world cyber activity. [5] [10]



Establish intended effect and select a target

Cyber actors, from cyber criminals to state-sponsored APT actors, target critical infrastructure to achieve a variety of objectives. Cyber criminals are financially motivated and target OT/ICS assets for financial gain (e.g., data extortion or ransomware operations). State-sponsored APT actors target critical infrastructure for

political and/or military objectives, such as destabilizing political or economic landscapes or causing psychological or social impacts on a population. The cyber actor selects the target and intended effect—to disrupt, disable, deny, deceive, and/or destroy—based on these objectives. For example, disabling power grids in strategic locations could destabilize economic landscapes or support broader military campaigns. Disrupting water treatment facilities or threatening to destroy a dam could have psychological or social impacts on a population. [11] [12]

Collect intelligence about the target system

Once the intent and target are established, the actor collects intelligence on the targeted control system. The actor may collect data from multiple sources, including:

- **Open-source research:** A great deal of information about control systems and their designs is publicly available. For example, solicitation information and employment advertisements may indicate components, and list specific model numbers.
- **Insider threats:** The actor may also leverage trusted insiders, even unwitting ones, for collecting information. Social engineering often elicits a wealth of information from people looking for a new job or even just trying to help.
- **Enterprise networks:** The actor may compromise enterprise IT networks and collect and exfiltrate ICS-related information. Procurement documents, engineering specifications, and even configurations may be stored on corporate IT networks.

In addition to OT-specific intelligence, information about IT technologies used in control systems is widely available. Knowledge that was once limited to control system engineers and OT operators has become easily available as IT technologies move into more of the control system environment. Control system vendors, in conjunction with the owner/operator community, have continually optimized and reduced the cost of engineering, operating, and maintaining control systems by incorporating more commodity IT components and technologies in some parts of OT environments. These advancements can make more information about some systems easily available, thereby increasing the risk of cyber exploitation.

Develop techniques and tools

Using the intelligence collected about the control system's design, a cyber actor may procure systems that are similar to the target and configure them as mock-up versions for practice purposes. Nation-state actors can easily obtain most control system equipment. Groups with limited means can still often acquire control systems through willing vendors and secondhand resellers.

Access to a mock-up of the target system enables an actor to determine the most effective tools and techniques. A cyber actor can leverage resident system utilities, available exploitation tools, or, if necessary, develop or purchase custom tools to affect the control system. Utilities that are already on the system can be used to reconfigure settings and may have powerful troubleshooting capabilities.

As the control system community has incorporated commodity IT and modernized OT, the community has simplified the tools, techniques, scripts, and software packages used in control systems. As a result, a multitude of convenient tools are readily available to exploit IT and OT systems.

A multitude of tools is readily available to exploit IT and OT systems.

Actors may also develop custom ICS-focused malware based on their knowledge of the control systems. For example, TRITON malware was designed to target certain versions of Triconex Tricon programmable logic controllers (PLCs) by modifying in-memory firmware to add additional programming. The extra functionality allows an actor to read/modify memory contents and execute custom code, disabling the safety system. [13] APT actors have also developed tools to scan for, compromise, and control certain Schneider Electric PLCs, OMRON Sysmac NEX PLCs, and Open Platform Communications Unified Architecture (OPC UA) servers. [9]

With TTPs in place, a cyber actor is prepared to do virtually anything that a normal system operator can, and potentially much more.

Gain initial access to the system

To leverage the techniques and tools that they developed and practiced, cyber actors must first gain access to the targeted system. Most modern control

systems maintain remote access capabilities allowing vendors, integrators, service providers, owners, and operators access to the system. Remote access enables these parties to perform remote monitoring services, diagnose problems remotely, and verify warranty agreements.

However, these access points often have poor security practices, such as using default and maintenance passwords. Malicious cyber actors can leverage these access points as vectors to covertly gain access to the system, exfiltrate data, and launch other cyber activities before an operator realizes there is a problem. Malicious actors can use web-based search platforms, such as Shodan, to identify these exposed access points.

Vendor access to control systems typically uses connections that create a bridge between control system networks and external environments. Often unknown to the owner/operator, this bridge provides yet another path for cyber exploitation and allows cyber actors to take advantage of vulnerabilities in other infrastructure to gain access to the control system.

Remote access points and methodologies use a variety of access and communication protocols. Many are nothing more than vendor-provided dial-up modems and network switches protected only by obscurity and passwords. Some are dedicated devices and services that communicate via more secure virtual private networks (VPNs) and encryption. Few, if any, offer robust cybersecurity capabilities to protect the control system access points or prevent the transmission of acquired data outside the relatively secure environment of the isolated control system. This access to an ostensibly closed control system can be used to exploit the network and components.

Execute techniques and tools to create the intended effects

Once an actor gains initial access to targeted OT/ICS system, the actor will execute techniques, tools, and malware to achieve the intended effects on the target system. To disrupt, disable, deny, deceive, and/or destroy the system, the malicious actor often performs, in any order or in combination, the following activities:

1. Degrade the operator's ability to monitor the targeted system or degrade the operator’s confidence in the control system’s ability to operate, control, and monitor the targeted system. Functionally, an actor could prevent the operator's display (human machine interface, or HMI) from being updated and selectively

update or change visualizations on the HMI, as witnessed during the attack on the Ukraine power grid. [5] (Manipulation of View [T0832][1])

2. Operate the targeted control system. Functionally, this includes the ability to modify analog and digital values internal to the system (changing alarms and adding or modifying user accounts), or to change output control points — this includes abilities such as altering tap changer output signals, turbine speed demand, and opening and closing breakers. (Manipulation of Control [T0831])
3. Impair the system's ability to report data. Functionally, this is accomplished by degrading or disrupting communications with external communications circuits (e.g., ICCP[2], HDLC[3], PLC[4], VSAT, SCADA radio, other radio frequency mediums), remote terminal units (RTUs) or programmable logic controllers (PLCs), connected business or corporate networks, HMI subnetworks, other remote I/O, and any connected Historian/bulk data storage. (Block Reporting Message [T0804], Denial of View [T0815])
4. Deny the operator's ability to control the targeted system. Functionally, this includes the ability to stop, abort, or corrupt the system's operating system (OS) or the supervisory control and data acquisition (SCADA) system's software functionality. (Denial of Control [T0813])
5. Enable remote or local reconnaissance on the control system. Functionally, an actor could obtain system configuration information to enable development of a modified system configuration or a custom tool. (Collection [TA0100], Theft of Operational Information [T0882])

Using these techniques, cyber actors could cause various physical consequences. They could open or close breakers, throttle valves, overfill tanks, set turbines to over-speed, or place plants in unsafe operating conditions. Additionally, cyber actors could manipulate the control environment, obscuring operator awareness and obstructing recovery, by locking interfaces and setting monitors to show normal conditions. Actors can even suspend alarm functionality, allowing the system to operate under unsafe conditions without alerting the operator. Even when physical safety systems should prevent catastrophic physical consequences, more limited effects are possible and

[1] T-codes correspond to the MITRE ATT&CK framework.
[2] ICCP – Inter-Control Center Communications Protocol
[3] HDLC – High-Level Data Link Control Protocol
[4] PLC – Power Line Carrier

could be sufficient to meet the actor's intent. In some scenarios though, if an actor simultaneously manipulates multiple parts of the system, the physical safety systems may not be enough. Impacts to the system could be temporary or permanent, potentially even including physical destruction of equipment.

Mitigations

The complexity of balancing network security with performance, features, ease-of-use, and availability can be overwhelming for owner/operators. This is especially true where system tools and scripts enable ease-of-use and increase availability or functionality of the control network; or when equipment vendors require remote access for warranty compliance, service obligations, and financial/billing functionality. However, with the increase in targeting of OT/ICS by malicious actors, owner/operators should be more cognizant of the risks when making these balancing decisions. Owner/operators should carefully consider what information about their systems needs to be publicly available and determine if each external connection is truly needed. [1]

System owners and operators cannot prevent a malicious actor from targeting their systems. Understanding that being targeted is not an "if" but a "when" is essential context for making ICS security decisions. By assuming that the system is being targeted and predicting the effects that a malicious actor would intend to cause, owner/operators can prioritize and employ mitigation actions.

However, the variety of available security solutions can also be intimidating, resulting in choice paralysis. In the midst of so many options, owner/operators may be unable to incorporate simple security and administrative strategies that could mitigate many of the common and realistic threats. Fortunately, owner/operators can apply a few straightforward ICS security best practices to counter adversary TTPs.

Limit exposure of system information

Operational and system information and configuration data is a key element of critical infrastructure operations. The importance of keeping such data confidential cannot be overstated. To the extent possible, avoid disclosing information about system hardware, firmware, and software in any public forum. Incorporate information protection education into training for personnel. Limit information that is sent out from the system.

Document the answers to the following questions:

1. From where and to where is data flowing?
2. How are the communication pathways documented and how is the data secured/encrypted?
3. How is the data used and secured when it arrives at its destination?
4. What are the network security standards at the data destination, whether a vendor/regulator or administrator/financial institution?
5. Can the data be shared further once at its destination? Who has the authority to share this data?

Eliminate all other data destinations. Share only the data necessary to comply with applicable legal requirements, such as those contractually required by vendors—nothing more. Do not allow other uses of the data and other accesses to the system without strict administrative policies designed specifically to protect the data. Prevent new connections to the control system using strict administrative accountability. Ensure strict agreements are in place with outside systems/vendors when it comes to sharing, access, and use. Have strong policies for the destruction of such data. Audit policies and procedures to verify compliance and secure the data once it gets to its destination, and determine who actually has access to it.

Identify and secure remote access points

Owner/operators must maintain detailed knowledge of all installed systems, including which remote access points are—or could be—operating in the control system network. Creating a full "connectivity inventory" is a critical step in securing access to the system.

Many vendor-provided devices maintain these access capabilities as an auxiliary function and may have services that will automatically 'phone home' in an attempt to register and update software or firmware. A vendor may also have multiple access points to cover different tasks.

Once owner/operators have identified all remote access points on their systems, they can implement the following recommendations to improve their security posture:

- Reduce the attack surface by proactively limiting and hardening Internet-exposed assets. See CISA's Get Your Stuff Off Search page for more information.

- Establish a firewall and a demilitarized zone (DMZ) between the control system and the vendor's access points and devices. Do not allow direct access into the system; use an intermediary service to share only necessary data and only when required. For more information see CISA's infographic Layering Network Security Through Segmentation. [14]
- Consider using virtual private networks (VPNs) at specific points to and from the system rather than allowing separate access points for individual devices or vendors.
- Utilize jump boxes to isolate and monitor access to the system.
- Ensure that data can only flow outward from the system – administratively and physically. Use encrypted links to exchange data outside of the system.
- Enforce strict compliance with policies and procedures for remote access, even if personnel complain that it is too difficult.
- If the system does not use vendor access points and devices, ensure that none are active. Use strict hardware, software, and administrative techniques to prevent them from becoming covertly active.
- Do not allow vendor-provided system access devices and software to operate continuously in the system without full awareness of their security posture and access logs.
- Install and keep current all vendor-provided security systems associated with the installed vendor access points.
- Review configurations to ensure they are configured securely. Operators typically focus on necessary functionality, so properly securing the configurations and remote access may be overlooked.
- Consider penetration testing to validate the system's security posture and any unknown accesses or access vulnerabilities.
- Add additional security features to the system as needed. Do not assume that one vendor has a monopoly on the security of their equipment; other vendors may produce security features to fill gaps.

- Change all default passwords throughout the system and update any products with hard-coded passwords, especially in all remote access and security components.
- Patch known exploited vulnerabilities whenever possible. Prioritize timely patching of all remote access points. Keep operating systems, firewalls, and all security features up-to-date.
- Continually monitor remote access logs for suspicious accesses. Securely aggregate logs for easier monitoring.

Restrict tools and scripts

Limit access to network and control system application tools and scripts to legitimate users performing legitimate tasks on the control system. Removing the tools and scripts entirely and patching embedded control system components for exploitable vulnerabilities is often not feasible. Thus, carefully apply access and use limitations to particularly vulnerable processes and components to limit the threat.

The control system and any accompanying vendor access points may have been delivered with engineering, configuration, and diagnostic tools pre-installed. Engineers use these tools to configure and modify the system and its processes as needed. However, such tools can also be used by a malicious actor to manipulate the system, without needing any special additional tools. Using the system against itself is a powerful cyber exploitation technique. Mitigations strategies include:

1. Identify any engineering, configuration, or diagnostic tools.
2. Securely store gold copies of these tools external to the system if possible.
3. Remove all non-critical tools.
4. Prevent these tools from being reinstalled.
5. Perform routine audits to check that these tools have not been reinstalled.

Conduct regular security audits

The owner/operator of the control system should consider performing an independent security audit of the system, especially of third-party vendor access points and systems. The owner/operator cannot solely depend on the views, options, and guidance of the vendor/integrator that designed, developed, or sold the system. The goal of such an

audit is to identify and document system vulnerabilities, practices, and procedures that should be eliminated to improve the cyber defensive posture, and ultimately prevent malicious cyber actors from being able to cause their intended effects. Steps to consider during an audit include the following:

1. Validate all connections (e.g., network, serial, modem, wireless, etc.).
2. Review system software patching procedures.
3. Confirm secure storage of gold copies (e.g., OS, firmware, patches, configurations, etc.).
4. Verify removal from the system of all non-critical software, services, and tools.
5. Audit the full asset inventory.
6. Implement CISA ICS mitigations and best practices. [15] [16]
7. Monitor system logs and intrusion detection system (IDS) logs.

Monitoring of access logs, system changes, IDS logs, and other tracking data should be performed continuously, with a deeper look at this data during periodic audits.

Implement a dynamic network environment

Static network environments provide malicious actors with persistent knowledge of the system. A static network can provide cyber actors the opportunity to collect bits of intelligence about the system over time, establish long-term accesses into the system, and develop the tools and TTPs to affect the control system as intended.

While it may be unrealistic for the administrators of many OT/ICS environments to make regular non-critical changes, owner/operators should consider periodically making manageable network changes. A little change can go a long way to disrupt previously obtained access by a malicious actor. Consider the following:

1. Deploy additional firewalls and routers from different vendors.
2. Modify IP address pools.
3. Replace outdated hardware (e.g., workstations, servers, printers, etc.).
4. Upgrade operating systems.
5. Install or upgrade commercially available security packages for vendor access points and methodologies.

Planning these changes with significant forethought can help minimize the impact on network operation.

Owner/operators should familiarize themselves with the risks to the system as outlined by the product vendor. These may be described in manuals as the system using insecure protocols for interoperability or certain configurations that may expose the system in additional ways. Changes to the system to reduce these risks should be considered and implemented when feasible.

Conclusion

The combination of integrated, simplified tools and remote accesses creates an environment ripe for malicious actors to target control systems networks. New IT-enabled accesses provide cyber actors with a larger attack surface into cyber-physical environments. It is vital for OT/ICS defenders to anticipate the TTPs of cyber actors combining IT expertise with engineering know-how. Defenders can employ the mitigations listed in this advisory to limit unauthorized access, lock down tools and data flows, and deny malicious actors from achieving their desired effects.▪

Works cited

[1] National Security Agency (2021), Stop Malicious Cyber Activity Against Connected Operational Technology. https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/0/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF

[2] National Security Agency and Cybersecurity and Infrastructure Security Agency (2020), NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems. https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF

[3] Tenable (2018), The Challenges of Securing Industrial Control Systems from Cyberattacks. https://www.tenable.com/blog/the-challenges-of-securing-industrial-control-systems-from-cyberattacks

[4] Cybersecurity and Infrastructure Security Agency (2022), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[5] Cybersecurity and Infrastructure Security Agency (2021), Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

[6] Cybersecurity and Infrastructure Security Agency (2021), Ongoing Cyber Threats to U.S. Water and Wastewater Systems. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

[7] Cybersecurity and Infrastructure Security Agency (2020), Ransomware Impacting Pipeline Operations. https://www.cisa.gov/uscert/ncas/alerts/aa20-049a

[8] Cybersecurity and Infrastructure Security Agency (2021), Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013 https://www.cisa.gov/uscert/ncas/alerts/aa21-201a

[9] Cybersecurity and Infrastructure Security Agency (2022), APT Cyber Tools Targeting ICS/SCADA Devices https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
[10] Cybersecurity and Infrastructure Security Agency (2022), Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
[11] The American Society of Mechanical Engineers (2016), Securing the Power Grid Against Cyber Attack. https://www.asme.org/topics-resources/content/securing-power-grid-against-cyber-attack
[12] PBS FRONTLINE (2003), Vulnerability: the power grid? https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/grid.html
[13] Cybersecurity and Infrastructure Security Agency (2018), Schneider Electric Triconex Tricon (Update B). https://www.cisa.gov/uscert/ics/advisories/ICSA-18-107-02
[14] Cybersecurity and Infrastructure Security Agency (2022), Layering Network Security Through Segmentation. https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf
[15] Cybersecurity and Infrastructure Security Agency, Recommended Cybersecurity Practices for Industrial Control Systems. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf
[16] Cybersecurity and Infrastructure Security Agency Industrial Control Systems Cyber Emergency Response Team (2016), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This advisory was developed by NSA and CISA in furtherance of their cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact Information

For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov. To report incidents and anomalous activity or to request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.gov.

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov