National Security Agency | Cybersecurity Advisory

Stop Malicious Cyber Activity Against Connected Operational Technology

Executive summary

A significant shift in how operational technologies (OT) are viewed, evaluated, and secured within the U.S. is needed to prevent malicious cyber actors (MCA) from executing successful, and potentially damaging, cyber effects. As OT components continue being connected to information technology (IT), IT exploitation increasingly can serve as a pivot to OT destructive effects[1, 2, 3]. Recent adversarial exploitation of IT management software and its supply chain has resulted in publicly documented impacts across the U.S. Government (USG) and the Defense Industrial Base (DIB). Malicious cyber activities directed at OT also continue to threaten these networks[4, 5, 6].

This paradigm shift applies to the stagnant OT assets and control systems installed and used throughout the USG and DIB, many of which are past end-of-life and operated without sufficient resources. To evaluate and improve the cybersecurity of connected OT and control systems, NSA recommends that National Security System (NSS), Department of Defense (DoD), and DIB network owners perform a detailed risk analysis prior to creating cross-domain connections (e.g., IT-to-OT, Internet-to-OT) and for all currently connected OT.

Following the steps below will enable OT owners and administrators to evaluate risks against their systems and use that knowledge to guide network changes with current resources to realistically monitor and detect malicious activity. Without direct action to harden OT networks and control systems against vulnerabilities introduced through IT and business network intrusions, OT system owners and operators will remain at indefensible levels of risk.

Take immediate steps to improve OT cybersecurity

From corporate leadership down to the OT system operators, many are asking “With such limited resources, how can we improve OT and control system cybersecurity and ensure mission success?” To answer this question, NSA created this pragmatic evaluation methodology and basic cybersecurity improvement approach for NSS, DoD, and DIB network owners.

Holistically evaluate the value vs. risk vs. cost for enterprise IT-to-OT connectivity

1. Acknowledge that a standalone, unconnected (“islanded”) OT system is safer from outside threats than one connected to an enterprise IT system(s) with external connectivity (no matter how secure the outside connections are thought to be). An intermittently connected OT system can be a good compromise because it is only at risk when it is connected, which should only be done when required, such as for downloading updates or during times when remote access is required for a finite period of time.
2. Determine the value to the enterprise of connecting the IT system to the OT network and/or control system environments. The value proposition could involve many aspects, including:
    a. Convenience for connectivity and use of process data/information.
    b. Leveraging existing abilities, such as the IT workforce.
    c. Utilizing or combining with IT tools for system monitoring.
    d. Theoretical synergies via IT integration, such as managing updates of OT assets.

3. Determine the risk to the enterprise of connecting the IT system to the OT environment. The risks could involve many aspects, including:
    a. Loss of process control.
    b. Failure of safety systems/equipment to operate as designed.
    c. Loss of revenue from process interruptions or shutdowns.
    d. Loss of human life should safety systems/equipment not operate appropriately.

4. Quantify the increased costs associated with mitigating the additional risks from connecting the existing OT networks and devices to the enterprise IT system. The costs could involve many aspects, including:
    a. Equipment to segment and protect the (typically) flat OT network and infrastructure to reduce risk of a wide-scale compromise.
    b. Renewed product or system licensing costs to download and update OT assets to the latest version. This is critical to mitigate potential vulnerabilities that are commonly known about outdated firmware, software, etc., and is necessary to reduce the risk of exploitation in a connected environment.
    c. Costs of OT systems upgrades if OT assets include devices that are at or approaching end-of-life for product support. This should include not only the cost of the equipment, but any potential loss of revenue or mission availability from the OT equipment change-out and testing.
    d. Additional personnel and resource needs to properly maintain and secure OT assets.

5. Present leadership with findings so they can effectively evaluate the value, risks, and expenses/resources.

Improve cybersecurity for connected enterprise IT-to-OT networks

At a high level, existing resources and freely-available OT tools should be applied to better secure enterprise IT-connected OT systems. Additionally, while not as critical, these same recommendations can be applied to “islanded” and to intermittently connected OT networks and systems to improve cyber resiliency and ensure mission readiness.

1. Fully manage, cryptographically protect (encrypt and authenticate), and apply an allowlist or a dial-back approach[1] to all access vectors. Be sure to log all access attempts. Access vectors could include many aspects, such as:
    a. Vendor or any outsourced OT asset support, including vendor laptops with known and unknown remote monitoring connections.
    b. Remote connectivity for monitoring and/or alarm notification.
    c. Internal access, especially via existing open, unmanaged network, server, or device connections.
    d. While not as risky as remote access, direct physical access can lead to compromises, too.

2. Wherever remote access is permitted, add sensors and monitor all cross-domain connections. It is recommended that all remote access connections be disconnected until such time that active monitoring is in place.

3. Create a known OT network map and device settings baseline, and validate all equipment on the network.
    a. Utilize topographical and physical network mapping and inventorying.
    b. Readily available open-source tools can meet this requirement[2].

4. Create a known OT network communication baseline.
    a. Readily available open-source tools can meet this requirement[2].

5. Assess and prioritize OT network cybersecurity needs to identify required mitigations and define short-, medium-, and long-term cyber-hardening outcomes.
    a. Depending on in-house IT/OT expertise and capabilities, this step may require external OT expertise. However, a “living” cybersecurity improvement plan will identify and prioritize specific OT cybersecurity risks. It will also provide a roadmap for continuously applying mitigations, near-term improvements, and strategies to achieve long-term cybersecurity goals.

6. Create an exemplar “gold copy” baseline to enable all OT networks and devices to be repaired and/or re-instantiated.
    a. Gold copy restoration files and capabilities should be stored in locked, unconnected locations. Do not store gold copy restoration data on-line or on-network.
    b. Practice OT network re-instantiation to ensure success and shorten OT network downtime if an issue or malicious activity occurs.

While there are very real needs for connectivity and automating processes, operational technologies and control systems are inherently at risk when connected to enterprise IT systems. Seriously consider the risk, benefits, and cost before connecting (or continuing to connect) enterprise IT and OT networks. Mindfully prioritize and consider the risks before allowing enterprise IT-to-OT connections. While OT systems rarely require outside connectivity to properly function, they are frequently connected for convenience without proper consideration of the true risk and potential adverse business and mission consequences. Taking action now can help improve cybersecurity and ensure mission readiness.

[1] formerly called a “whitelist” approach – a default deny, with only specific needed items allowed
[2] Contact your cybersecurity service provider or appropriate government point of contact to help identify the appropriate available tools.

Works Cited

[1] Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency, and Multi-State Information Sharing and Analysis Center (2021). Alert (AA21-042A): Compromise of U.S. Water Treatment Facility. Available at: https://us-cert.cisa.gov/ncas/alerts/aa21-042a

[2] Canadian Centre for Cyber Security, Communications Security Establishment (2020). National Cyber Threat Assessment 2020. Available at: https://www.cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[3] Cybersecurity and Infrastructure Security Agency (2020). Alert (AA20-049A): Ransomware Impacting Pipeline Operations. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-049a

[4] Abir Shehod, MIT Cybersecurity Interdisciplinary Systems Laboratory (2016). Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US. Available at: https://web.mit.edu/smadnick/www/wp/2016-22.pdf

[5] Kevin E. Hamsley, Dr. Ronald E. Fisher, Idaho National Laboratory (2018). History of Industrial Control System Cyber Incidents. Available at: https://www.osti.gov/servlets/purl/1505628

[6] National Security Agency, Cybersecurity and Infrastructure Security Agency (2020). NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems. Available at: https://www.media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.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 document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov