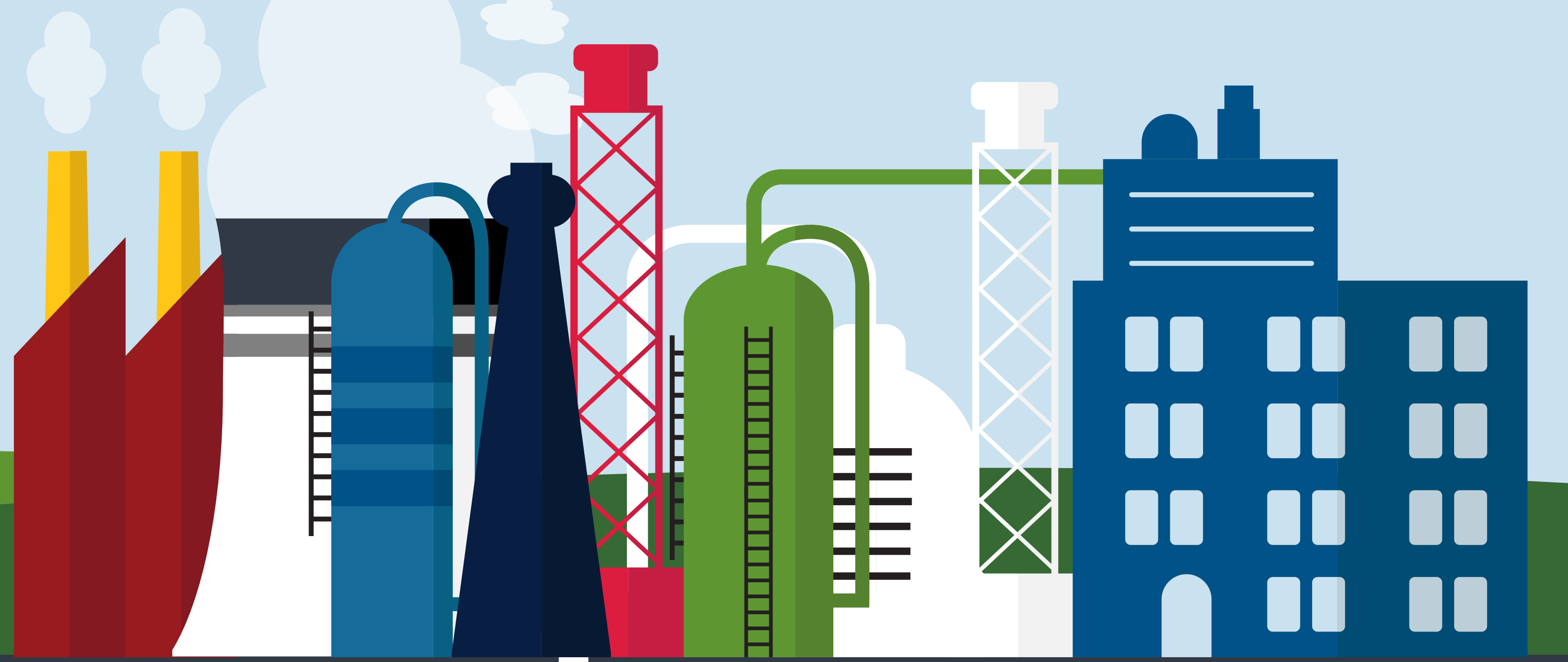
Recommended

Cybersecurity Practices

for Industrial Control Systems



CYBERSECURITY CONSIDERATIONS

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.

As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting operational technology (OT) to enterprise information technology (IT) systems and Internet of Things (IoT) devices.

Among the risks, are:

- Expanding ICS cyberattack surface, which may lead to an increase in security events.
- Eliminating ICS network segmentation from traditional business IT systems or internet devices, resulting in greater access to critical systems.
- Increasing susceptibility to IT commodity malware and ransomware, which can lead to a potential disruption of physical processes.

PRINCIPLES-LED DESIGN

If you need to create an ICS architecture that's resilient against cyber attacks, then consider the UK National Cyber Security Centre's (NCSC), "Secure Design Principles and Operational Technology": https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech

CYBERSECURITY EVENT IMPACTS

SHORT-TERM IMPACTS

- Operational shutdowns
- Loss of visibility over production and safety systems
- Financial loss due to outages and downtime
- Intellectual property theft
- Health and personal safety risks
- Damage and destruction of property and equipment
- Loss of availability
- Loss of control
- Denial of service

LONG-TERM IMPACTS

- Significant unplanned labor, overtime, and idle equipment costs
- Increased or denied insurance
- Degraded equipment performance and quality
- Fees and lawsuits due to negligence or non-compliance
- Loss of customers
- Redirection of organizational expenditure toward recovery efforts

CISA ASSESSMENTS: FISCAL YEAR 2019 MOST PREVALENT IT AND OT WEAKNESSES AND RISKS

Boundary Protection

RISK
Undetected unauthorized activity in critical systems

RISK
Weaker boundaries between ICS and enterprise systems

Principle of Least Functionality

RISK
Increased vectors for malicious party access to critical systems

RISK
Opportunity for rogue internal access to be established

Identification and Authentication

RISK
Lack of accountability and traceability for user actions if an account is compromised

RISK
Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access

Physical Access Control

RISK
Unauthorized physical access to field equipment provides increased opportunity to:

- Maliciously modify, delete, or copy device programs and firmware
- Access the ICS network
- Steal or vandalize cyber assets
- Add rogue devices to capture and retransmit network traffic

Account Management

RISK
Increased opportunity for unapproved system access from shared or system accounts

Defend ICS Processes Today

- ✓ Check, prioritize, test, and implement ICS security patches.
- ✓ Backup system data and configurations.
- ✓ Identify, minimize, and secure all network connections to ICS.
- ✓ Continually monitor and assess the security of ICS, networks, and interconnections.
- ✓ Disable unnecessary services, ports, and protocols.
- ✓ Enable available security features and implement robust configuration management practices.
- ✓ Leverage both application whitelisting and antivirus software.
- ✓ Provide ICS cybersecurity training for all operators and administrators.
- ✓ Maintain and test an incident response plan.
- ✓ Implement a risk-based defense-in-depth approach to securing ICS hosts and networks.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

DEPARTMENT OF ENERGY UNITED STATES OF AMERICA

For additional information, including advisories, alerts, and recommendations, please visit CISA's Industrial Control Systems website: https://www.cisa.gov/ics

For additional information on Department of Energy (DOE) cybersecurity initiatives, please visit: https://www.energy.gov/ceser

PROACTIVELY PROTECT TOMORROW

RISK MANAGEMENT AND CYBERSECURITY GOVERNANCE

- Identify threats to the organization.
- Maintain ICS asset inventory of all hardware, software, and supporting infrastructure technologies.
- Develop cybersecurity policies, procedures, training and educational materials that apply to organization's ICS.
- Develop and practice incident response procedures that join IT and OT response processes.

PHYSICAL SECURITY

- Lock down field electronics and set up alerting mechanisms for device manipulation such as power removal, device resets, and cabling changes.
- Ensure only authorized personnel have access to controlled spaces that house ICS equipment.
- Use multi-factor authentication, guards, and barriers to control logical and physical access to ICS equipment and facilities.

ICS NETWORK ARCHITECTURE

- Utilize segmentation of networks where possible.
- Implement a network topology for ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Use one-way communication diodes to prevent external access, whenever possible.
- Set up demilitarized zones (DMZ) to create a physical and logical subnetwork that acts as an intermediary for connected security devices to avoid exposure.
- Employ reliable and secure network protocols and services where feasible.

ICS NETWORK PERIMETER SECURITY

- Configure firewalls to control traffic between the ICS network and corporate IT network.
- Utilize IP geo-blocking as appropriate.
- Harden the remote access process to reduce risk to an acceptable level.
- Use jump servers as a central authorization location between ICS network security zones.
- Do not allow remote persistent vendor or employee connection to the control network.
- Catalog and monitor all remote connections to the network.

HOST SECURITY

- Promote a culture of patching and vulnerability management.
- Test all patches in off-line test environments before implementation.
- Implement application whitelisting on human machine interfaces.
- Harden field devices, including tablets and smart phones.
- Replace out-of-date software and hardware devices.
- Disable unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Implement and test system backups and recovery processes.
- Configure encryption and security for ICS protocols.

SECURITY MONITORING

- Measure the baseline of normal operations and network traffic for ICS.
- Configure Intrusion Detection Systems (IDS) to create alarms for any ICS network traffic outside normal operations.
- Track and monitor audit trails on critical areas of ICS.
- Set up Security Incident and Event Monitoring (SIEM) to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

SUPPLY CHAIN MANAGEMENT

- Adjust ICS procurement process to weigh cybersecurity heavily as part of the scoring and evaluation methodology.
- Invest up front in secure ICS products, evaluating security against current and future threats over the projected product lifespan.
- Establish contractual agreements for all outsourced services that ensure: proper incident handling and reporting, security of interconnections, and remote access specifications and processes.
- Consider ICS information integrity, security, and confidentiality when contracting with a cloud service provider.
- Leverage test labs to test vendor-provided software for malicious code and defects before implementation.

HUMAN ELEMENT

- Issue policies that outline ICS security rules, including expected rules of behavior and required controls.
- Issue procedures that state how personnel should manage ICS in a secure manner.
- Train IT operators, OT operators, and security personnel to recognize the indicators of potential compromise and what steps they should take to ensure that a cyber investigation succeeds.
- Promote a culture of dialogue and information exchange between security, IT, and OT personnel.

For more detailed information, please review CISA's publications: https://www.cisa.gov/ics/Recommended-Practices
and DOE's Cybersecurity Capability Maturity Model (C2M2) Program: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0