Industrial Control Systems Cybersecurity

Office of the New York
STATE COMPTROLLER
Thomas P. DiNapoli

Local Government and
School Accountability

INFORMATION TECHNOLOGY SERIES

Table of Contents

Industrial Control Systems (ICS) Cybersecurity

One area of information technology that is receiving a lot of attention lately is industrial control systems (ICS) cybersecurity. ICS is a generic term used to describe any system that gathers information on an industrial process and modifies, regulates or manages the process to achieve a desired result. ICS can take many forms including: SCADA (supervisory control and data acquisition), EMS (emergency management system) and PCS (process control system).

Much of the nation's critical infrastructure is run with help from ICS. The United States[1] has designated 16 critical infrastructure and key resource sectors that are vital to public confidence and the nation's safety, prosperity and well-being. The sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, transportation systems, and water and wastewater systems. ICS or some sort of industrial automation is used in each of these sectors and is implemented in ways suited to the processes they are running or monitoring.

ICS is a generic term used to describe any system that gathers information on an industrial process and modifies, regulates or manages the process to achieve a desired result.

Since most ICS are computer-based and many have Internet connectivity, they are exposed to the same cyber threats as traditional information technology (IT) systems. Reducing the vulnerability of the ICS and the nation's critical infrastructure to cyberattacks is considered a high priority and is the primary objective of several State and Federal agencies and programs. Many local governments have one or more ICS and should be aware of their responsibilities relating to ICS cybersecurity.

Background

Years ago, ICS were considered low-risk because they were isolated from entity networks and the Internet. They also typically had proprietary control protocols using specialized hardware and software, the inner workings of which were not widely known and hence more difficult to attack. The physical gap between the control network and an organization's business network and the Internet was called an "air gap." The major risk to totally isolated or air-gapped ICS, unauthorized physical access to the system, was primarily mitigated through use of the physical security controls such as locks, gates and guards.

The risk landscape changed drastically, however, as Internet-based technologies began making their way into ICS design. Organizations started shifting toward widely available, lower-cost IT solutions that support connectivity to the municipal network and remote access capabilities so that ICS operators, engineers and other support personnel can monitor and control systems from afar. These connectivity changes dramatically increase the possibility of cybersecurity vulnerabilities and incidents.

The security solutions that work in a typical IT environment may be inappropriate, ineffective and even harmful in an ICS environment.

Further complicating the risk landscape is the fact that ICS-related IT security requires special precautions. The security solutions that work in a typical IT environment may be inappropriate, ineffective and even harmful in an ICS environment. In addition, while typical IT components have a lifetime of approximately three to five years due to the quick evolution of technology, the lifetime of ICS technology, developed for very specific use and implementation, is around 10 to 15 years or longer. Older ICS components do not have the same features we see in modern IT.

Since ICS have different risks (e.g., significant risk to health and safety of human lives), priorities (e.g., safety and efficiency), functionality and life spans from traditional IT systems, there can be conflicts with traditional IT controls. For example, many ICS environments, especially legacy systems, may not have some of the typical desired IT security features, such as encryption capabilities, error logging and password protection. Likewise, many ICS cannot be easily stopped and started without affecting production. This makes bringing systems down for routine maintenance, such as applying software patches or updates, difficult. In addition, patches may not even be available for legacy systems or components. Lastly, tools for performing network vulnerability assessments and penetration tests for typical IT networks have been known to cause ICS to malfunction.

Best Practices

Interconnectivity with the outside world is now a reality for many ICS and while the convergence of industrial process operational technology with information technology presents challenges, there are many steps entities can take to improve the cybersecurity of their ICS environment(s).

- **Assemble a Team** – Assemble a team responsible for gaining a thorough understanding of your ICS environment and conducting a risk assessment to identify potential security weaknesses. Due to the complexity and interactions of ICS with traditional information technology, the team should include ICS personnel (operators, engineers and ICS vendors), IT personnel (internal support staff and/or IT vendor) and the governing board, as appropriate.

- **Maintain an Inventory of System Components** – Identify and maintain a current list of all critical operational and IT hardware and software components. It is difficult to protect your ICS environment unless you know what resources you have and where those resources reside. In addition, since IT security alerts often mention specific makes, models and versions of system components, knowing what you have will help you determine if the alerts are relevant to your system.

Assemble a team responsible for gaining a thorough understanding of your ICS environment and conducting a risk assessment to identify potential security weaknesses.

- **Determine if ICS are Internet-Accessible** – Periodically audit the ICS environment for Internet-accessible configurations using search engines (e.g., SHODAN) specifically designed to identify Internet-facing ICS devices.[2] If such devices are found, personnel should take the necessary steps to remove them from direct or unsecured Internet access. ICS often have Internet-accessible devices installed without the organization's knowledge (e.g., a consultant installs a newly-purchased component that by default is Internet-enabled), putting those systems at increased risk of attack.

- **Change Default Settings** – Change all factory-default authentication credentials (e.g., user names and passwords) on system components and applications upon installation.

- **Examine Access Rights** – Identify everyone (e.g., municipal personnel, third parties, former municipal personnel and third parties) who can access your ICS. You should know all points of entry to the ICS and ensure that all access, whether by wired or wireless network connectivity, remote access or physical access, is authorized, monitored and secure.

- **Incorporate Key, Traditional IT Security Practices** – Incorporate key IT security practices to the extent possible.
  - Passwords should be complex and periodically changed;
  - Antivirus programs should be installed and updated routinely;
  - Firewalls should be configured securely;
  - Wireless connectivity should be established only if absolutely necessary and should be configured securely; and
  - Software should be patched, updated and maintained at vendor-supported levels in order to reduce the risk of security breaches.

The use of unauthorized removavable media in an ICS environment should be prohibited to prevent the inadvertent introduction of malware and loss or theft of data.

- **Control Use of Removable Media and Printed Materials** – Organizations should establish, enforce and monitor security policies and procedures for the use, storage and eventual disposal of removable media (e.g., CDs, DVDs and USB drives) and printed materials (e.g., reports) that contain sensitive ICS information. The use of unauthorized removable media in an ICS environment should be prohibited to prevent the inadvertent introduction of malware and loss or theft of data. Likewise, security over printed materials should be maintained to prevent the accidental disclosure of information that could assist an attacker in harming an ICS.

- **Ensure Sensitive System Information Is Not Disclosed on Municipal or Vendor Websites** – Your public website should not contain sensitive information (e.g., details about your ICS and/or IT components, environments or plant schematics) that could assist someone in attacking your ICS or physical plant. In addition, you should ensure that ICS (e.g., engineering firm) and IT vendors do not disclose sensitive information on their websites, possibly as part of their promotional materials. Your expectations concerning the protection and disclosure of ICS information should be discussed with vendors and included in contractual provisions as necessary.

- **Ensure Sensitive System Information Is Not Disclosed on Social Networking Sites** – Social networking sites should be free of information that could potentially enable someone to harm the municipality's ICS. For example, if municipal personnel post résumés on professional networking websites, the résumés should not include details relating to the ICS and/or IT systems currently in use at your municipality.

- **Stay Informed** – Municipal personnel should regularly review ICS security alerts and advisories that are available free of charge from several reputable sources such as the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT; **http://us-cert.gov**), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT; **http://us-cert.gov/ics**) and the Multi-State Information Sharing & Analysis Center (MS-ISAC; **http://cisecurity.org/ms-isac/**).

Additional Resources

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
http://us-cert.gov/ics

Industrial Control System Sector-Specific Guidance:

- American Water Works Association (AWWA)
  http://awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
- ICS Sector-Specific Information Sharing & Analysis Centers
  http://nationalisacs.org/member-isacs
- United States Environmental Protection Agency (EPA)
  http://epa.gov

Multi-State Information Sharing & Analysis Center (MS-ISAC)
http://cisecurity.org/ms-isac/

National Institute of Standards and Technology (NIST)

- Special Publications
  http://csrc.nist.gov/publications/sp
- Voluntary Framework for Reducing Cyber Risks to Critical Infrastructure
  http://nist.gov/cyberframework

United States Computer Emergency Readiness Team (US-CERT)
http://us-cert.gov

Notes

[1] **http://dhs.gov/cisa/critical-infrastructure-sectors**.

[2] For further information, see ICS-ALERT-12-046-01A Increasing Threat to Industrial Control Systems (Update A), **http://us-cert.gov/ics/alerts/ICS-ALERT-12-046-01A**

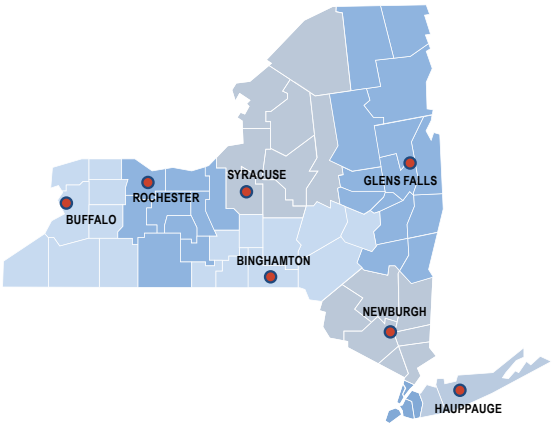
Contacts

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th Floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.ny.gov/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Robin L. Lois, CPA, Deputy Comptroller
Simonia Brown, Assistant Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

New York State & Local Retirement System
Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6530 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Statewide@osc.ny.gov

osc.ny.gov

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.ny.gov/local-government

Updated October 2019