Office of the New York State Comptroller
Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

Industrial Control Systems Cybersecurity

For additional copies of this report contact:

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th floor
Albany, New York 12236
Tel: (518) 474- 4037
Fax: (518) 486- 6479
or email us: localgov@osc.state.ny.us

www.osc.state.ny.us

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

October 2015

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 toward the process they are running or monitoring.

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.

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.

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

Background

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

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.

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, for example, 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.
- **Create or Update an Inventory of System Components** – Identify 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.
- **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.

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

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

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.

- **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 patches and updates should be maintained at vendor-supported levels in order to reduce the risk of security breaches.
- **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 resumes on professional networking websites, the resumes 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; **https://www.us-cert.gov/**), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT; **https://ics-cert.us-cert.gov/**) and the Multi-State Information Sharing & Analysis Center (MS-ISAC; **http://msisac.cisecurity.org/**).

Additional Resources

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

Industrial Control System Sector-Specific Guidance:

- American Water Works Association (AWWA)
  http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx

- ICS Sector-Specific Information Sharing & Analysis Centers
  http://www.isaccouncil.org/memberisacs.html

- United States Environmental Protection Agency (EPA)
  http://www.epa.gov/

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

National Institute of Standards and Technology (NIST)

- Computer Security Division, Special Publications
  http://csrc.nist.gov/publications/PubsSPs.html

- Voluntary Framework for Reducing Cyber Risks to Critical Infrastructure
  http://www.nist.gov/cyberframework/index.cfm

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

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive	474-4037
Gabriel F. Deyo, Deputy Comptroller	
Audits, Local Government Services and Professional Standards	474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)	
Local Government and School Accountability Help Line	(866) 321-8503 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)	

New York State & Local Retirement System

Retirement Information Services	
Inquiries on Employee Benefits and Programs	474-7736
Bureau of Member and Employer Services	(866) 805-0990 or 474-1101
Monthly Reporting Inquiries	474-1080
Audits and Plan Changes	474-0167
All Other Employer Inquiries	474-6535

Division of Legal Services

Municipal Law Section	474-5586

Other OSC Offices

Bureau of State Expenditures	486-3017
Bureau of State Contracts	474-4622

Mailing Address for all of the above:

Office of the New York State Comptroller,
110 State Street, Albany, New York 12236
email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Gabriel F. Deyo, Deputy Comptroller (518) 474-4037

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313 • **Email:** Muni-Binghamton@osc.state.ny.us
Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • **Fax** (716) 847-3643 • **Email:** Muni-Buffalo@osc.state.ny.us
Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE - Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • **Fax** (518) 793-5797 • **Email:** Muni-GlensFalls@osc.state.ny.us
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (845) 567-0858 • **Fax** (845) 567-0080 • **Email:** Muni-Newburgh@osc.state.ny.us
Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • **Fax** (585) 454-3545 • **Email:** Muni-Rochester@osc.state.ny.us
Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (315) 428-4192 • **Fax** (315) 426-2119 • **Email:** Muni-Syracuse@osc.state.ny.us
Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

STATEWIDE AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

Office of the New York State Comptroller • Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236