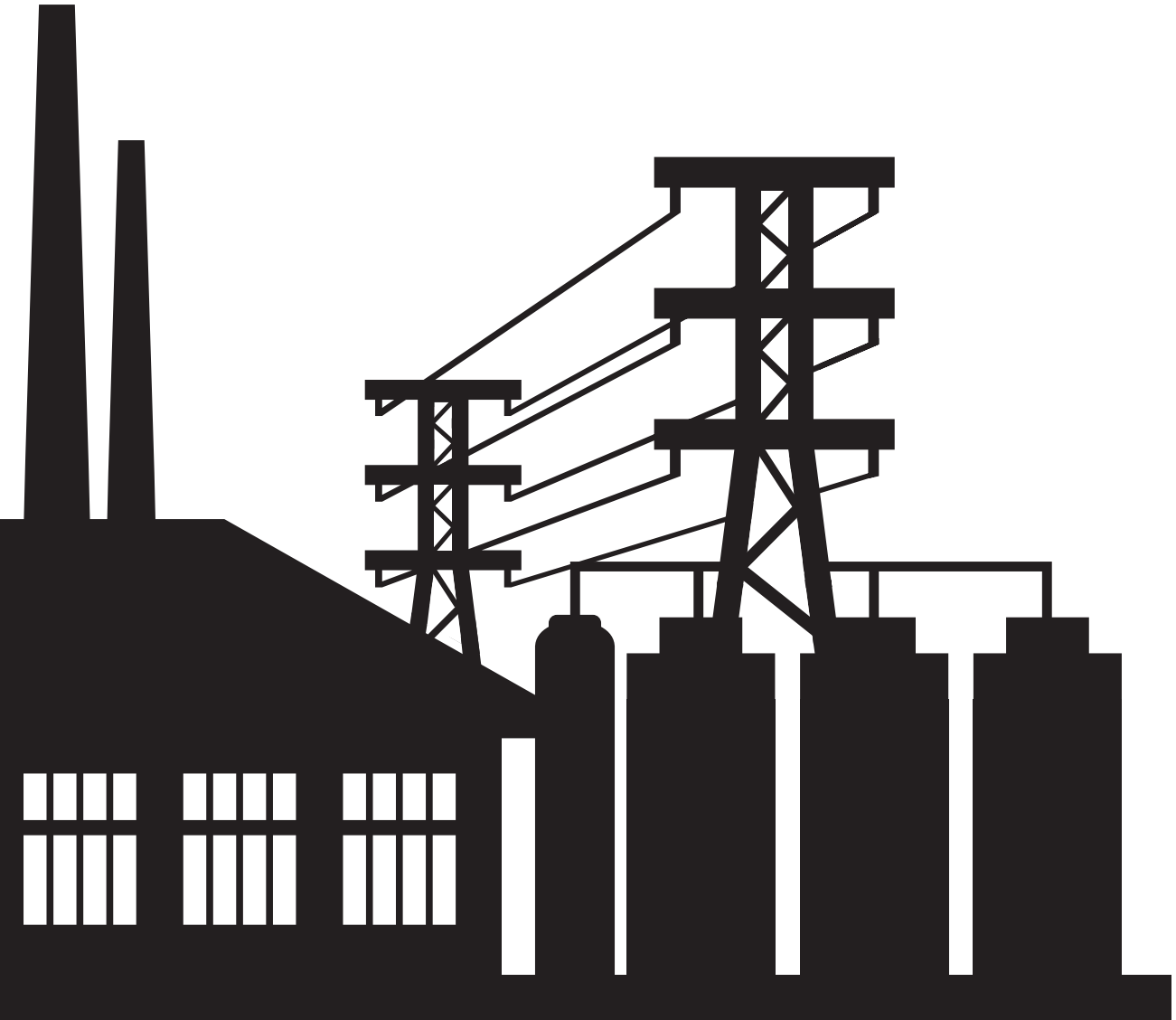
PROTECTING OUR CRITICAL UTILITIES WITH INTEGRATED CONTROL SYSTEMS



CRITICAL INFRASTRUCTURE SECURITY

The wellbeing and security of all nations depends on the availability of critical infrastructure, such as the electric grid, water supply infrastructure, oil and gas facilities and public warning systems, which are often managed using Integrated Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) or other similar types of control systems.

In many cases, the ICS technology is outdated, resulting in inefficiencies and unsecured systems that can present a security risk. For example, in North America, three major electric blackouts in the past nine years have caused subsequent disruption in the operation of other utilities.

There is widespread agreement among those responsible for critical infrastructure that it is time to upgrade the security of these Integrated Control Systems to increase overall system availability and reliability with upgrades that will leverage distributed intelligence and high-speed, broadband communication. While these new capabilities bring benefits, appropriate decisions must be made to ensure that these updates do not increase exposure to outside forces and introduce new vulnerabilities.

A SAMPLE OF SECURITY BREACHES

2009 – *The Wall Street Journal* reported that spies hacked into the US electric grid and left behind computer programs that could disrupt services.[2]

2009 – At the Black Hat Conference, researchers demonstrated a proof of concept worm attack on commercial smart meters that allowed full system control of meter functions including remote power on/off and usage reporting.[3]

2008 – The CIA confirmed that a cyber attack from an Internet intrusion caused a multi-city power outage.[4]

2007 – An intruder installed unauthorized software and damaged the computer used to divert water from the Sacramento River.[4]

2005 – Security consultants reported that hackers targeted the US electric power grid and gained access to utility electronic control systems and caused an "impact" in a few cases.[2]

CYBER INCIDENTS

A substantial number of confirmed, unconfirmed, and potential cyber incidents that directly or indirectly impact control systems have been documented worldwide.[1] The numbers of these incidents were small until around 2000 when they began to increase dramatically. The majority of attacks have come from the Internet through opportunistic viruses, trojans and worms, but a surprisingly large number represent direct acts of sabotage.

One reason for a historical small number of incidents is the relative isolation of older, autonomous control systems; prior to 2000, many Integrated Control Systems relied on proprietary networks and hardware and were not connected to other networks. Another possible reason is the higher level of technical sophistication required to carry out a cyber attack against an ICS.

However, with the continued pervasiveness of Internet connections and the adoption of open standards for computing hardware, operating systems and software in control systems, the number of incidents will increase. The Department of Homeland Security (DHS) US-CERT (Computer Emergency Readiness Team) and ICS-CERT have reported significant increases in the number of cyber incidents and advanced persistent threat activity affecting critical infrastructure.

THE RISK IS INCREASING

A string of government reports detail the growing concerns of a cyber attack on critical US energy infrastructure.

A June 2010 Government Accountability Office (GAO) report revealed that federal agencies cited an increase of more than **400%** in the number of incidents reported to US-CERT compared to 2006.[5]

The ICS-CERT 2010 Year-in-Review reported that the number of cyber incidents in 2011 was up over **200%** from 2010 and the vulnerability analysis and coordination rose a staggering 600%.[6]

The April 2012 GAO report, "Cybersecurity Threats impacting the Nation," noted that over the past six years, the number of incidents reported by federal agencies to the federal information security incident center (US-CERT) has increased by nearly **680%**.[7]

ICS VULNERABILITIES

The increased connectivity of ICS to other networks and the Internet has exposed critical security issues related to integrated control systems and SCADA.

- ICS protocols were not designed with security in mind, since by and large they would use a physically isolated network for communications. In typical protocols, particularly open standard ones like Modbus or DNP3 with no built-in authentication, packets are processed without any additional user or system authentication. In the case of IP-encapsulated protocols, most devices are currently enabled with their own proprietary IP stack, making them very susceptible to various attacks since they were not designed or tested outside of normal SCADA only data.[8]
- Older systems were primarily made up of proprietary software and hardware components. However, with the decreasing prices of commodity software and hardware, as well as increased requirements for connectivity outside of the control system network, ICS vendors now employ commodity components, such as commercial computers and Microsoft® Windows® operating systems, which increase the vulnerability of these new systems.
- Many controllers (RTUs or PLCs) in use provide some functionality for flexible configuration and digital communication capabilities to enable remote access and control. While the added complexity and communication capability of the software provides additional functionality, it can lead to additional points of penetration and an increased opportunity to exploit system vulnerabilities.

> "Our information infrastructure – including…embedded processors and controllers in critical industries – increasingly is being targeted for exploitation and potentially for disruption or destruction… Cyber exploitation activity has grown more sophisticated, more targeted, and more serious."[9]
>
> J. Michael McConnell, Director of National Intelligence

- The move to open standards, such as Ethernet, TCP/IP and Web technologies, makes it easier for an adversary to obtain the necessary knowledge, via the source code, to attack a system. Commonly released worms and viruses now affect not only consumer computers but also impact the computer systems of critical infrastructure and manufacturing industries.
- IP-based communication within the ICS network is typically not encrypted, which exposes the communications to potential eavesdropping and session hijacking.
- Some systems have very limited logging and permission-enabled access, making them vulnerable to penetration from within and outside the organization. And, in many cases, a security event may go completely unnoticed.

ICS THREATS

Since 2000, there has been a drastic increase in the number of successful cyber attacks against Integrated Control Systems at power generation, petroleum production, nuclear energy, water treatment and other facilities. Many of these cyber intrusions have resulted in damage to the facilities; confirmed damage includes an intentional discharge of millions of gallons of sewage, opening breaker switches, tampering with boiler controls resulting in shutdown, and shutdown of combustion turbine power plants and several industrial facilities.

Threats to ICS can be divided into two main categories: directed threats such as sabotage and terrorist attacks; and indirect threats like operational errors and viruses. The potential outcomes for incidents include:

- Malfunction of critical infrastructure
- Lack of system availability
- Damage to equipment
- Data loss
- Personal safety issues
- Revenue loss
- Penalties

While ICS attacks are less numerous than cyber attacks on the general business community, the motivation and mechanisms of ICS incidents reflect a more focused intent by external sources to infect malware.

> Greg Schaffer, DHS deputy undersecretary, revealed, "US utilities and other crucial industries face an increasing number of cyber break-ins by attackers using more sophisticated methods." The DHS reports that the number of US-CERT deployments continues to increase substantially every year, as does the number of private organizations requesting the department's help to protect their automated control systems.[10]

Regulatory agencies are now publishing ICS security best practices, but most countries do not currently have absolute requirements or associated timelines, penalties and auditing for the identified practices. This approach is gradually changing; for example, in 2008, the Federal Regulatory Commission (FERC) approved eight new critical infrastructure protection (CIP) reliability standards intended to safeguard the US's bulk power systems from cyber security breaches. Other industry areas are following at different paces, but it is quite clear that mandatory security requirements will come in the near future.

The emergence of Stuxnet, the first malware created specifically to target ICS, signaled a true paradigm shift for the control systems community in 2010. It showed that organizations must be operationally prepared with tools, systems, and personnel to detect malicious activity and effectively mitigate the impact to their control systems. Stuxnet highlighted the interdependencies and vulnerabilities of legacy control systems and demonstrated that motivated groups are interested in attacking critical infrastructure.[11]

FIELD DEVICES: ASSUMPTIONS AND THREATS

In most Integrated Control Systems, field devices like RTUs are located in remote, unmanned sites. The capabilities of these devices vary from simple measurements and control to sophisticated devices that execute large programs and control complex processes. Field devices generally communicate directly to an HMI (human machine interface) or front-end device located in a control center.

The level of protection required for field devices relies on the following assumptions and threats identified by the U.S. National Institute of Standards and Technology (NIST):

- Authorized users and administrators are properly trained and will not take actions that intentionally affect the security of the device
- The device is placed in a secure physical location to prevent unauthorized physical access and modification
- The device is used in a physical environment that meets the manufacturer's specifications for power, temperature, humidity, and other environmental factors
- Authorized users will protect their log-in credentials from unauthorized disclosure

> "We are a nation at war. And that war is raging 24 x 7 in Cyberspace. It's not only hitting stock exchanges and websites. They're also hitting power systems."[12]
>
> Curtis Levinson, Technical Director to NATO

The main threats for field devices include:

- Unauthorized access
- Malicious compromise of the device
- Unidentified actions
- Equipment damage
- Resource exhaustion
- Replay attack
- Masquerade
- Unsecured programming

Kevin Helmsley, a leader in the emergency-response effort in the Control systems Security Program at ICS-CERT, said the count of "incident tickets" related to reported incidents at water and power generating utilities is going up. While only nine incidents were reported in 2009, the number grew to 198 in 2011. Just over 40% came from water-sector utilities, with the rest coming from various energy, nuclear energy and chemical providers. "There's a lot of exposed water systems."[12]

EFFORTS TO SECURE ICS NETWORKS

To deal with the growing need to protect control systems against malicious cyber attacks, multiple industrial and government-led efforts to improve ICS security have been initiated.

In the US, the electric sector has led the way with the North American Electric Reliability Corporation (NERC) cyber security standards for control systems. NERC is authorized to enforce compliance to these standards and levy monetary penalties.

The American Gas Association (AGA) has developed a series of recommended practices, which focus on ensuring the confidentiality of communications, to protect ICS communications against cyber incidents.

The American Petroleum Institute (API) provides guidelines for managing ICS integrity and security for the operators of oil and natural gas pipeline systems. The guidelines (API standard 22) are specifically designed to give operators both a set of industry practices in ICS security, as well as a framework to help individual operators develop sound security practices for their particular organization.

The Chemical Sector Cyber Security Program 23 (CSCSP) is a strategic program of the Chemical Information Technology Center (ChemITC) of the American Chemistry Council. The Program focuses on risk management and reduction to minimize the potential impact of cyber attacks on chemical-related business and manufacturing systems.

The ISA (International Society of Automation) ISA99 Committee brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security. The Committee created the ISA99 Industrial Automation and Control Systems Security Standards, a security standard for use in manufacturing and general industrial controls.

Several organizations including the EPA (Environmental Protection Agency), AWWA (American Water Works Organization), AMWA (Association of Metropolitan Water Authorities) and DHS have collaborated in developing a series of recommendations and guidelines to secure control systems in the water sector.

> "On a daily basis, the US is being targeted," said Sanaz Browarny, chief, intelligence and analysis, control systems security program at DHS. One of the basic problems observed at utilities is that "a lot of folks are using older systems previously not connected to the Internet," she said. "The mindset is the equipment would last 20 or 30 years with updates. These systems are quite vulnerable."[12]

In May 2012, DHS issued an alert warning that computer networks connected to privately owned natural gas pipelines are under cyber attack in an intrusion campaign. The "amber" alert, the second highest cyber threat level, has been in place since December 2011, when DHS noted that multiple natural gas pipeline organizations reported either attempts or intrusions related to this cyber attack campaign.[13]

Other government agency and standards organization efforts include:

- The National Cyber Security Division (NCSD) of DHS established the Control Systems Security Program (CSSP) and the US-CERT Control Systems Security Center (CSSC) to reduce risks to control systems. CSSP coordinates efforts among federal, state and local governments, as well as control system owners, operators and vendors to improve control system security, while CSSC coordinates control system incident management, provides timely situational awareness information, manages control system vulnerability and directs threat reduction activities.
- The Department of Energy (DOE) established the national ICS test bed program at Idaho National Labs (INL) for securing control systems in the energy sector. Sandia National Laboratories, a contractor for the DOE National Nuclear Security Administration (NNSA), established the Center for Control System Security.
- The UK Center for the Protection of National Infrastructure (CPNI) performs protection research to mitigate electronic attack risks to the UK national infrastructure. They also provide forums for sharing information on SCADA threats, incidents and mitigation in the UK and Europe. CPNI also maintains close working relationship with the organizations developing security programs in the US, Canada, Australia, New Zealand and Europe.
- The Cyber Security Act of 2012 legislation, which has not yet been approved, would give DHS the authority to set and oversee security standards for critical networks. If the Act passes, DHS will assess cyber security risks, establish a procedure for designating critical infrastructure and develop cyber security performance requirements, which will likely include a directive to report significant cyber incidents that affect critical infrastructure.

KEY ELEMENTS OF ICS SECURITY

Security strategy goals should protect all points of entry to the network, limit points of vulnerability and prevent attempts to compromise the network, and the data it transmits and uses.

Security methods that have been effectively used in critical enterprise networks can also be applied for securing ICS. A short list of the most successful enterprise methods includes:

SECURITY POLICY ENFORCEMENT

Ensures that system users, devices and system tools adhere to the system security policy settings put in place by system administrators.

FIREWALL

Permits or denies data transmissions – into a network, a network segment or a device – based on rules and other established criteria. All IP messages pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.

ACCESS CONTROL

User authentication identifies a specific user and verifies that the user is legitimate and is allowed to access a network or a device. Access is typically controlled by an authentication server and a required authentication procedure to establish – with a high degree of confidence – the identity of the user. User name and password are the most common credentials required for user authentication.

"Utility cyber security is in a state of near chaos. After years of vendors selling point solutions, utilities investing in compliance minimums rather than full security, and attackers having nearly free reign, the attackers clearly have the upper hand."[14]

ROLE-BASED ACCESS CONTROL (RBAC)

Restricts types of system access to authorized users. Roles in an organization are created for various job functions, and permissions to perform certain operations are assigned to specific roles. Since users are not assigned permissions directly, but acquire them through their role or roles, management of individual user rights is done by assigning appropriate roles for the user account. The administrator can define roles and assign a different combination of permissions to each role.

INTRUSION DETECTION SYSTEM (IDS)

Monitors events occurring in the network and identifies activities that are potentially malicious or in violation of security policy, such as an unauthorized attempt to alter a device firmware, and reports that event to a management station. The more sophisticated systems can react in real time to block or prevent certain activities like dropping unauthorized data packets, while still allowing legitimate traffic.

DEMILITARIZED ZONE (DMZ)

Combines firewall and intrusion prevention system to tightly regulate traffic entering company servers, usually at the control center. When a DMZ is in use, there are no common communication ports between the outside world and the internal controlled zone.

ANTI-VIRUS SOFTWARE

Detects, prevents and removes damaging code like worms, viruses and Trojan horses from computers. Workstations and servers that support utility applications in control centers, such as SCADA HMI, should have anti-virus software installed for protection from such threats. However, it is important to note that the need for an online connection for signature updates and risk management increases vulnerability.

APPLICATION CONTROL SOFTWARE

Also known as white list software, application control software blocks unauthorized applications and code on servers, corporate desktops, workstations and field devices. A "white" listing solution thwarts advanced threats by allowing only pre-identified programs to run.

ENCRYPTION

Uses an algorithm that makes data readable only by a device with a specific key to decrypt the message. Communication data encryption prevents eavesdropping, as well as spoofing where a person or program masquerades as another to gain access. Data stored in devices and applications should be encrypted to prevent attacks on the data and maintain system data integrity. Symmetric encryption uses the same key for both encryption and decryption. The longer the encryption keys, in general, the stronger the encryption.

AUDITING

Monitors the processing in each device and logs any suspicious activity or deviations from policy when detected. Any attempt of unauthorized access will be blocked and logged in the device's internal security log. Based upon severity, an event can trigger an alarm to alert designated personnel.

UNUSED PORT DEACTIVATION

Disables communications in ports that are not in use. Since an active, unused port is a target for unauthorized access attempts, it is critical to block ports that are not in use to reduce device vulnerability.

> While no major cyber attacks on the US electric grid have been reported, Russia and China have "probed the electrical grid to find vulnerabilities to exploit if they needed to attack it," said James Lewis, technology program director at the Center for Strategic & International Studies in Washington. Citing the National Security Agency, he said, "The risk is that the attack capabilities are spreading, and countries like Iran and North Korea, along with jihadists and anarchists, will eventually be able to attack."[15]

TIME-WINDOW COMMAND LIMITS

Adds another layer of defense to limit the risk of replay attacks and other malicious activities. For critical messages, a time stamp is added to the command message; the subsequent "action" message must be received within a designated window of time, and it must contain elements that match those in the notification message. If it does not, the action is rejected.

SECURED PROGRAMMING

Includes methodologies and techniques for eliminating vulnerabilities stemming from common programming errors. Identifying unsafe coding practices and developing secure alternatives allows software developers to take practical steps to reduce or eliminate vulnerabilities before deployment. Secure programming also refers to techniques like code obscurification designed to disable reverse code engineering that could be used to expose vulnerabilities or eliminate encryption of auxiliary data related to debugging and testing.

MOTOROLA BRINGS IT ALL TOGETHER

Motorola is actively working with the NIST Cyber-Security Coordination Task Group (CSCTG), DHS and other organizations to identify the appropriate security requirements and solutions for critical infrastructure.

With over three decades of experience providing ICS solutions to public utilities and serving as the leading provider of secure land mobile radio systems for public safety, federal and Department of Defense (DOD) applications, Motorola has the vision and the experience needed to deploy the sophisticated systems necessary to ensure that stringent security requirements are met.

Our long experience in SCADA systems and data communications allows us to offer solutions with a large selection of communication media and data protocols. Numerous Motorola ICS installations with more than 150,000 RTUs are operating worldwide, serving the oil and gas industry, electric and water utilities, municipal authorities and public safety agencies.

Managing and maintaining a secure ICS or SCADA system is as vital as developing, deploying and integrating the initial secure solution. Motorola leverages our deep expertise in mobility, security and systems integration to help customers identify, control and manage security risk globally.

Securing ICS requires a comprehensive solution including many components, as outlined in this paper. New, sophisticated tools will be essential to ensure the security and integrity of any critical infrastructure. And Motorola has all the pieces to provide the right security solution for ICS and critical infrastructure protection.

SOURCES

1. Cyber Incidents Involving Control systems, Robert J. Turk, Idaho National Laboratory, Oct. 2005, page iv
2. Cyber Security for PUC's, Jeffrey Pillion, 2009 Mid-America Regulatory Conference, Traverse City, Michigan, June 2009, page 3
3. The Four Layers of Smart Grid Security, Ernie Hayden, ICS Joint Working Group 2011 Spring Conference, Dallas, Texas, May 2011, page 21
4. http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5
5. Cybersecurity: Continued Attention is needed to Protect Federal Information Systems from Evolving Threats, GAO, June 2010, page 3
6. CSSP Year in Review: FY 2011, DHS, January 2011, page 6
7. Cybersecurity: Threats Impacting the Nation, GAO, Testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, April 24, 2012
8. A Strategic Approach to Protecting SCADA and Process Control Systems, IBM Internet Security Systems, Inc., July 2007
9. Annual Threat Assessment of the Intelligence Community for the House Permanent Select Community on Intelligence, February 7, 2008, page 15
10. http://www.msnbc.msn.com/id/44724508/ns/technology_and_science-security/t/us-cyber-attacks-utilities-industries-rise/#.UCEJuFIWm80
11. ICS-CERT 2010 Year in Review, DHS, January 2011
12. http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html
13. http://oilprice.com/Energy/Energy-General/US-Gas-Pipelines-under-Cyber-Attack-Says-DHS.html
14. Utility Cyber Security Research Report, Pike Research LLC, 4Q 2011, page 1
15. http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com**

MOTOROLA