INDUSTRIAL CONTROL SYSTEM SECURITY CURRENT TRENDS & RISK MITIGATION

Reducing Critical Infrastructure Risk — An Imperative in Today's Interconnected World.

Donald J. Fergus

Intekras, Inc.
21515 Ridgetop Circle
Suite 260
Sterling, VA 20166
(703) 547-3500
www.intekras.com

December 2009

white paper

intekras

intekras

Insight. Innovation. Integrity.

Information Assurance

Technical Services

Workforce Development

WHITE PAPER

Table of Contents

Critical Infrastructure systems - such as electricity, energy, water/ wastewater, and transportation - are vital to our daily lives and the global economy, yet these critical systems face a growing risk of cyber security threats that are doubling every year. Driven by the growth of malicious software, hacker attacks, an increased threat of cyber-terrorism, and the considerable impact from insider attacks, an effective means of protecting these systems – and mitigating the associated risks - is needed.

Background to Industrial Control Systems

In the past, process control operators implemented distinct, dedicated networks to ensure the isolation of monitoring and control functions from externally connected networks. Emphasis was on physical separation of the networks, and minimal data security was thus included in network design. The assumption was that the data was protected because it was not accessible. Physical security (guards, doors, fences) was the primary method of ensuring access control for these critical system environments. However, the proliferation of Internet use has changed this model. Many process control industries, including public utilities, now take advantage of the flexibility and availability offered by public networks. Internet connectivity offers many conveniences, including remote access and control of systems, process efficiencies through integrated supply chains and outsourcing, centralizing of database information, and inter-connection of various private and public networks to create grids and trading exchanges.

The size and scale of the enterprise side of plant operations has also grown, due to increased regulatory and reporting requirements and expanded use of commercial off-the-shelf software for administration. Often, applications like email, enterprise resource planning, and accounting now

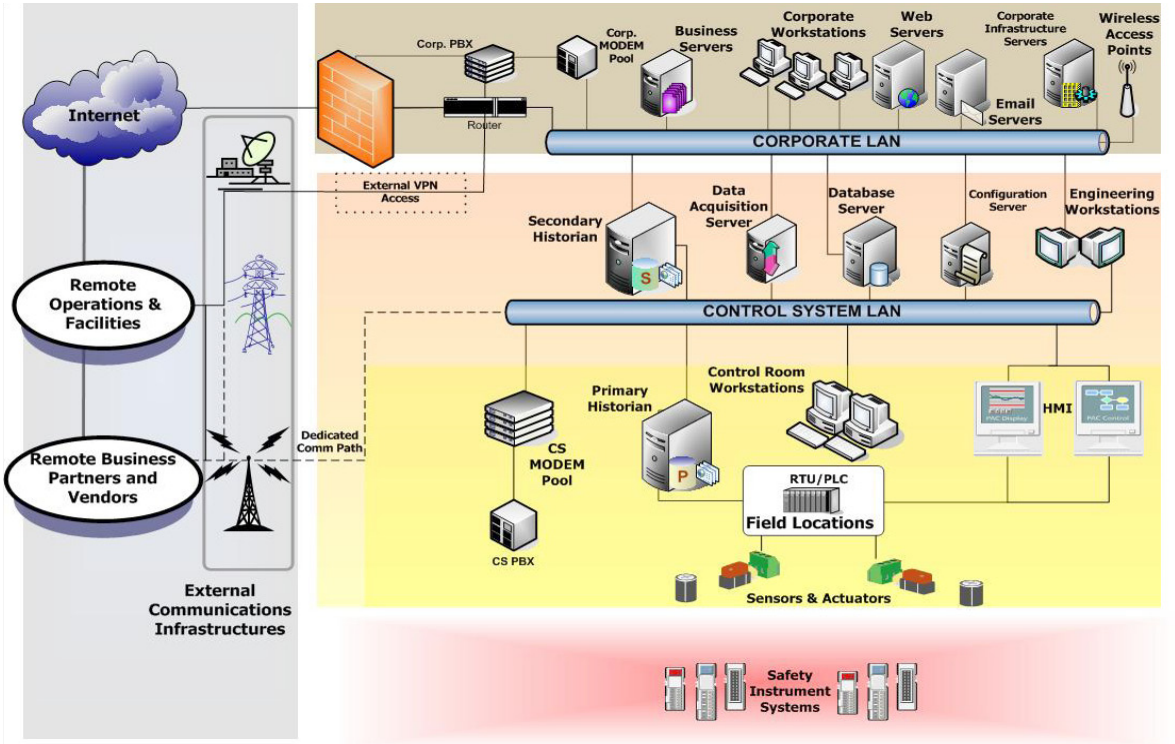

Figure 1 - Interconnected ICS Network

share industrial control network resources and use external network access for collaboration and updates. These administrative, communication, and third-party interfaces present risks for which process control networks were not designed, so new cyber-security mitigations are now needed.

Industrial control systems (ICS) include distributed control systems (DCS), programmable logic controllers (PLC), master and remote terminal units (MTU/RTU), intelligent electronic devices (IED), smart transmitters and drives, continuous emission monitoring systems (CEMS), meters, vibration monitoring systems, and more. These control systems also include Supervisory Control and Data Acquisition (SCADA) systems - used to monitor and control dispersed components at remote sites. In the past, SCADA networks were completely isolated and used proprietary control protocols running on specialized hardware and software. Since then, TCP/IP based systems have made their way into the SCADA environment. The use of new IT systems provides better connectivity across the SCADA network and remote access capabilities. By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide great efficiency and are widely used. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to a nation's critical infrastructure. A typical interconnected ICS network is depicted in Figure 1 above.

Such a convergence of technical developments, governmental mandates and productivity improvements has led to the "opening up" of control system infrastructures – and an increase in the risks associated with their use.

In 2000, hackers cracked Gazprom in Russia, compromising a gas-flow controller. "We were very close to a major natural disaster" commented a Russian minister. In 2001, a former employee of the software development team repeatedly hacked into the SCADA system that controlled a Queensland, Australia sewage treatment plant, releasing about 264,000 gallons of raw sewage into nearby rivers and parks. In 2003, the "Slammer" worm crashed an Ohio nuclear plant network. In 2005, the gauges at the Sauk Water Storage Dam in St. Louis, Missouri read differently than the gauges at the dam's remote monitoring station, causing a catastrophic failure which released one billion gallons of water. In 2006, a foreign hacker penetrated security of a water filtering plant in Harrisburg, Pennsylvania through the Internet. The intruder planted malicious software that was capable of affecting the plant's water treatment operations. In 2007, an intruder installed unauthorized software and damaged the computer used to divert water from the Sacramento River. In 2008, the CIA confirmed that cyber intrusions into utilities (followed by extortion demands) had been used to disrupt power equipment in several regions outside the United States. In 2008, a teenage boy hacked into the track control system of the Lodz, Poland city tram system, derailing four vehicles, after adapting a television remote control so it could change track switches. And this year, power went out for more than two hours in Rio de Janeiro, Sao Paulo and several other major cities after transmission problems knocked one of the world's biggest hydroelectric dams offline. Airport operations were hindered and subways ground to a halt. The cause of this outage has not been fully determined, but many experts are pointing to a potential cyber attack.

These are just some of 135 industry reported cyber incidents against industrial control systems around the world over the past 4.5 years. While a sobering thought, it is fair to suggest that the majority of plants and control systems that run our critical infrastructure are vulnerable to cyber attack. Unfortunately, many of these organizations have not applied the same level of security thinking to protecting their control systems as they do for their business systems. Ironically, in some cases a plant operator's website is far more protected than the systems running the control network they run

and that nations depend upon.

Differences Between Industrial Control & IT Systems

ICS environments have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses and negative impact to a nation's economy. ICS have different performance and reliability requirements and use operating systems and applications that may be considered unconventional to typical IT support personnel. As a result, ICS and IT systems have differing operating (and risk) profiles:

- In a typical IT system, data confidentiality and integrity are typically of primary concern. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns.

- The primary focus of security in IT systems is protecting the operation of IT assets, whether centralized or distributed, and the information stored on or transmitted between these assets. In some configurations, information centrally stored and processed is more critical and is afforded more protection. For ICS, edge clients (for example, a PLC, operator station, or DCS controller) need to be carefully protected because they are directly responsible for controlling the end processes.

- Control Systems are generally time-critical, and the criteria for acceptable levels of delay are dictated by the individual installation. High throughput is typically not essential to ICS, in contrast to IT systems.

- Many ICS processes are continuous in nature, requiring high availability. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensure high availability for the ICS. In addition to unexpected outages, many control systems cannot be easily stopped and started without affecting production. As a result, the use of typical IT strategies such as rebooting a host are usually not acceptable due to the adverse impact on the requirements for high availability, reliability and maintainability of the ICS.

- ICS operating systems (OSs) and applications may not tolerate typical IT security practices. Legacy ICS systems are especially vulnerable to resource availability and timing disruptions. Control networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware are more difficult to upgrade in an operational control system network. Many control systems may not have security features such as encryption, error logging, and password protection.

- ICS and their real time OSs are often resource-constrained systems that usually do not include typical IT security capabilities. There may not be computing resources available on ICS components to retrofit these systems with current security capabilities (e.g., anti-virus, intrusion prevention, etc.). Additionally, in some instances, third-party security solutions are not feasible due to ICS vendor license and service agreements, and loss of service support can occur if third party applications are installed without vendor acknowledgement or approval.

- Communications protocols and media used by ICS environments for field device control and intra-processor communication are typically quite different from the generic IT environment, and in many cases may be proprietary.

- Patch management - paramount to maintaining the integrity of IT systems – cannot be performed on a timely basis in an ICS environment because these updates need to be thoroughly tested by the vendor of the industrial control application and the end user of the application before being implemented and as a result must be planned and scheduled days or weeks in advance. In addition, many ICSs utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable.

- IT components have a lifetime on the order of 3-5 years, due to the swift evolution of technology. For ICS, where technology has been developed in many cases for very specific use and implementation of the type of plant, the lifetime of the deployed technology is often in the order of 15-20 years and sometimes longer.

- Access control in IT systems can be implemented without significant regard for data flow. For some ICSs, automated response time or system response to human interaction is very critical. For example, requiring password authentication and authorization must not hamper or interfere with emergency actions for ICS. Information flow must not be interrupted or compromised, and access to these systems is restricted by strenuous physical security controls.

- Normally, there is not a physical interaction with the environment in IT systems. ICSs can have very complex interactions with physical processes and consequences in the ICS domain that have a direct impact on physical events. All security functions integrated into the ICS must be rigorously tested to prove that they do not compromise normal ICS functionality.

- Typically, IT components are local and easy to access, while ICS components can be isolated, remote, and may require extensive physical effort to gain access to them.

- The computing resources for ICS (including central processing unit speed and memory) tend to be very limited because these systems were designed to maximize control system resources, with little to no extra capacity for third-party security software. Additionally, in some instances, third-party security solutions are not allowed due to vendor license and service agreements, and a loss of service support can occur if third party applications are installed.

Table 1 below describes the differences in security focus between traditional IT and ICS environments. As a result, the operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cyber security and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS engineers need to understand the reliability impacts of information security technologies before deployment. And some of the OSs and applications running on ICSs may not operate correctly with commercial-off-the-shelf IT cyber security solutions because of specialized ICS environment architectures.

Security Controls	Information Technology (IT)	Industrial Control System (ICS)
Anti-Virus and Mobile Code	Very common; easily deployed and updated	Can be difficult due to ICS impact; legacy systems cannot be modified
Asset Classification	Common practice and performed annually; results drive security expenditure	Only performed when obligated; critical asset protection associated with budget
Change Management	Regular and scheduled; aligned with minimum-use periods	Requires strategic scheduling; non-trivial process due to operational impact
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded capability in systems	Uncommon beyond simple resumption; no forensics beyond event re-creation
Patch Management	Easily defined; enterprise-wide remote and automated	Very long run-up to patch install; device/component specific; potential for performance impact
Physical and Environmental Security	Poor (office systems) to excellent (critical systems)	Excellent (operations centers, guards, gates, etc.)
Secure Systems Development	Integral part of development process	Usually not an integral part of systems development lifecycle
Security Compliance	Limited regulatory oversight	Specific regulatory guidance in some sectors
Security Testing & Audit	Modern methods and processes in place	Testing needs to be tied to system; modern methods inappropriate for ICS
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor

Table 1 - Differences Between IT & ICS Security Controls

Threats to Industrial Control Systems

Cyber events can affect system operations in a variety of ways, some with potentially significant adverse effects in public health, financial viability, or legal actions. For example, cyber attacks could result in the following:

- Sending inaccurate information to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions;
- Changing alarm thresholds or disabling them;
- Interfering with the operation of plant equipment, which can cause modification to safety settings;
- Blocking or delaying the flow of information through ICS networks, which could disrupt ICS operation;
- Making unauthorized changes to programmed instruction in local processors to take control of master-slave relationships between MTU and RTU systems;
- Modifying the ICS software or configuration settings, or infecting ICS software with malware;
- Blocking data or sending false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions;
- Preventing access to account information;
- Overtaxing staff resources due to simultaneous failures of multiple systems; or
- Being used to extort monies or further political aims.

Risk Assessment is Key

So how should plant operators, utilities and government organizations respond in a world where such

a proliferation of threats and vulnerabilities has intensified cyber security risks? While no silver bullet will solve ICS security issues, the core of any security strategy is appropriate risk management.

ICS security specialists should take a holistic, multi-disciplined approach by applying standards-based risk management techniques in order to identify and treat cyber risks and base mitigation solutions on individual threat assessments. Through a process of risk identification and categorization, appropriate mitigating controls can be selected and implemented for treatment.

As is well-known, risk is a function of the likelihood or probability that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact or consequence. The risk induced by any given vulnerability is influenced by a number of inter-related indicators, including:

- Network and computer architecture and conditions;
- Installed countermeasures;
- Technical difficulty of the attack;
- Probability of detection (e.g., amount of time the adversary can remain in contact with the target system/network without detection);
- Likelihood of Attack Success;
- Site Conditions; and
- Consequences of the incident (including cost, safety, national security, loss of life, etc.);

When studying the possible security threats and vulnerabilities, it is easy to get caught in a trap of trying to address issues that are technically interesting, but are ultimately of low risk. With cyber attacks, the technical difficulty of an attack is probably the most critical indicator of possible attack success. This “degree of difficulty” can be broken down as follows:

- Trivial: Little technical skill required
- Moderate: Average cyber hacking skills required
- Difficult: Demands a high degree of technical expertise
- Unlikely: Beyond the known capability of today’s best hackers

After identifying base risk and environmental assumptions, a risk assessment team should brainstorm possible attacker objectives in order to determine all the attacker goals that an intruder might attempt to achieve. The following are typical goals in attacking a SCADA network:

1. Gain SCADA System Access
2. Identify Control Device
3. Disrupt Master-Slave Communications
4. Disable Slave
5. Read Data from Slave
6. Write Data to Slave
7. Program Slave
8. Compromise Slave
9. Disable Master
10. Write Data to Master
11. Compromise Master
12. Denial of Service against a Networked Device
13. Intercept or Modify Data through a Man-in-the-Middle (MITM) Attack
14. Monitor (Sniff) Traffic

A thorough understanding of the risks to network and computing resources from threats and vulnerabilities is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of information assets. Initially, a baseline risk analysis should be performed based on an analysis of threats in order to establish a mitigation strategy; however - due to rapidly changing technology and the emergence of new threats on a daily basis - an ongoing risk assessment/management process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. A fundamental aspect of risk management is the identification of residual risk with a protection strategy in place and the acceptance of that risk by management.

Don't Forget to Test

In addition to brainstorming possible vulnerabilities and attack objectives, ICS and SCADA environments should be subject to independent assessments of critical information systems from an adversary point-of-view. Penetration Testing has been widely accepted as the only way to know for sure if a cyber attacker can actually gain access to ICS systems, aside from a real breach. These testers use the same proven techniques and methodologies that hackers use to gain unauthorized entry to systems, while at the same time, posing absolutely no actual risk to an industrial network or control system. Penetration Testing can be done in collaboration with the engineering staff for "proof of concept" and feasibility of any key vulnerabilities identified.

Like a penetration test, a "Red Team" test is an attempt to gain access by exploiting all vulnerabilities – not only those that are cyber-related. It is a complete attempt to gain access to industrial network and control systems using all or a combination of network vulnerabilities, social engineering, and physical weaknesses. A Red Team test is one of the most comprehensive ways to verify vulnerabilities, threats, and resulting risks inherent in ICS and SCADA systems.

Penetration and Red Team tests are invaluable in identifying and exploiting assumed and unknown vulnerabilities and threats, improving security design, and assisting decision makers with choices in development, security and use of ICS and SCADA.

Vulnerabilities Drive Risk Mitigation

In December of 2006, the North American Electric Reliability Council (NERC) Control Systems Security Working Group identified a list of typical vulnerabilities for control systems. Experienced information security professionals will recognize these ICS vulnerability types as similar to those found in earlier, unsecured IT systems[1]:

1. Inadequate policies and procedures governing control system security.
2. Poorly designed control system networks that a. fail to compartmentalize communication connectivity with corporate networks and other entities outside of the control system electronic security perimeter, b. fail to employ sufficient "defense-in-depth" mechanisms, c. fail to restrict "trusted access" to the control system network, and d. rely on "security through obscurity" as a security mechanism.
3. Mis-configured operating systems and embedded devices that allow unused features and functions to be exploited; untimely implementation of software and firmware patches; and inadequate testing of patches prior to implementation.
4. Use of inappropriate wireless communications.

[1] NERC, *Top 10 Vulnerabilities and Their Associated Mitigations – 2007*

5. Use of non-deterministic communication for command and control such as Internet-based SCADA; inadequate authentication of control system communication protocol traffic.
6. Lack of mechanisms to detect and restrict administrative or maintenance access to control system components; inadequate identification and control of modems installed to facilitate remote access; poor password standards and maintenance practices; and limited use of VPN configurations in control system networks.
7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity among the volumes of appropriate control system traffic.
8. Dual use of critical control system low-bandwidth network paths for non-critical traffic or unauthorized traffic.
9. Lack of appropriate boundary checks in control systems that could lead to "buffer overflow" failures in the control system software itself.
10. Lack of appropriate change management or change control on control system software and patches.

The assessment of vulnerabilities present in an ICS environment is a critical first step in effective risk management. Once such an assessment is complete, a risk mitigation strategy can be crafted that identifies a range of controls that should be implemented. The following actions should be considered:

- Develop policies and procedures that outline personnel security requirements and provide guidance on such areas as passwords and incident response;
- Ensure that network administrators understand security and are kept up to date with on-going security training;
- Apply operating system and application patches as they are made available, always testing for negative impacts on system functionality first;
- Remove all unnecessary applications and services;
- Apply the principle of "least privilege" in granting system access permissions to users and applications and in allowing access to files;
- Plain-text protocols should be eliminated and data validation should be added, where appropriate;
- Segment networks in order to greatly increase security;
- Identify, manage, and monitor all connections into the control system LAN; and
- Use firewalls to segment the network into security zones and add tight, complex rules to allow only necessary communication between network segments.

Conclusion

The threat of cyber attacks, where politically motivated terrorists and financially-motivated malicious insiders and outsiders target critical information control systems to deliberately cause harm, is high on the security agenda for many governments and organizations in charge of public infrastructure around the world.

As industries connect their previously isolated Industrial Control and SCADA systems to larger TCP/IP networks to gain better accessibility and to lower costs, they will also potentially subject these critical industrial controls to higher security risks. As connectivity becomes ever more ubiquitous throughout organizations, it is certain that more ICS security incidents will occur and, given how much of the world's infrastructure they control, they could potentially have serious repercussions. However, merely attempting to sever all connections between the SCADA and business networks may be futile without regularly assessing all connectivity to ensure that no connections between the ICS network and the corporate network appear.

It is imperative that Industrial Control Systems possess strong safety systems and that operators conduct frequent and regular controls-based as well as vulnerability-based security assessments in order to:

- Close risk-related gaps in Governance, Security, and Compliance;
- Review and improve Physical, Operational, and Cyber risk management processes;
- Align security operations that comply with industrial guidelines, regulations, and best practices established by such organizations as ISO, ANSI/ISA, NIST, NERC, etc.;
- Establish robust Incident Response, Disaster Recovery, and Business Continuity Plans; and
- Develop an on-going risk scorecard by providing executive management with an enterprise, metrics-based overview of risks.

In this way, a nation's critical infrastructure will not fall prey to unforeseen security risks such as cyber attacks.

Conveniently located in the Loudoun Technology Center in Sterling, Virginia, Intekras is a privately owned small business, offering integrated solutions in Information Assurance & IT Risk Management, Technical Services and Workforce Development.

Our executive team has over 125 years of combined experience in our core disciplines. Intekras has an outstanding track record in the public sector including DHS, DoD, Navy, Army, HUD, Peace Corps, HHS, OPM and VDOT as well as strong past performance with such companies as Northrop Grumman, Lockheed Martin, SRA International, Raytheon and others. Our private sector experience includes such Global 100 & Fortune 500 companies as Citibank, AOL/Time Warner, Bridgestone and others.

Intekras: bringing insight, innovation and integrity to your business and technology challenges.