

SANS

ANALYST PROGRAM

Sponsored by Industrial Defender

Managing Insiders in Utility Control Environments

**A SANS Whitepaper in Association with
SANS SCADA Summits, Q1, 2011**

Written by Matthew E. Luallen – March, 2011

**Insider Threats to Utility
Control Systems**

Exploiting Trust

**Associating Insider Threats
with Cyber Attacks**

**Regulations, Standards, and
Guidance**

**Protecting Against Insider
Threats**

Advisor: Jonathan Pollet





Abstract

Over the past two years, attackers and saboteurs have unleashed highly public attacks against power control generators, their supply chains and partner organizations. In April of last year, for example, Dark-Reading reported a 30 percent rise in focused attacks against power utilities and a 300 percent rise in incidents against water and wastewater control systems as well. Insiders were responsible for 30 percent of those attacks.¹

Insider threats are also being executed through social engineering techniques, which convince insiders to unwittingly divulge information—a trend expert Gary S. Miliefsky says in Hakin9 Magazine is going to be a growing problem in 2011 and beyond.²

Appropriate controls must be implemented to combat the growing incidence and sophistication of insider threats in utilities environments. However, organizations are facing significant challenges in implementing security controls against the legacy and proprietary systems that are commonplace in the utilities industry.

This paper discusses techniques attackers use to exploit missing insider controls. It also offers a cohesive set of cyber, operational and physical controls to manage a range of user access types for better security and compliance in utility control environments.

¹ www.darkreading.com/insider-threat/167801100/security/attacks-breaches/224400280/index.html

² www.scmagazineus.com/hired-guns-whats-in-the-name-cyberpmc-or-cyberpsc/article/193959/





Insider Threats to Utility Control Systems

The Institute for Information Infrastructure Protection (I3P) has defined an insider as “anyone who has approved access, privilege, or knowledge of information systems, information services and missions.”³ In the case of utility control systems, the definition expands to additional trust relationships with external parties, including:

1. Employees with direct access to the control systems (those who use the systems to manage specific operations)
2. Employees with highly privileged access (system administrators)
3. Employees with indirect access to the system (such as front office staff calling up control data for accounting and administrative reports)
4. Contractors with access to specific systems for production or support operations
5. Service providers with access to specific systems in order to administer or manage them

Consider the relationships when an organization uses contractors or representatives from specific vendors to service its utility control systems. The utility systems under contract interact with a long chain of vendors and suppliers, each representing additional attack vectors into the critical systems that are targeted. An example of service provider dependencies that can provide a pathway for an attack is the electric sector’s Inter-Control Center Communications Protocol (ICCP) trusted links, which, if attacked, could impact a wide range of generation control systems across multiple asset owners.

While most employees are honest, some may have malicious intent, and others may be turned by terrorist organizations or simply duped by a social engineer. For example, unsuspecting personnel may be asked to install software, reveal private keys, carry USB flash drives, perform operations or establish trusted pathways that let an attacker into the system at whatever level that user has access.

In the case of workers with indirect access, employees working in the front office systems are also targets for social engineers who can gain details such as a time of day shift changes, flow reports and other data that can be used to further the intrusion into the control systems.

Shared control and delivery applications are also rendering these once isolated systems more vulnerable to insider threats. For example, businesses leveraging SCADA (Supervisory Control and Data Acquisition) networks inherently have perimeter-less business models in which an outsider can quickly become an insider by entering through the weakest link (e.g., field networks, vendors and the supply chain).

³ How to Protect Digital Assets from Malicious Insiders, I3P and MITRE Corporation
www.thei3p.org/research/mitremi.html





Exploiting Trust

With so many layers of access leading toward and into control systems, organizations need a way to identify who their insiders actually are and set up the appropriate access, monitoring and configuration controls around them. The first step in getting started, then, is to identify who your insiders are and what level of trust they have in the control system network. This will be referred to as the organization's circle of trust and includes personnel, contractors, vendors, customers and critical capital assets. Table 1 provides some examples of organizational trusts and the exploits associated with those trusts.

Tangible Trusts		Exploits
Personnel (Employees, Contractors)	People touching, operating and maintaining control systems directly; or conducting other business operations with indirect access to control systems	Disclosing to the outside (wikileaks/other social media leaks); SEC insider trading; Accidental/social engineering (Stuxnet); or Sabotage (CAL-ISO red button) ⁴
Vendors	Contracted vendors for services, hardware and applications supporting and interacting with control systems	GoToMyHMI.com includes all exploits associated with cloud applications described by the Cloud Security Alliance ⁵ ; PLC programming in shared facilities
Systems and Communications	Trusted communication channels, systems, applications and firmware interacting with control systems	Zigbee local area and cellular wide area communications using KillerBee ⁶ or Software Defined Radios with USRP2s ⁷ (to snoop traffic, attack encryption and more)
Tangible Trusts		Exploits
Personal Lives of Employees, Contractors, Partners	Extended association of control and information to individuals outside of the organization	What they tell others in person, on Facebook, LinkedIn or in the media
Vendor's Supply Chain	Vendor contracts with additional entities for hardware, personnel or applications	PLCs purchased internationally with modified firmware; Vendor contracts with rogue external parties
Asset's Physical Jurisdiction	Governmental rule (nation, state, municipality or any other jurisdictional mandate)	Geopolitical events in the Middle East associated with defined cyber, personnel and operational trusts

Table 1. Trust Associations

⁴ <http://articles.latimes.com/2007/apr/21/business/fi-grid21>
⁵ <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
⁶ <http://code.google.com/p/killerbee/>
⁷ www.ettus.com/products



The goal of this important starting point is to depict a circle of trusted activity during operational states. This trust is continuously earned and maintained throughout the lifecycle of every relationship. For instance, an individual's trustworthiness may be decreased if they travel to specific regions of the world or form additional associations with competitors.

Table 2 is designed to help organizations inventory their trust relationships and prepare for associated insider risks.

Controls	Advice
<p>Assess and inventory all access to networks, systems and specific resources</p> <p>Set a baseline for access, roles and privileges</p> <p>Develop policy for indirect and direct access, including:</p> <ul style="list-style-type: none"> • Strict controls and separation of duties (SOD) for direct access and monitoring of control room operators, administrators and others with direct access • Unidirectional gateways to provide critical real-time data to users needing indirect access without exposing any operations systems to communications initiated by those users. • Monitoring and alerting thresholds for those with direct and indirect access • Additional policies for geopolitical and other conditions that impact employees, contractors and partners working in remote locations 	<ul style="list-style-type: none"> • Inventory all direct and indirect trusts and associations (e.g., personnel, vendors, contractors, supply chain partners). This can be done by monitoring access (including physical access, when relevant) over time. Pay particular attention to those with too much privilege such as administrators, who should not have super access to the entire system contents or use shared passwords. • Monitor systems and networks users are accessing over time for typical behavioral information between these trusts, their applications and their traffic. • Set a baseline with the time-developed monitoring information and information gathered from business units and partners. • Create and use checklists to review and approve trusted interactions (e.g., operations mapped to cyber and physical assets). These checklists can then be translated to policies that will wrap into the overall monitoring program for violations. These lists can also be used to program system, application and network whitelists. • Perform site walk; interview personnel at a vendor's facility. • Ensure sufficiency of personnel and vendor screening. • Review vendor's history of vulnerabilities at http://nvd.nist.gov and ICS-CERT

Table 2. Controlling Trust Relationships





Associating Insider Threats with Cyber Attacks

External attacks against utility control systems also contain insider elements. Using Stuxnet as an example, Table 3 shows how even automated attacks leverage several direct or implied insider trusts.

Tangible Trusts	Tangible Trusts	Exploits
Cyber	Traditional IT hardware supply chain	Two code-signing, private key certificates were stolen from hardware vendors (JMicron Technology Corp and Realtek Semiconductor Corp.).
	SCADA/DCS supply chain	SCADA/DCS equipment can enable exploits (vulnerable firmware, manipulated firmware updates, anonymous ladder-logic reprogramming, PLC rootkit).
Physical	Local technology access (e.g., USB, RF, network)	One vector programmed into Stuxnet requires a trusted insider to connect an infected USB flash drive or system to an interconnected SCADA system
Operations	Systems and users with information access	Extensive as-built details of the environment enable exploits (e.g., programmed centrifugal frequency and ladder logic tags, as well as specific vendor vulnerabilities).

Table 3. Insider Trust Associations Exploited by Stuxnet

Stuxnet exploited the technology hardware supply chain, operating system, inside personnel, SCADA/DCS equipment and contractual trusts. Two excellent demonstrations of these trust exploitations are available on Youtube by Joel Langill, Control Systems Security Consultant (alias SCADAhacker).⁸

⁸ www.youtube.com/user/SCADAhacker





Regulations, Standards and Guidance

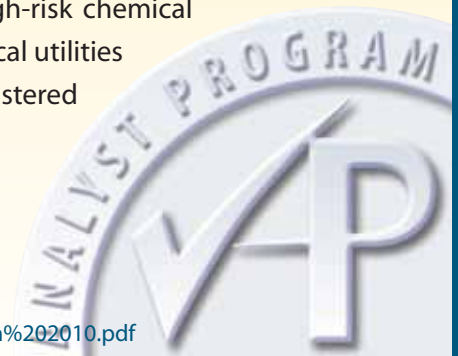
Governments and private organizations around the world have collaborated to develop regulations, standards and guidelines to deploy physical, operational and cyber security controls in and around the automated environment of critical control systems. These include:

- American Gas Association (AGA)
- Federal Information Processing Standards (FIPS)
- International Society of Automation (ISA) 99 Standards
- Chemical Information Technology Center (ChemITC) Guidance
- Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27
- American Petroleum Institute (API) Guidelines
- International Electrotechnical Commission (IEC) Data and Communications Security [IEC 62351]
- Institute of Electrical & Electronics Engineers (IEEE) Guide for Electric Power Substation Physical and Electronic Security [IEEE 1402]
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 2
- International Organization for Standardization [ISO 17799/27001]
- National Institute of Standards and Technology (NIST) Special Publication 800-53
- Office of Nuclear and Regulatory Research Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities.

To compare recommendations in the various standards, the Department of Homeland Security (DHS) “Catalog of Control Systems Security: Recommendations for Standards Developers” contains a useful appendix comparing these documents.⁹ The catalog does not reflect the rapid modifications to the NERC CIP reliability standards (e.g., Versions 3 and 4); the recent DHS CFATS RBSP Guidance; the recent nuclear regulations; or newer IEEE, ISO and IEC standards. However, none of the standards except NIST 800-53 Revision 3 are interpreted to have controls for trustworthiness or covert channel analysis.

The CFATS 6 CFR Part 27 and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards represent the most mature requirements due to their strict enforcement programs. CFATS directly applies to over 6,000 high-risk chemical facilities, whereas NERC CIP is prescribed for approximately 1,500 electrical utilities in the United States. The NERC CIP reliability standards apply to NERC-registered entities in the United States, Canada and Mexico.

⁹ www.us-cert.gov/control_systems/pdf/Catalog%20of%20Recommendations%20March%202010.pdf



These regulations call for controls around the critical cyber assets supporting identified critical Bulk Electric System (BES) facilities and Chemicals of Interest (COI). The regulations include controls for screening of personnel, training and awareness, defining physical perimeters, securing cyber assets, monitoring and identifying security events and responding to incidents. As with the NERC CIP reliability standards, CFATS standards are open to interpretation as to their implementation methods.

Electric utilities should also review their operations associated with other requirements contained within protective relay and control (PRC), emergency preparedness and operations (EPO), communications (COM), personnel (PER), modeling, data and analysis (MOD), and facilities design, connections, and maintenance (FAC) reliability standards. These NERC reliability standards include information pertaining to control system components and communications during normal and emergency operations, modeling, facilities and personnel training. The asset owners and NERC should provide additional guidance pertaining to the specific security alignment between NERC CIP and these other operational standards to aid in mitigating the insider threat.





Protecting Against Insider Threats

Many physical, operational and cyber controls are being tailored to bridge the gaps between old, proprietary utility control systems and new security monitoring and management tools. This section provides recommendations based on specific roles, supply chain, cyber assets and psychosocial profiling.

Regardless of user's level of trust, some basic controls apply to most trust groups, although they must be applied differently. These include:

1. Assessment of networks, systems, applications and access (as defined in Table 2)
2. Access controls and authentication
3. Application whitelisting
4. Monitoring for compliance, vulnerabilities, access (including physical), suspicious behavior, new system attempts to connect, and so on
5. Centralized management of security information and events, including alerts, reports and dashboards for drill down

These controls are broken down into more detail in the following sections.



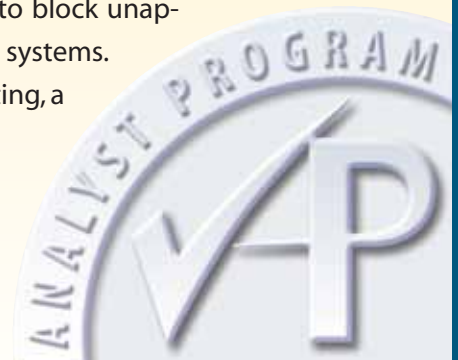
Users with Direct Access to Control Systems: Personnel and Control System Vendors

In addition to thorough background checks and education of employees and contractors working directly with control systems, strict procedures must be followed for granting access to facilities and cyber assets. These procedures should include documenting all administrator and shared accounts and vendor default accounts. Procedures should also include a two-person rule for specific changes, assignment of unique user accounts using multifactor authentication, and immediate revocation of access for cause.

Specific access rights to control systems, administration and documentation containing operating procedures, blueprints, ladder logic and the configuration of special protection and control systems should be limited by the principle of least privilege and separation of duties.

End point protections on the servers and control consoles are also critical to prevent Stuxnet-like intrusion from insiders purposefully or haplessly installing malware from USB drives (or from installing external attack code that made it into the control network). Rather than blocking all USB drives (some may be required for field workers, for example), an easier control would be to block unapproved communications or applications from running on the protected systems.

This can be achieved through communications and application whitelisting, a mature technology embedded into many end point monitoring suites.



These end points, then, should also be monitored for security state, attempted access violations, malicious behavior and vulnerabilities. Control networks should also be protected with advanced communication profiling technologies that can capture attempts at sending critical data and commands through uncommon network paths.

Tools exist to monitor all of these areas, and they have also matured to the degree that some suites are available to manage all or most of these monitoring needs under one management dashboard in the form of SIEM (Security Information and Event Management) or log management systems.

Such monitoring technologies also are introducing capabilities to integrate with physical security to analyze events. For example, when entering facilities, control system personnel swipe badges, initiating a monitoring sequence that follows the operator to specific buildings, rooms and workstations. This access should be automatically validated, logged and video-monitored by the physical security systems being accessed, and then compared against the employee's approved work schedule and the correct sequence of success and failure events. For instance, the shift operator would be denied access if he where to attempt to log into the workstation prior to physically entering the facility or control room.

With the proper monitoring and controls, remote access to field equipment can also be locally controlled by control room operators using SCADA points so that the managing operator is not only aware of the access, but also has control of the access. Completing the lifecycle, terminated personnel should have their electronic and physical credentials immediately revoked, preferably automatically through the access management system.

Users with Indirect Access to Control Systems: Staff, Partners, Customers

To begin with, direct bidirectional access from indirect employees and partners should never be allowed unless absolutely required (such as in the case of an emergency operating condition, and even then, access should be allowed only to the specific area of the system the partner is responsible for).

Unidirectional gateways transfer valuable data from control networks to external networks using a hardware mechanism, which makes reverse communications impossible. On the sending side of the gateway, in the control network, the gateway uses conventional operations protocols to acquire real-time data from systems and devices in the control network. On the receiving side of the gateway, in the external network, the gateway provides that real-time data to external, less-trusted users through conventional communications protocols. Inside the gateway, information can flow only from the control network to the external network.

Modern gateway solutions can keep external copies of real-time data up to date with latency penalties of only milliseconds. This means that when a front office worker, optimization engineer, or business partner requests real-time data, they are not accessing the control system directly, but still have access to timely copies of the real-time data needed to meet their business objectives.





Prevention and Detection for Supply Chain

When acquiring a new control system, review the environment in which the programming occurs, and examine the vendor's circle of trust. Review the vendor's security controls and perform vulnerability assessments during Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT). Do not assume anything pertaining to their environments, because many are located in shared facilities where even unintentionally a network file share or USB flash drive installation may spread across multiple asset owners' systems. Vendor personnel may also span the globe and multiple jurisdictions, some of which may represent stronger insider threats.

Screening of the vendor's personnel working with your system should be performed by your screening mechanisms, not the vendor's. Additionally, the staff should be required to learn policies and operating procedures that apply to your organizational needs, not the vendor's. Finally, if a vendor provides any test equipment for your environment, ensure its trustworthiness. Many vendors migrate test and demonstration equipment from customer to customer, potentially exposing your systems to a previous exploited environment.



Prevention and Detection for Cyber Assets

SCADA hardware and systems must adhere to strict change controls, integrated and centralized event monitoring, and well-defined trusted physical and logical perimeter controls. Change controls must include procedures for commissioning new cyber assets, modifying existing cyber assets and decommissioning existing cyber assets. Once a modification is approved, it should be tested prior to implementation. Any unapproved modifications or anomalous events should be detected by an integrated event monitoring system (a SIEM or log manager) and should include a direct association to the specific user who made the change or was operating/transmitting through the cyber asset at the time of the event.

The cyber assets must reside in a logical trusted perimeter using an advanced firewall with integrated intrusion prevention and malware signatures. Prior to exiting the logical perimeter, the cyber assets and their communication media should be protected with a six-wall border to limit physical tampering with the systems and media. If routine remote access is necessary, jump hosts should be used to limit and monitor network and application interactions. Jump host remote connections should be limited to specific physical and logical locations based upon current physical GPS location, logical IP address and geopolitical situations.

Rogue communication detection devices should be used to identify the attempt to setup new systems, connectivity, applications and wireless provisioning. This requires maintaining a list of all approved cyber assets, their connectivity (wired or wireless) and communication profiles between SCADA devices.

The system health of each cyber asset should be monitored for suspected system use of memory, CPU and number of network connections. Upon decommissioning of the cyber asset, all media containing sensitive information should be physically destroyed.





Psychosocial Profiling and Situational Awareness

The Pacific Northwest National Laboratory¹⁰ (US DOE Research Laboratory) recommends using both cyber and psychosocial mechanisms to further investigate and prevent insider abuse. These tools include receiving vulnerability announcements and maintaining associations with organizations such as US ICS-CERT, NERC, United States Secret Service, the FBI, DHS, the SANS Institute, High Technology Crime Investigation Association, local law enforcement, and hardware and software vendors. External personnel monitoring can be accomplished through content analysis of social media (e.g., LinkedIn, Facebook, Twitter, Youtube) using tools such as Maltego and content scraping and search engines like Devon Technologies. Critical vendor partners should also be monitored for new business relationships, financial results, organizational changes and governmental associations.

For additional help, the University of Nebraska, with funding from the Department of Defense Counterintelligence Field Activity Office, describes numerous suspicious personnel behaviors, which may serve as indicators of an insider threat.¹¹ Behaviors particularly tied to insider threat include IT/technical violations, disloyalty, threatening or intimidating behavior, financial malfeasance, misuse of travel, and suspicious foreign contacts.

Finally, plans should also include emergency operating conditions that must be dealt with separately as they occur. Guidance is currently being drafted for electric utilities by NERC and the industry through the Severe Impact Resilience Task Force (SIRTF).¹²

¹⁰ www.pnl.gov/coginformatics/media/pdf/TR-PACMAN-65204.pdf

¹¹ <http://ppc.nebraska.edu/userfiles/file/Documents/projects/ThreatAssessment/BehavScienceGuidelinesforInsiderThreat.pdf>

¹² www.nerc.com/news_pr.php?npr=727





Summary

Preventing and detecting insider abuse is the ultimate challenge in today's critical control networks. The starting point for most organizations is to define who their insiders are, including employees, contractors, vendors and partners.

The steps to take after identifying that circle of trust can be incremental, starting with fully engaging the systems and controls already in use and expanding to comprehensively monitor, protect and manage access to critical utility control systems. These systems need to start with intelligent perimeters between control systems and indirect access for the rest of the circle of trust. Other controls at the end point (such as application whitelisting, USB controls and configuration/asset management) and on the network (advanced monitoring of access and traffic), as well as physical security protections all need to be centralized and integrated, likely through SIEM or log management system interfaces.

Ultimately, protection against insiders should be self-learning and able to help improve risk management around critical control systems for a stronger national infrastructure. Protection should also mature so that it can even enhance productivity through simplified and predictable operations.





Appendix A: Reference Guide

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors United States Secret Service and CERT Program at Carnegie Mellon University

www.cert.org/archive/pdf/insidercross051105.pdf

What Works in Implementing the 20 Critical Security Controls & SANS Cyber Attack Threat Map SANS Institute

www.sans.org/whatworks/20-critical-controls-poster-062010.pdf

Stuxnet Dossier

www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Risk-Based Performance Standards Guidance Chemical Facility Anti-Terrorism Standards (May 2009)

www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment

David Albright, Paul Brannan, and Christina Walrond, Institute for Science and International Security

http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Project DATES DistribuTech 2010 Demo, March 23-25, 2010

SRI International, ArcSight, Sandia National Laboratory

www.csl.sri.com/projects/dates/distributech.html

The Insider Threat to U.S. Government Information Systems (July 1999)

Michael Hayden, National Security Agency

<http://handle.dtic.mil/100.2/ADA406622>

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

M. Bishop and D. Frincke, "A Human Endeavor: Lessons from Shakespeare and Beyond," IEEE Security & Privacy Magazine, 3(4) pp. 49–51 (July 2005).

<http://nob.cs.ucdavis.edu/bishop/papers/2005-spcolv3n4/human.pdf>

Front Companies: Who Is the End User?

Defense Security Service (DSS), Department of Defense

www.dss.mil/isp/count_intell/front_comp_who_user.html

Chemical Facility Anti-Terrorism Standards Overview for Law Enforcement, January 2011

Patrick Coyle, Chemical Facility Security Specialist

http://leaps.tv/go-LEAPSTVprogramdescription.php?program_code=201102161300

NERC Critical Infrastructure Protection Reliability Standards CIP-001 through CIP-009

www.nerc.com/page.php?cid=2|20

Office of Nuclear and Regulatory Research Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities.

<http://nrc-stp.ornl.gov/slo/regguide571.pdf>

Department of Homeland Security Catalog of Control Systems Security: Recommendations for Standards Developers

www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf



About the Author

Matthew E. Luallen is founder of CYBATI, a critical infrastructure and control system security consulting company. Mr. Luallen has been strategically and tactically involved with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards and the DHS CFATS (Department of Homeland Security Chemical Facility Anti-Terrorism Standards) cyber controls.

He has also provided cybersecurity consulting and instruction for a variety of public and private organizations, including healthcare, financial, government, utility, and educational institutions.

Mr. Luallen holds a Bachelor's degree in industrial engineering from the University of Illinois at Urbana-Champaign and a Master's degree in computer science from National Technological University. He serves as adjunct faculty for DePaul University's capstone cybersecurity and control system courses. He is a 10-year CISSP, an 11-year CCIE and certified instructor for Cisco Systems, and a certified instructor for the SANS Institute. Mr. Luallen is also the author of a new two- to four-day onsite hands-on control system cybersecurity course.



SANS would like to thank this paper's sponsor

