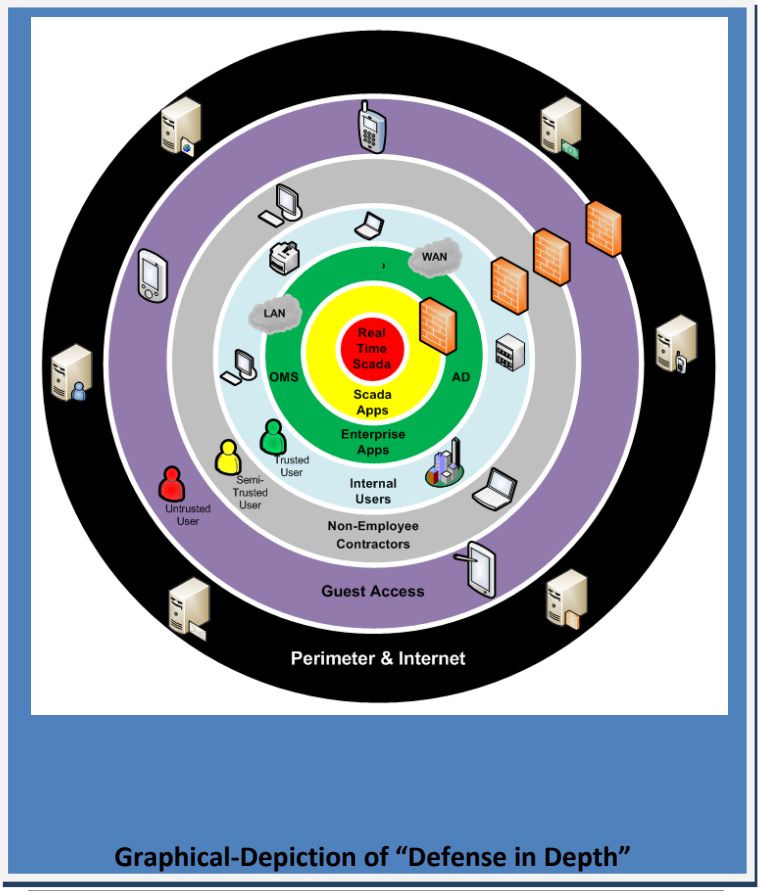
American Gas Association

Protecting the Nation's Natural Gas Pipeline SCADA Infrastructure: Focus on Cybersecurity

Natural gas utilities and pipelines actively engage in cybersecurity management, with the primary objectives to minimize cyber vulnerabilities and increase the system's ability to detect malicious cyber traffic, mitigate impact, and implement security measures so to not disrupt the safe and reliable delivery of natural gas to customers.

Cybersecurity effectiveness in the natural gas industry is maximized in the diversity of the protective approaches, while achieving the same overall objectives. In general, operators across the industry use the "defense in depth" strategy to protect their control systems. This military strategy, adapted to cybersecurity defense, seeks to delay rather than prevent the advance of an attacker and entails the "layering" of tools and mechanisms as appropriate for the particular operating system so to protect against, detect, and mitigate compromise. This strategy begins with corporate cybersecurity governance consisting of policies, standards and guidelines designed to protect Supervisory Control and Data Acquisition (SCADA) systems. Constantly changing risks are regularly assessed and mitigated.



Graphical-Depiction of "Defense in Depth"

Acronym/Abbreviation Key:

Apps – applications	AD – Active Directory
LAN – Local Area Network	OMS – Outage Management System

SCADA consists of software and hardware for system operations. SCADA monitors critical data from sensors in local and remote locations and sends the compiled data to a central computer for a human operator to analyze and to determine if signals need to be sent out to control field equipment and pipeline conditions. The introduction of SCADA technology to natural gas operations significantly increased natural gas delivery efficiency, reliability, and safety.

The information below highlights cybersecurity measures taken by natural gas operators to ensure their SCADA systems are safe.

POLICY

The first step in establishing a comprehensive, robust cybersecurity program is the development of a security policy that accounts for operational system criteria and limitations. The following list identifies a sample of cybersecurity policy components found in various operators' programs across the Nation:

- Security awareness
- Specialized security training on control systems
- Personnel background checks
- Zero-tolerance policy enforcement
- Alert and incident management/response
- Email filtering and quarantine
- Configuration and change management, e.g., strict processes for granting, modifying and terminating access to applications and systems
- Electronic access control, e.g., strict password criteria; account login lockout; no email and Internet on SCADA systems

PREVENTION

ACCESS CONTROL

Access control refers to authorized and unauthorized access to SCADA systems. Examples of access control mechanisms in use include:

- Remote access through strictly regulated software controls and multi-level user log-on credentials
- User's rights assignment based on principle of *Least Privilege*, i.e., users' access defined by job function and authorization granted on a "need to know" basis
- Human connection to SCADA system from beyond control room regulated by policies that deny email and internet access from the SCADA system and prevent connection of unauthorized hardware and software to control system network
- SCADA password management
- Log-on activity tracking and audit trails

ASSESSMENTS

Assessments provide the knowledge needed to determine vulnerabilities, acceptable risks, and what should be protected. Assessments performed and a variety of related programs include:

- Risk and vulnerability assessments routinely conducted by internal and by external security experts
- Penetration tests of internal assets performed on external connections to identify and remove potential opportunities for attack
- Audits routinely conducted by internal and external security experts
- Partnerships with federal and state governments, e.g., DHS TSA onsite review of cyber security posture, and state public utility commission onsite assessments

ISOLATION

Isolation is the intentional compartmentalization of network architecture to limit cyberattacks from proliferating throughout a system. Access is generally centralized to provide limited points of egress and ingress. Below are examples of how this is achieved:

- SCADA system located on separate network from the corporate network as a result of 'air gaps' (physical isolation) and/or communication links dedicated solely to SCADA
- Internal and external firewalls that isolate the SCADA network and devices from the corporate network
- Multiple access layers protect access to gas control system applications
- SCADA data traffic encryption
- Removal of unnecessary access points to the SCADA network
- No internet access on SCADA system

DETECTION

Detection is an ongoing process achieved through virus protection, monitoring, and intrusion prevention systems. Success is bolstered through the layering of detection products and related software applications. The following list identifies examples of mechanisms in use:

- Virus scans regularly updated, implemented, and tested for possible gaps
- Intrusion prevention and detection systems that look for signatures or identifiers in data that have the potential to cause harm
- Security logs actively monitored to identify security anomalies
- Contact from DHS when abnormal cyberactivity noted targeting industry or particular operating systems
- 'Whitelisting' identifies entities, applications and/or users pre-approved by the operator to access the system
- Firewalls monitored for attempted access to internet sites
- Network behavioral analysis tools designed to spot traffic flow patterns indicative of malicious behavior

MITIGATION

Mitigation encompasses actions and measures taken to lessen the impact of compromise. The type of mitigation techniques deployed depends upon the specific operational criteria of the control system. The following is a sample of mitigation activities deployed by various operators across the industry.

- Default System Account Management Process – removes, disables, or renames default system accounts that were set-up by the manufacturer, not-specified by the operator
- Indicator and mitigation advisories issued by the DHS, ICS-CERT, media reports or other potential threats are jointly reviewed by company IT security and gas control departments
- Patch Management Process – actively seeks, applies and keeps current software security patches to address detected vulnerabilities
- All ports and services not needed for operations shut off
- Firewall ports that can be used to communicate with the Internet disabled

RESPONSE & CONTINGENCY PLANNING

Data centers have redundant power and controls. Contingency and rapid recovery planning further protects critical applications. Facilities use and regularly test automatic redundant or standby capabilities, including but not limited to,

- Redundant communications interfaces to gas control centers
- Redundant isolated paths for electric power into the control room and critical cyber asset areas
- Multiple electric power sources for control centers and critical cyber asset areas
- Written procedures for responding to varying levels of critical incidents

TRAINING & AWARENESS

Cybersecurity program effectiveness starts with employee training and awareness of cybersecurity risks and how they may be used by the perpetrator to gain unauthorized access to the control system network. The following list identifies a sample of activities, which help increase employee and overall corporate awareness.

- Employee training and awareness programs
- Internal cybersecurity teams participate in multi-industry working groups to share threat information and mitigation strategies
- Internal company intelligence groups monitor cyber activities and policy
- Internal cybersecurity teams have access to classified cyber threat information through DHS sponsored SECRET level security clearances
- Regular information security training modules for all employees
- Cybersecurity issues discussed internally at all levels of organizations (including senior management and boards of directors), and communicated to applicable operating groups for security awareness and mitigation
- Timely information sharing through advisories, alerts and briefings (classified and unclassified) with government intelligence community
- Information exchange in industry-led workshops

GUIDELINES/STANDARDS

Gas utilities and transmission operators apply a myriad of cyber standards, guidelines, and regulatory practices from other industries in their cybersecurity portfolio. The following is a list of such references used within the natural gas industry.

- American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*
- *AGA Report 12 – Part I, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*
- AGA and Interstate Natural Gas Association of America (INGAA), *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, (May 2008)
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-CDV3, *Enterprise-Control System Integration Part 1: Models and Terminology,* (2008)
- American Petroleum Institute (API) & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum & Petrochemical Industries*
- API, *Security Guidelines for the Petroleum Industry*, (April 2005)
- API, *Standard for Third Party Network Connectivity*, (November 2007)
- API Standard 1164*, Pipeline SCADA Security*, (June 2009)
- ANSI/ISA0-99.00.01-2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models,* (Oct. 2007)
- ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- DHS Control Systems Security Program, *Cyber Security Evaluation Tool* (CSET)
- International Organization for Standardization (ISO) and International Electrochemical Commission (IEC), *17799/27001/27002, Information technology - Security techniques - Code of Practice for Information Security Management*
- INGAA, *Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry*, (Mar. 2011)
- National Institute of Standards and Technology (NIST) SP 800 series
- North American Electric Reliability Corporation (NERC), NERC-CIP Standards
- The Whitehouse, National Strategy to Secure Cyberspace (Feb. 2003)
- U.S. Department of Energy (DOE), Office of Cyber Security, Computer Incident Advisory Capability
- DOE, *21 Steps to Improve Cyber Security of SCADA Networks*
- DHS, *National Infrastructure Protection Plan,* (2009)
- DHS, National Cyber Security Division, *Catalog of Control Systems Security: Recommendations for Standards Developers,* (Jun. 2010)
- DHS, National Cyber Security Division, *Cyber Security Procurement Language for Control Systems Security*, (Sep. 2009)
- U.S. DHS Transportation Security Administration (TSA), *Pipeline Security Guidelines*, (Dec. 2010)

- U.S. General Accounting Office (GAO)-04-321, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection,* (May 2004)
- U.S. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* (Mar. 2004)

PHYSICAL SECURITY MEASURES

Physical security measures are deployed at gas control and SCADA data centers to protect against physical intrusion. Measures vary depending upon facility location and construction. In general, access is restricted and regularly reviewed. Sample measures as reported by AGA gas utility and transmission companies include.

- Access only available through secure primary and secondary control rooms
- Restricted physical badge access
- Identification card reader
- Cameras and closed circuit TV
- Security guard presence and monitoring
- Biometric scanners at the most sensitive areas of cyber assets and gas operations
- SCADA systems physically protected by electronic locks
- Vehicle traps, blast walls, and reinforced structures at building entrances
- Multiple secured doors protected by individually programmed card readers
- Physical segmentation of Control System network from the corporate networks

ELECTRONIC APPLICATIONS

As cybersecurity risks and threats change, so do vulnerabilities. Ongoing implementation of new tools and capabilities is vital to adapting to the dynamic cyber environment. For instance, operators are implementing or evaluating the application of *whitelisting* technology (i.e., all access control is pre-approved by the operator) in SCADA environments. The following is a sample of cyberprotection operating system applications used by gas pipeline and utility companies. The diversity in the deployment of electronic applications and tools bolsters the overall gas utility cybersecurity posture.

- Encrypted communications between field equipment and remote devices
- Proprietary SCADA data communication protocols
- Virtual Private Networks - establish encrypted data tunnels over internal and external networks
- Dedicated Wide Area Networks (WAN)
- Intrusion detection through network monitoring, configuration management, and antivirus software at the network perimeter
- Host intrusion prevention software - identifies and stops anomalous behavior
- Encrypted mobile assets (i.e., laptops)
- Security Patch Management – deployment of cybersecurity software patches depending on threat to address vendor software and hardware vulnerabilities
- Multiple factor authentication – requires user to satisfy login credentials, such as knowing something (e.g., a password or pin) and have something (i.e. a token or other device) prior to granting access
- Biometrics (e.g., fingerprint analysis, eyescan, etc.)
- Firewalls used internally to further isolate sensitive applications and systems.