American Gas Association

A Publication for AGA Members

Prepared by the AGA Operations Section
Natural Gas Security Committee –
Physical Security Subcommittee
400 North Capitol St., N.W., Suite 450
Washington, DC 20001
U.S.A.
Phone: (202) 824-7000
Fax: (202) 824-7082
Web site: www.aga.org

Emerging Technologies for Securing Remote Locations

PREFACE

AGA would like to extend a special thank you to the AGA Natural Gas Security Committee Emerging Technologies Task Group chaired by Matt Miller of Dominion Energy West. Members of the Task Group included, Pete Grandgeorge (Berkshire Hathaway) , Paul Gustafson (National Fuel), Jason Hatfield (NiSource), Wade Hardy (Consolidated Edison of NY), Jonathan Harrison (Southern Star Central), Kathy Judge (National Grid), Dennis Laughlin (Black Hills Corp.), John Malaer (Enbridge), Brian Markus (Duke Energy), Al Moore (Spire Inc.), Jodi Nicalek (National Grid), Mike Ruffalo (South Jersey Industries), Greg Robinson (Chesapeake Utilities), and David Sellen (Southwest Gas).

DISCLAIMER

The American Gas Association's (AGA) Operations and Engineering Section provides a forum for industry experts to bring their collective knowledge together to improve the state of the art in the areas of operating, engineering and technological aspects of producing, gathering, transporting, storing, distributing, measuring and utilizing natural gas.

Through its publications, of which this is one, AGA provides for the exchange of information within the natural gas industry and scientific, trade and governmental organizations. Many AGA publications are prepared or sponsored by an AGA Operations and Engineering Section technical committee. While AGA may administer the process, neither AGA nor the technical committee independently tests, evaluates or verifies the accuracy of any information or the soundness of any judgments contained therein.

AGA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of or reliance on AGA publications. AGA makes no guaranty or warranty as to the accuracy and completeness of any information published therein. The information contained therein is provided on an "as is" basis and AGA makes no representations or warranties including any expressed or implied warranty of merchantability or fitness for a particular purpose.

In issuing and making this document available, AGA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is AGA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

AGA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does AGA list, certify, test or inspect products, designs or installations for compliance with this document. Any certification or other statement of compliance is solely the responsibility of the certifier or maker of the statement.

AGA does not take any position with respect to the validity of any patent rights asserted in connection with any items that are mentioned in or are the subject of AGA publications, and AGA disclaims liability for the infringement of any patent resulting from the use of or reliance on its publications. Users of these publications are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Users of this publication should consult applicable federal, state and local laws and regulations. AGA does not, through its publications intend to urge action that is not in compliance with applicable laws, and its publications may not be construed as doing so.

Changes to this document may become necessary from time to time. If changes are believed appropriate by any person or entity, such suggested changes should be communicated to AGA in writing and sent to: ***Operations & Engineering Section, American Gas Association, 400 North Capitol Street, NW, Suite 450, Washington, DC 20001, U.S.A. Suggested changes must include: contact information, including name, address and any corporate affiliation; full name of the document; suggested revisions to the text of the document; the rationale for the suggested revisions; and permission to use the suggested revisions in an amended publication of the document.***

Audience

This document is intended for those individuals with responsibilities for conducting risk/vulnerability assessments, security technical support, compliance personnel/team (to address security requirements), owners/operators of critical infrastructure, owners/operators of facilities in general (e.g., maintenance, construction projects, etc.).

Objective

The objective of this technical note is to provide operators with information related to emerging technologies that enable them to protect company assets remotely. This technical note assumes operators have conducted criticality, vulnerability, and threat assessments to determine risk for facilities under consideration for remote security technologies. This technical note further assumes operators have reviewed and understand physical security requirements relevant to industry standards and company operations. This technical note provides insights into types of technologies that may be utilized to secure operator facilities and/or assets, to include remote locations. This technical note does not articulate the physical security assessment process. The need to implement every practice and the timing of any implementation of the practices described in this document will vary with each natural gas utility and their specific operations. Therefore, not all of the practices described in this document will be applicable to all operators. As used herein, the term "should" is not mandatory but is to be acted upon as appropriate.

Physical security is best achieved when a layered approach is utilized. This technical note addresses multiple layers of emerging technologies (i.e. perimeter/intrusion detection, access control, video management, mapping/adjudication software, security operations centers, etc.) for the operator to consider. By developing and sharing through this technical note leading industry practices in emerging technologies, industry operators will be better prepared to protect the Nation's critical gas infrastructure.

Considerations

1. Maintenance

Technology changes and improves at a rapid pace. This technical note serves as a baseline; operators are encouraged to meet with vendors and security integrators on a regular basis to ensure technology considered for deployment at facilities are appropriate and adequate for specific operator requirements.

2. Cybersecurity

Internal cybersecurity teams should be consulted in the design and planning stage as well as prior to testing electronic devices on the corporate infrastructure. Supply chain cyber integrity and cyber practices of service providers should be considered. Consult with your corporate professional responsible for the cybersecurity of operation technology.

Different Types of Communication – Redundancies & Connectivity

Alarm output may be local, remote, or a combination. Remote alarm systems are used to connect the control unit to a predetermined monitor. High-end systems connect to a central station via a direct phone wire, a cellular network, a radio network (i.e. GPRS/GSM), or an internet protocol (IP) path. In the case of a dual signaling system, two of these options are utilized simultaneously.

Alarm monitoring includes not only the sensors but also the communication transmitter, itself. While direct phone circuits are still available in some areas from phone companies, they are becoming less common due to their cost and the advent of dual signaling. Direct connections are now typically seen only in federal, state, and local government buildings, or on a school campus that has a dedicated security, police, fire, or emergency medical team.

More typical alarm monitoring systems incorporate a digital cellular communication unit that will contact the central station via the Public Switched Telephone Network (PSTN) and raise the alarm. A dual signaling system would raise the alarm wirelessly via a radio path, e.g., General Packet Radio Service (GPRS) or global system for mobile communications (GSM), or through a cellular path using the phone line or broadband line as a back-up to overcome compromise to the phone line. Many alarm panels are equipped with a back-up communication path for use when the primary PSTN circuit is not functioning. In some cases, where a remote building may not have PSTN phone service, and the cost of trenching and running a direct line may be prohibitive, it may be possible to use a wireless cellular or radio device as the primary communication method.

1. Modes of Connectivity

a. Cellular
b. Microwave
c. Fiber
d. T1
e. Satellite
f. Internet

2. Redundancies

a. Utility Power as First Option
b. Generator Power Back-Ups
c. Back-Up System/Site/Mechanisms – if one fails, operations can be run off of secondary system; active stand-by (coop – continuous operation plan); fail-over site; back up system that is independent of the primary security system; high-visibility fail-over
d. Batteries
    i. Each access control boards have battery power (keeps current information functioning until update)
    ii. UPS – uninterrupted power supply – can run a site system for extended period off of battery
    iii. Solar panels to charge batteries for remote security cameras on trailers

Alarm Technology – Software & Mapping Platforms and End-devices

In an industry where operators have multiple facilities equipped with security systems – often in rural/remote locations – alarm management and adjudication are critical. Ideally, operators have an established and operating security operations center (SOC) where security system alarms are monitored and adjudicated. Access control and video management systems can serve as primary platforms for alarm management of end devices and security system mapping. It is common for larger access control and video management software to integrate with one another. In the event integration has not been established between access control and video management software systems, the parallel system for integrating impact models and sectors (pSIMS) can be utilized to integrate such systems.

The incorporation of integrated mapping tools/software can be beneficial for alarm management and adjudication. Icons can be created for end devices, placed on a facility map, and incorporated into the operator's alarm management platform. Mapping software may also allow for the incorporation of on-screen instructions for SOC operators to follow for each type of alarm received. Additionally, mapping software may allow for the incorporation of on-screen contact information for facility management, emergency responders, etc., relative to a specific facility. Security systems, platforms, software, and end devices continue to evolve and improve at a rapid rate. Operators are encouraged to seek out, review, and evaluate such devices on a continuous basis.

1. Mapping Software

a. Access control platform for access control and intrusion detection
b. Alarms may come into SOC as an identified point on a map
c. May help adjudicate and mitigate alarms
d. May include point of contact and response instructions
e. Possible features for multi-state territory:
    i. Geo-fencing – may be used to provide alert; triggered when anything unusual to the normal environment
    ii. Social-media monitoring – identify geographic region and social media monitoring of that region
    iii. Mapping software/capabilities – often available on AC systems and Vendor Management System (VMS)

2. Intrusion Detection Devices

Intrusion detection devices provide early detection of unauthorized persons or vehicles into an area. These can be single devices or technology that work alone or in-tandem with other devices. The capability sought should provide a sphere/boundary around the area to be protected using integrated technology to detect intrusion by surface, air, underwater, or underground. Desirable capabilities are detailed below.

a. Seismic detection
b. Communication into remote locations – e.g., speaker, bullhorn, "automated intrusion alarm system"; live communication; talk-down features ("voice of god")
c. Traditional fence disturbance/detection – may be passive or active technology, depending on weather and terrain conditions, to detect climbing or cutting of fence structure.
    i. Measures should be employed to reduce nuisance alarms, as well as integration with other technology to detect or deny options to bypass fence detection devices (tunneling, above crossing, etc.)
    ii. Fence-mounted cabling that captures variations of movement on a fence. Programing may allow for adjustments in sensitivity to cutting, climbing, lifting, and vibrations along the fence. Programming may allow for integration with video management systems and mapping software for adjudication.
d. Virtual fence provides an invisible-to-the-eye, line-of-sight beam – typically infrared, laser or microwave technology, which detects a disturbance based on an object breaking the beam. Programming may allow for integration with video management systems and mapping software for adjudication.
    i. Microwave sensors generate an electromagnetic field between transmitter and receiver. This creates an invisible detection zone. Programming and integration may be available.
    ii. In newer technology, artificial intelligence (AI) exists that can further detect the type of object breaking the beam, which reduces false alarms. As with other detection technologies, this works best when integrated with other detection devices.
e. Ground radar – a surveillance and detection technology often utilized for large detection areas/zones.
    i. Provides real-time surveillance and detection. Programming may allow for target classification and area masking.
    ii. Programming may allow for integration with video management systems and mapping software for adjudication.
f. Thermal imaging – picks up heat sources and has combo camera that follows heat sources; can mask out unnecessary images (such as racoons, etc.); capable of creating detection perimeters, image radar (IR) video.
g. Cameras & Video analytics
    i. Gate stations
    ii. Regulator stations, if critical facility
    iii. Remote camera
    iv. Video management system in the camera – acts like a VMS

h. Gunshot detection
    i. In-camera technologies / dual-sensing capabilities
    ii. Mass notification integration (e.g., email, text, warning lights, 911, etc.)
i. Wireless alarms on gates
    - Virtual fencing – IR sensors in ground; certain height for detection and certain width for detection
j. Motion sensors
    - Microwave
k. Air space sensors
    - Applicable for Unmanned Aircraft Systems (UAS) detection, e.g., alerts operator if drone flies into facility's airspace
l. Infrared beams – laser technology
    - Passive/active infrared

Attention: Proper maintenance and updating of video cameras, video control, motion detection, and light systems are important.

Access Control & Alarm Management

Access control refers to the practice of restricting entrance to a property, a building, or a room to only authorized persons. Physical access control can be achieved by a human (a guard or receptionist) through mechanical means such as locks and keys or through technological means such as access control systems. Physical key management may be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access control is a matter of who, where, and when. An access control system determines **who** is allowed to enter or exit, **where** they are allowed to exit or enter, and **when** they are allowed to enter or exit. Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked. Access control and associated alarm management technologies are highlighted below.

1. Visitor Management (software-based)

a. Access control platforms can integrate a visitor management component.
b. Temporary badge technologies may include some of the following features:
    i. Visitor can be e-mailed a barcode (pre-registering for future visit)
    ii. Receptionist/security has list of all planned visitors
    iii. Photographs stored
    iv. Kiosk/touch screen support (e.g., unattended reception area)

v. Reusable or per-visit identification (paper or badge printers) printed including host company's logo
vi. Host notification (visitor arrival and departure)

c. In-house front-end hardware/software for visitor management, may include:
   i. Automated data extraction from government identification
   ii. Email notification of company host
   iii. Data input into real-time emergency evacuation accountability list
   iv. Visitor check-in/-out process
   v. Visitor checkout reminder if not completed by end of the work-day

2. Access Control

a. Surveillance and "security officer"
   i. Patrol robotics
   ii. Drone technology
   iii. Anti-tailgating/anti-piggybacking technology
      - Admits only one person into a restricted area per valid authorization (e.g., one entry per badge swipe)
      - Compatible with any badge or access system
      - Sounds alarm or makes announcement to alert security or reception of unauthorized entry (upgrade available to control door locks)

b. Turnstiles
   i. Various styles – waist high, full height, revolving door, and optical (e.g., drop arm, swing arm, swing glass, flap barrier, retractable glass)
   ii. Aesthetic considerations – may help with executive buy-in/support (e.g., glass revolving door more aesthetically pleasing than full height steel)
   iii. Installed in areas of building not staffed by security officer or receptionist

c. Mobile credentials – accessing facilities via mobile devices

d. Intercom/camera combinations – connected to SOC and human approval for access

e. Card readers

   Attention regarding badging – with the availability of inexpensive equipment and online instructions, as well as the relative ease of cloning access cards, serious consideration should be given to the type of access card used.

f. Dual factor authentication
   i. Pin code
   ii. Biometrics
   iii. Facial recognition
   iv. Fingerprint
   v. Retinal scan
   vi. Opisthenar scan (back of hand)

3. Alarm Management – System Integration Software

Such software has the potential to increase an operator's capacity to efficiently manage alarms. Different types of software exist for managing different risks. By integrating the different software types into a single platform, the operator may more effectively adjudicate/mitigate alarms. It's worth noting that different software platforms are starting to integrate among themselves; operators are encouraged to identify such requirements so they can be designed into the system. Utilities that do not have a SOC may have intrusion detection monitored by a third-party.

a. General practices of utilities with a SOC
    i. A single SOC for all alarms, including those of subsidiaries
    ii. Video analytics for day and night
    iii. Use of same products across the different states
    iv. Third-party integration software
    v. Maximize existing software capabilities
b. Challenges
    i. Some sites have zero connectivity
    ii. Limitations on system flexibility
    iii. Up-keep with constantly changing firmware
    iv. Potential supply chain risks
c. Products
    i. Access control
    ii. Configure different scripts for different sites
d. Leading practices
    i. Segmentation of all security camera traffic in dedicated Virtual Local Area Network (VLAN) channels to address the risks of physical access to the network and potential lateral access as well as SOC monitoring.
    ii. Regular remote and in-person physical inspection of camera enclosures as circumstances allow.
    iii. Consult with your cybersecurity professionals to ensure not introducing cyber vulnerabilities to network, e.g., video surveillance equipment on the network.

Key Control – Who Owns Key Control; Who Makes the Keys

The ability for physical security to manage, audit, and control the access to company facilities is a critical part of protecting the company assets as well as for safety of its employees. There are many different types of access control equipment and alarm systems that are used in the natural gas industry. One area that can be overlooked or mismanaged is "lock and key" to facilities. Developing a system to formulate door hardware cores and assigning keys to individuals to specific facilities or groups of facilities will allow better key control and security.

1. Key Control & Key Management

a. Benefits of effective Key Management

i. Select personnel authorized to issue keys

ii. No duplication of keys without approval

iii. Reporting system for lost or stolen keys

iv. Key retrieval upon separation from company (e.g., resignation, retirement, termination and temporary suspension)

v. Recordkeeping of repairs and/or replacement of locks, keys, and hardware

vi. Key storage

- Worth noting are key boxes –hold master keys; access via cardswipe; sends alarm to SOC or operator; the key within can be checked out; logs electronically who accessed and which key was taken
- Vet out the hardware, its capabilities, and flexibility to fit operating environment

b. Electronic locks and keys

i. WITH network access

Wireless padlock (battery-operated) ties into access control system – for manned gates; tied access control system through network; since battery-operated, not dependent on system being online; card-swiped; hard-wired

ii. WITHOUT network access

Intelligent key devices can be utilized to secure remote facilities where network is not available. Intelligent keys will allow the use of mobile credentials (Bluetooth©) to program locks and provide access to facilities. Network access is not necessary. Mobile credentials will update automatically while in cellular network service areas. Cellular service is not necessary for the mobile credential to unlock intelligent locks in remote locations.

2. Use Case for Management of Non-Electronic Keys

Step #1 Determine how your key system should be organized best for your company.

i. Keyed by Individual Facility. An example of this would be by specific service centers. Each service center would have a different group of formulated cores and stamped keys. Another example would be by region or by working group.

ii. Keyed by a Large Area of Facilities. This could be addressed by the same group of formulated cores and stamped keys. An example would be a large region where a pipeline supply division is operating and there are several buildings cored and keyed alike. A working group may be the specific department.

Step #2 Develop a key agreement sheet and reliable mechanism to track the assigned keys.

i. The keys may be stamped with core number and key number. Determine who will be responsible for the assignment of keys and management of the key tracking mechanism (e.g., software, spreadsheet, etc.). When keys are assigned to an individual, the key agreement sheet may be sent out to that person to sign and to acknowledge possession. When the key is returned, the key agreement sheet and tracking mechanism note as such.

ii. Note: The transition from regular door hardware to interchangeable door hardware can benefit the operator with the ease of removing and exchanging cores using a core key. The interchangeable core system will also allow for different levels of keys to be distributed as well. For example, the general operation key, sub master key will open everything in that series and a grand master key will open everything.

Rural Areas

Rural Areas pertain to those areas that are outside of the publicly populated areas (cities and towns), often referred to as the country or farm areas. Critical infrastructure are often found in these areas, and infrequently visited, which make these easy targets that go undetected until an employee does a site visit. More technology allows more data that helps operator understand what the intruder is doing.

1. Low-bandwidth Solutions

a. Retrofitted deer cameras that provide IR at night
b. Allows virtual network so can support network access

2. Camera Analytics / Thermal Imagers to Monitor Staff in Remote Facilities

a. Detect and alarm when someone is near or in protected space
b. Provide instant verification of true or false alarms
c. Edge devices (e.g., edge camera recording)
    i. Cellular – Provides a video or snapshot of what triggered the alarm soon after it is triggered
    ii. Non-Cellular – Provides a video or snapshot to a SD card in which you have to retrieve and review

3. Drones

a. Potential to provide visibility when alarms go off
b. Feasibility limited by current drone operation regulations (e.g., must be in line of sight)

4. Nuisance Alarms
    a. Farm animals
    b. Wildlife (Deer)
    c. Insects (Spider Webs)
    d. Head Lights
    e. Weather (fog)
    f. Vegetation
    g. Blocked zone by vehicles or materials
    h. Human performance (employees not arming or disarming system)
5. Talk Down

    Provides instant notification to anyone in the area that should or should not be in that space. We often find that local law enforcement cannot respond quickly to these locations.
6. Back-up Power
7. Communications
    a. Getting communications at a rural site is often time challenging
    b. Cellular (Modem)
    c. Satellite