BURNS McDONNELL

WHITE PAPER

Protecting Critical U.S. Natural Gas Infrastructure

By PJ Kolnik, PE, and Jared Oakden

Keeping natural gas pipelines and other infrastructure secure is vital to the operation of our nation. Utilities that seek help determining the criticality of pipeline assets and operations and implement relevant security strategies are the ones that will be most prepared if an attack occurs.

The movie "How to Blow Up a Pipeline" has brought a new level of awareness to the challenges the natural gas pipeline industry is confronted with every day — the very real challenge of physically protecting the natural gas infrastructure that is critical to our nation's energy system.

About 3 million miles of pipelines connect customers with natural gas production and storage facilities. Information from the Homeland Infrastructure Foundation-Level Data website shows that there are over 2,000 records of natural gas compressor stations plotted approximately every 50 to 100 miles along just these gas pipelines, in both remote and populated areas.

These pipelines and stations are essential for the transportation of energy resources. Natural gas supports the electric power generation grid by supplying approximately 40% of the fuel to generation assets. This gas flows through an intricate network of compressor stations, pipeline networks and metering/regulator stations. By interrupting any segment of this flow, power generation and other industry and commercial/residential loads are impacted. These sites are vulnerable to physical attack from both foreign and domestic groups seeking to disrupt the country's energy infrastructure.

Physical security attacks can take many forms, such as cutting or drilling holes in the pipeline, detonating explosives near the pipeline, or tampering with valves or other controls. Simple acts like closing valves to disrupt gas flow to a residential community can result in days of no gas for furnaces, hot water heaters and cooking appliances. Pipeline operators must assemble large quantities of qualified personnel to restore gas deliveries safely and without leaks. Pipeline operators without effective physical security are finding their pipeline assets increasingly exposed to new residential and commercial developments.

Secure perimeter fences, surveillance systems including cameras, and other technology can provide increased levels of security for pipeline operators. Security countermeasures and strategies should be risk-based and threat-informed.

Lessons From a Natural Gas Pipeline Attack

Attacks on natural gas systems have highlighted physical vulnerabilities for system operators around the country. Take the attack on a pipeline feed in Colorado as an example. Saboteurs targeted three separate valve locations on the same night. In their wake, they left more than 3,500 customers without gas for heat or hot water for three days in the midst of single-digit temperatures in December. During the attack, valves were accessed and turned to the closed position. Pressure and volumes subsequently dropped for the busy community down the line.

In response to the crisis, city officials distributed over 4,000 space heaters to affected homes and businesses, while hundreds of field operators worked around the clock to resolve the issue. The cost of the attack was estimated at $1.4 million, with most of the cost going toward labor, including hotel costs and per diems for out-of-town workers.

The process of restoring gas service was time-consuming, technical and labor-intensive. Technicians had to manually turn off gas meters at each individual customer location and purge each service line and distribution main back to where gas was lost to remove air from the line. Once that was complete, the pipeline operator had to re-pressurize the entire system and then test it. Finally, technicians went individually back to each residence and business, one by one, to turn on meters again, relight appliances and verify that there was no presence of gas.

The investigation into the sabotage was a monthslong process. Footprints in the snow, cellphone data and the writing, “Earth First!” (indicating a possible environmental motive for the attack) was the only physical evidence for the local and federal authorities. There were no access records to pull from or video footage to review. This attack affected 3,500 customers. Scale this up in comparison and if a similar coordinated attack occurred on a larger system with customers in the hundreds of thousands, the chaos, damage and costs would be even more significant.

The potential at-risk sites related to the natural gas industry are extensive (see Figure 2). The industry is facing a time where the cost of doing nothing to protect assets can quickly exceed the cost of doing even minimal security upgrades.

Infrastructure Security Requirements

The Pipeline and Hazardous Materials Safety Administration (PHMSA) through 49 CFR Part 192 has only a few physical security requirements for pipeline infrastructure — primarily for compressor station buildings; 49 CFR Part 193 contains more prescriptive code requirements for liquefied natural gas

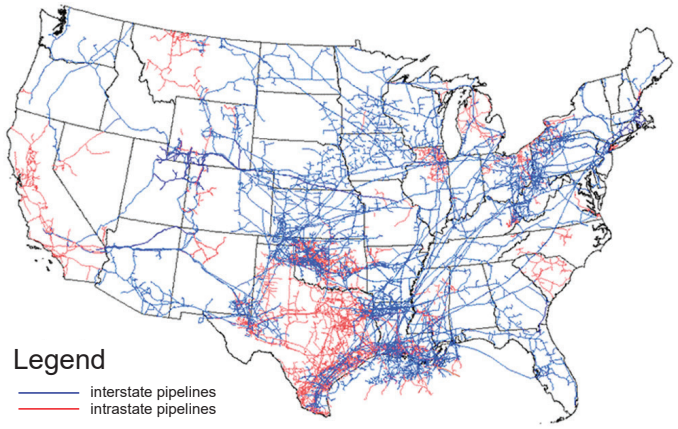

***Figure 1:** Map of U.S. interstate and intrastate natural gas pipelines. The natural gas pipeline network is a highly interconnected system. (Source: U.S. Energy Information Administration).*

(LNG) facilities, including physical security, lights and backup power generators to protect each LNG site.

As we look at 49 CFR Part 193 in more detail, perhaps there is wisdom in applying principles of LNG physical security to the broader portfolio of natural gas assets across the country, including pipelines, compressor stations and M&R stations. The PHMSA regulations for LNG facilities focus on the safe and secure design, construction, operation, and maintenance of these facilities. Some key security requirements for LNG plants under PHMSA’s jurisdiction include:

1. Security plans: LNG facilities must develop and implement comprehensive security plans that address potential security threats, vulnerabilities and mitigation measures. These plans outline security procedures, access controls, personnel screening, surveillance systems and emergency response protocols.
2. Physical and electronic security countermeasures: The regulations specify various security countermeasures that LNG facilities must incorporate, such as physical barriers, intrusion detection systems, video surveillance, security lighting and perimeter controls. These measures aim to prevent unauthorized access, detect security breaches and protect critical infrastructure.
3. Personnel security awareness training: LNG facility operators are required to provide security awareness training to employees and contractors who have access to sensitive areas or perform security-related functions. This training shows that personnel are knowledgeable about security procedures, threat identification and appropriate response measures.
4. Coordination with authorities: The regulations emphasize the importance of collaboration and

coordination with law enforcement agencies, emergency responders and relevant government authorities. Facilities' effective communication, incident reporting and coordination during security incidents or emergencies is imperative.

In 2018, The Transportation Security Administration (TSA) released "Pipeline Security Guidelines" as a federal guideline and resource for natural gas operators and owners. The TSA guide provides utilities with information including:

1. Site criticality: A large component of the TSA guidelines is helping gas utilities identify their most critical sites based on specific criteria and characteristics of each location.
2. Risk assessments: Conducting comprehensive risk assessments to identify and evaluate potential security threats, vulnerabilities and consequences is important. The assessments help prioritize security measures based on the level of risk and types of threats.
3. Corporate security governance: To achieve a utility's security goals, recommendations for the establishment of a formal corporate security program and organizational structure must be made and strategic implementation of the program must be set in place.
4. Security plan: In order to effectively guide a utility's security decisions, the utility should develop a corporate security plan that encompasses various security topics and policies.
5. Physical and electronic security measures: Establishing recommendations for baseline and enhanced security measures, access controls, surveillance systems and intrusion detection systems are vital. These measures aim to deter, detect and delay unauthorized access and potential security incidents.
6. Personnel security: The need for background checks, security clearances and training for personnel with access to critical pipeline infrastructure is a fundamental necessity. This helps utilities see to it that individuals with malicious intent or those who pose a security risk are not granted access to sensitive areas.
7. Security awareness and training: The importance of developing and implementing security awareness programs and training for employees, contractors and other personnel cannot be overemphasized. These programs should educate individuals about security threats, best practices, emergency response protocols and reporting suspicious activities.
8. Incident response and reporting: Focusing on having robust incident response plans and procedures in place should be a priority. Pipeline operators are encouraged to establish effective communication channels, coordinate with law enforcement agencies and report

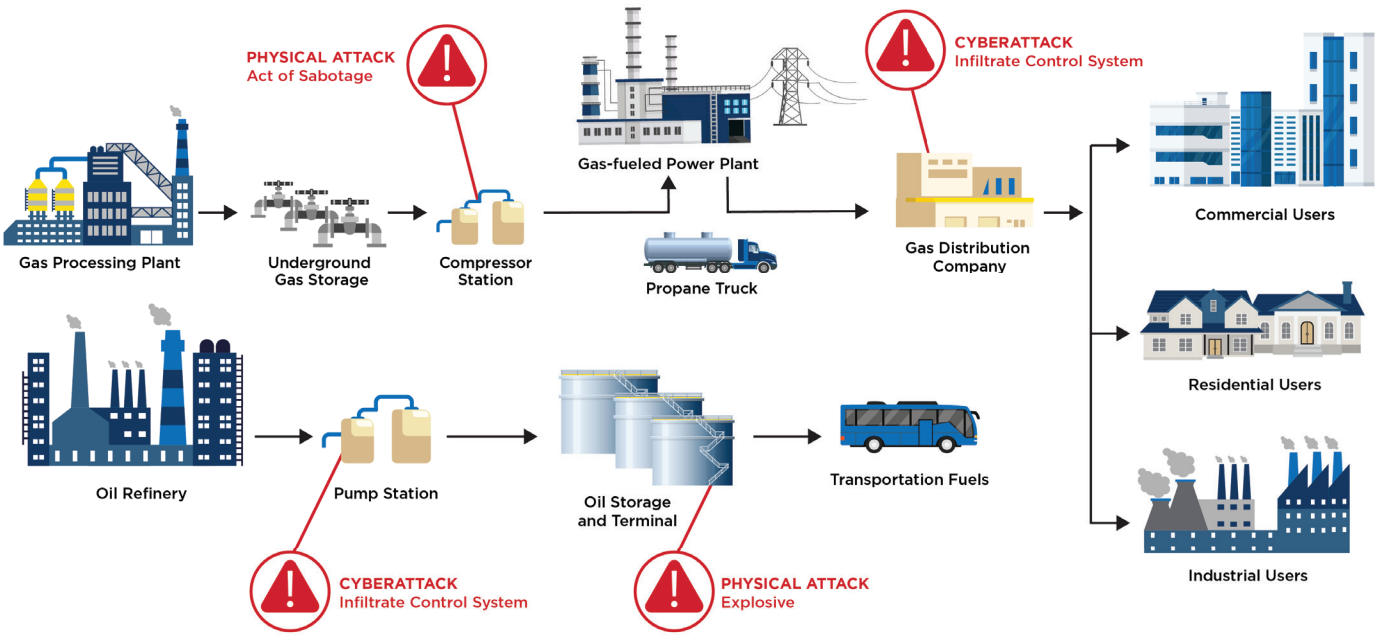

***Figure 2:** U.S. pipeline assets and threats. The U.S. pipeline system is susceptible to a variety of attacks. By combining layered and holistic security measures with threat intelligence, natural gas utilities can better prepare for the unexpected. (Source: U.S. Government Accountability Office).*

any security incidents or suspicious activities to the appropriate authorities.

9. Cybersecurity: Implementing safeguards against cyberthreats and following industry best practices to protect against unauthorized access, data breaches and disruptions to pipeline operations is crucial.
10. Collaboration and information sharing: The significance of collaboration among pipeline operators, government agencies, law enforcement and other stakeholders must be understood and valued. Sharing information, intelligence and best practices enhances overall security posture and helps identify emerging threats and vulnerabilities.

Safeguarding an Essential Resource

TSA has announced that it will be auditing physical security sites that are located in critical energy infrastructure locations. It is expected that in the coming years TSA will release physical security directives regarding site criticality determination, threat and vulnerability assessments, and security countermeasures that will come with compliance requirements and consequences, similar to NERC CIP requirements for electric utilities. A knowledgeable, strategic partner can help utilities prepare for and respond to relevant directives; and should have the experience to evaluate pipeline infrastructure and determine which facilities should be classified as critical and how they can be defended.

For decades, energy system operators, both gas and electric, have relied on the rural/undeveloped locations of their system assets to be a significant component of their security strategy, best described as out of sight, out of mind. This approach needs to evolve. A more holistic method to mitigate the risk of physical attacks includes layers of security countermeasures such as physical barriers, surveillance systems, intrusion detection and access controls.
Beyond that, utilities can get left of bang through deliberate and thoughtful threat intelligence analysis. Threat monitoring and coordination between law enforcement agencies and private companies will help utilities proactively anticipate, detect and respond to threats of sabotage and other attacks. Lastly, public awareness campaigns are helpful in educating the public about the risks of pipeline attacks and encouraging individuals to report any suspicious activities near critical infrastructure.

Security mitigation measures can come at great cost to pipeline distribution operators. Depending on each state's public utilities commission, there may be opportunities to include new security measures to existing sites through the rate case process. That said, these projects still must balance the needs of customer affordability, system reliability, safety and security. With each new attack, the need for security considerations to influence these decisions becomes increasingly important.

An experienced team made up of security professionals and pipeline engineers working in-house together to provide consulting for both business-critical infrastructure and critical energy infrastructure as defined by TSA is ideal. A team such as this could seamlessly conduct threat and vulnerability assessments of key facilities, offer risk management consulting, write security standards and policies, and design efficient electronic security systems enterprisewide in an effort to keep important infrastructure assets protected.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

401503-0723