Is America's Natural Gas Pipeline Network Prepared for Cyber-Attacks?

The members of the Interstate Natural Gas Association of America are committed to promoting the security, reliability and resilience of their natural gas transmission pipelines. Our industry has established robust and comprehensive protocols and safeguards to ensure the reliability of America's natural gas network.

System Operational Characteristics

The natural gas transportation network is diverse and interconnected, offering multiple pathways to reroute deliveries in the event of a disruption.[1]

Pipeline operators purposely design systems to limit points of failure.[2]

Natural gas under firm delivery contracts is delivered with 99.79% percent reliability.[3]

Supply flexibility is ensured by geographically dispersed production and storage systems.[4]

Most components of the natural gas pipeline infrastructure are underground and protected from the elements, making them far more resilient to extreme weather events or external threats.[5]

Natural gas pipelines continue to operate during power outages because most of the compressors that keep gas flowing through the lines are fueled by natural gas .[6]

Natural gas pipelines have numerous backups and fail-safes. They ensure that the system can continue to operate in the event of an outage of the computer systems that help operate the pipeline (called "SCADA").[7]

Cyber Practices

The NIST cybersecurity framework is just one of many standards that pipeline operators use to improve the security and resilience of critical infrastructure.[8]

Pipeline operators use resources like the Oil and Natural Gas Information Sharing and Analysis Center and Downstream Natural Gas Information Sharing and Analysis Center to share threat intelligence and recommended mitigations in real-time.[9]

Gas pipeline and electric grid operators conduct joint tabletop exercises to test response plans and increase gas-electric coordination, reliability and resilience.

Pipeline operators routinely maintain both backup control rooms and backup data rooms at alternate locations to ensure quick system and data recovery in the event of a successful cyber intrusion.[10]

Pipeline Operators Use a Variety of Tools

- ✓ API Standard 1164: Pipeline SCADA Security
- ✓ Department of Energy Electricity and Oil and Natural Gas Subsector Cybersecurity Capabilities and Maturity Models
- ✓ Transportation Security Administration Pipeline Security Guidelines
- ✓ NIST Guidelines for Smart Grid Cyber Security (NISTIR 7628)
- ✓ TSA, DHS, DOE Pipeline Cybersecurity Assessment Initiative

Natural gas operators partner with academic and research organizations to design and improve cyber-reliance systems, including:

CREDC Cyber Resilient Energy Delivery Consortium

SEEDS Cybersecurity Center for Secure Evolvable Energy Delivery Systems

[1] Interstate Natural Gas Association of America, 2018. Pipeline Security.
[2] Massachusetts Institute of Technology, 2013. Interdependence of the Electricity Generation System and the Natural Gas System and Implications for Energy Security.
[3] Natural Gas Council, 2017. Natural Gas Systems: Reliable & Resilient.
[4] American Petroleum Institute, 2017. Diversity of Reliability Attributes: A Key Component of the Modern Grid.
[5] Natural Gas Council, 2017. Natural Gas Systems: Reliable & Resilient.
[6] American Gas Association, 2014. Natural Gas Pipeline Systems: Delivering Resiliency.
[7] Massachusetts Institute of Technology, 2013. Interdependence of the Electricity Generation System and the Natural Gas System and Implications for Energy Security.
[8] National Institute of Standards and Technology, 2018. Cybersecurity Framework.
[9] DNG-ISAC, 2018 and ONG-ISAC, 2018.
[10] Transportation Security Administration, 2018. Pipeline Security Guidelines.

INGAA
Interstate Natural Gas Association of America