Process Solutions

Honeywell

Success Story

Cyber Security Vulnerability Assessment Reduces Risks to Gas Pipeline Operation

> "Thanks to Honeywell's cyber security expertise for industrial control and SCADA systems, along with its advanced assessment tools and techniques, we have addressed a wide range of potential risks to the safety, security and reliability of our natural gas distribution system." –SCADA Supervisor, Natural Gas Pipeline Company

The organization recognized the importance of the cyber security profile of its gas distribution pipelines and equipment.

Benefits

As a result of Honeywell's cyber security vulnerability assessment solution, a natural gas pipeline company was able to empirically identify and quantify all of the steps required to improve the security and reliability of its natural gas distribution pipeline network, and therefore increase the uptime and availability of its system.

The Honeywell cyber security assessment identified all critical gaps within the enterprise. Once gaps were identified, Honeywell helped the customer develop, implement and manage a comprehensive information security program to ensure current compliance with applicable industry regulations and ongoing protection of information and systems.

Thanks to the Honeywell solution, company personnel are now more aware of potential cyber security threats and can take action to ensure gas continues to reach residential and commercial customers throughout the company's service area.

Background

The pipeline organization, which was incorporated in the USA in the early 1900s, is one of the largest combination natural gas and electric utilities.

There are approximately 20,000 employees who carry out the transmission and delivery of energy. The company provides natural gas and electric service to approximately 15 million people. They operate tens of thousands of miles of natural gas distribution and transportation pipelines.

While large interstate natural gas pipelines may serve major wholesale users such as industrial or power generation customers directly, it is the distribution system that actually delivers natural gas to most retail customers, including residential natural gas users.

A gas utility's central control center continuously monitors flow rates and pressures at various points in its gas distribution system. Sophisticated computer programs are used to evaluate the delivery capacity of the network and to ensure that all customers receive adequate supplies of gas at or above the minimum pressure level required by their gas appliances.

Challenge

Today's natural gas transmission and distribution systems are heavily dependent upon computer technology and supervisory control and data acquisition (SCADA) systems to operate safely and efficiently.

For gas utilities, the challenges involved in ensuring effective cyber security are similar to those faced by bulk electric system and local power distribution providers, except that natural gas systems transport molecules, not electrons, and are equipped with safety devices, which are, in most cases, manually operable as federally required. But all of these groups depend on communications infrastructures, computer technologies, and people to safely and efficiently transport the energy product to the end user.

Designing, operating, and maintaining a pipeline facility to meet essential availability, reliability, safety, and security needs as well as process control requirements requires the careful evaluation and analysis of all risk factors. Attacks on a cyber system may involve only the cyber components and their operation, but those impacts can extend into the physical, business, human, and environmental systems to which they are connected. A cyber event, whether caused by an external adversary, an insider, or inadequate policies and procedures, can initiate a loss of system control, resulting in negative consequences.

The client recognized the importance of the cyber security profile of its gas distribution pipelines and equipment. An operational incident underscored the need to better manage networks and data access. It had become clear that the company required expertise in the niche market of IT security as applied to critical control networks.

Solution

Honeywell Industrial Cyber Security Solutions provided quality service and professional results to the client on more than one previous occasion. In this instance, they needed help assessing and remediating the cyber security vulnerabilities of their gas distribution pipelines and equipment.

Honeywell's solutions for oil and gas pipelines promote safety, environmental responsibility, and efficient operations.

The cyber security vulnerability assessment is designed to examine the three core facets of an organization's cyber security:

- **People:** What is the cyber security awareness level in the organization? Are staff members following security policies and procedures? Have they been adequately trained to implement the security program?
- **Process:** What are the cyber security policies and procedures in place in the organization? Do these policies and procedures meet key requirements?
- **Technology:** What cyber security technologies are in use in the organization? How are these technologies configured and deployed?

Today's natural gas transmission and distribution systems are heavily dependent upon computer technology and SCADA systems to operate safely and efficiently.

The assessment process takes inventory of all cyber assets, how they're connected, and how they're programmed. This includes:

- Servers
- Network switches
- User terminals
- Desktop and laptop PCs
- PLCs and controllers
- Terminal racks
- Wireless transmitters and receivers
- Mobile devices on the network

Through the assessment, Honeywell's team documented the vulnerabilities in all facets of the client's pipeline operation, interpreted and assessed the associated cyber security threats, and provided a roadmap to mitigate risks. This included:

- **Site and system assessment**—Review of particular site- and system-specific vulnerabilities.
- **Policy and procedures assessment**—Review of current policy and procedure documents.
- **Compliance assessment**—Review of operations and processes against applicable compliance standards and best practices.
- **Security baseline**—Gauges progress against current status and operating model for security.
- **Risk assessment**—Identifies appropriate levels of security for each asset.

The final analysis included suggestions for improvement by order of importance, a project plan, and order-of-magnitude costs for budgetary purposes.

Going forward, Honeywell will help the client further develop or refine and execute their cyber security program.

For More Information
Learn more about how Honeywell's Industrial Cyber Security Solutions can help improve cyber security at your facility, visit our website www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com