Honeywell
THE POWER OF CONNECTED

Connected Industrial

GAS METERING AND DATA MANAGEMENT: UNDERSTANDING GROWING CYBER SECURITY THREATS

White Paper

Abstract / Introduction

Natural gas companies are under pressure from many forces in the world. Among these is the multiplicity of computer and communications systems that must be protected from those who would do harm to gas transmission and distribution capabilities.

Natural gas is the foundation fuel for a clean and secure future, providing benefits for the economy, environment and energy security. Alongside the economic and environmental opportunities of natural gas, there comes great responsibility to guard vital distribution assets from cyber-attack.

In today's highly connected world, with increasingly sophisticated electronic threats, it is unrealistic to assume gas delivery systems are isolated or immune from various forms of electronic compromise.

The following whitepaper describes the comprehensive cyber security measures implemented by Honeywell as part of its Gas Measurement and Data Management Services (GMDMS) solution. Honeywell's approach helps natural gas providers proactively identify and mitigate cyber-risks. Companies gain greater visibility into their security posture and how to address threats to critical gas metering and data management infrastructure.

Table of Contents

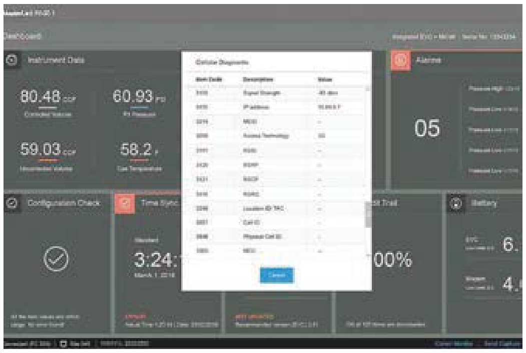
To thrive amidst difficult industry challenges, the natural gas company of the future must embrace fully digital systems. This means they face a digital transformation of their organization, operations and business – along with corresponding cyber security challenges

In the natural gas industry, the trend towards smart metering has demonstrated the importance of Meter Data Management (MDM) in realizing the full potential of Advanced Metering Infrastructure (AMI).

Demands on Gas Operations

Natural gas utilities have historically enjoyed a simple and predictable relationship with their customers. The strategy to ensure business success was based on two easily articulated goals: deliver timely, informative and accurate bills and avoid high-profile infrastructure failures.

Today, however, natural gas providers need the tools and know-how to effectively store, transport and deliver gas to meet rising demand and stay competitive. Regulatory bodies require higher levels of calibration and safety, Millennial-age workers with new expectations are entering the workforce, and seasoned engineers are retiring.



By pairing advanced MDM software with the latest instruments for gas measurement and volume correction, gas industry firms can enhance efficiency, reduce costs, and minimize risks to operations.

Relevant operational and business data are available in many places on the gas grid, most of the time. Companies want to be as easy as possible to take this information and make it useful. This includes solutions that regularly pull and store relevant gas meter data in a secure cloud. Gas metering data must also be collected more frequently and in smaller increments.

Role of Meter Data Management

To support the implementation of Advanced Metering Infrastructure (AMI) strategies, many gas utilities are deploying robust Meter Data Management (MDM) solutions. These systems are the critical linchpin that integrates a complex collection of Information Technology (IT) assets. They are essential tools for handling the huge volumes of data generated through automated gas metering.

Leading automation suppliers like Honeywell provide advanced gas measurement, volume correction and MDM solutions to the natural gas industry. Honeywell's complete, end-to-end offering is future-ready for emerging technologies and provides a host of valuable productivity benefits. Its gas measurement and data management products can help companies exercise control over their gas regulating and measuring needs at a lower cost. The company's integrated solutions portfolio provides seamless connectivity and round-the-clock access to critical data and diagnostics.

Honeywell's Gas Measurement and Data Management Solutions (GMDMS) offering is comprised of five main components for gas transmission and distribution customers:

- EC 350 PTZ gas volume corrector
- Elster rotary gas meter
- Cloud Link 4G low-power wireless modem (which connects to the volume corrector and includes a Bluetooth Low Energy radio for onsite wireless connectivity)
- MasterLink configuration and calibration software
- PowerSpring meter data-management software

Honeywell provides a fully integrated, end-to-end technology platform for gas transmission and distribution.

Using a fully integrated platform for data collection/management and remote meter monitoring, gas operators can improve the output from equipment assets, avoid unplanned downtime, implement preventive maintenance, and maximize Return on Investment (ROI). By pairing advanced MDM software with the latest instruments for gas measurement and volume correction, they're able to enhance efficiency, reduce costs, and minimize risks to operations.

Emerging Technology Trends

More than the latest industry buzzword, the Industrial Internet of Things (IIoT) is a global infrastructure for interconnecting (physical and virtual) "things" based on existing and evolving interoperable information and communication technologies. The IIoT is part of a larger concept known as the Internet of Things (IoT). The IoT is a network of intelligent computers, devices, and objects that collect and share huge amounts of information.

Strong authentication processes are mandatory to prevent hackers from accessing crucial gas measurement data, uploading malicious software or turning meters on and off.

It should come as no surprise that the primary value of IIoT is in the data, more specifically, the enhanced decision-making and automation that arise from the convergence of analytical insights, enabled by connected devices, with people.

In the natural gas industry, companies now employ the capabilities of the IIoT to do automated meter reading. But, they need to do more than just collect reams of data for billing and back office analysis. Gas operators must be able to make decisions and take action at every level of their distribution system, optimizing analytics where it makes sense and enabling multiple applications to run edge devices to solve problems in new ways.

For example, Honeywell's GMDMS solution leverages the power of the IIoT to optimize the performance of gas meters. It integrates devices in the field (edge-enabled through the Cloud Link modem) with smart configuration and maintenance software, as well as advanced MDM software and services. This solution reduces operational costs by streamlining maintenance and remote support.

Growing Security Challenges

In any IIoT-based communication system, it is essential to ensure that sensitive information reaches its intended recipient, and that it cannot be intercepted or understood by a malicious individual or device.

For gas utilities, the challenges involved in ensuring effective cyber security are similar to those faced by bulk electric system and local

Attacks on a natural gas delivery 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.

power distribution providers, except that natural gas systems transport molecules, not electrons. But these groups depend on communications infrastructures, computer technologies, and people to safely and efficiently transport their product to the end user.

Gas suppliers need to protect vital measurement and data management assets from ever-increasing cyber threats.

Designing, operating, and maintaining a gas transmission and distribution infrastructure to meet essential availability, reliability, safety, and security criteria requires the careful evaluation and analysis of all risk factors.

For instance, a hacker could attempt to falsify the data from hundreds or even thousands of gas volume correctors in the field – leading to millions of dollars in losses to the gas provider. Indeed, there are serious consequences to either overcharging or undercharging a customer for gas delivery.

Another vulnerability exists with pressure monitoring. A cyber intruder might try to change the system pressure by manipulating field devices in some way, causing alarms to malfunction and the pressure modifications to be overlooked.

Cybercriminals seeking to launch an attack over a utility's complete install base are most likely to seek entry through a cellular device. A major modem supplier recently reported that the "Mirai" malware was able to gain access to a network gateway by logging in to the system with a default password and using a firmware update function to download and run and copy of itself. Once the malware is running on the gateway, it deletes itself and resides only in memory. The malware then proceeds to scan for vulnerable devices and report its findings back to a command and control server, which may instruct the malware to participate in a Distributed Denial of Service (DDoS) attack on specified targets.

Addressing Cyber Threats

One of the key trends in the natural gas industry is the digitization of data and systems. While these mobile interfaces, cloud computing, and digital data acquisition solutions have offered tremendous benefits to gas industry firms, including lower costs and increasing efficiency, they have also opened the door to cybercrime.

A cyber-attack on devices that control the gas grid could result in disruption of operations or damaged equipment. Any device or system controlled by network communication that "faces" the Internet is at risk of being hacked.

Experience has shown there is no "silver bullet" to do away with all cyber security vulnerabilities. Rather, gas industry enterprises should consider integrating advanced cyber threat protection processes into their operational and business networks. Companies also need to prioritize security in their quest to create end points for all their field assets.

Planned cyber security integration is important because, in many cases, bolt-on fixes are not scalable. Ad hoc solutions usually only work in single instances, or are application-specific, and can result in increased overhead management and costs.

Security planning must keep pace with operational shifts precipitated by the inclusion of interconnected tools, processes, devices and evolving compliance mandates. These changes are reflected in the trend toward industry-wide convergence of Information Technology (IT) and Operations Technology (OT).

Effective Protective Measures

As gas providers worldwide move more into a connected state of business, key partners will become increasingly important to help analyze the wealth of data to make smarter decisions for both the grid and customers – and protect vital gas metering assets from ever-increasing cyber threats.

Honeywell is a leading supplier of measurement and control technologies to the worldwide oil and gas industry. Its solutions for the natural gas firms promote safety, environmental responsibility and efficient operations.

Thanks to Honeywell's cyber security expertise, along with its advanced tools and techniques, gas utilities can address a wide range of potential risks to the safety, security and reliability of their gas measurement and data management systems. Honeywell engineers have performed extensive threat modeling to anticipate likely cyber risks affecting the GMDMS solutions, and this has resulted in robust security features being "designed in" to the company's gas metering and data management products.

Honeywell's Development Process has been certified to ISASecure™ SDLA Level 1.Its robust security features provide:

- Role-based login mechanisms with different levels of authorization for greater flexibility and secure access control. This includes support for PAP/CHAP to authenticate PPP sessions.
- Security for electronic volume corrector integrated radios.
- Cryptographic security for BLE communication between the EVC's integrated radios and field configuration application.
- Safe list to enter trusted IP addresses, thus preventing incoming connections from any unwanted device.
- Configurable UP times (system is communicable only during the configured times, thus reducing the attack possibilities).
- IPv6 built-in security to reduce chances of hacking and phishing.
- Push notifications on critical alarms or events.
- Choice of privilege levels – Read/Write or Read Only.
- Cloud storage and AMR software providing redundancy on multiple levels.
- Advanced event log to record each user access and changes made.
- Integrated security for secure database access.
- Industry standard account management practices (e.g., strong passwords, inactivity timeouts, exponential account lockouts, password expiry).

Honeywell's fully integrated, end-to-end technology platform for gas transmission and distribution is based on a single design standard and follows strict cyber security and IT data security guidelines uniformly across all components. As such, there is no weak link to be exploited by cyber criminals.

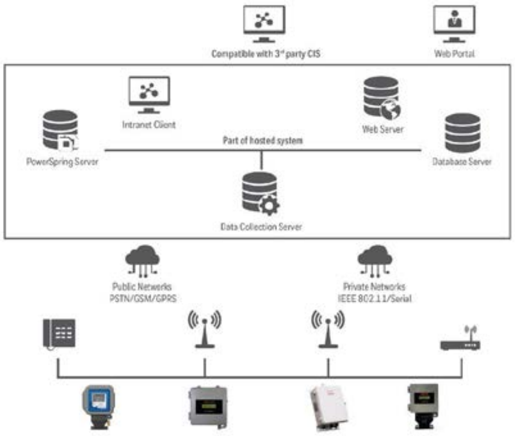
Honeywell's industrial cyber security expertise has been evolving over the last decade, combining best practices from traditional IT with the needs of increasingly complex operational environments.

Honeywell's end-to-end technology platform for gas transmission and distribution follows strict cyber security guidelines uniformly across all components.

Honeywell's cyber security solutions are specifically intended to protect sensitive gas consumption information at both the data storage and data transfer levels.

In addition, the company's architectural design ensures that it's integrated, low-power cellular modems operate on the network for the shortest possible time – perhaps only a few minutes per day. This greatly reduces cyber vulnerabilities compared to approaches where modems remain on continuously.

With Honeywell's cyber security know-how, gas industry customers can improve the overall security of their metering installed base and reduce the chances of vulnerabilities being exploited.



Honeywell's gas metering system architecture

For Honeywell's MasterLink meter configuration & calibration software and PowerSpring MDM software, for example, there is a stringent registration process requiring utility administrators be provided with registration keys by Honeywell's global Technical Assistance Center (TAC). Authentication and authorization procedures are in place at the application level (i.e., role-based access control) along with a strong password requirement for MasterLink users. Passwords are encrypted in the database using a proprietary, unpublished protocol.

Rigorous authentication and authorization measures are also employed at the device level. The EC 350 gas volume corrector contains a user table listing personnel allowed to access the device and make changes. Each login/password can be unique. Additionally, rich auditing information is available via the event log of the EC 350 and audit log of the MasterLink software. Access and changes to the instrument configuration are recorded in the alarm and event logs. Changes are made using the EC 350 user interface or via MasterLink; alterations performed in the software are recorded in its activity log.

Honeywell's security measures are further intended to prevent brute force-exponential lockout upon login failure at the gas volume corrector. They apply to keyboard and serial-tentative accesses. The user can try to login up to three times, and then the algorithm slows down to prevent repetitive access attempts.

Lastly, there is robust protection of all gas metering communication. This includes safeguards against general attacks on an entire population of gas metering devices using Bluetooth. The Bluetooth Low Energy (BLE) protocol's six-digit passkey warranties authentication, and communication is encrypted using 192-bit keys. At the same time, the TCP/IP protocol performs authentication and encryption using cryptographic keys and provides whitelisting of Internet Protocol (IP) addresses.

Conclusion

Natural gas providers are seeking to run a better business by implementing smarter, more responsible solutions for the customers they serve. Key to this effort is ensuring that all critical gas metering and data management assets are protected from cyber threats. There is no substitute for sound, well-engineered cyber security processes, which reduce risks, mitigate hazards and keep sensitive operational and business data safe and secure.

For More Information

Learn more about Honeywell's Smart Gas Metering Solutions, visit www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell,
Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Industrial Park, Pudong New Area,
Shanghai 201203

www.honeywellprocess.com

WP-17-16-ENG
August 2017

Honeywell