Focus on
INTEGRITY
P&GJ

Three Strategies for More Secure Pipeline Operations

By ERIC CYTRYNOWICZ and MARTIN JOHNSON, Emerson

The safe movement of liquids and gases across the pipeline infrastructure of the United States is critical. Whether pipelines are delivering fuels for transportation or home energy, feedstocks used to manufacture a wide variety of plastics and specialty chemicals, or any of the myriad other products that keep nations running, pipeline companies must ensure that operation continues without incident 24/7.

Recently, the strategies to keep pipelines operational have come under even more scrutiny. A series of attacks targeting grids, pipelines, and terminals since 2012 has revealed that "security through obscurity" – the assumption that pipelines are outside of hackers' notice, so they are unlikely to be targeted – is no longer a viable option. Today, organizations must take an active role in implementing strong cybersecurity to protect their pipelines.

In fact, to promote cyber-resilience and increase security of the nation's critical infrastructure, the U.S. Transportation Security Agency (TSA) has issued three mandatory security directives for pipeline owners and operators. The directives provide a baseline of secure operation that organizations must follow, and it is safe to assume that these guidelines are only the foundation of more security requirements to come.

As cyberattacks increase in number and complexity, organizations will want to be prepared with their own flexible, secure, and up-to-date cybersecurity infrastructure to meet new guidelines and mandates.

To accomplish this shift to increased cybersecurity, companies must focus on building layers of defense from the supervisory control and data acquisition (SCADA) system all the way down to individual field devices.

Every organization will use a different set of technologies and solutions to secure their unique infrastructure and operational needs but following these three key guidelines should help any pipeline company successfully get started on their journey to more cybersecure operations: develop secure practices, enact solutions to ensure compliance, and use more secure protocols.

SECURE PRACTICES

Historically, it was common for remote terminal units (RTU) and flow computers to have limited security settings. Many legacy devices had username and password limits of a few characters, and often supported only lowercase letters. Numerous organizations simply left default usernames and passwords enabled on their devices in the field to simplify and speed service calls.

Increased security through better passwords: To meet today's more stringent TSA guidelines, pipeline companies must focus on improving the credentials they use to access devices across the fleet. Modern devices, and even older devices with updated firmware, support modern password and username best practices.

This is, perhaps, the simplest cybersecurity feature to enact, as it mimics security best practices users are accustomed to in their everyday lives. From online banking to shopping, today's users are digital natives used to the rigors of more advanced password management.

As a baseline, cybersecurity coordinators should insist on passwords of at least eight characters to increase the difficulty of an attacker guessing a password through brute force.

Requiring a combination of special characters, uppercase and lowercase letters, and numbers are also significant deterrents to bad actors hoping to access devices and systems. And those same passwords should be changed on a regular basis to ensure they do not become stale or end up compromised due to data breaches (**Figure 1**).

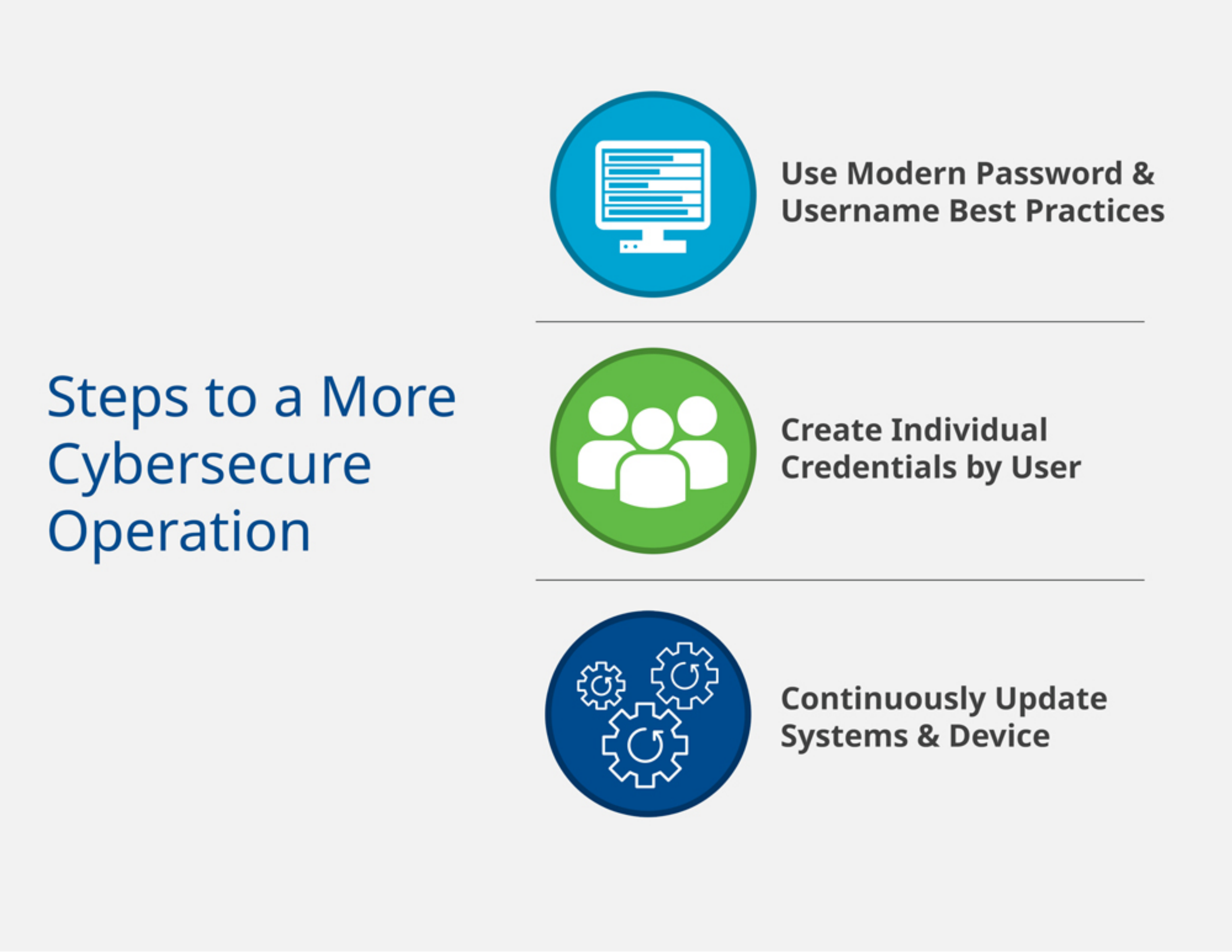

Steps to a More Cybersecure Operation
Use Modern Password & Username Best Practices
Create Individual Credentials by User
Continuously Update Systems & Device

Figure 1. A flexible, secure, and up-to-date cybersecurity infrastructure provides a strong layer of protection against cyberattacks. (Credit: Emerson)

In addition, some RTUs and flow computers offer lockout features which, after a specific number of failed logins, lock the system and prevent further login attempts for 10 to 15 minutes. Account lockout is a best practice that dramatically reduces the ability of attackers to perform brute force attacks using bots and other automated tools.

Individual credentials are key: While it is often easier to have one username and password shared among all field personnel for system access, most pipeline companies are moving away from such a practice. When everyone uses the same credentials, it not only opens more systems up to attack or human error, but also makes it difficult, if not impossible, to track the source of cybersecurity breaches.

Moreover, if every user in the organization has the same username and password on devices and systems, when a staff member leaves, the company is put in a difficult position. Either personnel perform the extensive work to change the username and password of each device, or they continue to operate using the same credentials, knowing a person who no longer works for the organization has access to critical technologies.

Today's high-performing organizations are ensuring each person on the network has an individual username and password. In addition, role-based security measures are recommended to ensure each person is assigned access rights based on his or her role or function. While the upfront work to put such a system in place can be time consuming, that commitment is far outweighed by the security gains and shortened change time when a person leaves the organization.

Companies employing this strategy know that only authorized personnel have access to the system, and they have solutions in place to track any unauthorized changes more easily, enabling faster and easier response and remediation of unexpected problems.

Continuous fortification of systems: Cyber-threats and their methods of delivery continually evolve. To reduce the footprint of attackable surfaces, operators should ensure systems across the pipeline network are locked down and up to date.

Creating this type of a cybersecurity structure starts with ensuring technicians apply security patches and firmware updates as they become available. Keeping systems and devices up to date removes known vulnerabilities as they are discovered, eliminating potential attack vectors.

One other key strategy many pipeline companies are using to defend their SCADA networks from intrusion is to limit or deny the use of unapproved external devices. Malware delivery via compromised USB devices is a common attack vector and has been responsible for some of the world's headline-generating security breaches. Computers can and should be locked down to block connection from any devices – thumb drives, optical devices, mobile phones, etc. – that are not explicitly approved.

ENACT SOLUTIONS

Even the best cybersecurity strategies are of little use if they are abandoned after a month or a year. Cybersecurity is a journey, not a destination, and as such, the most successful companies put systems in place to ensure their cybersecurity strategy is carried out and updated across the lifecycle of their systems.

A cybersecurity champion keeps programs running: The TSA's security directive 2021-01B requires pipeline facilities to designate a cybersecurity coordinator who is available 24/7. The cybersecurity coordinator monitors policies to ensure they are being followed, and he or she develops and directs vulnerability assessments to ensure policies and systems work as expected.

In addition, the directive requires organizations to conduct regular reviews of their current practices to identify any gaps, and to perform remediation measures to address cyber-related risks. In fact, as part of the guidelines, such findings and resolutions must be reported to the TSA and Cybersecurity and Infrastructure Security Agency within 30 days.

While the cybersecurity coordinator does not need to be a dedicated role, organizations that have the most success select individuals who have the time and experience to be successful in this position.

Simplifying compliance: Many organizations have tens of thousands of miles of pipelines, so managing the security of RTUs and flow computers in the field often requires sending engineers or field technicians hundreds of miles to remote sites to check on equipment, perform calibration, or collect data.

As organizations begin to implement more stringent cybersecurity policies across their field devices, sending a technician out to make required change quickly becomes unmanageable.

Moreover, more and more facilities are operating with a skeleton crew as personnel shortages make it difficult to maintain a full staff. Whether an organization has 100 or 10,000 RTUs, updating them individually to change passwords or manage accounts is costly and time consuming.

Today's forward-thinking companies are instead employing credential management software, which empowers field supervisors to handle account control from a central location. Using a credential management software package, companies can roll out new credentials and change old ones with the push of a button from a central location. All changes are instantly replicated across every device in the fleet.

This level of field device management allows cybersecurity coordinators to ensure all devices have adequate security more easily. The coordinator can quickly and easily remove and replace users – providing unique credentials – as staff changes occur. Simultaneously, they eliminate the errors in account creation that occur when rushed technicians must manually update credentials (**Figure 2**).

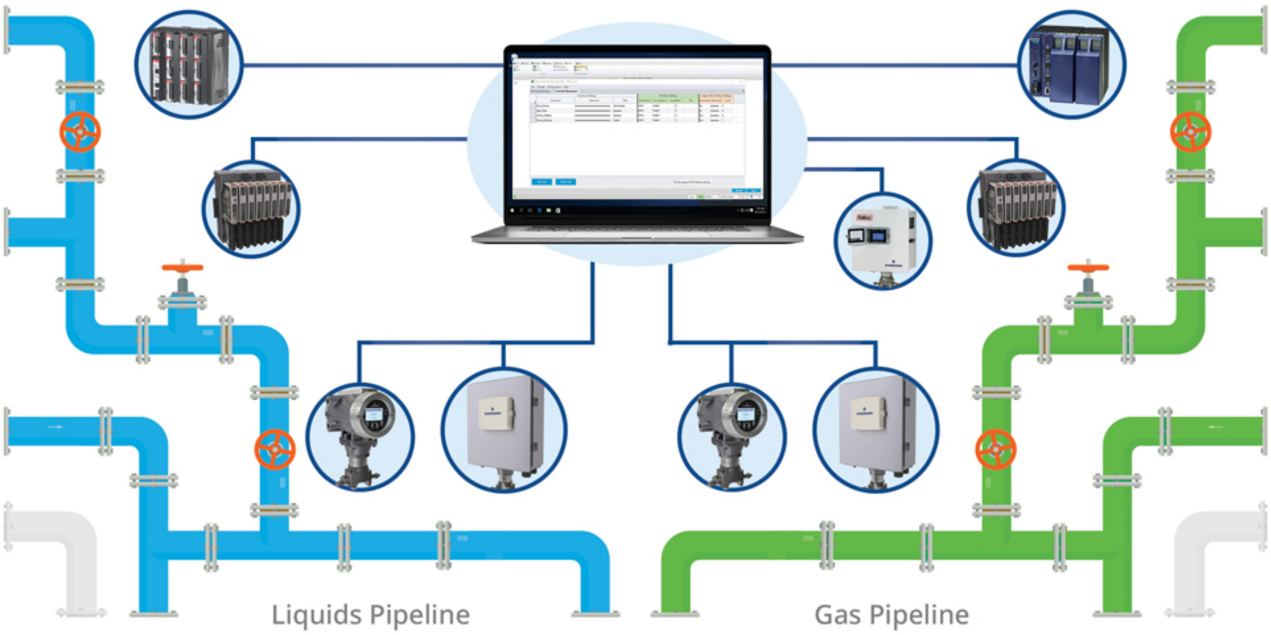


Figure 2. Emerson's new credential management tool enables users to perform bulk updates of TSA-compliant credentials rapidly and remotely across large install bases of Emerson RTUs and flow computers. (Credit: Emerson)

MORE PROTOCOLS

Until recently, security was not a primary concern in the design of most SCADA protocols. But the world has changed, and security is becoming more important to safe and sustainable operations. As a result, much of today's installed base of communications protocols does little or nothing to protect pipeline equipment – a serious liability that must be addressed.

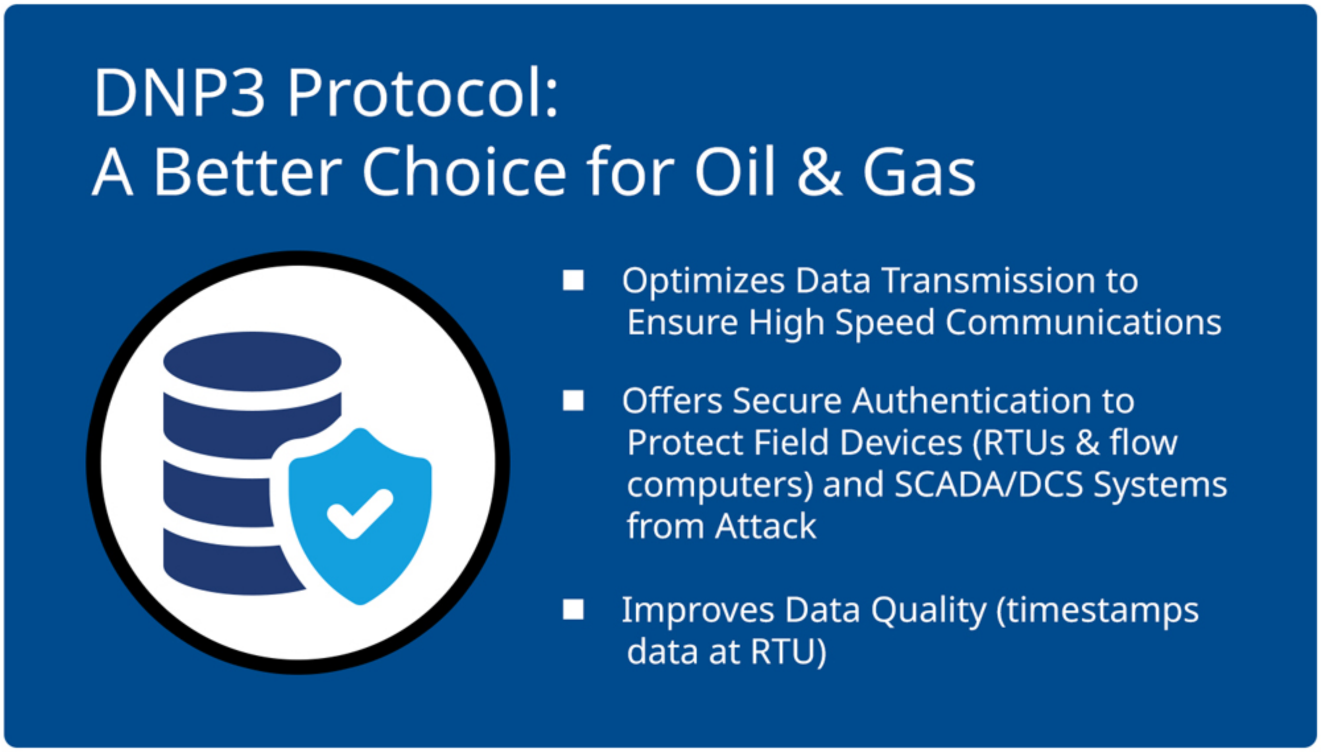
Modbus, the most well-known protocol used in pipeline systems, is insecure, providing no protection against unauthorized control actions. Proprietary protocols sometimes include basic security but are still subject to vulnerabilities.

To heighten security, a SCADA protocol must authenticate all devices, so unauthorized devices cannot participate in the network. It must also securely protect all credentials while in transit, and during login and while being changed. Using open but secure protocols that are subject to third-party review also helps pipeline companies avoid vulnerabilities.

Taking advantage of widely adopted modern protocols can help ensure the company has access to many different devices from a wide array of manufacturers. However, operators should ensure any protocols used still meet industry requirements for efficiency, reliability, and ease of use – regardless of the complexity or communication challenges in the network environment.

Employing DNP3 for secure, fast connectivity: To increase security across their networks, many organizations are looking to a protocol relatively new to the pipeline industry, but widely used by electric utility companies: Distributed Network Protocol 3 (DNP3).

This protocol is secure yet optimized for high-speed communications. To reduce traffic on the network, authentication is only performed when necessary to complete sensitive activities, making it suitable for use with even low-performance field equipment (**Figure 3**).



DNP3 Protocol:
A Better Choice for Oil & Gas

- Optimizes Data Transmission to Ensure High Speed Communications
- Offers Secure Authentication to Protect Field Devices (RTUs & flow computers) and SCADA/DCS Systems from Attack
- Improves Data Quality (timestamps data at RTU)

Figure 3. Many of the most well-known protocols may lead to vulnerabilities. Safe, sustainable pipeline operations require secure protocols like DNP3. (Credit: Emerson)

When a user performs a critical action, such as opening a valve or shutting down a device, the RTU and SCADA authenticate across the network to ensure each device is exactly what it claims to be. If a device does not authenticate properly, such as in the case of replay and modification attacks using false messages on the network, the action will not be performed.

DNP3 offers operators the best of both worlds: improved cybersecurity across the pipeline's SCADA system and field equipment, but without the overhead and delays that come with increased network traffic.

TODAY'S BASELINE IS A FOUNDATION FOR THE FUTURE

Recent events in the media have made it clear that pipeline organizations can no longer simply hope to be overlooked by cyber attackers but building a more secure foundation is not an insurmountable task. Pipeline information technology and operational technology personnel have a wide array of technologies and strategies at their disposal to begin building a more secure, effective infrastructure.

Putting such a foundation in place will help organizations defend their systems today while preparing them to meet the threats and institutional guidelines of the future more easily through incremental changes and upgrades that continue to secure systems across their lifecycles. **P&GJ**

ERIC CYTRYNOWICZ, RTU product manager with Emerson's Energy and Transportation Solutions business, is responsible for development of scalable, high-performance automation that also offers ease-of-use simplicity. Eric received a Bachelor of Science degree in chemical engineering from Penn State University and an MBA from Temple University.

MARTIN JOHNSON, director of product marketing with Emerson's Energy and Transportation Solutions business, focuses on modern data-driven flow measurement automation for reliable, safer, and more sustainable operations. Martin received a Bachelor of Engineering degree from the University of Surrey.

Scroll down to read