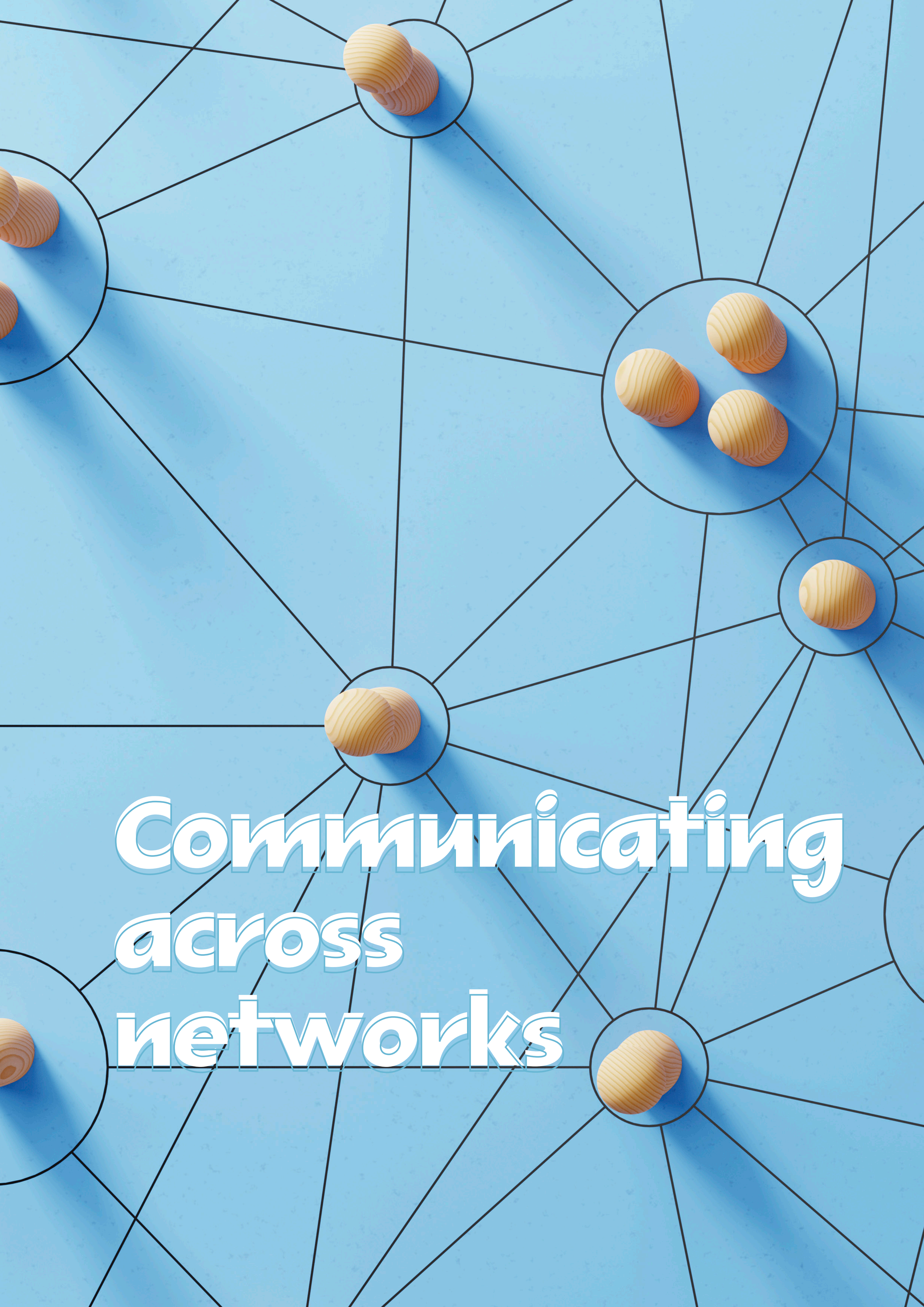
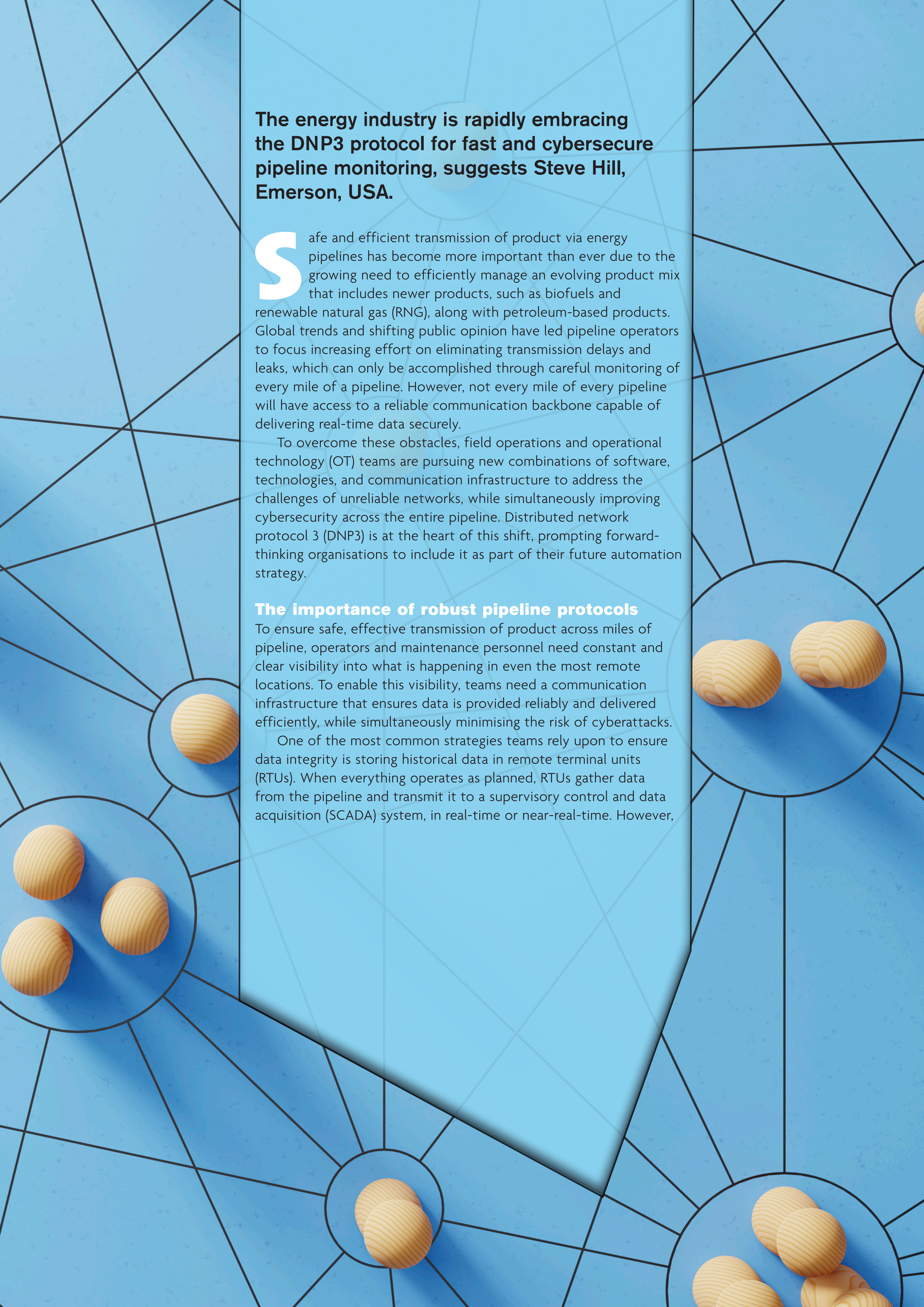


Communicating across networks



The energy industry is rapidly embracing the DNP3 protocol for fast and cybersecure pipeline monitoring, suggests Steve Hill, Emerson, USA.

Safe and efficient transmission of product via energy pipelines has become more important than ever due to the growing need to efficiently manage an evolving product mix that includes newer products, such as biofuels and renewable natural gas (RNG), along with petroleum-based products. Global trends and shifting public opinion have led pipeline operators to focus increasing effort on eliminating transmission delays and leaks, which can only be accomplished through careful monitoring of every mile of a pipeline. However, not every mile of every pipeline will have access to a reliable communication backbone capable of delivering real-time data securely.

To overcome these obstacles, field operations and operational technology (OT) teams are pursuing new combinations of software, technologies, and communication infrastructure to address the challenges of unreliable networks, while simultaneously improving cybersecurity across the entire pipeline. Distributed network protocol 3 (DNP3) is at the heart of this shift, prompting forward-thinking organisations to include it as part of their future automation strategy.

The importance of robust pipeline protocols

To ensure safe, effective transmission of product across miles of pipeline, operators and maintenance personnel need constant and clear visibility into what is happening in even the most remote locations. To enable this visibility, teams need a communication infrastructure that ensures data is provided reliably and delivered efficiently, while simultaneously minimising the risk of cyberattacks.

One of the most common strategies teams rely upon to ensure data integrity is storing historical data in remote terminal units (RTUs). When everything operates as planned, RTUs gather data from the pipeline and transmit it to a supervisory control and data acquisition (SCADA) system, in real-time or near-real-time. However, many pipelines traverse remote areas with little or no reliable communication infrastructure (Figure 1).

In remote areas, operators and maintenance personnel rely on cellular modem, satellite communication, or other technologies to transmit data to the SCADA system. Often, these communication technologies are too unreliable to guarantee consistent real-time communication. The teams monitoring the pipeline know they will intermittently lose connection and design their infrastructure accordingly.

When the connection drops, modern RTUs typically store historical data, with metadata including an accurate time stamp to ensure accuracy of information. When the connection is restored, the RTU automatically transmits stored data to the SCADA system, which backfills the information in its database. This ensures that consistent, contiguous datasets are available for data analysis, which may not be possible, or as accurate, if even a small subset of the original raw data is missing.

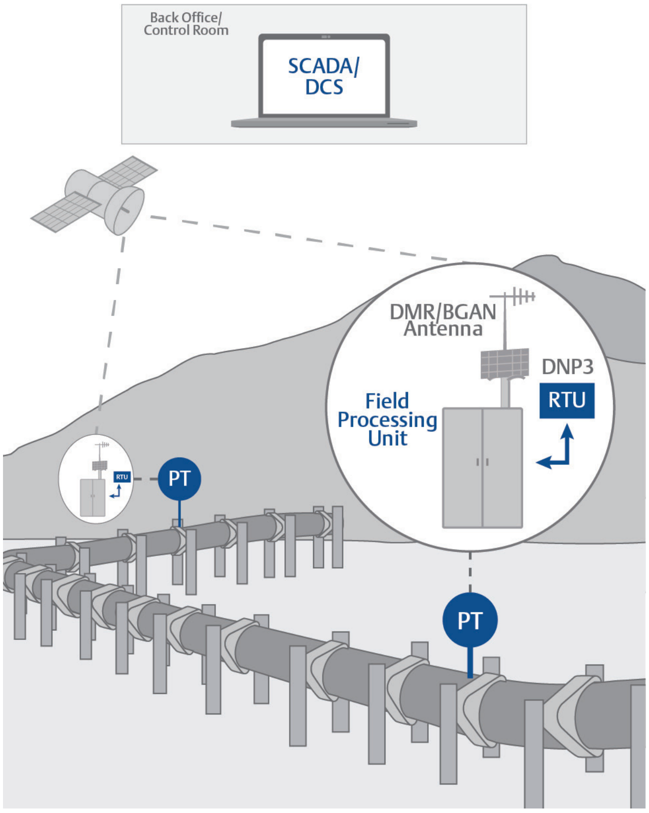


Figure 1. Emerson is at the forefront of bringing the DNP3 protocol to the energy industry to provide fast and secure transmission of data between RTUs in the field and the SCADA system.

One of the most critical tasks when analysing this historised and backfilled data is leak detection. The calculations for leak detection are complex, requiring a complete view of variables – such as temperature and pressure – across the pipeline, requiring data timed accurately with no gaps. For many leak detection mechanisms, it is important that the data is gathered at the same time, with a need for accuracy in the millisecond range. Because it takes time to transmit data – either due to intermittent communications or simple latency on the network – backfilling data with accurate timestamp metadata generated at the RTU is essential to timely and accurate leak detection.

Moreover, speed of the network is essential. Even with historised data, operators and technicians want visibility as quickly as possible. As a result, they rely upon protocols that minimise bandwidth requirements to ensure fast and reliable communication.

New challenges stem from modern problems

Many of today's pipeline operators – especially in the US – rely on the Enron Modbus protocol to transmit critical data from RTUs in the field to the SCADA system in the control room. When it was developed, Enron Modbus was the gold standard for fast, reliable transmission of data across pipelines because it allowed users to transmit historised data across the network by using extensions to the Modbus RTU industry standard protocol.

Decades after its introduction, however, Modbus is showing its age. Because pipelines are critical infrastructure, they are prime targets for cyberattacks; today's pipeline operators need cybersecure technologies to move data across their networks, and Modbus is not a cybersecure protocol.

Figure 2. Modern RTUs designed for the DNP3 protocol enhance the reliability and security of critical data, while helping to future-proof pipeline operations.

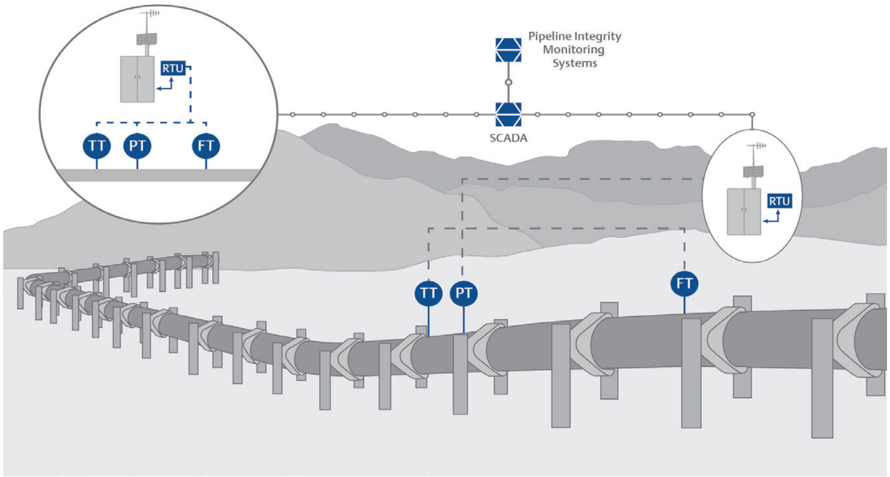


Figure 3. **The DNP3 protocol is optimised to allow data from multiple devices, including Emerson's FB3000 RTU and Rosemount™ transmitters, to be transferred by exception across the network.**

It is possible to mitigate the cybersecurity risk of Modbus by implementing additional defence-in-depth layers, such as encryption and firewalls. However, best practices for defence-in-depth require each layer to be cybersecure on its own, meaning the protocol running inside of those firewall and encryption layers should itself be cybersecure.

Moreover, Modbus has never been fully defined as a standard. As a result, using Modbus can make it difficult to troubleshoot connection issues between devices and the control system. Varying data types, byte order differences, floats, and more can all create issues when they differ between RTUs and the SCADA system, making the integration of devices and software from different vendors even more complex.

Some SCADA systems and RTUs support secure proprietary protocols in addition to Modbus, but even this solution has its drawbacks. While proprietary protocols can increase cybersecurity and simplify connectivity, they significantly limit the selection of equipment available for use in the field. Users are limited to RTUs and other devices that support those same protocols, which can often result in vendor lock-in and difficulty finding and retaining personnel who can support the more obscure protocols.

A better alternative

In a world of more open automation, pipeline operators are recognising the value of protocols with a wider range of connectivity to devices, while still supporting cybersecure communication. Teams planning projects no longer accept a binary choice between proprietary protocols which limit their options, and Modbus which is not cybersecure. Fortunately, the electrical industry had a similar issue for years, and it developed a secure and extensible protocol that eliminates the need to choose between security and flexibility: DNP3.

While the electrical industry uses DNP3 to manage digital, high-speed data, it can also be used to transfer slower, analog data – like that used to monitor pipelines. As a result, the pipeline industry is rapidly adopting DNP3 as a standard to transfer oil and gas electronic flow measurement data from RTUs to SCADA systems.

The greatest value of DNP3 is that it is secure, yet fast. DNP3 is optimised for high-speed communications, allowing data to be transferred across the network by exception as it changes, while including the same timestamp metadata as Enron Modbus. In addition, DNP3 includes support for secure authentication between RTUs and the SCADA system.

Any time a user performs a critical transaction – for example, writing to outputs to open a valve or shut down a device – the RTU and SCADA must authenticate with each other for confirmation that both are exactly the devices or systems they claim to be. This authentication also prevents person-in-the-middle attacks, where messages are tampered with in transit across the network.

But in pipelines, cybersecurity cannot come at the cost of availability or performance. If every protocol interaction on the network is encrypted, the bandwidth required will generate network latency that can cause availability issues, making it difficult to implement with relatively low-performance field equipment.

To avoid this problem, DNP3 is not an encrypted protocol. Most communication via DNP3 is unencrypted, and authentication is only performed when required for sensitive activities. This makes the most efficient use of available bandwidth, and it has the advantage of allowing for the capture and analysis of communications with off-the-shelf network analysis tools. This empowers engineers and technicians with powerful and familiar tools when troubleshooting issues, giving them similar capabilities to the familiar legacy Modbus protocol.

Moreover, the unencrypted nature of DNP3 enables the use of third-party network analysers and dissectors, for example, artificial intelligence and machine learning algorithms to further increase oversight of the network. These technologies can monitor DNP3 traffic for suspicious activity and send alerts when they detect aberrations, adding an additional layer of warning, even if the SCADA system is compromised. Teams needing additional cybersecurity can add encryption over the top with transport layer security or a virtual private network.

DNP3 is also extensible, offering additional flexibility. For example, Emerson has extended the DNP3 protocol to carry RTU files containing critical electronic flow measurement data, alarms, and events. Should communication be lost when an event – such as overpressure – occurs and dissipates quickly, logged alarms in the devices, transmissible by extended DNP3, ensure operators have visibility to the alarm, even if it occurred during the communications outage. The inclusion of historical metering data in these files provides a level of buffering and backfill beyond that supported by standard DNP3, even allowing data to be re-collected if it is lost after the initial collection (Figure 3).

Modernisation is an opportunity for a DNP3 foundation

Being ready for the future of pipeline operation means starting to lay the foundation for DNP3 as a standard protocol. Winning the future of energy transmission will mean moving away from legacy standards and embracing the technologies that will drive secure and efficient pipeline operations well into the coming decades. Already in the Middle East, Asia Pacific, and Europe, many pipeline operators and production facilities are requiring DNP3 in their requests for proposal on new projects.

While adoption in the US has been slower, it is starting to gain momentum. As the popularity of DNP3 as a standard grows across the globe, it will offer pipeline operators and production facilities a wider selection of equipment and greater flexibility of design when considering new designs as part of a modernisation.

To prepare for this transition, leadership can begin adding DNP3 as a requirement in the request for proposal process for any new automation projects. Typically, the lifecycle of a control system is about 15 years, so preparing today for a foundational technology will help future-proof investments, avoiding the need to rip and replace equipment that was not prepared for a technology shift on the horizon.

Preparing for the future

The need for devices that store and contextualise historical data to support trending and diagnostics across a pipeline network is not going away any time soon. But while many companies use RTUs supporting that technology today, those same devices are often not able to provide the secure communication required to keep their investments and reputations safe as cybersecurity threats increase (Figure 2).

Defence-in-depth is only as strong as its weakest layer, and a layer with no security is a liability to the entire system. Open technologies like DNP3 provide the security pipeline operators need, without sacrificing the performance that supports availability. In the coming years, more and more vendors will begin to support DNP3 in SCADA systems and RTUs, likely making it the de-facto standard for communication, and unlocking flexible pipeline management options that will become the new industry best practices. It is not too soon to begin preparing for that transition, building a foundation of flexible, secure communications infrastructure that will protect investments for years to come.