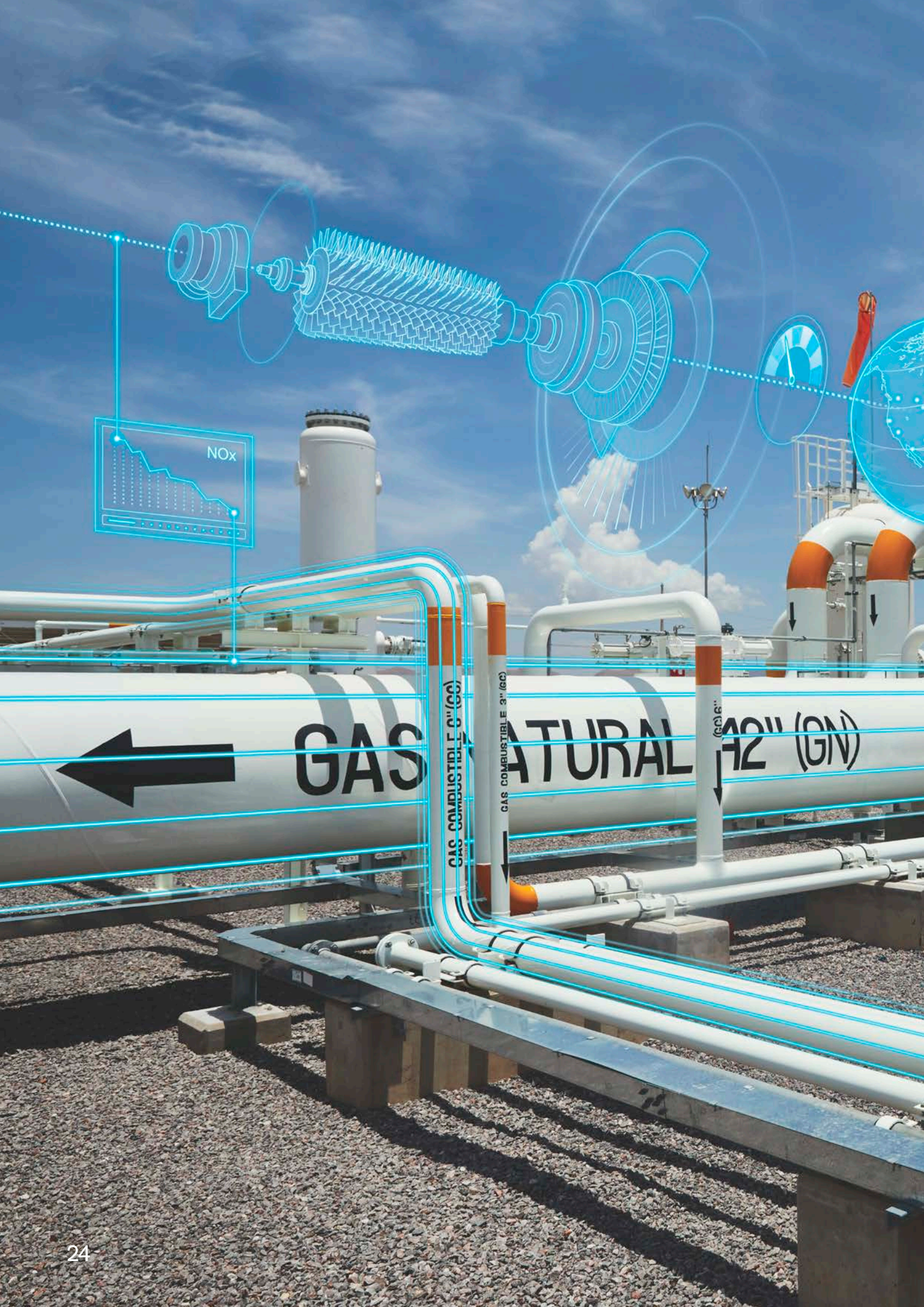
NOx
GAS
ATURAL
42" (GN)
GAS COMBUSTIBLE 3" (GC)

TWO SIDES OF THE SAME COIN

Carmen Garibi and Bob Skiebe, Siemens Energy, USA, discuss why digitalisation and cybersecurity go hand-in-hand when it comes to protecting assets against cyber intrusions.

Digitalisation continues to unlock tremendous value for operators across the oil and gas supply chain. From artificial intelligence (AI) and machine learning (ML) to virtualisation and digital twins, the benefits and capabilities provided by sophisticated software technologies are becoming harder and harder to ignore.

The midstream industry has not been immune to this trend. In recent years, an increasing number of forward-thinking pipeline companies have begun leveraging the power of data to improve efficiency and safety, lower costs, and optimise the lifecycle performance of their assets. Many, however, have done so by simply bolting digital solutions on top of legacy systems without implementing sufficient measures to protect against cyber intrusions. The number of operators leveraging remote services is also increasing. Together, these factors have created an entirely new set of risk parameters that just a few short years ago were not part of the equation.

In this article, we discuss how the industry can address the new normal by adopting a more holistic approach to cybersecurity (i.e. cybersecurity by design). We will also look at how recent advancements in AI and security analytics can help operators quickly detect and respond to cyberattacks, so that the full potential of digital transformation can be realised.

The cost of not digitalising

When discussing the topic of cybersecurity in oil and gas, it is important to preface the conversation by stating that the benefits of digitalisation and cloud connectivity (when properly implemented) significantly outweigh the perceived risks. This is true across the entire industry, but it is especially the case for pipelines, where even a marginal efficiency increase at a pumping or compression station can potentially translate into millions of dollars in annual savings.

Consider, for example, the application of cloud-based data analytics to the operation of electric motors driving centrifugal pumps. The costs to energise these pumps often represents one of the most substantial expenses for pipeline operators. In an 800 mile pipeline with 18 pump stations and electricity costing 7.5 cents/kWh, the utility bill over five years can be as high as US$150 million.

Now consider the massive volume of data coming from the automation and SCADA systems controlling the pipeline. One of North America's largest pipelines generates more than 20 000 points of data every five seconds from scores of pump, valve, and monitoring stations.

This raw data holds enormous potential that can be unlocked by processing and analysing it against the delivery schedules of various customer products, each with its own hydraulic characteristics. Analytics can take into account the power demands of those hydraulic characteristics and propose parameters aimed at helping operators reduce pumping station electrical loads, in a process known as batch optimisation.

In the case of the hypothetical 800 mile pipeline, just a single percentage point reduction in power by each of 18 pumping stations along the route can save US$7.5 million in utility costs in the first five years. A 1% reduction in power usage could also translate into upwards of 70 000 metric t of CO_2 savings.

This is just one of many examples that illustrates the benefits that operators stand to miss out on by not leveraging digitalisation. In addition to 'smart pumping' solutions, there is now a wide range of field-proven digital innovations that operators can apply to reduce costs and improve pumping and compression performance, including drivetrain analytics, remote diagnostic services (RDS), and digital twins, to name a few.

Pipeline cybersecurity challenges

In the context of pipelines, it is impossible to talk about digitalisation and cloud connectivity without mentioning cybersecurity. They are, as they say, two sides of the same coin.

Cyberattacks now threaten the core value proposition of every oil and gas organisation, and companies today must be prepared to operate in an environment where attacks are not just probable, but inevitable. Unfortunately, pipelines often make for a desirable target due to their interconnected and distributed nature, as well as the high impact outcome that can arise from a successful attack.

One such attack took place as recently as February of this year, when a ransomware event caused a natural gas company to shut down a pipeline for two days.[2] The malware infected the IT network and then spread to the operational technology (OT) network in a gas compression station. The hackers then initiated the ransomware, which went on to encrypt data and block critical systems and equipment from operating correctly.

For the operators of the 2.5+ million miles of pipelines across the US, it is events like these that highlight the vulnerabilities pipeline infrastructure possesses. It also makes evident the importance of adopting cybersecurity by design principles, which focus on designing infrastructure with the expectation that cyberattacks will inevitably occur. This is as opposed to implementing security measures and merely hoping that they never have to be put to the test.

As mentioned previously, much of the legacy pipeline infrastructure in operation today was not explicitly designed with cloud connectivity or remote services in mind. This convergence of IT and OT systems within compressor and pumping stations represents a potential vector for cyber intrusions. That risk is magnified when digital technologies are not securely implemented.

Many operators are under the false impression that the only way to truly protect against a cyberattack in today's environment is not to connect at all (a practice referred to as 'air gapping'). However, air gapping does no protect against inside threats. In fact, in the February ransomware attack, the malicious party gained access via a link that was sent through email.

Overall, inside threats pose a severe risk to pipeline operators. In a survey conducted by Siemens and the Ponemon Institute of nearly 400 oil and gas security professionals, approximately two-thirds said that a

negligent or careless insider was their top cybersecurity concern.[2]

Air gapping is also problematic in that it limits visibility into the operating environment, which makes it all but impossible to recognise abnormalities and react when a cyberattack does take place. Quite simply, it is not an effective method for protecting against intrusions, especially in the case of older automation and control systems that have not updated, as they are often the easiest for attackers to gain access to.

Gaining visibility with AI

Today, the primary challenge when it comes to protecting pipeline assets from cyberattacks is visibility. After all, organisations cannot protect what they cannot see. Most operators are not even aware of the threats that lie within their fleets, and many lack a comprehensive response plan if a cyberattack does occur.

Ironically, the key to addressing the cybersecurity challenge is digitalisation, and more specifically, the use of analytics and AI, which can quickly detect when an attack is occurring. AI-based solutions can also provide contextualised information so that effective action can be taken to eliminate the threat. These tools have been successfully applied across a wide range of industries; however, they have historically been cost-prohibitive to implement and scale for pipelines, which have distributed IT and OT networks spread over millions of square miles of remote terrain.

Siemens Energy set out to solve this problem by partnering with SparkCognition to deploy DeepArmor® Industrial, fortified by Siemens, which is a new cyber defense system designed to protect endpoint and remote OT assets across the energy value chain.

DeepArmor features an AI-driven system that provides continuous monitoring and the capability to quickly detect cyberattacks, delivering next-generation antivirus, threat detection, application control, and zero-day attack prevention to endpoint oil and gas transmission and distribution assets. The partnership aims to help the midstream and broader oil and gas industry address its cybersecurity challenges by, for the first time, providing operators with fleet-level monitoring and protection capabilities.

AI-based technology recognises and reports new devices or behaviour changes that characterise insider threats. Its predictive analysis enables DeepArmor to prevent malicious code from executing, even if that code is not yet part of threat intelligence packages.

The system also recognises and reports changes to system conditions that characterise a digital-physical attack, either mitigating the threat or making it easier to diagnose. This means DeepArmor Industrial provides unique, unprecedented protection to edge assets in the field – even if new threats emerge between updates or attacks arrive at isolated sites before patches can be deployed.

Most current cybersecurity technologies rely on updates. A system updated on Monday is ineffective on Friday against any new attacks emerging on Tuesday, Wednesday, or Thursday. DeepArmor, on the other hand, leverages a machine-learning detection engine, which uses advanced classification algorithms to predict and prevent zero-day industrial attacks without frequent updates or cloud access.

Siemens Energy and SparkCognition tailor the machine learning models for the OT environments. They are built using samples of known clean files and malicious files targeting OT environments. This results in a protective layer that includes script control, USB control, application control, and model control. Once installed and serviced by Siemens Energy, it remains steadily effective – without regular updates, and in the face of innovative attacks developed any day of the week, month, or year.

If a threat is detected, Siemens Energy's OT specialists can then work with customers to take quick and decisive action to mitigate the threat. It is important to note that in many cases, this will not mean shutting down the system, which is what most attacks to date have forced pipeline operators to do. Instead, it is about developing a proportionate response that balances operational, safety, and cost objectives.

Building resiliency

Regardless of whether infrastructure is digitalised or not, pipeline operators should begin to operate on the premise that the probability of a cyberattack at some point in the not-so-distant future is 100%. Given this reality, the focus should be on improving resiliency and putting in place the necessary systems to detect and respond to events when they do inevitably occur.

When evaluating the risk of cyberattacks, it is easy for operators to focus on the financial impact (i.e., the monetary loss associated with an unplanned shutdown). Too often, however, the health, safety, and environmental (HSE) elements are not given the same level of attention. Pipelines are unique in that a cyberattack has the potential to not only put employees tasked with operating and maintaining equipment at risk, but also the people and communities located close to the route.

Ultimately, the process of securing oil and gas infrastructure is both a sprint and a marathon. As the sophistication and frequency of cyberattacks increases, we also see advancements in the technologies needed to counter them, with AI and security analytics leading the way. By leveraging these tools, organisations can own their environment so that the full potential of digital transformation can be realised.

References

1. "Ransomware Impacting Pipeline Operations"(2020, February). Cybersecurity & Infrastructure Security Agency , https://www.us-cert.gov/ncas/alerts/aa20-049a
2. The State of Cybersecurity in the Oil & Gas Industry: United States. (2017, February). Ponemon Institute Research Report. http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf