Originally appeared in:
February 2020, pgs 63-65.
Used with permission.
HYDROCARBON PROCESSING®

HP | Cybersecurity

C. GARIBI, Siemens Oil and Gas, Houston, Texas

Cybersecurity visibility and resilience: Keys to protecting HSE/margins in operations

As digitalization accelerates in today's downstream refining and petrochemical facilities, operators need to stay ahead of ever-growing cyber vulnerabilities in the operational technology (OT) layer—prime targets for threat actors—that may not be covered by traditional IT safeguards. Unfortunately, too often, that is not the case for a variety of reasons.

The situation is a good news/bad news story. Let us start with the good news. The downstream industry segments are rapidly digitalizing, with a significant number of operators seeing improvements in their capital efficiencies and operating margins as a result of their digital investments.

In fact, according to a joint study,[1] oil and gas companies report that they are benefiting from digitization; however, 66% of respondents are concerned that it has made them more vulnerable to security compromises. These increases have made organizations more aware of the need to have security analytics. Sixty-eight percent of respondents say this technology is essential or very important.[1]

The bad news is that, as the digitalization of downstream refining and petrochemical operations increases, their vulnerabilities inevitably increase, as well. As the number of interconnected digital assets, controls and networks increase, a wider span of plants is crossed and the overall cybersecurity risk exposure—what cybersecurity experts call the "attack surface"—of the operations is increased.

Greater transparency needed: You can only predict what is visible. Despite accelerating the digitalization of plant facilities, plantwide visibility of capital assets (and the controls and networks interconnecting them) can be limited. This can be due to the deployment of single-point-of-use digital solutions that are not well integrated, resulting in disconnected data repositories and islands of digitalized assets and production capabilities.

One critical effect of a lack of visibility is this: *You can only protect what is visible.* If this expanded attack surface is not fully visible, then it cannot be adequately protected. Consequently, downstream operators can become more exposed to hackers, malware, malicious bots (self-propagating malware), ransomware, phishing exploits and many other types of threats than they once were.

Hackers can range from malcontents simply seeking to test an operation's defenses, to "hacktivists" wanting to disrupt refining and petrochemical operations for political reasons, to sophisticated, state-sponsored professionals using advanced tools to penetrate defenses and cause significant and costly operational disruptions, with potentially catastrophic health, safety and environmental (HSE) consequences.

The latter type of threat actors can hide malware that can sit undetected in a network for months or longer, awaiting an external or preset internal trigger to begin stealth espionage, or the theft of data and/or intellectual property, or both. Alternatively, this hidden malware can be programmed to disrupt operations when activated, which can cause huge costs in terms of lost production, missed customer commitments and, worst of all, the compromised safety of plant personnel and surrounding communities. These are not only potential scenarios but are also the kinds of attack attempts that are happening in the field. In a recent OT cyberattack on a petrochemical plant, safety systems were attacked by the deployment of dangerous malware. The goal of this attack was to disrupt operations and cause physical harm to people.

Downstream digitalization deployments outpacing cybersecurity safeguards. Another issue is that cybersecurity safeguards are not keeping pace with the downstream sector's digitalization efforts. One reason is that, when it comes to digitalization initiatives, cybersecurity usually takes a back seat to what might be considered more strategic concerns.

For example, metrics such as capital efficiencies and operating margins may command more attention of plant managers, company executives and their board members as being strategic to maximizing shareholder value and market capitalization. However, when they think about cybersecurity, they often consider it to be a lower-level tactical concern best delegated to the security experts that they presume to exist in their IT organizations. Those experts may not exist, or, if they do, they may be oriented toward enterprise IT cybersecurity, not the special needs of OT. While IT staff must certainly be involved in protecting a downstream plant's assets, controls and networks, most of them lack the knowledge and skills to fully address OT's unique cybersecurity requirements in downstream refineries and petrochemical plants.

The availability of IT teams to get involved can be limited, as well. They have many other pressing daily responsibilities. They can be too busy running the enterprise/front-office side of a plant's operations and providing back-office, data-center and end-user support, while also working with their OT counterparts to maximize production efficiencies and output.

Chances are, they simply do not have the time to learn how to properly set up, monitor and continually update the kind of

layered, defense-in-depth OT cybersecurity safeguards that can protect plants from determined adversaries with much higher and more focused skill levels. Furthermore, a plant's IT professionals lack the ability to respond quickly and effectively to a detected cyber intrusion or disruptive direct attacks, such as ransomware or denial-of-service attacks.

Traditional IT cyber safeguards: Insufficient for demanding OT environments. For decades, just like in other industries, downstream plants have used industrial control systems (ICSs) to automate workflow processes, operating them over standalone supervisory control and data acquisition (SCADA) and OT networks. While the latter may be linked to and communicate with higher-level systems, they would not typically be connected externally. However, that is changing with increasing digitalization. For example, more multi-plant owners may want to monitor their equipment fleets and capital assets across a region or their entire enterprise for performance optimization, remote diagnostics, functional issue resolutions, regulatory compliance and various operating analyses. Similarly, original equipment manufacturers (OEMs) of plant equipment may want access to their equipment for remote performance monitoring.

How will they do it? This is accomplished with external Internet connections that can expose plants to external threats. To safeguard against intrusions, virtual private networks, firewalls and identity-and-access management are important (and necessary) protections. In a complex refinery or petrochemical plant, they add to the administrative and maintenance burden of the plant's IT group. However, that is a small consideration when compared to an even greater distinction between IT and OT cybersecurity concerns.

OT vs. IT infrastructure security. In general, a plant's enterprise IT network connects employees not only with each other (via email, web collaboration tools and even voice communications), but also with information via different company databases, file-sharing servers and various software applications. Should typical enterprise cyber threats (such as malware, data theft, or corrupted data or devices) occur in front-office or back-office environments, user productivity and a company's transactional capabilities could be disrupted.

Those consequences can be costly, but the key difference between OT and enterprise IT digital infrastructures is: *If the latter is compromised, there are no known injuries to people.* In addition to this critical life-safety security distinction, OT differs from non-industrial enterprise IT digital infrastructures in other significant ways, as shown in **TABLE 1.**

Another difference is that OT digital infrastructures used by the downstream sector typically operate around the clock, in real time or near-real time, and require 99.9% uptime or better. In contrast, enterprise IT infrastructure can run on a best-effort basis. This means that a break in one part of an IT network forces routers to send data packets down alternate paths. One-second or two-second delays are not a problem for end users, who may not notice the delays. However, given that deterministic ICSs must operate within millisecond latencies or less, one-second or two-second delays can cause a costly production shutdown with potential HSE impacts. The disruption risks of a security breach in the OT infrastructures can be much greater than for an enterprise IT network.

Finally, a key distinction between IT and OT digital infrastructures is that the OT infrastructures must operate inside a much more intricate, multi-vendor context of varied versions and configurations of components, firmware and software. Enterprise IT digital infrastructures usually feature much more standardization.

As a result, there can be many undocumented interdependencies that only come to light when a change in one area of production causes unplanned impacts elsewhere in a plant's operations. For example, introducing an anti-virus software update to an OT network, despite being an IT cyber-protection best practice, can potentially introduce unwanted latencies in production processes, enough to upset ICS deterministic communications and disrupt those processes.

Digitalization and cybersecurity: Two sides of the same coin. How should downstream industries proceed to meet their cybersecurity challenges today and in the future? Most fundamentally, they must consider cybersecurity as intrinsic, even foundational, to their digitalization efforts. Too often, as previously mentioned, it is considered a tactical afterthought and in an IT context, which are notions that can undermine the best-intentioned digital initiatives.

Digitalization and cybersecurity are two sides of the same coin. In combination, they support greater asset reliability, availability, safety and resilience. Ultimately, this can mean more asset utilization, return on asset equity and profitability.

Best practices in OT cybersecurity go beyond good "security

TABLE 1. Security issues compared between enterprise IT and industrial OT infrastructures

Category	IT system	ICS
Risk management requirements	Data confidentiality and integrity are paramount	Human safety is paramount, followed by protection of the process
Time-critical interaction	Less-critical emergency interaction	Response to human and other emergency interactions is critical
Communications	Standard communication protocols	Many proprietary and standard communication protocols
Managed support	Allow for diversified support styles	Service support is usually provided via a single vendor
Component lifetime	Lifetime of 3 yr–5 yr	Lifetime of 15 yr–20 yr
Access to components	Components are usually local and easy to access	Components can be isolated or remote, and require extensive physical effort to gain access

Source: National Institute of Standards and Technology's (NIST's) *Guide to Industrial Control Systems (ICS) Security*

hygiene" involving careful network segmentation; the upkeep of security layers, both physical and virtual (e.g., firewalls, malware protection); and comprehensive, role-based identity-and-access management. While these elements are necessary, they are insufficient to deliver the holistic visibility needed to achieve the most impenetrable operating model possible.

Downstream operators can no longer think about security as an out-of-the-box solution, especially because their plants are far too complex for such an approach. Instead, they must think in a more expansive context—across entire asset classes of machines, systems and processing units, as well as the ICSs and networking systems commanding and linking them together.

Therefore, forward-thinking downstream plant operators will evaluate adding OT analytics—augmented with artificial intelligence (AI) and machine learning (ML)—to their digital infrastructure's software stack. Once deployed, OT analytics can make hardened, threat-proof cybersecurity an outcome of the high-visibility, integrated inventory management of a plant's various, yet critical, operating assets, including:

- Distributed control systems
- SCADA systems
- Safety instrumentation systems
- Historian databases
- Remote terminal units
- Smart field instrumentation and sensors
- Programmable logic controllers
- Networks and their components
- Human-machine interfaces
- Computer numerical control machines
- Radiofrequency identification systems
- Roaming transporters, such as automated guided vehicles.

Such a comprehensive and integrated approach to asset management, combined with OT analytics, can enhance a plant's ability and improve the visibility of three key facets of its asset operations: their vulnerability, configuration and compliance with both plant standards and regulatory requirements. It also supports the backup and recovery of data and affected/infected assets—thereby minimizing or eliminating production disruptions and boosting plant resilience to disruptive events.

In addition, integrated asset management plus AI/ML-driven OT analytics can offer plant operators a real-time asset monitoring model that draws data from various operational dimensions into a "single source of truth" that eliminates silos of isolated data repositories. This can provide a complete view of suspicious activities, as indicated by anomalous asset behaviors, and produce actionable recommendations that are fully contextualized.

The latter can support a more collaborative response to adverse events from IT and OT teams, including engineers and technicians, so they can gain a quicker jumpstart on detecting intrusions, quarantining the offending agents to prevent their spread, and determining and enacting mitigating or remedial responses much faster.

The time to get started is now. Digitalization's economic benefits and competitive imperatives are too compelling to ignore, which is why more downstream operators are stepping up their investments in the latest digital assets, controls and networks. OT connectivity across all of them is fundamental to their interoperability and a single integrated view of their operations, including vulnerability, configuration and compliance.

Should a cyber threat manifest itself in an adverse event, plant management can be confident that a plant's integrated asset management model, supported by OT analytics ensures enough resilience to contain the threat and to prevent production disruptions and HSE impacts.

The time to get started on the road to realizing this operating model is now. Digitalization and cybersecurity must be strategically aligned throughout the design, engineering and implementation of this model. IT and OT teams must collaborate on this effort and be fully supported by executive management and company boards of directors.

All stakeholders must understand that perpetrators of cyber threats against the downstream sector will continue to regard this sector's plants as prime targets and assume that operators will continue considering cybersecurity to be a tactical afterthought and not a strategic priority. Smart plant operators know differently and will act proactively. HP

LITERATURE CITED

[1] The State of Cybersecurity in the Oil & Gas Industry: United States, Ponemon Institute, February 2017, https://sie.ag/36zF369

CARMEN GARIBI leads cyber and digital security for Siemens Oil & Gas and provides consulting services to customers needing to strengthen their defenses against the ever-increasing frequency and sophistication of cyber threats. She is part of a vast, global network of Siemens cybersecurity experts and resources.