SAFETY AND SECURITY ON TWO FRONTS

Justin Maloney, Atlas Field Services, USA, outlines the importance of integrating cyber and physical security measures in downstream facilities.

Every day, while working onsite in downstream facilities, safety professionals are thinking about the various components of their safety programme, including US Occupational Safety and Health Administration (OSHA) regulations, daily or hourly safety checks, and hundreds of workers meeting guidelines and standards. But how often are operators and facilities able to step back and take a holistic look at their safety strategy and the external threats facing their plan that are not on a standard or required checklist?

Cybersecurity, operating practices, public information, emergency mock drills, modernisation, and a proactive vs reactive culture: these are the key elements driving safety discussions across downstream organisations. Fully understanding these areas of opportunity is the backbone to maintaining safe and secure assets and facilities.

Figure 1. Atlas Field Services carries out right-of-way ground patrol field training to recognise real world perspectives and security vulnerabilities to multiple forms of infrastructure, including downstream systems and tank farm security. Here is a real-world example of an improvised explosive device (IED).

An integrated approach to cybersecurity

Cybersecurity is common in today's news, but where the safety industry is seeing tremendous improvement and innovation is the blend of addressing both cybersecurity and physical threats. Identifying both possibilities takes the successful collaboration of two worlds and two different types of professionals. Supervisory control and data acquisition (SCADA) systems are the brains of many facility and right-of-way assets. These systems detect pressures, open valves, direct flow, coordinate product deliveries and help with the safe operation of utilities. They are monitored 24/7 from control facilities under strict security. It is these systems that are at the heart of the cybersecurity threat.

As technology develops, energy companies are continuously updating their communication systems to improve their infrastructure operations. These steadfast improvements also contribute to the integrity and reliability of critical assets that deliver into and transport out of plants and refineries. This opens the discussion for successfully pairing the focus on cybersecurity with infrastructural security vulnerability assessments to maintain their safe operations.

Preventing a 'domino effect' of safety threats

When cyberattacks occur on SCADA systems or any other type of platform, they often leave some type of trail. For every firewall that is put into effect, there is opportunity for an opposing party to attempt to breach that firewall. However, the mechanical operations that go into these critical forms of infrastructure are often poorly understood. While the focus on cybersecurity is extremely important, it is equally important to understand the fundamental operations of these assets to complete a well-rounded assessment. Addressing both the physical aspects related to operations and the cyber aspects paints a complete picture for maintaining security and safety of the downstream systems feeding plants and refineries. There are mechanical safety devices in place that are regularly checked that help protect the system from failure resulting from over-pressure, third-party excavator contact or integrity failures.

Even if a SCADA system were to be breached, there are mechanical pressure relief valves, rate of drops for mainline valves and manual valves. While anything mechanical can fail, SCADA system remote operations coupled with mechanical safeguards provide safety and security for downstream assets. It is the ongoing discussions and implementation of detailed ground patrols of right-of-ways that provide this high level of protection. While facility operations remain in secure safe rooms with authorised personnel signs posted, increased safety ground patrols complete the circle of protection. Operators and qualified safety consultants, such as Atlas Field Services (AFS), walk down these facilities and right-of-ways inspecting corrosion, natural disaster impacts, third-party encroachments, cathodic protection systems, facility security and proper markings that often exceed OSHA and Pipeline Hazardous Material Safety Administration (PHMSA, a US Department of Transportation agency) requirements and recommended practices. It is the knowledge provided by specialised safety consultants that goes into these ground patrols, coupled with constant attention towards cybersecurity, that enables the safe and secure transportation of fossil fuels, electricity and water.

Engaging the community

Public information is critically important and must be successfully conveyed to the communities surrounding downstream systems and plants. While there are many different approaches to a successful public awareness programme, all build strong working relationships and partnerships with the

communities within which many energy companies operate. This creates an environment of safety as these programmes promote identification of potential threats, information sharing, and coaching on both proactive and reactive measures in the event of an unanticipated fail in operations.

Over the last two decades, there has been a focus on dialling back exactly what is shared with the general public. Today, the public mapping of some infrastructure facilities accessible on the internet is questionable. There exists healthy debate regarding whether maps for these forms of infrastructure need to be shared with the public. While it is fully agreed that the public needs to know what precautions are taken to protect energy assets, some argue that the amount of information shared on where these assets are located should remain exclusive to utility and facility operators and emergency responders. Safety contractors continue to experience tremendous success with improving public awareness programmes by pairing with public relations and ground disturbance divisions, and providing a technical explanation of how and why different forms of infrastructure are safe. This includes in-depth conversation regarding pressure relief systems, coating technologies, distributed acoustic sensing, electrical phase switching, environmental best practices, and operation safe practices for emergency responders.

Targeting specific threats

Emergency mock drills are another way that energy companies are meeting today's threats towards critical forms of infrastructure. AFS has helped industry leading energy companies modify their emergency mock drills to include the Transportation Security Administration (TSA, another US Department of Homeland Security agency) in their practice emergency responses. This has addressed today's security vulnerabilities and increased awareness of terrorism, improvised explosive devices (IEDs) and potential operation improvements. These proactive efforts have also nurtured relationships between energy operators, safety consultants and state fusion centres that have assisted in the monitoring of plants and right-of-ways following reported threats.

Bridging the communication between specialised professionals has assisted in maintaining safe plant operations while providing an environment to help prevent new threats. An increased frequency of mock emergency drills has closed vulnerability gaps, identified security improvements, and lowered the cost of repairs, due to the improvements made from ground patrol feedback.

Update infrastructure to meet safety standards

Modernisation projects also provide upgrades to older infrastructure by adding key operating equipment such as mainline valves, launchers, receivers, and navigable waterway replacements. Operators looking to focus on these modernisation projects should weigh the pros and cons of 'as builds' in the field. Often when a project is designed, it lacks practical goals during the construction phase. Field consultants who specialise in modernisation projects can help meet tomorrow's PHMSA, Natural Environmental Research Council (NERC), Federal Energy Regulatory Commission (FERC) and US Code of Federal Regulations (CFR) guidelines, as well as implement recommended practices, to sustain a safe form of infrastructure for the surrounding public and owning company. Pairing the right consultant with a client can aid in corrosion identification, horizontal directional drilling (HDD) best practices, safe wetland construction methods, and project security.

Case study

In the spring of 2018, AFS identified a 30 in. dia. natural gas pipeline system that was feeding a large refinery during a right-of-way ground patrol for a client. This pipeline entered the refinery property on the edge of a navigable waterway and also ran under a major interstate bridge going over the navigable waterway. Upon further investigation of the region, AFS discovered that the bridge was responsible for over 60% of tractor trailer traffic that fed one of the largest trucking terminals in the US Midwest. During a meeting to discuss the findings of the security vulnerability assessment during the right-of-way ground patrol, AFS recommended security improvements to the mainline valve sites on both sides of the navigable waterway to reduce exposure to unauthorised personnel. Considerations that were brought to attention included a domino effect on the pipeline infrastructure that would cause a release of product that would likely shut down the refinery and bridge. This would have impacted the safety of the public, pipeline critical infrastructure, roadway infrastructure, refinery security, and commerce. These solutions offer continuous improvement for safety and security on multiple energy systems.

Conclusion

Not only is it critical that plans are implemented for tackling safety and security threats facing refining plants today, but operators need to take into account that their safety strategies must continually evolve. Whether it is through the use of disruptive technologies such as artificial intelligence, drones, mobile apps or robotics to better train and prepare the workforce, or by partnering with a third-party safety specialist to develop an end-to-end strategy, safety and security must be at the forefront of downstream operators' plans. Modern society relies heavily on fossil fuels and refining, and plants cannot afford to overlook threats and security concerns.