SIA Practitioner Insights:
Oil and Gas Sector Report

End User Perspectives on Security Technologies,
Plus Analysis of Current and Emerging Risks

securityindustry.org

The Security Industry Association, in partnership with American Fuel and Petrochemical Manufacturers, recently convened a focus group of six security practitioners in the oil and gas sector to learn more about their security technology needs. This paper summarizes their comments in the interest of sharing with SIA members key acquisition trends within the energy vertical market.

Assessment of Robotics Solutions: Impacting Manned Guarding but Facing Technology Limitations

Focus group members said they are looking to reduce their reliance on manned guarding, but, at this point, they are not convinced that robotics technology can do that to a significant degree.

> "We have been involved in that technology innovation space now for the last couple of years trying to find new technologies to replace manned guarding, where possible. That's been really driven by the desire for improving safety records. Technology doesn't have recordable injuries. Recordable injuries are a big deal in the petrochemical space. So we're looking at and experimenting with and testing not only security drones for surveillance, reconnaissance and incident response, but also, to a lesser extent, only because there's not a lot of companies that have it yet…robots for the utilization of vehicle screening and people screening at your vehicle gates and at your high-volume people gates."

> "I very much see [robotics technology] evolving over the next two to three years, and it's going to be transformational for the manned guarding industry, but it's not quite there yet. Our results, in both the security drones and the robots, while they've been very, very promising, they're not quite to the point where they're ready for primetime yet."

While there is a desire to have robots replace – or at least ease the burden on – humans in performing inspections at gates, focus group members said they have been unable to equip robots with the needed sensors.

> "We want to go out and do those inspections for weapons or for contraband or for unauthorized personnel, and the sensors that they have available right now on the robots really are limited just to high-definition thermal cameras, which are great at picking up unauthorized people in a cab or in a truck storage compartment, but we haven't been able to get any successful tests on utilization of other sensors, such as for controlled dangerous substances or for explosives. What we would like to test is putting a sensor in place for particular items that we manufacture that would give off a chemical signature that the robot sensor could detect on the outbound so that we could detect somebody that's transporting, say, just for argument's sake, ethanol that they're not supposed to have…Those types of sensors just aren't quite there yet."

Assessment of Drone Solutions: Promising Technology, Regulatory Challenges

Focus group members said they see drones as a valuable way to provide enhanced surveillance to their security personnel.

"We're running [drones] as a complement to our existing program. And it continues to get better."

"We're using the data analytics with our drones extensively, and we've actually had some really good results with that, if for no other reason than the drones never blink. They see things that people might not see just because they're not paying attention. They're able to do comparative analysis very rapidly that people aren't necessarily able to do quickly. So the drones have been a big success story in the data analytics space."

"A good example is that, on one of our sites, which is quite large, several miles square, of which much of the land is undeveloped, the security guards had been patrolling that area for years and they had never seen on that land, inside the forested area, an abandoned trailer that was actually being used by a local criminal gang to make methamphetamine. The drone found it literally on its third patrol because it…said wait a minute, this isn't right. I'm seeing things in this area that I'm not seeing in any other area and, therefore, that is an anomaly. And it sent back an alert that we then followed up on, and, lo and behold, we stumbled on the meth lab."

The main frustrations expressed regarding drones were with the regulatory environment, not the technology.

"The only lagging indicator then is government regulation…That's the weakness right now. Our goal is to have this completely automated: Literally, push a button and it goes off and flies on a preset flight pattern. We haven't been able to entirely achieve that. We only have an extended visual line-of-sight waiver, not a beyond visual line-of-sight waiver…The FAA has been very slow in implementing them, and that's going to be the key to success for the drones, just being able to push a button and send them off on a flight path and have that all automated. The good news is the FAA is making slow progress…I'm optimistic that we're going to get there, where we need to go, but it's going to be on a staggered basis."

Assessment of Drone Solutions: Promising Technology, Regulatory Challenges

There were also, however, comments that “Drones have a tendency to be romanticized a little bit” and that the “inability to rely on technology all the time” means that there are still benefits to “having proverbial boots on the ground.”

“One of the things that I’ve noticed over the last couple of years is there is a tendency to kind of fixate on drones and what they *could* do, not so much what *can* do. I kind of look at it as R&D; it’s still in the research and development phase. It’s obvious what the benefits are now and could be in the future. But there’s still this hybrid approach of technology and humans, with drones being a piece of that technology, almost in a standalone category.”

“I do think, at least presently, there is a hybrid approach to security in the oil and gas sector, and I don’t see that changing with the flip of a light switch. I think, as…the regulatory space opens up a bit and the threat picture changes and develops, as it always does, what tool we put against the risk or the threat is probably going to vary. From a military background, sometimes humans are the best and sometimes they’re the worst resource for the problem.”

Assessment of Video Analytics: Force Multiplier Potential, Privacy Limitations

Focus group members identified video analytics as a useful tool but noted that there are restrictions on their use in certain areas.

> “[Fixed cameras] are primarily used as a reaction, as a follow-up when we have an incident. There is some proactive aspect of it, but for the big sites, you’ve just got too many cameras for one person to sit there and monitor…We don’t use data analytics nearly as aggressively on our fixed cameras as we do with the drones, but that certainly is something that is going to be growing over time because it is truly a force multiplier.”

> “What we’ve tried to do is to have a uniform technology that we can apply throughout all of our businesses, and with operations in [many] different countries, we’ve got very different privacy requirements as to what camera analytics can and can’t do. So we’ve tried to stay within the channel enabling us to use these on a global basis, so we’re not really taking advantage of some of the technology that could be employed here that maybe couldn’t be employed in Germany or China or Indonesia or wherever.”

It was noted, however, that while analytics can be useful in performing relatively simple tasks like highlighting a human or animal or vehicle on screen – a product of humans “telling it what we want it to tell us – they have limitations and are not yet a proactive “smart” threat identification tool.

> “What you want to try to do is reduce the number of false alarms or repeat alarms that numb that officer or whoever’s monitoring that camera system to those alarms. And that’s a struggle, because if you have the same animal that shows up every night or the same animal that shows up multiple times, it has a numbing effect on whoever’s monitoring that system. It’s just not that smart yet…The AI may get us there at some point, but it’s just not there yet.”

Assessment of Temperature Screening Solutions and Thermal Cameras:

Outdoor Accuracy Concerns, Throughput Challenges

Focus group members said they have not been able to acquire thermal cameras that reliably perform temperature screening in variable outdoor conditions. There was an expectation that this would change during the next several months as companies adjust their technologies to meet this new demand.

> We've tested a dozen different technologies, and none of them work. That doesn't mean the technology doesn't exist to take the temperature screen, but it requires high maintenance, it requires a lot of recalibration and a lot of adjustment to stay on target, and as a result, you don't get the flow-through that you need, particularly for a large refinery or a large petrochemical site where you've got thousands of people coming in per shift. You can't afford two to three minutes processing time per person. Simple things like you start doing the screening at 4:30 in the morning when it's dark, and by 5:15, the sun is up, and that's now changed the ambient light behind each of the people, and the technology isn't able to adjust to that yet.

Regarding more traditional uses of thermal cameras, it was noted that, in some cases at least, they can be more resilient than sensors for perimeter protection.

> What we found out really quickly is that weather doesn't impact it. We still get the readings. It doesn't wear [out] when you put it in a high-sun application like [in] Arizona. … The thermal systems don't deteriorate [under the UV light] as quick as a physical item on a fence line."

Assessment of Other External Risks: Terrorism, Protests and Natural Disasters

While oil and gas facilities must guard against crime and terrorism – including, it was noted, eco-terrorism – focus group members stressed that they also must address other external threats, including natural disasters, which "aren't necessarily security issues in themselves; however, they do bring on a tremendous amount of security issues during or after the event," and protesters. The specific challenges and countermeasures, they said, depend on each facility's location, size, terrain, proximity to ports and airports, nearby population density and other factors.

"In 10 years or so on the corporate side of oil and gas, I've seen more in the way of protest activity than I have terrorist threats or attacks."

"[With protesters,] we have to bring in legal, we have to bring in HR and we have to bring in public affairs and compliance and so forth and work with them to ensure that our messaging is getting out right. So security, from our standpoint, isn't always kinetic; it's not always hands-on. It's lighting and access control, but it's also messaging: How are we going to, through proper messaging, deter [threats to] our infrastructure, our facilities, our people, our property, reputation and so forth…So it's a bit of an academic drill sometimes, as well, not just the physical security piece."

"You go hands-on with one of these [protestors] with one of your private security guards at the front gate, that's a whole different world and it opens us up to a whole slew of threats. Those could be threats to our people on Facebook, Instagram, Twitter and so forth."

"I don't see any of the organized international terrorist groups posing a threat to the U.S. operations, but there are indigenous environmental groups that potentially pose a threat."

"The exercise and the drill components of [incident response planning] are crucial. You have to drill worst-case a lot of times in order to understand where your weaknesses are."

Assessment of Other External Risks: Terrorism, Protests and Natural Disasters

> "We don't include [security systems] in our overall [natural disaster response] plan because we have to assume they're not going to work. We have to assume there's no power, no internet, no signal and so on and so forth, and therefore they're not going to be available when we most need them. So, from that perspective, they're not an integral part of our overall response to a hurricane…The battery life that's going to sustain it, the generators if they're going to be operating, are only going to be able to run for so long, and you can't depend on it. And if you're in an area where there's a mandatory evacuation…there's not going to be anybody there to maintain it."

Assessment of Insider Threats: Identifying Unusual Behavior, 'Our Biggest Risk'

Focus group members identified insider threats as one of their most significant security challenges.

"More importantly and more likely [than international terrorism], and the thing that we've actually had to deal with, unfortunately, has been the internal, disgruntled employee who decides to carry out a terrorist-type act on the site. That's what we see as our biggest risk."

"You look at it in the context of a system of systems in which physical security plays one part of that overall role to try to get some sort of early warning…You're really looking for unusual activity by that employee to give you some forewarning that something is developing. That's the thing that keeps me up at night. I would argue that the much bigger threat is the internal threat than the external threat. If we were only facing the external threat, I don't think we would have many of the people on this call losing much sleep at night, but the internal threat actually is one that is very difficult to defend against."

"One of the things that's important is keeping that person employed, but limiting access for the appropriate amount of time, because once they're outside of the facility and are no longer an employee, then there are times, I'd say more often than not, when their ire, their hate toward the company, increases, and then the physical security pieces really become important, keeping them out. Access control, identification of that person or people [and] vehicle by guards or the analytics if they're advanced enough…Same thing with workplace violence. We have the ability to effect change and mitigate risk in most cases, I would say, when the employee is still an employee instead of booting them out and saying, man, I wish we had been able to at least kind of monitor them and check email, which obviously we have access to, and chat messages and text messages on their company phones. So, again, it's a delicate balance across the board. While there are some rolling themes, each case is pretty different."

Common Operational Uses of Security Technologies: Leveraging Devices as Inspection Solutions

Security cameras, including those on drones, are used significantly for operational uses, focus group members said, including:

- Leak and spill response
- Damage assessment
- Flare stack inspections
- Tank inspections
- Building inspections
- Roofline inspections
- Railcar tracking
- Post-incident investigations

They noted that they are also interested in using security products and services for employee accountability purposes during an emergency.

> “One of the pieces that we’re leaning heavily on, especially in the current market, is multi-use monitoring…It’s safety and operational in nature, and we’re trying to combine and package all of those things into one – fit for purpose, of course. It depends on the type of facility and the location and the weather and a number of factors…We can go back and look at spills or leaks…but, at the same time, who breached the fence, who left whatever component on or open or didn’t lock it up. We’re trying to maximize the use of all of that technology.”

> “We have an internal working group, and we’re trying to figure out how to maximize the use of drones across the board. Again, not just limited to security, but also operations and safety and so forth. From the standpoint of what we can do now, I think the things that are on the ground or mounted on poles or fences are, I don’t want to way easier, but are probably more accessible than the drone piece while a lot of those details are still being hammered out.”

There was a comment that “consolidating” multiple applications is a goal for the operational uses of drones.

> “Rather than having, say, five different drones doing five different things, it’s trying to get to one drone to do five different things.”

Practitioners' Message to Integrators: Understand Our Risks Before Presenting Solutions

Focus group members said they want integrators to bring them solutions that will be relevant to them, not just the latest technologies.

> "One of the things that we require of our integrator is that they understand our business. We don't want them just bringing us stuff because it's a new technology. We want them to understand where our risks are and where our concerns are, and if something comes up that would enhance our ability to manage that, then we're very happy to hear that."