Analytics in Critical Infrastructure

Integrating safety, security, and operations

August 2024 | Axis Communications, Inc.

AXIS COMMUNICATIONS

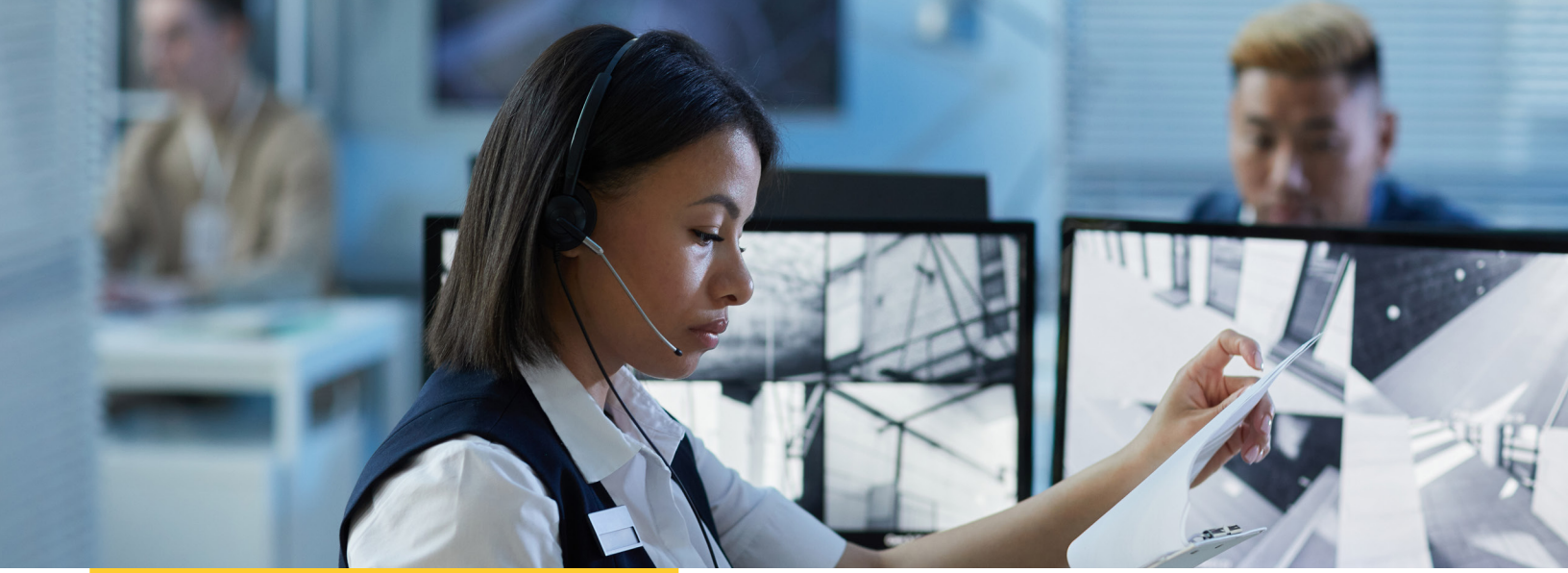

Table of contents

Summary

The rise of analytics has changed the way critical infrastructure locations are protected. Technology like analog video is no longer enough to secure those locations—and even IP video solutions can be too reactive when not supported by video analytics. Instead of reviewing footage after an incident has occurred, incidents need to be identified and responded to in real time. Modern solutions that enable a more proactive security posture are having a significant impact on physical security—but also on safety and operations. As analytics become commonplace, their uses have expanded dramatically.

As of this writing, the Chemical Facility Anti-Terrorism Standards (CFATS) regulation is awaiting reauthorization, but most chemical plants maintain compliance with the expectation that it soon be renewed. Even without active federal oversight, the regulation serves as an effective example of the security standards to which manufacturers can expect to be held. CFATS establishes clear guidelines for protecting sensitive facilities against potential security incidents in the name of national security—and those that fall under its purview must ensure they have the necessarily solutions in place to maintain an acceptable level of protection against both internal and external threats. While CFATS is just one example of the security regulations that apply to the critical infrastructure industry, it is also one of the most thorough.

Today's security devices have more processing power than ever, giving organizations important new tools to comply with regulations like CFATS—and to go beyond them. These new capabilities have made it possible for an individual device to run advanced analytics designed to improve safety, security, and operations—all at the network edge. Modern devices are no longer just security tools. They can keep property and personnel safe and increase operational efficiency as well, ensuring that organizations can reap not just safety and security benefits, but a financial windfall as well.

Introduction

Because critical infrastructure encompasses a wide range of sectors—including water, energy, transportation, communications, IT, defense, and others—it can be difficult to paint the industry with a broad brush. Each of those sectors has highly specific security and surveillance needs, making "one-size-fits-all" or "plug-and-play" solutions impractical. Critical infrastructure organizations need security tools tailored to their specific needs.

Modern video analytics have helped to make that a reality. Today's solutions are capable of addressing problems across the breadth and depth of the critical infrastructure industry, including many of the unique security, safety, and operational challenges faced by organizations involved in the delivery of services like food, power, and water. Today, the same devices and analytics already being used to keep critical infrastructure sites secure can also be used to keep personnel safe and operations efficient. Integrators and device manufacturers can help those organizations ensure they are receiving maximum value from their security solutions.

Security

Critical infrastructure sites are often extremely sensitive. They include water treatment plants, energy facilities, communications hubs, and other locations that represent prime targets for vandalism, theft, sabotage, and even terrorism. Sites like solar farms, hydroelectric dams, and radio towers are often in remote locations, making them uniquely difficult to protect. These factors combine to make critical infrastructure sites notoriously difficult to secure—which presents an ideal use case for modern analytics.

Regulations like CFATS establish clear guidelines for protecting high-risk critical infrastructure facilities, while industry organizations like the North American Electric Reliability Corporation (NERC) publish guidelines of their own to help organizations understand and address potential risks. In all cases, the ability to reliably monitor critical infrastructure locations for potential threats is critical, and having the right security solutions in place can make all the difference.

Security Use Cases for Analytics

Increasing the Security Buffer Zone. One of the most important ways video analytics can be leveraged by critical infrastructure sites is by increasing the security buffer zone. Early analytics solutions could draw a perimeter line and alert when that line was breached or crossed, which was an important way to identify potential trespassers and intruders. Today's solutions are no longer limited to outer perimeter protection: improved image quality allowed cameras to survey a wider area with greater accuracy, allowing them to identify potential security threats before they breach the designated perimeter.

Improved image quality also helps generate higher quality alerts. By improving the ability to differentiate between a human trespasser and a wandering deer, modern analytics ensure that security teams can trust that the alerts they receive are accurate. This has increased trust in analytics while also helping to alleviate the problem of alert fatigue and excessive false alarms. After all, more capable cameras with a high false alarm rate would be of little use to security teams. Good, trustworthy data is key. It's also important to note that radar detection and low-light cameras have extended where and how detection is possible, further broadening the security buffer zone and providing security teams with more actionable information.

Establishing Sub Perimeters. While protecting the outer perimeter is essential, it's important for integrators to remember that critical infrastructure sites often have sensitive areas within the primary perimeter that require additional protection. Generators, server rooms, maintenance areas, and other locations may require a higher degree of security, and modern video analytics can help restrict access to those

areas more effectively. Analytics can be used to track those entering and exiting certain rooms or areas during both high- and low-traffic periods and monitor them for after-hours intruders. They can even be used to monitor how long individuals linger in those areas and flag potentially suspicious behavior—after all, an employee who spends an hour doing a job that should take five minutes may be up to no good.

Complying with Regulatory Standards. As critical infrastructure sites become prime targets for both physical and digital attacks, a growing number of government and industry regulations now govern the way utilities and other critical infrastructure organizations maintain and protect their locations. These regulations help to establish security standards, emissions guidelines, storage requirements, and other baselines against which organizations can be measured. Modern video analytics can be leveraged to ensure that these standards are being met, issuing real-time alerts when a potential violation is detected so corrective action can be taken immediately.

Protecting Remote Facilities. Because remote (and, in particular, unmanned) facilities are often difficult to protect, an effective suite of video analytics can have a significant impact on security. One of the most common problems at secure facilities is "piggybacking," which occurs when an intruder follows an authorized person through a secure entrance. This often occurs when an unauthorized vehicle follows a delivery vehicle through a gateway, and surveillance systems can struggle to differentiate one object from two when they are spaced closely together. Modern video analytics operate with a higher degree of accuracy, and improved object recognition can easily identify two objects where there should only be one. The system can then raise an immediate alarm or swiftly contact the appropriate authorities.

Improving Object Permanence. Security incidents don't always happen quickly. Sometimes they take time to develop, or start with would-be intruders conducting careful reconnaissance. The ability to detect objects over a long period of time is critical to identifying when such activity may be taking place, and modern analytics can now identify and recognize an object for hours at a time—a significant improvement over the technology of just a few years ago. This makes loitering detection significantly easier: it is now possible to determine when the same person has been lingering near a given location for an abnormal period of time. If an individual is loitering for more than a few minutes, the security team can be notified immediately.

The ability to identify a vehicle stopped near a sensitive location may also be important for critical infrastructure organizations. Modern analytics can help give context to the situation. Did the car recently pull over? How long has it been stopped? Is the driver just changing a tire, or is there a person pointing binoculars at the facility? Rather than raising an alarm every time a vehicle stops on the side of the road, the system can now recognize when a vehicle has been stopped for a suspicious length of time. There is a behavioral element to this detection as well: modern analytics to determine whether a vehicle stopped quickly, whether it is slowly creeping closer, or engaging in other suspicious activity predefined by the AI. This can improve detection and provide more complete context for security teams, reducing false alarms.

This technology can also be applied to drone detection. In states like Texas, flying drones near critical infrastructure facilities is illegal, and it is important to know when someone may be casing the property for potential unlawful activity. As drones become more common, they are frequently being used by bad actors to conduct reconnaissance. It's important to ensure critical infrastructure organizations are aware of the ways in which today's analytics solutions can detect and deter drone activity.

Safety

Critical infrastructure sites can be highly dangerous, which means surveillance devices are used to monitor for more than just security risks. These sites may involve extreme heights, running water, electrical currents, heavy vehicle traffic, toxic chemicals, explosives, and other safety hazards, and injury or even death can result from the failure to maintain health and safety protocols. This means critical infrastructure organizations have significant regulatory concerns, and solutions that can help maintain compliance with Occupational Safety and Health Administration (OSHA) guidelines and other workplace safety frameworks—particularly in hazardous areas—are essential. Those found to be negligent in their enforcement of safety protocols risk significant fines and other penalties. These organizations also have a vested interest in keeping their employees and visitors safe.

Safety Use Cases for Modern Analytics

Maintaining Established Safety Standards and Regulations. There are many safety standards that apply to critical infrastructure sites, and modern analytics can help identify when potential violations are taking place. For example, contractors on work sites are held to strict speed limits (often as low as 5 MPH) to lower the potential for accidents. Exceeding that limit is viewed as a serious offense, and can lead to suspension or dismissal. Modern video analytics can raise a security alert if excessive speeds are detected, but they can also be used to warn drivers when they are approaching or exceeding the limit, prompting them to lower their speed. This protects the facility, but it also helps avoid unnecessary conflicts with workers who may feel blindsided by what they perceive to be excessive penalties.

Actively Monitoring Personal Health and Safety. Because the potential for injury is high at critical infrastructure sites, keeping careful track of personnel is essential. That means critical infrastructure organizations can benefit significantly from analytics that enable the tracking and monitoring of individuals

during both high-traffic and low-traffic times. Turnover periods and shift changes can be particularly chaotic, and the ability to identify specific individuals throughout the process can help ensure that none go missing. This also makes it easier to detect confined entry accidents: by tracking how long an individual has been inside a hazardous area, how many employees are in a given area, and when personnel have not been seen for a certain amount of time, these analytics can help ensure that help is dispatched in a timely manner when needed.

This is equally important during low-traffic periods when an injured employee may not be discovered for some time. Fall detection and man-down detection analytics can detect a fallen individual in a prone position who may have suffered a medical event. It can then quickly alert the appropriate parties, reducing response time and improving the odds of a positive outcome. This is particularly valuable during overnight shifts when a small number of employees may not interact with one another for hours

Actively Monitoring Personnel and Equipment. At many critical infrastructure sites, it is critical to ensure that proper personal protective equipment (PPE) is worn at all times. Today's analytics can detect equipment like reflective vests, hard hats, safety harnesses, and other wearables to ensure that they are being worn when mandated by policy or law. They can also detect items like cell phones and other distractions in areas where they are not permitted for safety reasons. When appropriate, these analytics can be integrated with audio solutions that trigger when proper PPE is not detected, providing an additional reminder to employees who risk being flagged for improper conduct. This is a critical element in maintaining OSHA compliance.

Verifying Incidents Quickly and Accurately. Clear sightlines can be a challenge at critical infrastructure sites, and both visual and thermal cameras can be placed in areas where line of sight would be difficult without them. They can be used to gauge things like pressure levels, heat levels, and other measurables in hard-to-reach areas, allowing employees to monitor sensitive equipment without being physically present. This enables immediate verification of a potential incident. For example, if a pressure or toxicity alarm is triggered, it can be visually verified before sending employees into a potentially hazardous situation. Even in the event of a false alarm, the ability to verify what is actually happening can prevent the expenditure of unnecessary time and manpower. Additionally, if the event is determined to be particularly hazardous, the security team may decide against involving humans at all.

Analytics like smoke detection can also help identify problems before they can escalate. Smoke rising from a piece of equipment may indicate a mechanical problem that can be addressed before a costly breakdown. This can even be useful in nonindustrial settings: in agriculture, certain foods (such as beets) can spontaneously combust when stored in large numbers. Identifying smoke and heat spikes in advance can allow organizations to both address potential dangers and prevent lost product. As they have evolved over time, advanced optics, image processing, and analytics capabilities have pushed solutions past typical perimeter security type applications.

Operations

At critical infrastructure sites, unnecessary interruptions and downtime can be a serious problem. No municipality wants to lose power, water treatment, internet, or other essential services for any period of time—especially when the sites that control those services are remote, making it difficult to respond to operations issues in a timely manner. It's important for critical infrastructure sites to be able to minimize maintenance needs in order to keep things running smoothly and efficiently, and analytics can be used to monitor facilities and identify potential problems and opportunities for improvement as they arise.

Analytics also provide the opportunity to improve operations as a whole. For example, understanding how long it takes a truck to enter, load or unload its payload, and exit the premises is valuable information that can allow organizations to consider where improvements may be possible. Decreasing that time even just from 20 minutes to 15 minutes can have a significant impact of efficiency and revenue. Analytics can also be used to ensure accurate billing, particularly for time-based work. They can be used to ensure the facility is getting what it pays for in a variety of important ways.

Operations Use Cases for Mordern Analytics

Monitoring Entry and Exit. License plate recognition and facial recognition have clear security applications, but they can also improve entry and exit efficiency. They can be used to track how often a delivery vehicle shows up and at what times, making it easy to track the number of deliveries, whether they are on time, and other important data points. Character recognition analytics can be used to recognize the logo on a delivery vehicle or a specific license plate number to facilitate easy entry and exit without the need for operator intervention. The ability to understand how vehicles come and go from a critical infrastructure location is important, and can provide key insights for the facility. Which hours are busiest? Can personnel be reduced during slower hours to reduce budget?

Facial recognition can be deployed similarly in sensitive areas. Not only can the technology be used to keep suspicious individuals out, but it can also recognize authorized personnel quickly, allowing them entry without the need to fumble with a keycard or QR code. Other biometric tools can also be used to facilitate simple and easy access control to secure areas, improving security without sacrificing operational efficiency.

Monitoring Sensitive Equipment Remotely. Like a human body, elevated temperature is often the first sign of equipment in distress. Thermal cameras can monitor critical machinery for elevated heat levels that might indicate grinding components and other malfunctions or misalignments. Modern video analytics can detect these problems at their earliest stage, allowing maintenance teams to address them before serious upstream or downstream problems occur as a result. Shutdown is the worst and most costly thing that can happen in critical infrastructure, and analytics capable of preventing disruption can create significant savings.

Monitoring Worksites and Conducting Work Verification. Overcharge protection is important for critical infrastructure organizations that often find themselves at the mercy of unscrupulous vendors. If a contractor promises four workers but only sends two, or bills six hours on a three-hour job, the ability to verify that discrepancy is critical. Body recognition analytics can count the number of bodies in vehicles entering the premises. It can also see when individuals are working and track when the arrived and departed. This allows organizations to hold contractors accountable and protects against overbilling for both personnel and time.

Delivery and takeaway verification is similarly critical, and this same technology can be used to monitor what comes in and out of a delivery vehicle. It is essential to know whether the goods were delivered, and the correct quantities. Likewise, critical infrastructure organizations need to know whether a vendor is removing what they promised to remove. Modern analytics can help verify this information, and can also be used to verify, for example, how full a truck is. If a salt truck is charging the city for a full load during a snowstorm but video reveals the driver is only filling the bed halfway, that needs to be rectified. Ensuring accurate billing can have a significant impact on finances. Even when a delivery goes smoothly, measuring the amount of time it takes to load or offload product can provide valuable information that can inform operations moving forward.

Final Considerations

Critical infrastructure organizations have a wide range of security, safety, and operational needs. Fortunately, modern video analytics can be leveraged in ways that enhance all three areas, providing organizations with the means to improve their security even as they also enhance their safety protocols and operational efficiency. Today's video analytics solutions can improve the effectiveness of existing surveillance systems while also enabling critical infrastructure organizations to comply with workplace regulations more easily.

Systems integrators will play an important role in helping critical infrastructure organizations identity which solutions are right for them by determining what their specific needs are and how modern analytics solutions may be able to address them. As analytics solutions grow more advanced, new capabilities will continue to arise, making education critical. Longstanding challenges like maintenance monitoring and work verification can now be addressed using the same technology that many organizations are already using to secure their locations, and it is crucial to ensure that those organizations are getting the most value out of their video surveillance solutions.