

A high-angle photograph of a large electrical substation. The substation is filled with rows of metal structures, insulators, and power lines. In the background, a wide river flows through a valley, surrounded by green trees and rolling hills. A large, grey metal transmission tower stands prominently on the left side of the frame. The sky is clear and blue, and the overall scene is bright and sunny.

## **Detect. Assess. Respond.**

**How to implement intelligent perimeter security for critical sites.**



# Perimeter Security

Perimeters of buildings and grounds can vary significantly – from industrial areas surrounded by concrete and fencing to remote locations with more challenging terrain and the potential for disturbances from wildlife. Regardless of the location, perimeter security is essential to maintaining safety, safeguarding assets, and ensuring continuity of business – especially at critical sites.

Hundreds of thousands and even millions of customers rely on the essential services provided by critical infrastructure sites, like electric, water, and natural gas utility facilities. As theft, vandalism, and terrorism constantly threaten these high-security facilities, regulations are becoming increasingly stringent and the need to safeguard the perimeters of these sites is vital. If critical assets are damaged or disabled, it can have a distressing effect on the communities and businesses serviced by the site and may pose risks to health and safety.



# Maintaining security and compliance

For critical sites, perimeter security is essential to meeting strategic and compliance objectives. Regulatory bodies that provide guidelines and standards for these facilities include the North American Electric Reliability Corporation with its Critical Infrastructure Protection plan (NERC-CIP) that covers the U.S., Canada, and the northern portion of Baja California, Mexico.

As part of these guidelines, critical site owners and operators must be able to detect, deter, delay, assess, communicate, and respond to objects approaching a perimeter, with the aim to safeguard the facility. Since threats come in many forms – from attempted perimeter breaches to shooters positioned outside of a facility as well as drones – a layered approach is essential to securing perimeters at critical sites.



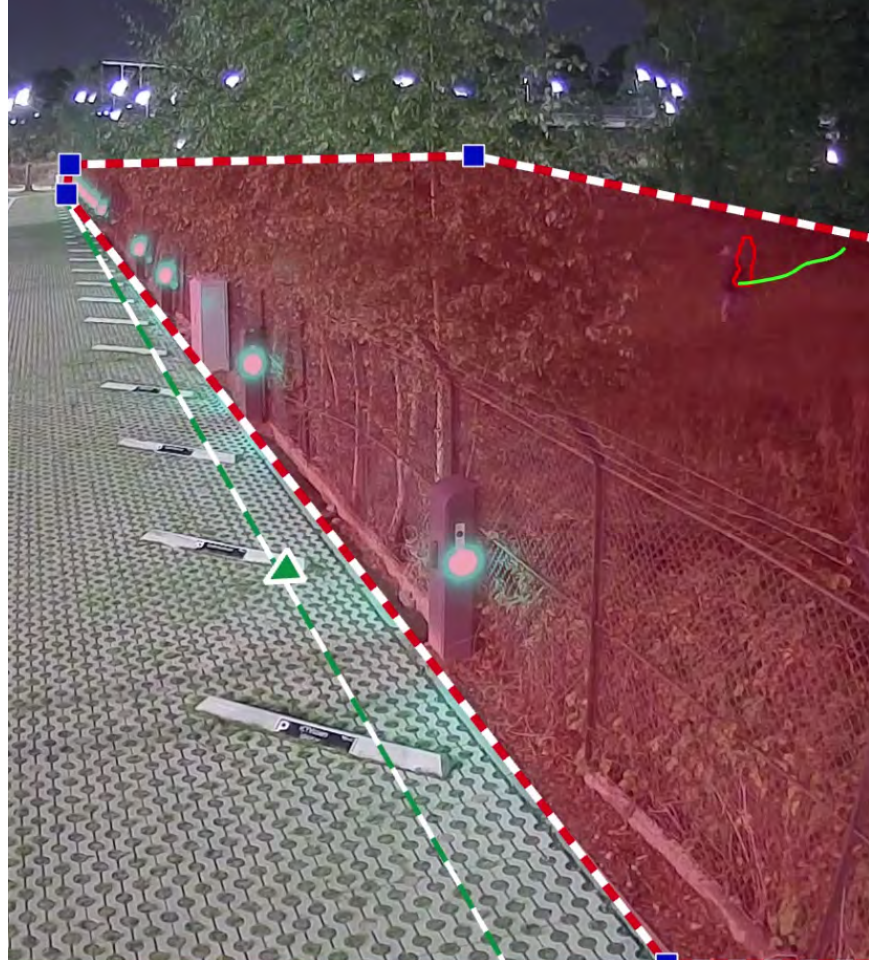


# A layered approach starts with detection

Advanced detection is essential to perimeter security. Staff need to know quickly if there is a risk, so they can respond faster. Video security cameras with built-in artificial intelligence (AI) or video analytics understand what they are seeing to interpret scenes, monitor risks against a threshold, and alert people if there is a real threat, the moment it happens.

Cameras enabled with on-board video analytics can keep watch over perimeters and help combat attempts to breach security. These capabilities include alerting to intruder approach, line crossing, loitering, fence jump, and more. These tasks will trigger alarms if the camera detects a person or vehicle crossing an invisible line in the scene, a person or vehicle entering an area without leaving after a specified time, and a vehicle parked or idling in an area near a perimeter fence. The latest advancements in video analytics are even able to detect intruders who roll, crawl, or hide in tall grass to breach fencing or entryways.

Cameras with this robust level of video analytics can alert to a person or vehicle at a perimeter while limiting false triggers from wildlife or environmental conditions. Accurate analytic alerts are important for efficiency when considering the time and expense of security operators investigating alarms across multiple locations. Video analytics with AI-based classification filter out false and nuisance alarms and provide alerts and alarms from actual threats.



# Incorporating gunshot detection

While detecting people or vehicles is important, there are other ways that perimeter breaches can happen at critical sites. In remote areas, such as at electrical utility substations, attackers seeking to disable critical assets may be able to do so from outside the perimeter with long-range, large-caliber firearms. When there's live fire at a critical site, security personnel need to act quickly. It is vital to detect events and identify the source as fast as possible.

By integrating gunshot detection technology with an automated video security system, the gunshot detection system can utilize geospatial-based commands to slew to cue the pan-tilt-zoom (PTZ) cameras to verify events. When a gunshot is detected, a nearby moving camera will pan, tilt, and zoom to the precise location in less than one second to help security personnel view the source of the gunfire and capture video evidence of the shooter and the surroundings. The camera can also automatically classify and track the shooter, dynamically adjusting the field of view to capture optimal clarity, helping security staff to respond quickly and appropriately.



# Detecting and tracking drones

Drones also pose a danger for critical sites with their ability to fly over fencing to breach physical barriers, and the risk of a drone incident is increasing due to the growing number of remote-controlled drones for private use, including video-equipped aerial vehicles. Operators need a visual perspective to assess these unmanned threats and determine whether a drone may be carrying cameras or even explosives.

By integrating radar technology with the video system, radar detection of the drone can trigger the closest ground-mounted security moving camera to pan, tilt, and zoom to the location and begin tracking the drone to help security personnel react more accurately to the threat.





## Deter to reduce the risk of damage or theft

Once a perimeter breach is detected, security personnel can take several actions to deter intruders from inflicting damage or stealing assets.

Video analytics can trigger a moving camera to track an object of interest. The latest deep learning AI technology enables cameras with on-board analytics to continue tracking even if the object stops moving temporarily in an attempt to hide from the view of the camera.

If the PTZ camera features an integrated white light illuminator, the detection can also cast a bright white light on the intruder. The object of interest is followed with this spotlight as the camera tracks its movement.

Simultaneously, video analytics can also trigger audio responses if communications capabilities are integrated with the system. Audio messages can play automatically or be initiated remotely by personnel when an intruder is detected. The message can broadcast through a loudspeaker warning the intruder they are under surveillance and that the local authorities have been contacted. Messages can be pre-recorded or relayed through live talk-down capabilities by security personnel monitoring the site.

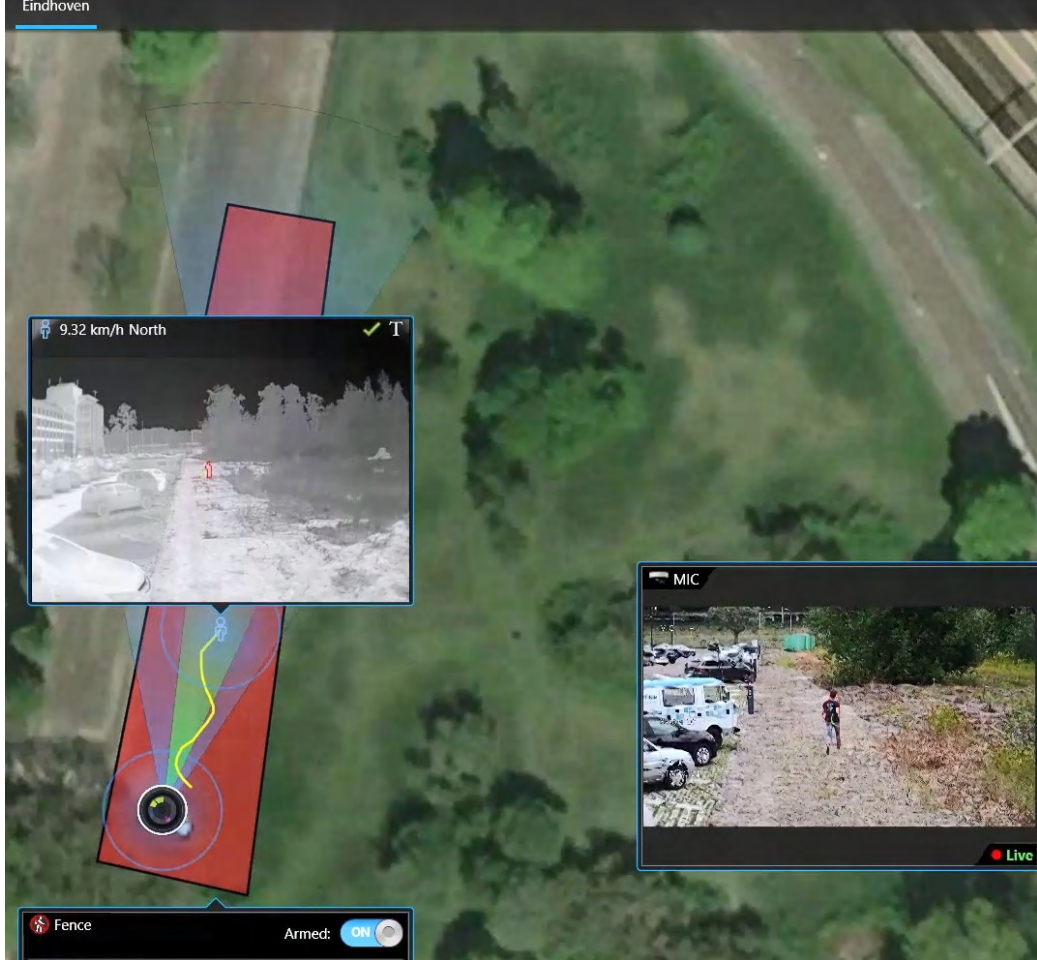
Together, the illumination and audio communications are powerful deterrents, which may cause the intruder to leave the area before causing damage.



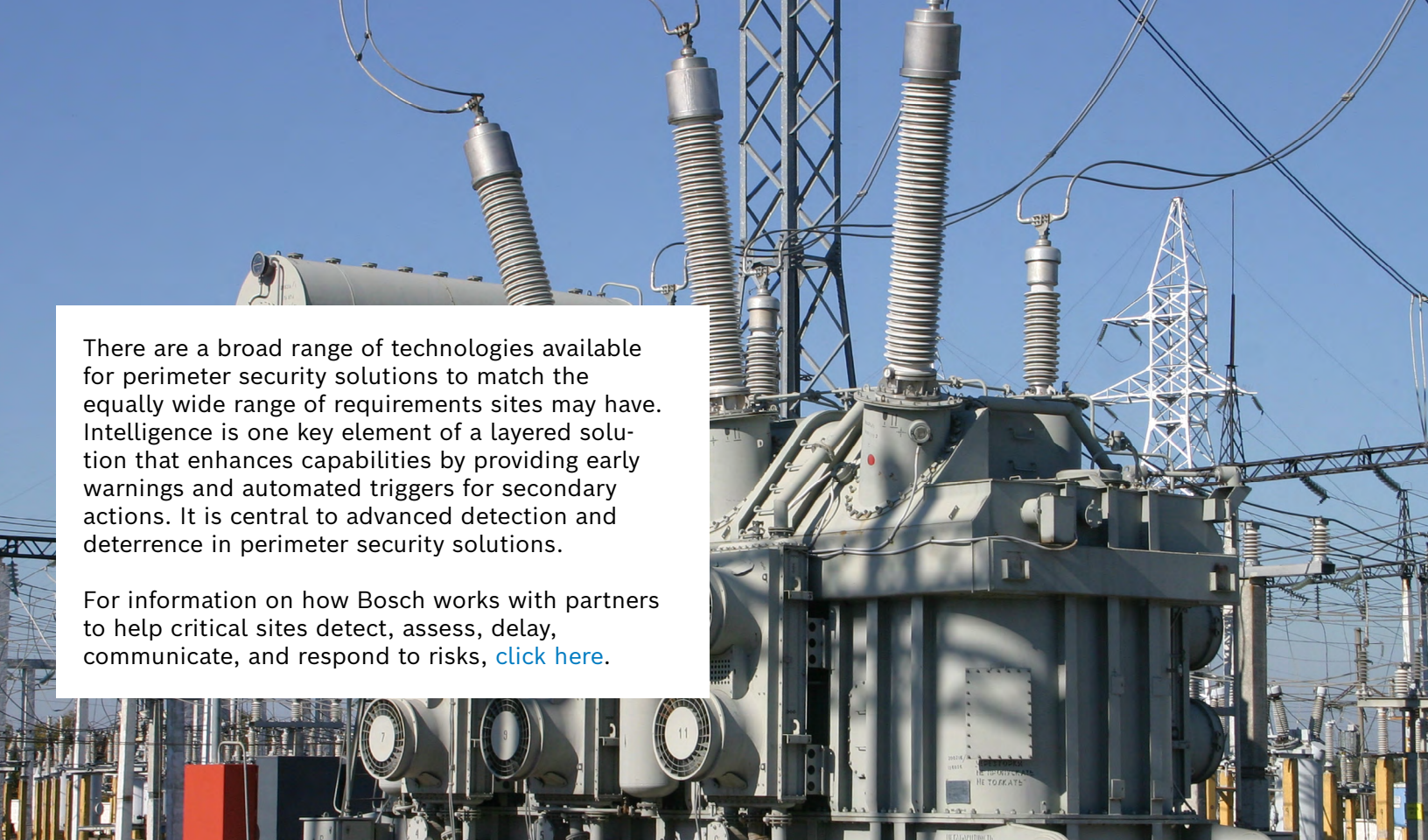
# More than detection and deterrence

Guidelines and standards for critical sites may require more than solutions to detect and deter threats. For example, NERC-CIP guidelines look for security measures to enable the organization to not only detect and deter risks, but also to delay, assess, communicate, and respond to potential physical threats.

As key components in solutions to help fulfill NERC-CIP standards, video security cameras as acting as sensors integrate with security platforms that are designed to help security personnel to monitor events, manage security policies, and run investigations when perimeter breaches occur.







There are a broad range of technologies available for perimeter security solutions to match the equally wide range of requirements sites may have. Intelligence is one key element of a layered solution that enhances capabilities by providing early warnings and automated triggers for secondary actions. It is central to advanced detection and deterrence in perimeter security solutions.

For information on how Bosch works with partners to help critical sites detect, assess, delay, communicate, and respond to risks, [click here](#).