Perimeter Security

3D Solutions

Deter, detect and delay are the three pillars of perimeter security for airfields, railways and logistics centers. Ian Harbison reports.

Deterrence can be provided by a physical barrier at the outer reaches of the facility to be protected, but if this is penetrated, intruders must be detected as quickly as possible, and alarms sent to the control center. Any response team will take time to react and deploy, so additional barriers further inside the facility can delay the intruders and give more time for them to be intercepted.

However, even the best-laid plans can be foiled by new, unforeseen threats. A graphic example of this occurred in June at the Royal Air Force base at Brize Norton in the U.K. Protesters penetrated the fence, sprayed paint in and around an engine on each of two Airbus A330 Voyager tanker/transport aircraft, causing £7 million of damage, and escaped. By using electric scooters, they were able to move at high speed, carry out the attack, and disappear before airfield security could react.

Aviation

Dave Solly, senior product manager at U.S.-based Gallagher Security, says each transport sector presents its own set of perimeter security complexities. In aviation, it is even more complex, as there is a significant difference in the requirements for an international airport versus a regional one.

Many international airports will have some form of perimeter detection —

By Ian Harbison

Gallagher image

often cameras and/or intrusion detection — rarely having the addition of deterrent as well on the perimeter. Their perimeters can be massive — up to 15 miles in length — and often segmented with buildings and multiple points of access, making them difficult to manage properly. They also have a large number of spectators, so visual aesthetics are important to their overall reputation — they don't want a fence that looks like it belongs around a prison, but they want one that works.

International terminals have a higher profile and, therefore, perceived higher risk. That means greater levels of protection, so regional airports are probably more vulnerable. These generally have much smaller terminals, and the perimeters are more continuous, but they often lack the supporting services infrastructure to allow the deployment of some security equipment, so it will be camera- or cable-based detection.

Zaun's ArmaWeave woven mesh high-security fencing has been designed specifically to be installed on sites of critical national importance. The CPNI-approved fencing system offers a more substantial delay from attack from hand and power tools than other traditional welded mesh fencing systems. The mesh pattern of 17 mm x 17 mm and use of high tensile steel wires means it offers no climbing aids and provides little room for blades and cutting tools to attack the fabric of the fence. Zaun image.

Stewart Plant, sales and marketing director at U.K.-based fencing specialist Zaun, explains that the main U.K. standard for perimeter security products is Loss Prevention Standard (LPS) 1175. Managed by the Loss Prevention Certification Board (LPCB), it categorizes how long it would take an intruder to breach physical security measures such as security grilles, fencing and gates, shutters, and doors. These are graded by threat level (A to H), corresponding with the tool kit used to evaluate the product's intruder resistance and the number of attackers involved, and the minimum delay (1, 3, 5, 10, 15 or 20 minutes) provided by the product when placed in a locked condition.

The perimeter fence may be A1, so it can be cut or scaled within a minute. However, there can be higher levels, such as B3, C5, or D10, requiring different tools and resistant for three minutes up to ten minutes, that surround more sensitive areas of the facility, which will slow down intruders.

In fact, he says aviation has probably been the sector most at risk from attack in recent years, but the reasons for intrusions have changed. The Brize Norton attack is the latest in which the aim was to generate publicity for the intruders' political cause. He adds that a weak point at any airfield is at the runway ends, as a frangible fence is required for aircraft overruns.

One solution might be the use of a double fence, with a sterile area between, that can be monitored by visual or acoustic sensors. This is in common use at prisons, but it does mean a reduction of the interior space of the facility, and many facilities are already surrounded, so the perimeter cannot be expanded outwards. Instead, as at London Heathrow Airport, which Zaun started working with in 2017, there is a clear trend that airport and airfield customers are not only upgrading their perimeter fences to higher security standards, but also increasing reliance on detection, including CCTV and electronic surveillance. In the case of airports, this additionally includes the threat from drones intruding into sensitive airspace.

Solly points out that protecting perimeters from drones is a complex problem in its own right, as the fence is not an obstacle and they can drop in from a height above the coverage area of cameras. Technologies for drone detection are continuing to evolve and become integrated into security management systems.

Plant says although improved fencing may increase deterrence, if an intrusion occurs it needs to be detected quickly. The control center can track intruders with cameras as they cross the area to their target, but the time taken to get there needs to be calculated beforehand to ensure it is outside the response time and that they will be intercepted en route. If it is not, then another, stronger fence may be necessary to ensure the correct delay time.

Rail

For the rail industry, Plant says the biggest non-security challenge is stray livestock getting on to the tracks, while the biggest criminal threat is cable theft — Eurostar services were badly hit in late June when

A Considered Approach to Perimeter Security

Effective perimeter security requires a considered approach, says Solly, one that addresses the customer's needs and balances the various threat levels and environmental factors that each situation requires. This demands a multi-layered, intelligent stance. At the core, deterrence is critical. Monitored pulse fencing, for example, can offer a proven probability of detection with an extremely low false alarm rate on the back of highly configurable application that can be scaled up or down as required. Adjustable voltages and dual-pulse configurations can be tailored to different threat levels and risk zones.

Detection-only systems also play an important role in effective implementation of perimeter solutions. There are highly practical instances where visual appearance (or lack of) is a key decision factor for a customer. It is how these technologies are combined, using the right product for the right purpose, that is important. For example, a large transport operation will have a large yard at the back of the property where the trucks are parked, loaded and maintained, yet this is often bounded by a simple chain link fence.

Adding pulse fencing to this brings a highly effective deterrent and detection capability; combining the intelligence of a high-quality vibration monitoring system with rapid validation/verification of alarms, defining the type of response necessary. Conversely, the front of the site often has office facilities and, while detection is equally important here, deterrence may be less important to the customer than the aesthetics of the site.

All of these elements can be managed through an integrated system, which allows operators to monitor multiple zones, initiate responses, and integrate with access control, video management and intrusion detection. This centralized control is especially beneficial for sectors like rail, where assets are distributed across vast geographies, or in aviation, where rapid coordination is crucial. The ability to retrofit these solutions onto existing fencing infrastructure ensures both flexibility and cost-effectiveness.

As well as providing a physical barrier, fencing like Zaun's HiSec Super 6 can be augmented with cameras for surveillance or a vibration monitoring system for intruder detection. Zaun image.

Many modern perimeter security technologies are developed with cross-sector applicability in mind. Core components such as fencing hardware, intrusion sensors, control systems, and integration-ready software platforms are typically designed to support a wide range of use cases. This consistency in architecture helps streamline product development, deployment, and ongoing support.

That said, each sector — and every individual site — presents its own operational demands. Factors like terrain, environmental conditions, wildlife presence, regulatory obligations and levels of human or vehicular traffic all influence how a system is configured. For example, a rail installation spanning remote landscapes may require weather-hardened equipment and low-maintenance operation, while an airport perimeter must align with aviation safety standards and accommodate frequent airside crossings.

However, the ability to adapt and tailor solutions to these site-specific needs — without re-engineering the foundational technology — is key to achieving both scalability and effectiveness.

When asked if the market is simply reactive or if it can anticipate threats to give enough time to find solutions, he said it's really dependent not just on the sector, but the scale of the organization. "If you take a large international airport, they have dedicated security experts that are not just looking at generating an alarm but also how they can maximize response, efficiency and safety around the site," he said. "Equally, for a small regional airport, their perceived risk is much lower, so there is less focus on what they would consider valuable in the perimeter security context. The fence line would be looked after by the facility maintenance team, not a dedicated security team like a large international airport. The same arguably applies in small transport — while efficiency and reputation is key to business success, the complexity of this is significantly lower than a multinational freighting organization."

The smaller organizations tend to be very reactive to an event occurring unless standards mandate a solution, typically focusing on the costs associated with a solution due to budget constraints. On the other hand, large organizations either have dedicated personnel or utilize the services of specialist consultants to proactively minimize the risk.

600 meters of copper cable were stolen in Lille, northern France. However, it is impossible to fence off the entire length of the tracks. Similarly, the HS2 high-speed rail project in the U.K. started off with high levels of security along the line, but cost and time pressures have seen simpler solutions being adopted.

Solly says it is difficult to monitor trains moving in and out of stabling yards and stations as they are often large and take a considerable time to transition through. Perimeters will often extend down the tracks for an extended distance to minimize the risk of someone simply walking around the edge of the fence and into the yard. The close proximity of the tracks to the perimeter fence can make selection of security technologies difficult. Trains generate a large amount of noise that may cause audio detection systems to potentially generate nuisance alarms. The carbon dust from the braking systems can also be problematic for some energized fencing as it can make the insulators conductive, leading to higher levels of maintenance required. Trespassing, vandalism, and theft are probably the biggest risks, although in some countries terrorism will be a significant factor, particularly for highly populated areas with passenger services.

Road

In the road transport sector, perimeter security is — most likely — largely reactive to events that have occurred on sites. Business continuity plays a huge role for a transport operator, says Solly; the risk of losing contracts because you are not seen as reliable is massive. Losing a customer's freight because someone either broke into the yard and emptied a trailer of the product, or worse still, a driver intentionally took the wrong trailer and never delivered it to the destination are common risks. For large freight operators, it has become increasingly difficult to track all their drivers. Gallagher recently had a customer that wanted to evolve their access control solution — not just manage access on the perimeter, but to also make access-related decisions based on the tractor-trailer combination leaving the yard — Tractor X is expected to have Driver Y and Trailer Z, and cannot leave the yard until this combination has been validated. In addition, if the truck does not arrive at a certain depot within a specific time frame, and if they don't arrive, alerts are raised.

A Gallagher trucking client recently asked to evolve their access control solution so that it could make access-related decisions based on the tractor-trailer combination leaving the yard as well as tracking to destination. Gallagher image.

However, perimeter protection on transport perimeters, with the exception of a few, is lax, generally consisting of simple chain link fences with three rows of barbed wire, comfortably living in the world of "it'll never happen to me." Solly gives an example of a transport operation that had an incident where batteries were stolen out of trucks parked in the yard (they had no security). He points out that the cost to replace the batteries was significant, but the cost of those trucks being off the road was far higher.

The customer installed cameras in the common belief that they provide a deterrent to thieves, only to watch the recording of the thieves doing the same thing again with hoods covering their features. The company now have a full-height pulse fence around the perimeter with an integrated camera system that allows it to manage and respond appropriately to threats.

As well as batteries, the transport sector is also at risk of losing fuel and high-value, recyclable materials. A further challenge is the high duty of care required for dangerous cargo, to prevent outsiders inadvertently, or intentionally, coming into contact with it, and, with responsibility sitting on business owners and directors, this is becoming as important as how the cargo is handled.

Market Areas

Solly says airports in Asia are experiencing notable growth in perimeter security upgrades. This is being driven by a combination of post-pandemic infrastructure investment, regulatory modernization, and an urgent need to counteract emerging threats such as drone incursions. There's also rising awareness of the security needs and threats across Australia as a result of a recent event involving a perimeter breach. The federal government has mandated that a greater focus on perimeter security be required across all airports, from international to regional.

Meanwhile in the Americas, road transport — particularly transportation of products — is growing significantly, with large operators covering multiple states with hundreds of rigs on the road. The difference between choosing transport operator A versus operator B is often based on reputation as much as it is based on goods. Being able to incorporate business efficiency systems integrated with security systems can be the difference in not just running an efficient business but also solidifying the reputation of reliability through how you track the trucks and consistently keep the customer's freight secure.

Across sectors, there is also a broader shift toward high-assurance, integrated solutions that combine physical protection with cybersecurity and centralized management. This is particularly relevant in environments governed by strict compliance requirements or government-level security standards. TSI