Picture credit: AdobeStock

LOCK DOWN!

Jon Hill *unlocks the key to safer prison security*

Modern prisons are among the most challenging of facilities to manage and secure. They are dynamic, high-risk settings where tensions can escalate quickly and where the consequences of even a minor lapse in security can be serious. The pressures facing these institutions are increasing. They're compounded by staff shortages, growing inmate populations, rising levels of organised crime and the use of new technologies for smuggling and disruption. All of which contribute to a demanding and often unpredictable environment.

At the heart of this challenge lies the question of how to keep prisons secure in a way that is effective, sustainable and responsive to change. While the best answer may vary from one facility to another, there is a shared truth that underpins safer prison environments.

It is never as simple as just adding more technology, fences or people. The key to safer prison security lies in integration. In systems that work together and present the right people with the right info at the right time to manage or even pre-empt threats. Without a precise understanding of what is happening inside the facility it's difficult to prioritise or make good long-term decisions.

For decades, perimeter security has been at the core of prison safety. The idea is simple, keep threats out and prevent inmates from leaving. But in practice, especially in modern prison estates, securing the perimeter is far more complex than installing a fence or a row of cameras.

The scale of some facilities, combined with blind spots, challenging terrain and legacy infrastructure, makes it difficult to achieve and maintain full situational awareness. And while the physical boundary is still essential, the true perimeter of a prison is now both physical and digital.

Security is more than just barriers and boundaries. For example, the growing use of drones for surveillance and the smuggling in of contraband drops shows how external threats are becoming more creative and harder to predict. A short lapse in security easily allows drugs, a mobile phone or a weapon to cross the boundary undetected. Even Alcatraz, synonymous as it once was with maximum security, would have needed to adapt when considering threats from above.

It is important to recognise that most prisons no longer have a single perimeter. Instead, they have multiple zones, each with different risk profiles and access requirements. There may be an outer boundary for deliveries, a restricted area for staff, a visitor zone and secure inmate yards. Each of these acts as a mini-perimeter, requiring different security measures and levels of oversight. This layered complexity means relying on one system or sensor is not enough.

As prisons adopt more sensors and surveillance tools, the volume of data increases significantly

By treating these areas as distinct security zones, prisons can apply more tailored safeguards. For example, a delivery bay can be monitored by motion sensors and license plate readers, while the staff entrance can integrate biometric access and personnel tracking. Visitor areas may need real-time monitoring and rapid ID checks.

Meanwhile, inmate yards benefit from surveillance with behaviour detection alerts and automated tracking. It is not just about stopping threats at the outermost point, but understanding how risk travels across these internal borders. And how to contain it quickly if it does.

This is where the value of a unified system becomes clear. In too many facilities, different technologies are still operating in silos. Video footage sits on one screen, while access logs are stored elsewhere and perimeter alarms come through a separate interface.

In a critical situation, security personnel are forced to jump between systems, trying to piece together a narrative from disconnected data. This is time-consuming and increases the chances of missing something important.

By contrast, a unified system brings everything together. It allows security staff to see incidents in their full context. An alert is no longer just a flashing light or a sound. It is a live situation, displayed with relevant video, access records, past events and clear guidance on what to do next. Operators can assess risk faster, act more confidently and make better decisions under pressure.

Unified systems can also improve training and shift handovers. When teams are working from a single source of truth, it becomes easier to maintain consistency from one shift to the next. Key incident data, flagged patterns and response procedures are clearly recorded, helping both new and experienced staff stay aligned in high-pressure environments.

This kind of integration also helps with internal access management, which is an often overlooked aspect of prison security. With large teams, regular contractor visits and varied schedules, managing who is authorised to go where, when and for how long is a constant task.

Physical Identity and Access Management Systems or PIAMS, can make this easier by linking access permissions to employment records, training certifications or role changes. If someone moves to a different department or leaves the organisation, their access rights update automatically. This reduces manual errors and ensures that only authorised people can enter sensitive areas.

It also creates transparency. When everyone's access is tracked and logged, there is less room for grey areas. Staff understand that their movements are accountable and administrators gain peace of mind knowing that security is not reliant on outdated lists or paper logs. This becomes especially important during incident investigations, where speed and accuracy in establishing timelines are key.

Beyond access, it reinforces the message that security is everyone's responsibility, not just the domain of control room operators or managers. It encourages a culture of compliance, awareness and shared ownership.

Automation plays an essential role in reducing the burden on security staff. As prisons adopt more sensors and surveillance tools, the volume of data increases significantly. Without smart filtering and event correlation, this data becomes overwhelming.

False alarms can waste time, while missed connections between incidents can delay critical responses. Unified systems help group-related alerts and guide staff through operating procedures to ensure consistency across shifts and reduce reliance on memory or experience alone.

Security operations centres handle hundreds of events each day, from minor anomalies to emergencies. Without prioritisation, operators can become fatigued and overlook key indicators. Smart alerting tools can highlight unusual combinations of behaviour. For instance, a door forced open and a camera disabled in the same zone will allow teams to focus their attention where it matters. It is not just about more data, but smarter data that tells a clear story.

> **STATIC SYSTEMS THAT DO ONE JOB WELL, BUT CANNOT EVOLVE ARE NO LONGER ENOUGH**

Facilities should also review how data is used during and after incidents. Data should not just be logged, but actively reviewed to inform staff training, identify system gaps and prevent repeat scenarios. Security strategies that learn and adapt from internal data perform better in the long run.

When it comes to security, it's crucial to look beyond the physical walls. The prison perimeter should not just be a line of defence, but a zone of awareness. Seismic sensors and external LiDAR systems can detect movement outside the fence to provide early warnings of suspicious activity.

Automatic number plate recognition can scan vehicles approaching the site, comparing them with watchlists or known associates. If a flagged vehicle is spotted multiple times near the site, this can trigger further investigation, all before it escalates into something altogether more serious.

Real-time data sharing across teams and with external agencies adds another layer of protection. When prisons are able to push relevant information to mobile devices, remote staff or response units, they improve coordination and reduce the chance of duplication or delay. During an incident, this visibility is crucial. After an event, it provides valuable insights that support debriefs, audits and long-term planning.

To strengthen these ties, many prisons are developing closer working relationships with local police, cyber crime units and emergency services. Sharing patterns, alerts and surveillance data can be mutually beneficial and provide additional layers of insight into wider organised criminal networks.

Another area where integration proves valuable is in incident verification. It is not enough to detect movement. Teams must know whether it is a genuine threat or a false alarm, what they are dealing with and how best to respond. There are all manner of different IoT devices that can help here, but only when managed through a unified platform. Otherwise they become hard to respond to in a timely fashion create more work for operators and risk triggering too many false

alarms. We all know what eventually happens when a person (or an alarm) continually cries wolf!

The combination of different IoT sensors with effective video analytics and smart classification tools can help to cut down on these distractions. For example, a cat, a bird or even a gust of wind can easily keep triggering a motion sensor, leading to it being ignored. Yet, secondary methods of verification, presented through one unified platform, can cut down on false positives and enable guards to view all the relevant information in one place.

SMART ALERTING TOOLS CAN HIGHLIGHT ANY UNUSUAL COMBINATIONS OF PRISONER BEHAVIOUR

Another example is the integration of covert or overt duress alarms with the existing systems used for video surveillance and access control. In isolation an alarm tells the control room very little, causing panic without providing the context that will be needed to shape the appropriate response. Yet an alarm that immediately shows those in the control room the view from the most appropriately placed cameras can indicate what they're dealing with. Helping with in the moment decisions such as how many personnel to send, from where and with which equipment. As well as which parts of the facility may immediately need to be locked down. By reducing ambiguity and surfacing only the most relevant information, unified systems help staff stay calm, decisive and focused during highly stressful events.

Ultimately, the goal is to create an environment where risks are understood in real time, responses are coordinated and systems support security personnel rather than confuse them. This involves investment, but more importantly, it involves a shift in mindset. Prison security teams must switch their approach from reaction to prevention and from surveillance to insight. Having a connected and unified system equips them with the tools they need.

Security is a continuous process that adapts over time. The facilities that will thrive in the future are those that treat integration, intelligence and coordination not as extras, but as essential. When digital systems and human experience come together, prisons can build the kind of operational resilience that protects both people and infrastructure in the long term.

As the security landscape continues to evolve, prisons must be ready not just for the threats they face today, but for the ones still to come. The next generation of security challenges may not always be visible at the fence line. They could arrive through network vulnerabilities, unmanned devices or increasingly coordinated criminal efforts that blur the lines between physical and digital intrusion.

In this environment, adaptability becomes just as important as strength. Static systems that do one job well, but cannot evolve are no longer enough. The future of safer prison security will rely on platforms that can grow, integrate with new technologies and support data-driven decision-making.

More correctional facilities recognise the value of proactive prevention over reactive enforcement. This means investing in training, streamlining communication and ensuring staff are supported by technology rather than burdened by it. Security systems should serve as an extension of the team, not an extra layer of complexity.

Ultimately, the safest prisons will be those that treat security as an ongoing process, not a fixed solution. With the right combination of people, processes and integrated systems, facilities can create secure environments that adapt, respond and improve over time. That, more than any single tool or upgrade, is the key to safer prison security ●

Jon Hill is an Account Executive for Genetec UK, specialising in the transport, public safety and correctional sectors.

The growing use of drones for smuggling in contraband shows how external threats are becoming more creative

Picture credit: Alamy