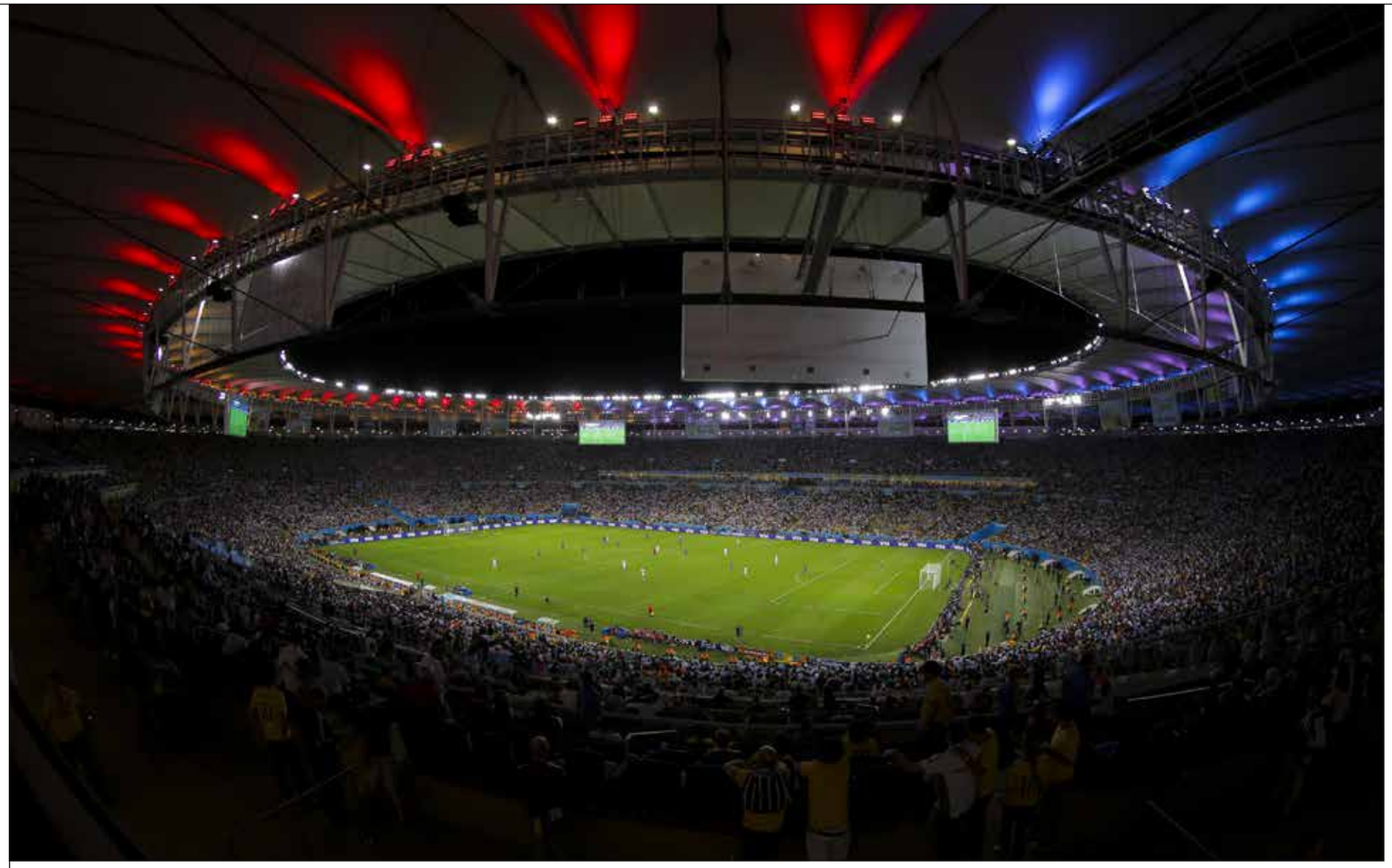

Picture credit: Danilo Borges

PLAY IT SAFE

Philip Tackett *explains why successful stadium security depends on the interplay of technology and a willingness to collaborate*

Imagine having to funnel up to 80,000 people and their belongings into a venue within 60 minutes. There are children and adults; journalists and VIPS; some will be irrepressibly excited and some will have enjoyed a few pints ahead of time. This sounds like a logistical nightmare but for stadium owners on game day, it's reality. Sporting events present a security challenge unlike almost any other public setting. Stadiums must process large surges of people in short windows of time, often under intense operational pressure, while maintaining both effective threat detection and a smooth visitor experience. Get that balance wrong and the result is not only slower entry, but greater crowd frustration, operational strain and unnecessary security risk.

That pressure has reshaped stadium security over the past three decades. When the United States last hosted the FIFA World Cup in 1994, manual checks and canine units were the primary detection methods. Today, the emphasis is increasingly on advanced screening technologies, software-assisted detection and more integrated operations.

Stadiums have successfully adapted to evolving threats without compromising the visitor experience, largely due to three key technologies: Computed Tomography (CT), dual-view X-ray and X-ray diffraction (XRD) – all of which are supported by increasingly capable software and analytics.

Successful stadium security typically spans multiple functions, from parcel screening and people screening to access control and surveillance

CT generates detailed 3D images that can be rotated and interrogated by operators, giving a far clearer view of bag contents than conventional screening. That makes it harder to conceal threats within cluttered belongings and gives screeners better spatial understanding of what they are seeing. Although CT has long been established in aviation, adoption in stadium environments has been slower because of cost, size and operational constraints. That is beginning to change as systems become more compact and more viable for non-aviation use.

Dual-view X-ray deploys advanced screening technologies that use two independent generators to simultaneously produce two independent views of an object. This eliminates blind spots within a bag, providing superior threat detection and reducing the need to reposition and/or rescan bags, all of which improves throughput and reduces waiting times. Dual-view transmission X-ray systems have been routinely used for more than 30 years, but began to seriously replace single-view systems in the aviation environment during the Advanced Technology programme overseen by the TSA after 9/11.

XRD is not new, but recent advances have made it far more relevant to integrated screening. Unlike conventional transmission X-ray, which primarily assesses density and atomic number, XRD analyses molecular structure. That allows it to distinguish between materials that may look similar on a conventional scan, making it particularly valuable when operators need greater confidence in resolving suspicious or ambiguous items.

Technology has not removed the human from stadium screening, but it has changed the nature of the role. As systems become more capable, operators spend less time on continuous manual review and more time on exception management: interpreting ambiguous images, resolving edge cases and making judgement calls quickly and accurately under pressure.

That does not necessarily make the job easier. In many operational environments, automation shifts human effort rather than removing it. As routine tasks are absorbed by machines, the remaining decisions are often the most complex, which can increase cognitive load and make it harder to maintain sharp judgement over time.

That means stadium operators must think beyond procurement. They need to also consider training models, rotation plans, user-interface design and operating procedures that help screeners stay engaged, retain judgement and intervene effectively when the technology flags uncertainty rather than certainty.

For all the attention given to new screening technologies, one of the most important enablers of effective stadium security is still collaboration. The strongest systems are not simply more advanced. They are better connected and better coordinated.

Stadium security typically spans multiple functions, from parcel screening and people screening to access control and surveillance. Each may be delivered effectively in its own right, but when those functions operate in silos, gaps emerge.

For example, parcel screening may detect a disassembled firearm component. Without coordination with people screening, other components could enter through different lanes and the weapon could then be assembled on site. Another potential issue is the development of incomplete threat libraries (which is a depository of images for the AI to learn from) that exclude location-specific risks because the contractor did not receive the right level of input from the stadium owner and/ or the other contractors, resulting in a security vulnerability. The ideal would be vendor-to-vendor coordination that allows for real-time sharing of parcel and people screening data.

Better intelligence-sharing between facilities and vendors is also required. Stadium operators need to communicate relevant threat profiles, prohibited items, expected audience characteristics and local risk factors so that systems and workflows can be configured appropriately. Without that input, screening programmes are less likely to be aligned to the venue's operating environment.

THERE IS NO SINGLE THREAT PATTERN AND NO SINGLE TECHNOLOGY THAT CAN ADDRESS EVERY RISK

Cross-agency data partnerships are the last key to thorough collaboration. Detection systems improve when they are informed by larger and more varied datasets, which is why collaboration with law enforcement, regulatory bodies and peer organisations is so valuable. Facilities that treat security data as entirely closed may limit their ability to benefit from wider operational learnings across the sector.

Open architecture can support that kind of collaboration. Platforms that allow hardware, software and algorithms from different suppliers to work together give operators greater flexibility in how they deploy detection tools, workstations and wider networked environments. In practice, that makes integration more achievable and reduces dependence on siloed systems.

Threat assessment in stadium environments now goes well beyond the traditional focus on obvious weapons. Security teams increasingly need to account for a broader and more varied threat set, including items that may be concealed, broken down into components or designed to evade conventional screening methods.

As mentioned above, that includes not only fully assembled firearms but also individual components such as barrels, firing pins and magazines, which could be brought in separately and assembled later. As a result, algorithms trained on component-level recognition, not just complete weapon profiles, is best practice.

Polymer-based weapons present another challenge. With limited metal content, they are less likely to be detected by traditional metal-focused people screening alone and increase the importance of imaging systems that can identify low-density items with suspicious shapes or characteristics. In response, new machine-learning-based techniques are being trained on the detection of synthetic components. Blunt-force objects such as hammers, pipes or heavy

tools also remain relevant. But detecting them is only part of the task. Operators must also be able to distinguish between legitimate equipment and items that may present a credible threat in context.

Explosive threats remain a major concern, particularly where improvised materials may not present the predictable characteristics associated with standard military-grade explosives. That increases the value of technologies that support stronger material discrimination and reduce ambiguity during inspection.

THREAT ASSESSMENT NOW GOES WELL BEYOND THE TRADITIONAL FOCUS ON OBVIOUS WEAPONS

The broader point is that there is no single threat pattern and no single technology that can address every risk. Stadium security is most effective when parcel screening, people screening, operator judgement and threat intelligence are treated as part of one connected system rather than separate layers working in isolation.

In many ways, stadium security is borrowing from aviation, where detection performance, alarm rates and operating standards are tightly defined. But stadiums face a different reality: less space, tighter budgets, heavier surges in footfall and visitors who do not necessarily expect screening to feel as structured or routine as it does at an airport.

The venues most likely to succeed will share a few characteristics: They will treat visitor experience as part of security performance, recognise that long queues and congestion create risks of their own, favour adaptable systems that can respond to changing crowd patterns and will work more closely with vendors and partners on threat assessment, data and operational design.

Looking ahead, there is no doubt technology will continue to advance. In the future we will likely see continuous motion people screening, real-time threat correlation across multiple detection systems and AI-driven predictive analytics – all of which will help keep us safer and provide a better stadium experience. But the limiting factor isn't technological capability so much as something more basic: a willingness to collaborate. When stadium operators, security vendors and regulatory agencies work together in a more integrated way than the sector has traditionally allowed, everyone benefits.

GOING FOR THE WIN

Stadium security at the 2026 FIFA World Cup is based on a layered approach designed to protect spectators, players and staff. Measures include secure perimeter fencing, multiple screening checkpoints, walk-through metal detectors and bag inspections at all venue entrances. Access to restricted areas will be controlled through accreditation systems and identity verification, while CCTV networks will provide continuous monitoring throughout stadiums and surrounding zones. Security personnel, law enforcement officers and specialist response teams will be deployed both inside and outside of venues. Crowd-management systems will be employed to help monitor spectator movement and prevent congestion, while emergency evacuation procedures will be in place for all host stadiums. Counter-drone technologies and real-time communications systems will provide further support to venue security operations during matches and related events ●

Philip Tackett is VP Technology at Smiths Detection.

Advanced screening technologies like those deployed by Smiths Detection for the Commonwealth Games are key to controlling entering stadiums

Picture credit: Smiths Detection