

Playbook on stadium security

Designing safer, smarter, and more seamless event-day operations

dormakaba

The connected stadium

Stadium security is not a single gate, door, or scanner.

90 min

Peak ingress window where most stadium failures occur

<$50

Cost of equipment to clone outdated RFID credentials online

Source: TSG Security, Access Control Card Reader and Credential Vulnerability, 2024

~20

Throughput per turnstile lane at full-height spectator entry

10

Distinct access zones requiring different hardware and credential logic

It is an operating system for people, vehicles, credentials, and movement. Most event-day failures trace back to disconnected decisions: parking planned separately from perimeter control, ticketing separated from accreditation, emergency exits tested on paper but not under crowd pressure. The right person, with the right credential, should move smoothly to the right zone at the right time.

Why stadium security fails

Operational blind spot

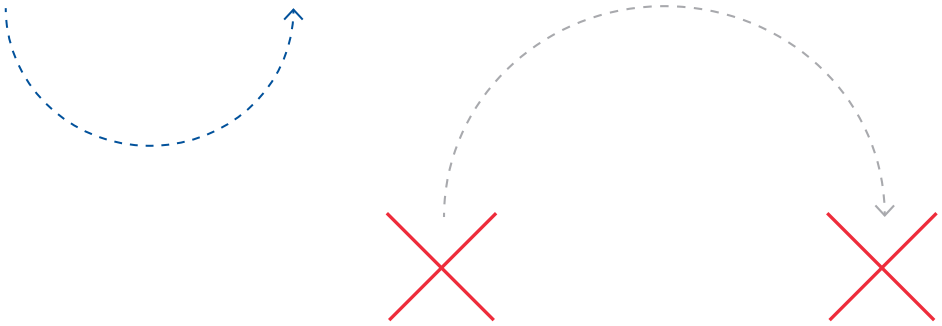
Emergency exits code-compliant on paper, untested under real crowd conditions. No post-event data review cycle.

Design gap

Gates positioned after pedestrian routes are fixed. Hardware selected by package cost, not lifecycle endurance.

Hardware limitation

Ticket validation considered separately from parking control. Systems that work on quiet days – not under event-day pressure.





Medium risk

Roads, parking & approach

Vehicle flow, VIP routing, bus bays, rideshare



Highest risk

Perimeter screening

Highest-risk window. Queue build-up, ticket fraud, crowd density peaks



High risk

Entry into the bowl

Throughput vs. credential trust – where surges expose design gaps



Medium risk

Concourse & vomitories

Internal bottlenecks, premium zone breaches, cross-flow



Managed risk

Seating & restricted zones

Back-of-house, player tunnels, control rooms – credential discipline



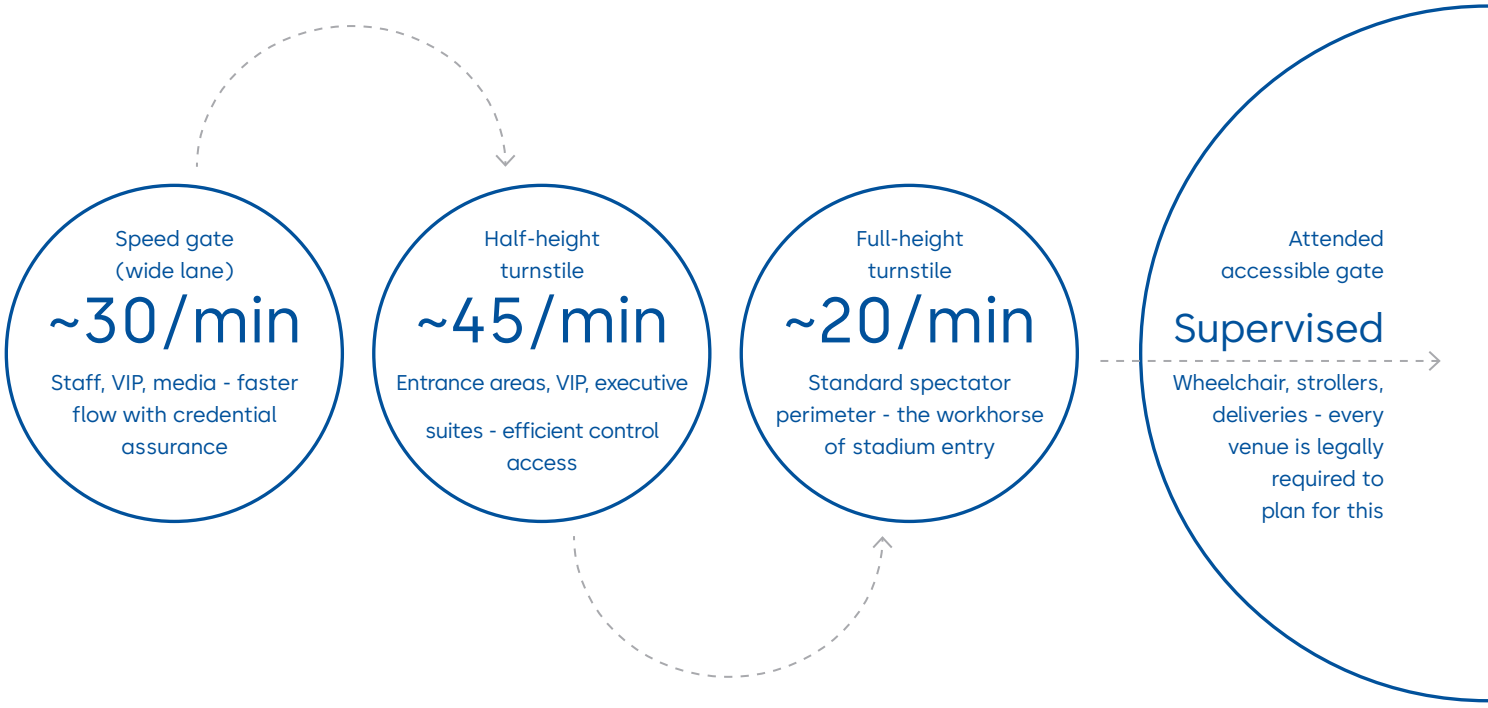
Medium risk

Post-event egress & reset

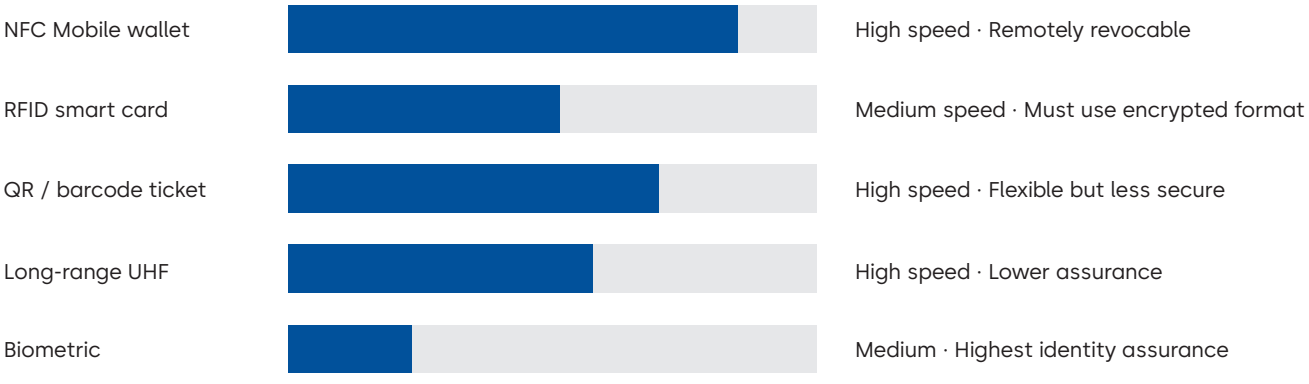
Dispersal, parking release, emergency access preservation

Event-day pressure, quantified

These operating numbers define the access strategy.



Credential hierarchy – security assurance vs. throughput speed



Illustrative graphic only

One playbook for six stakeholder views.

Every role has different risks and challenges to deal with. The playbook gives all teams a shared language for safer event-day decisions.

Safety & compliance · Security & zoning · Fan & staff experience

01

Owners & governing bodies

Protect venue value, reduce reputational exposure, and unlock a wider event portfolio with lower operational risk.

02

Venue operators & security leaders

Run event day with clearer lanes, stronger visibility, and faster, more predictable incident response.

03

Architects, specifiers & consultants

Design security into every zone from the start, aligned with stadium terminology, hardware needs and circulation flows.

04

Integrators & technology partners

Connect ticketing, access, CCTV, parking, and command systems with clear interfaces and defined fail states.

05

Event partners & third-party operators

Simplify overlays, credentials, service routes and broadcast access across temporary teams and event windows.

06

Regulatory & risk-compliance stakeholders

Make decisions defensible with tested solutions, commissioning evidence and maintainable compliance documentation.

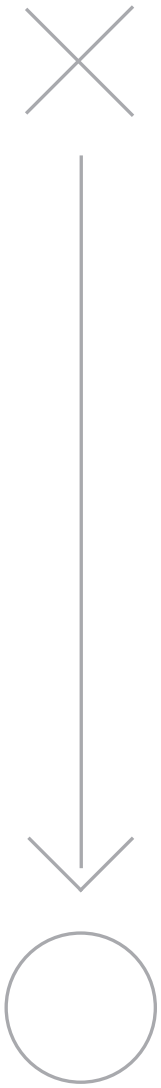
About this playbook

This playbook is written for the teams that design, upgrade, and operate stadiums.

It supports early visioning, design coordination and event-day planning without becoming a product catalog. The central idea is simple: stadium security performs best when access, life safety, and crowd flow are planned as one connected system. The playbook shows how to connect vehicle approach, perimeter control, credential logic, circulation, zoning, egress, and post-event review before event-day pressure exposes the gaps.

Please note:
This is a strategic guidance document and not a substitute for code analysis, crowd modeling, or project-specific engineering.

Terms
The following terms appear throughout the playbook and reflect common stadium operations language.



Term	Meaning
Access control	The systems and procedures that manage who enters each venue area.
Accreditation	Named or role-based approval for staff, media, contractors, teams, and event partners.
Airlock / vestibule	Secure double-door or gate transition where one door closes before the next opens; used for high-assurance areas.
Anti-passback	A credential control rule that prevents the same access token from being used to enter a zone twice without an intervening exit scan, used to prevent ticket sharing and detect tailgating at spectator entry lanes.
Back-of-house (BOH)	Restricted operational areas such as loading, plant, stores, offices and control spaces.
Bowl access	Movement from concourse or vomitory into the seating bowl.
Credential	Any access token: ticket, QR code, smart card, mobile wallet, vehicle credential, or biometric.
Egress	Movement out of the venue during normal departure or emergency release.
Fail-safe	Hardware or release logic that unlocks on power loss or emergency signal to support free egress.
Fail-secure	Hardware that stays locked on power loss on the controlled side; use only where code-required egress remains protected.
Full-height turnstile	Floor-to-ceiling rotating barrier used for strong perimeter control; approx. 20 people per minute.
Ingress	The arrival and entry phase, usually the highest-pressure access window.
Long-range credential	UHF vehicle credential or transponder that enables hands-free authentication at barriers.
Perimeter	The first controlled boundary between public approach and venue envelope.
Speed gate	Wide-lane, fast-throughput gate used for staff, media, VIP or accessible entry; approx. 30 people per minute.
Tailgating	Unauthorized following through a controlled point behind an authorized user.
Throughput	People processed per minute per lane or access point.
Vomitory	A tunnel or passage connecting concourse and seating bowl.
Zone	A venue area with a specific risk level, user group and access logic.



Content

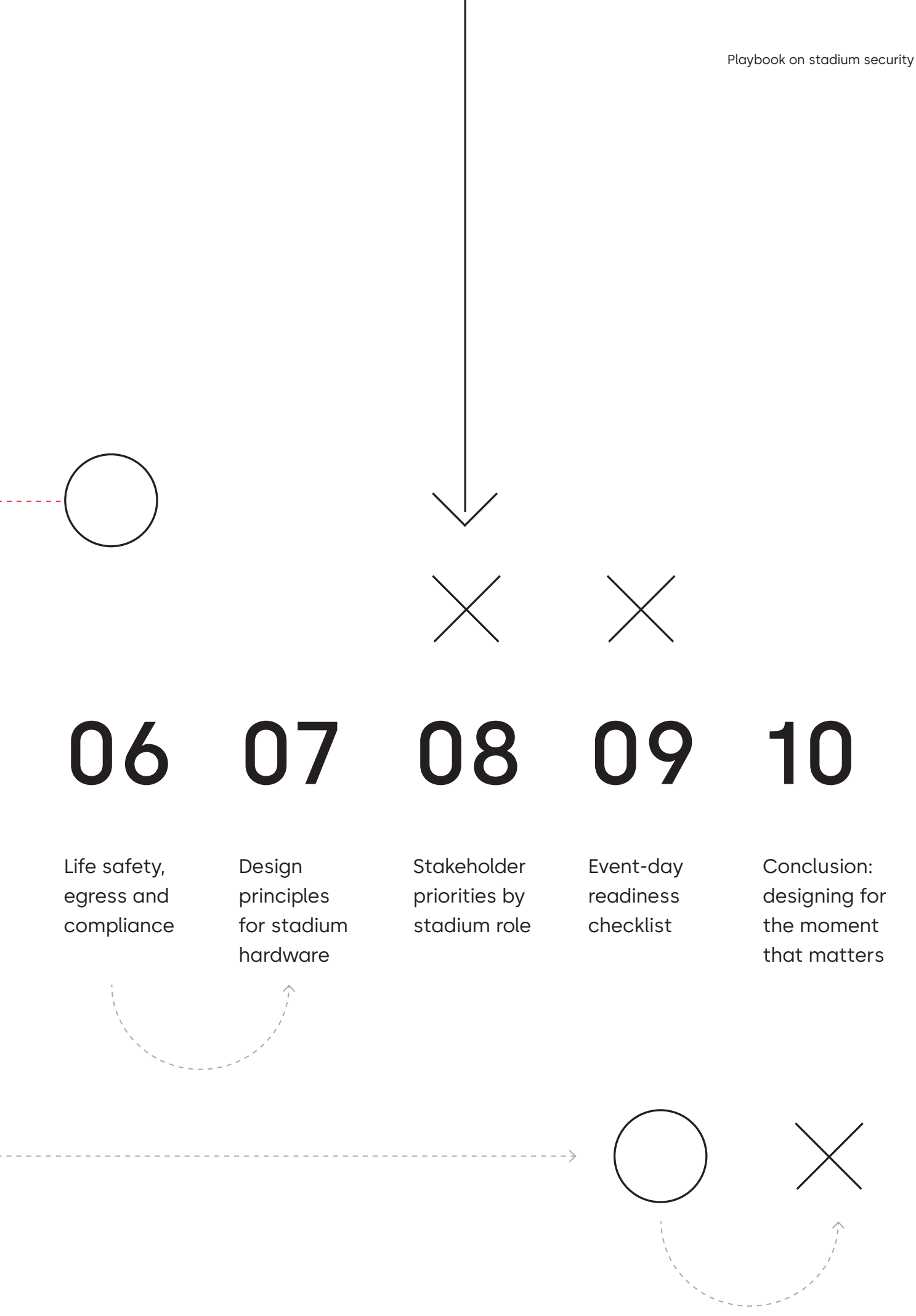
01 Why stadium security is different

02 The three value pillars

03 The event-day journey

04 Zone-by-zone stadium design

05 Technology that works under event-day pressure



06 Life safety, egress and compliance

07 Design principles for stadium hardware

08 Stakeholder priorities by stadium role

09 Event-day readiness checklist

10 Conclusion: designing for the moment that matters

01 Why stadium security is different

A stadium can feel deserted on Tuesday and overloaded on Saturday.

A regular switch from quiet building to high-volume event environment. It must receive, screen, direct, and safely accommodate tens of thousands of spectators, staff, media, teams, contractors, and VIP guests under constant time pressure.

Takeaway

Stadium failures are rarely caused by one component. They usually come from design gaps, hardware limitations, and operational blind spots working together.

Design for the crowds, not the quiet days

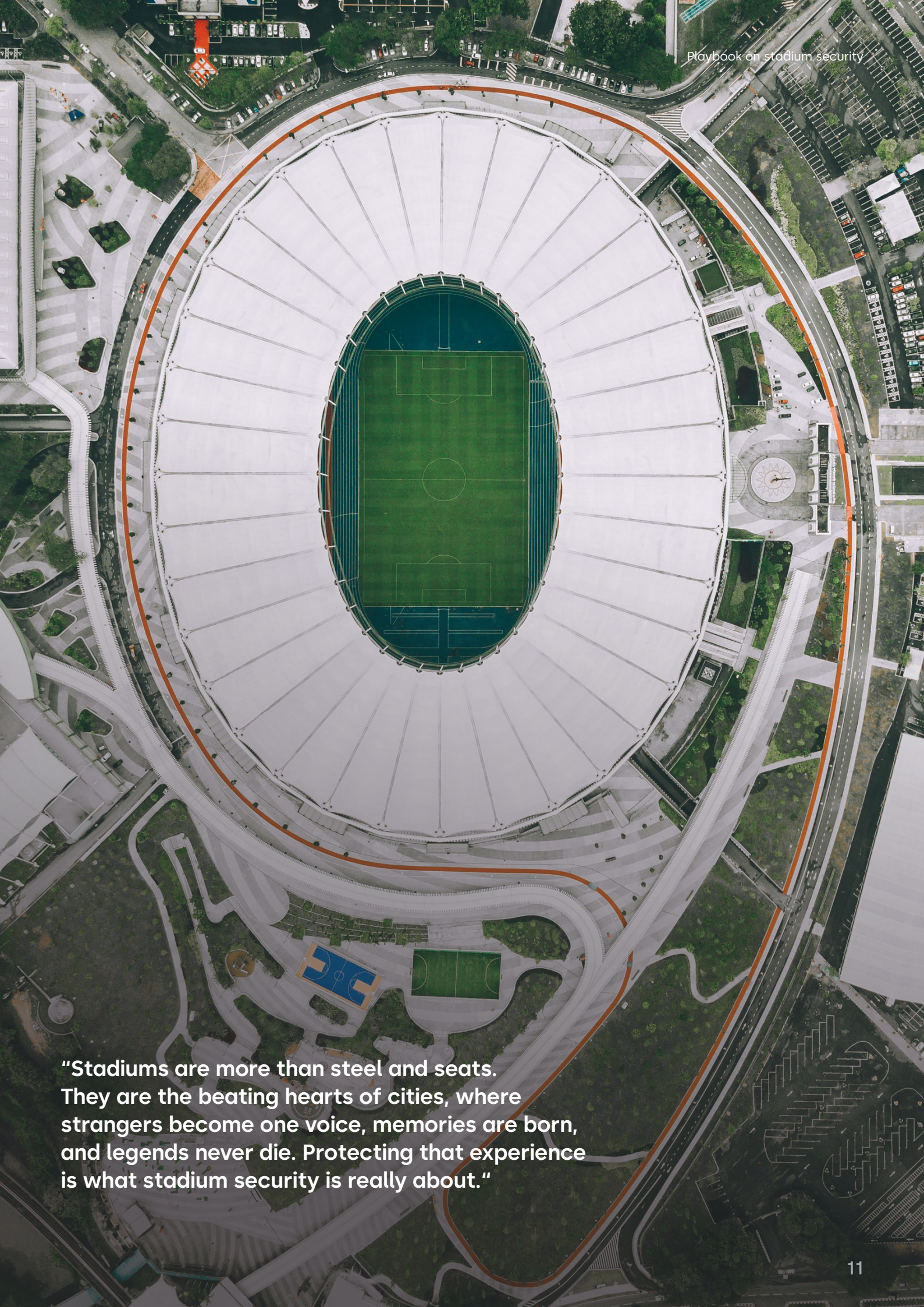
The challenge is not simply keeping unauthorized people out. It is keeping the venue safe, compliant, secure, and easy to use when crowd density rises. Parking, approach roads, perimeter lanes, accessible entry, hospitality access, player movement, media accreditation, BOH routes, and emergency egress all need one connected access model.

Late security design decisions create avoidable friction: gates after routes are fixed, door hardware selected by package cost, ticket validation separated from parking and emergency exits that are code-compliant on drawings but untested in event conditions.



How this helps stakeholders

- Owners and governing bodies gain a more resilient venue concept with lower reputational and operational risk.
- Operators gain a stadium that is easier to run under event-day pressure.
- Security leaders gain clearer zoning, stronger credential control, and better incident readiness.
- Architects and specifiers gain a framework that integrates security with circulation, accessibility, and design intent.
- Integrators gain a clearer basis for connecting ticketing, access control, video, parking, and command systems.



"Stadiums are more than steel and seats. They are the beating hearts of cities, where strangers become one voice, memories are born, and legends never die. Protecting that experience is what stadium security is really about."

02 The three value pillars

Under event-day pressure, every access point has three jobs.

It must protect people, control movement, and preserve the stadium experience. These three pillars give every stakeholder a shared lens for judging every gate, door, route, credential, and procedure.

Takeaway

Stadium security works best when safety, security, and experience are treated as three outcomes of one coordinated design – not as three separate problems assigned to three separate teams.

Safety & compliance
Life safety, emergency egress, fire-rated hardware, accessible movement, and compliance with assembly occupancy codes. Security hardware is part of the life-safety system – not separate from it.

Security & access zoning
Layered access across all venue zones, from the public perimeter to the most restricted back-of-house areas. The right credential should work only in the right place at the right time.

Fan & staff experience
Fast, frictionless movement that feels invisible to the user. Great security is not what fans notice – it is what they do not notice.



"Every recommendation in this playbook supports at least one of three outcomes. The best stadium schemes support all three at once."

How this helps stakeholders

- Owners can evaluate decisions against clear outcome pillars instead of isolated product choices.
- Operators can align event-day procedures with design intent.
- Security leaders can justify zoning and credential decisions in business terms.
- Design teams can balance visual quality, code compliance, and operational performance.



03 The event-day journey


JESUS
IS
LORD

The 6-stage people flow

A stadium should be planned as a sequence of movements.

The journey starts before a visitor even reaches the turnstile. And it continues until the site is clear. Planning should follow the operating sequence of the venue, not just the position of doors.

A	B	C	D	E
Before arrival	Perimeter screening	Concourse and vomitories	Entry into the bowl	Seating and restricted zones



Stage A
Before arrival

The first security layer begins outside the building line.

Parking capacity, coach bays, rideshare zones, VIP drop-off, pedestrian routes, service roads, and emergency access all influence pressure at the perimeter.

Route assignment should happen early: by stand, block, hospitality category, home/away policy, staff role, or credential type. The best time to correct a visitor heading to the wrong gate is on the approach, not at the front of a dense queue.



F

Egress
and reset



Takeaway

Plan vehicle validation, lane separation, license plate recognition where appropriate, approved vehicle lists, overflow and weather resilience as part of one operating policy.

Stage B: Arrival and perimeter screening

The perimeter is often the highest-risk event window.

Ticket misuse, wrong-gate arrivals, queue frustration, and density all peak before entry. The operating discipline is similar to an airport, without the inconvenience: validate early, distribute demand, separate user groups, and keep exceptions away from the final checkpoint.





Takeaway

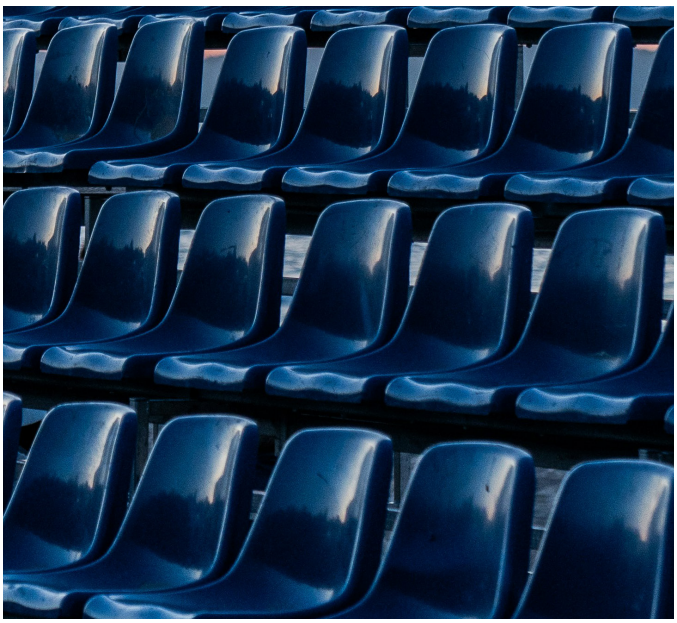
Separate standard ticketed entry, accessible entry, family lanes where used, away-supporter segregation, hospitality, staff, delivery, and accredited access. A spectator lane should not process deliveries; a media or player entrance should not sit in uncontrolled public circulation.


VAUXHALL
THE ENGLAND TEAM SPONSOR
Currys

Stage C: Concourse and corridor

Inside the venue, security becomes movement management.

Concourse routes, corridor, concessions, restrooms, retail, hospitality thresholds, and seat-block circulation all create dwell and cross-flow. If these are not actively managed, bottlenecks simply move from the perimeter to the concourse.



Takeaway

Use zoning, signage, occupancy displays, and crowd management staffing to reduce unnecessary crossover, especially where supporter segregation or premium-zone control applies. People-counting tools and congestion alerts should support action: redirect flow, adjust staffing, and keep emergency routes clear.





Stage D: Entry into the bowl

Throughput planning must be based on peak arrival, not average hourly flow.

Operators need to know how many people must be processed, through how many lanes, in what window, and at what realistic throughput once bag checks, rescans, accessible support, and exceptions are included.

Takeaway

Credential compatibility matters. A QR ticket, hospitality mobile credential, staff smart card and vehicle credential can all coexist — if each is accepted only by the right reader in the right zone.



Entry solution	Throughput (approx.)	Best application
Full-height turnstile	~20 per minute	Spectator perimeter
Speed gate (wide lane)	~30 per minute	Staff, VIP, media
Attended gate (accessible)	Supervised	Wheelchair, strollers, deliveries
Tripod turnstile	~45 per minute	Ticket controlled entrances

Stage E: Seating, premium, and restricted zones

The route to the seat is part of the security journey.

The route to the seat is part of the security journey. Public bowl access may prioritize speed and seat-zone validation. Premium lounges, tunnel clubs, media tribunes, player corridors, medical spaces, and control areas require stronger assurance and lower tolerance for tailgating or credential misuse.

Takeaway

A spectator ticket should not open BOH. A media pass should not open the control room. A contractor badge valid during fit-out should not remain valid during a high-risk event unless deliberately reauthorized.



Stage F: Egress and reset

Departure is part of the design.

Departure is part of the design. A venue that admits thousands quickly must also support controlled dispersal across concourses, exits, transport nodes, parking release, rideshare demand, and emergency access routes.

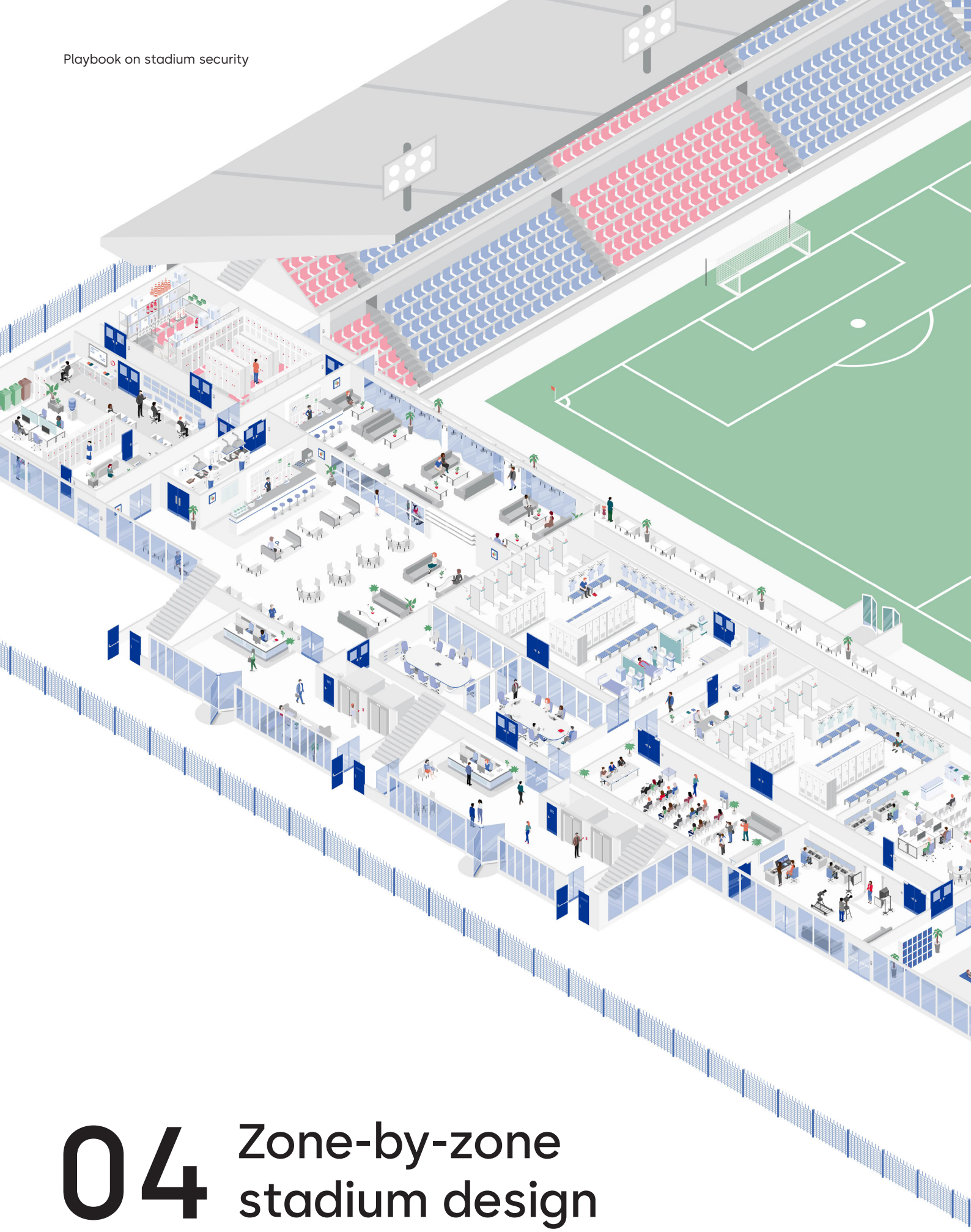
Event-day operations do not end when the last visitor leaves the stadium. Access logs, occupancy curves, exception reports, incident notes, and hardware faults should be reviewed to improve staffing, lane allocation, credential policy, and maintenance planning.



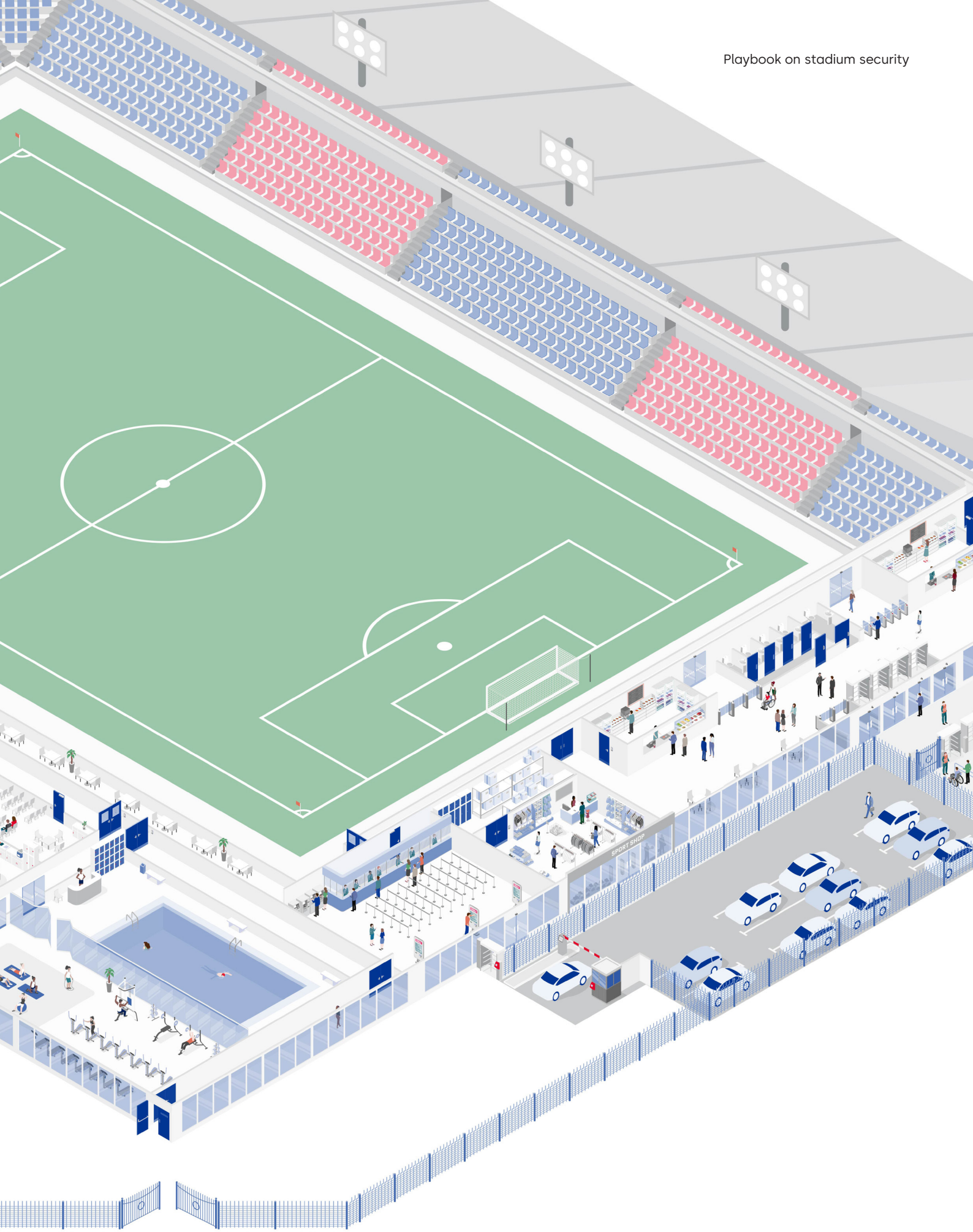


How this helps stakeholders

- Owners gain a more credible operating narrative from parking to seating rather than a gate-only concept.
- Operators gain a practical framework for event-day planning, lane allocation, staffing, and after-action review.
- Security leaders gain stronger control over exceptions, misuse, and zone transitions.
- Architects gain clearer inputs for approach geometry, ingress distribution, and internal circulation.
- Integrators gain a clearer map of which systems need to exchange data at each stage of the event journey.



04 Zone-by-zone stadium design


SPORT SHOP

The 10-zone map

A stadium should be planned as a series of zones.

Each zone has its own risk profile, user groups, hardware needs, and credential logic. The question is not “Which door?” It is “Which zone, which user, which event condition?”

01 Parking and vehicle approach

02 Perimeter and outer security line

03 Main spectator ingress

04 Concourse and vomitories

05 Seating bowl access

06 Hospitality, VIP, and VVIP zones

07 Player, official and media circulation

08 Back-of-house, service, and plant areas

09 Control room and critical operations areas

10 Emergency exits and protected routes

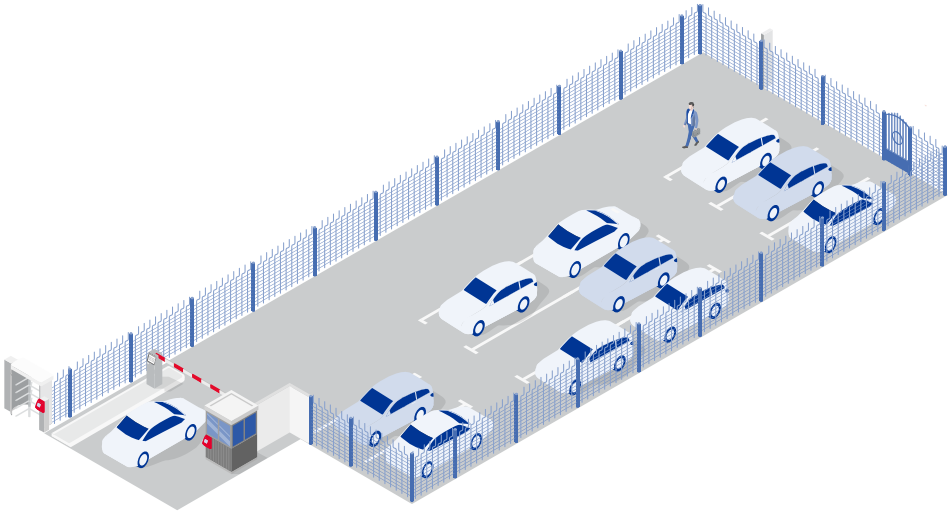
01

Parking and vehicle approach

Separate spectator parking, VIP, team, and official arrival, broadcast compound access, deliveries, and emergency routes.

Use barriers, lane separation, approved vehicle lists, license plate recognition where appropriate, intercoms, bollards, and weather-resilient equipment as one access policy.



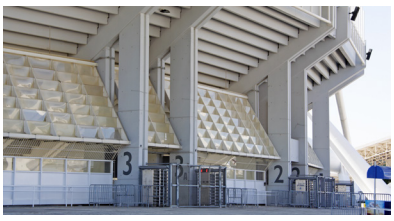


02

Perimeter and outer security line

The perimeter is the first formal control point. Separate ticketed entry, accessible entry, family lanes, away-supporter segregation, hospitality, staff, and non-spectator access.

Full-height and half height turnstiles can provide strong control when paired with supervised accessible and exception lanes.



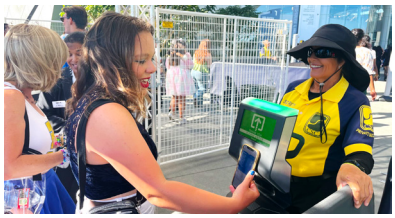


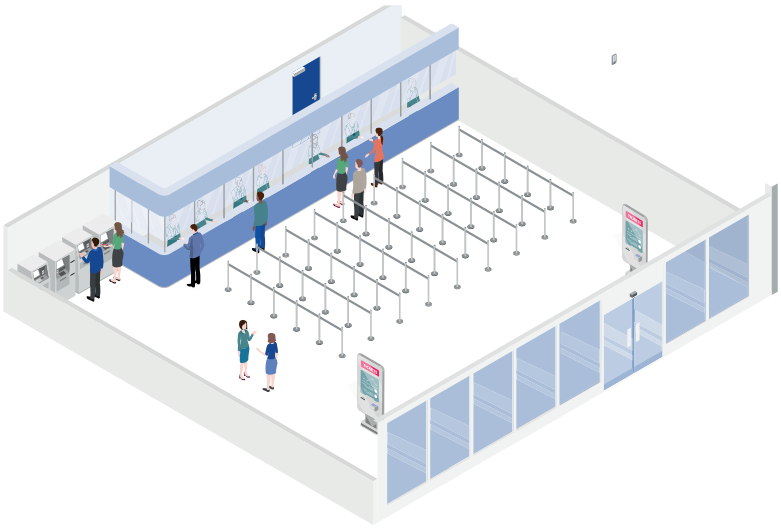
03

Main spectator ingress

This is where ticket validity, identity assurance and throughput meet. Assign entry by stand, block, vomitory catchment, or segregation policy, not vague gate naming alone.

Signage, screens and crowd management staffing should redirect visitors before they commit to a queue.





04

Concourse and vomitories

The concourse is circulation space and destination space. Protect flow to concessions, restrooms, retail, and seat access while preventing uncontrolled movement into premium or restricted areas.

Half-height control points, automatic doors, and supervised transitions may all have a role.





05

Seating bowl access

Where seat-zone validation is required, the solution must support speed without creating a new pinch point.

Plan bowl re-entry, duplicate scans, mis-seated visitors and section crossover rules before live events expose them.





06

Hospitality, VIP, and VVIP zones

Premium spaces need discreet assurance. Speed gates, readers, automatic doors, visitor handling, and elevator control should protect the zone without an institutional feel.

Time-limited credentials, named guest access, and service route separation often matter more than heavy barriers.





07

Player, official, and media circulation

Player tunnels, locker rooms, mixed zones, press rooms, commentary positions, and media tribunes require managed routes and accreditation discipline.

Crossovers with public spectators should be minimized and intentionally supervised where unavoidable.





08

Back of house, service and plant areas

Loading routes, stores, MEP rooms, control cabinets, and contractor access are common blind spots.

Time-window logic, role-based access, and route separation reduce the risk that service movement becomes an unauthorized path through the venue.



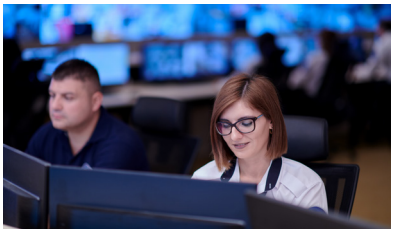


09

Control room and critical operations

The control room is the operational brain of the venue. Access should be tightly restricted, reliably logged and designed for high availability.

For critical spaces, hardwired infrastructure is often the prudent basis because reliability matters more than convenience.





Takeaway

Every credential should be valid only at the access points, zones and time windows it is designed for. The credential logic should be mapped before hardware is specified.

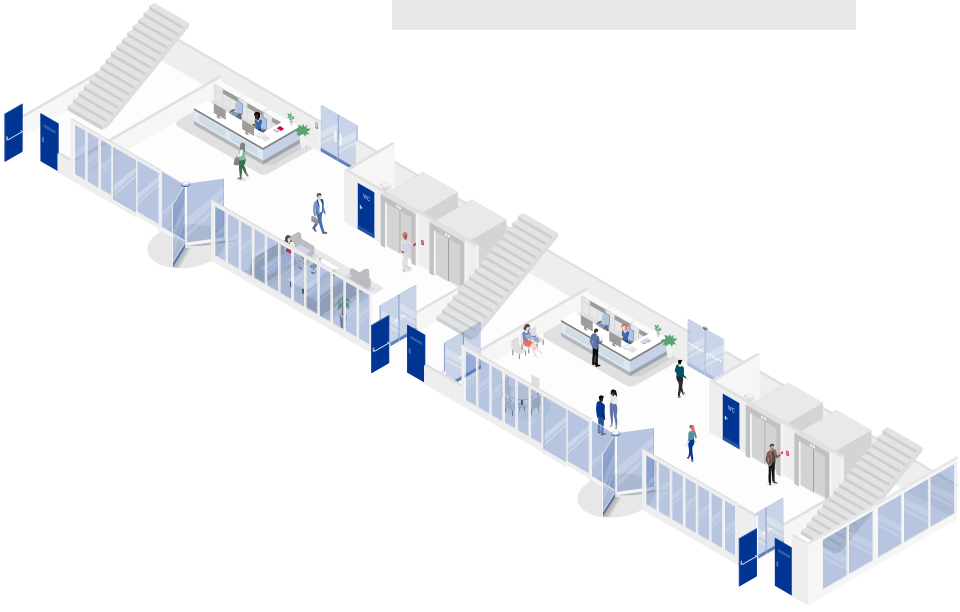
10

Emergency exits and protected routes

Emergency routes must always support free egress from the safe side while preventing unauthorized ingress from the unsecured side under normal conditions.

Coordinate fire-rated assemblies, closers, panic hardware, signage, and release logic as one package.





Zone hardware and access logic

Zone	Hardware and system categories	Access logic
Parking and vehicle approach	Automated vehicle barriers, long-range credential readers, license plate recognition cameras, intercom units, anti-vehicle bollards, handheld terminals	Ticket or permit credential; separate lanes for spectators, VIP, delivery
Perimeter and outer security line	Full-height turnstiles, attended gates (accessible), automatic sliding doors, handheld terminals	Valid event ticket, with credential-matched reader per zone
Main spectator ingress	Half-height and full-height turnstiles, speed gates (accessible lane), people-counting sensors, access control software, handheld terminals	Ticket validation; segregated home/away sections
Concourse and vomitories	Half-height turnstiles, automatic swing doors, emergency exit devices, manual swing doors with door closers, handheld terminals	Ticket holder access; restrooms and food and beverage open; controlled bowl re-entry
Seating bowl access	Half-height turnstiles, access control readers at entry points, handheld terminals	Seat-zone specific credential for high-capacity events
Hospitality, VIP, and VVIP zones	Speed gates, revolving or sliding entrance doors, elevator control units, visitor management terminals, handheld terminals	Dedicated credential; time-limited access; visitor management log
Player tunnel and dressing rooms	Automated sliding folding door systems, manual double doors with pull handles, cabinet locks	Biometric or high-security credential; strictly limited access list
Media, press, and commentary	Automatic swing doors with access control, double doors with acoustic hardware, facial authentication readers	Accreditation credential; no general access at any time
Back-of-house, service, and plant areas	Full-height turnstiles (wide format), automatic sliding doors, utility locks, master key systems, facial authentication readers	Staff credential and delivery time-window logic
Restricted and admin areas	Manual swing doors with access control, demountable partitions, cabinet locks, utility locks, master key, facial authentication readers	Staff role-based access; no event-day credential crossover
Control room	Manual swing doors with access control, facial authentication readers	Senior security personnel only; hardwired, no wireless dependency
Emergency exits and protected routes	Emergency exit devices with crash bars, automatic door releases, fail-safe hardware. Electronically controlled emergency exit systems	Free egress always; controlled entry only from secure side

Note:
Access control software should integrate with ticketing and accreditation across all relevant zones.



Argus barrier with integrated SafeRoute system



How this helps stakeholders

- Owners see how the whole venue can be divided into manageable risk zones.
- Operators gain a zone map that can inform SOPs, crowd management staffing plans, and incident response.
- Security leaders gain a basis for credential hierarchy and anti-tailgating measures.
- Architects and specifiers gain a structure for coordinating doors, hardware sets, power, and data routes.

05 Technology that works under event-day pressure

Technology in a stadium must work at full load.

Not just in a test lab or empty venue, but in the presence of 80,000 people, all of them carrying smartphones, all connected to stadium Wi-Fi, all generating radio frequency noise simultaneously.



5.1
Ticketing and credential trust

Different credential types serve different operating needs. QR tickets are convenient for high-volume spectator ingress. Smart cards can support staff and recurring accreditation. Mobile wallets, NFC and barcode credentials can support VIP, hospitality, selected staff, media, and temporary event accreditation, where fast access, remote provisioning, time-limited validity, and immediate revocation are important. Long-range credentials can support vehicle access. In the highest-security locations, stronger identity assurance may be justified.

The important point is not to declare one technology universally best. The important point is to match credential type to risk, throughput need, and user experience. When fraud risk is material, operators should consider anti-duplication controls, timed validity, zone mapping, reissue rules, and exception escalation procedures.



Specification warning

Weak credentials create avoidable risk. Legacy Bluetooth (pre-4.0) and unencrypted RFID present known risks; modern BLE and NFC mobile wallet credentials using encrypted provisioning offer significantly stronger protection. Specifications should require modern encrypted credential platforms, aligned reader capabilities, and security levels matched to each zone.

Credential technologies: a hierarchy of trust

Trust should rise with risk. Each credential type should be selected for the access zone it protects. Not simply for cost or convenience

- Long-range UHF transponders: vehicle access at parking barriers; hands-free authentication at speed
- QR code / barcode tickets: general spectator entry with anti-duplication logic; low-cost and mobile-friendly
- RFID smart cards: staff, media, and accreditation; encrypted formats reduce cloning risk
- Mobile NFC credentials: VIP, hospitality, and selected staff access; remotely revocable with secure provisioning
- Biometric verification: highest-security zones such as control rooms; strongest assurance, lowest throughput; modern facial recognition at scale can match speed gate throughput in optimized deployments

5.2
Wired and wireless architecture

Stadium environments place unusual stress on communications infrastructure, from high spectator density and temporary networks to broadcast activity and event-day device volumes. For that reason, critical-path access points are often best supported by robust wired infrastructure, especially where uninterrupted operation is essential. Wireless can still be appropriate in lower-risk, lower-traffic, or retrofit scenarios, provided performance limits, maintenance implications, and cyber controls are clearly understood. The right architecture depends on zone criticality, event profile, site constraints, and failure consequences.

5.3
Video, parking, and command integration

Access control should not operate in isolation. In practical stadium operations, the strongest outcomes come when ticketing, access events, CCTV or VMS, parking systems, intercoms, occupancy tools, and the venue command function can share relevant data. This enables faster verification of incidents, better lane management, stronger exception handling, and clearer post-event review.



5.4
Occupancy and congestion visibility

People counting, occupancy dashboards, and congestion alerts can help operators manage concourse build-up, toilet pressure, concession clustering, and delayed egress. These tools should support decisions, not replace them. Data quality, calibration, and response procedures matter as much as the sensor itself.

5.5
Cybersecurity and fail states

Where systems can unlock doors, release barriers, or influence route control, cyber and resilience thinking are part of physical security design. Segmented networks, controlled privileges, encrypted communications where appropriate, and clear fail-safe or fail-secure logic should be defined at design stage. The key question is always operational: if a subsystem degrades, how does the stadium continue safely?

How this helps stakeholders

- Owners gain a technology strategy based on resilience, not gadget value.
- Operators gain better visibility, fewer workarounds, and more useful event data.
- Security leaders gain stronger credential logic and clearer exception handling.
- Integrators gain a clearer basis for architecture, interfaces, and testing.



06 Life safety, egress, and compliance





Takeaway

The best evacuation plans are the ones that are never needed but always tested. Scheduled drills, regular verification of emergency exit hardware function, and post-event review of egress data all contribute to the confidence that the system will perform when it is called upon.

Life safety must work before anyone needs it.

Emergency routes, door hardware, fire-rated openings, crowd movement and staff response all come together in the moments that matter most.

A stadium can only be considered safe when its evacuation logic works as an operating reality — not just as a code statement, drawing note, or specification line.

In short: Protected routes. Clear decisions. Tested performance.

How this helps stakeholders

- Owners gain stronger defensibility and long-term asset resilience.
- Operators gain confidence that abnormal-event plans will work.
- Security leaders gain aligned emergency logic across teams and systems.
- Regulatory and risk stakeholders gain evidence of intent, testing, and maintainable compliance.



Egress as an operating scenario

Design emergency egress around real event conditions. Route capacity, door release logic, signage, crowd management staffing and command decisions must work together under pressure.



Protected route integrity

Fire-rated routes depend on the full opening set: door leaf, frame, hardware, glazing where used, and closer or operator behavior. One incompatible component can compromise the whole route.



Evidence-based capacity

Avoid generic throughput assumptions. Calculate lane counts, door widths, and route capacities against local code, stadium geometry, expected occupancy and event scenarios.



Accessibility as part of safety

Accessible movement belongs in the primary safety strategy. Ingress, refuge where required, supervised gates, elevator policy, signage, and crowd management staffing support must work for everyone.



Testing, drills and readiness

The strongest life-safety feature is proof that the system has been tested. Drills, pre-event checks, and post-event findings should be treated as part of the safety system itself.

07 Design principles for stadium hardware

Stadium hardware must earn its place twice.

It must withstand sharp event-day peaks and exposed conditions, and it must integrate so naturally that fans and staff barely notice it.

In short: Reliable enough for the busiest day. Discreet enough for every other day.



High-cycle endurance

Select hardware for the zone's real use volume and exposure. Endurance supports uptime and reduces disruption, but maintenance still matters.



Weather resilience

External and semi-exposed openings must account for moisture, corrosion, dust, heat, and UV exposure.



Maintainability

Plan service access, diagnostics, replacement cycles, and maintenance windows before specification.



Accessibility and inclusive use

Accessible gates, clear widths, automatic operation, mounting heights, and route legibility belong in the main design.



Discreet, safe, and non-obtrusive design

Security should not create trip hazards, awkward projecting elements or a hostile visual language where a softer solution is appropriate.



How this helps stakeholders

- Owners gain lower disruption and better total-cost outcomes over time.
- Operators gain higher availability on event days.
- Architects gain solutions that support design quality and user safety.
- Maintenance teams gain more serviceable installations with clearer replacement planning.



08 Stakeholder priorities by stadium role

Security only works when every stakeholder has a common understanding of what success means.

A stadium project brings together many decision-makers: owners, operators, security teams, architects, consultants, integrators, event partners, and regulators.

Each role has different priorities. The purpose of the playbook is to turn those priorities into a shared security intent. From the owner commissioning the venue to the integrator commissioning the system.

In short: Different roles.
One operating logic.





Owners and governing bodies

Protect reputation, event readiness and long-term asset value. Security should support venue resilience and the ability to host more competitions, concerts and non-matchday events — not sit as a compliance afterthought.



Venue operators and security leaders

Need operational control when the venue is busiest. Design should support live visibility, staffing efficiency, incident response and predictable performance during ingress, peak movement and egress.



Architects, specifiers, and consultants

Need security decisions to fit the stadium fabric. Access control, circulation, bowl, concourse, hospitality areas, door schedules, services, and code alignment should be coordinated early.



Integrators and technology partners

Need clarity on interfaces, reliability, commissioning, fail states, and maintainability. The playbook is designed to showcase what needs to connect, why it matters, and how performance will be tested.



Event partners and third-party operators

Need security that works with temporary overlay and live operations. Accreditation, F&B, housekeeping, broadcast, logistics, and service routes must stay controlled without slowing event delivery.



Regulatory and risk-compliance stakeholders

Need evidence of intent, readiness and maintainable compliance. The playbook is to be used as a strategic guide and to promote coordinated, tested and defensible solutions, supported by relevant authority, federation or event-owner guidance where applicable.

09 Event-day readiness checklist

This checklist is intended as a practical reference for venue operators and security teams. It covers the key verification points before, during, and after an event.

Pre-event checklist

Access control systems & credentials

- ☐ All access control readers tested and confirmed online
- ☐ Credential database updated with correct ticket allocations and time windows
- ☐ Verify ticketing and accreditation databases are current and correctly mapped to access zones
- ☐ Anti-passback logic enabled and tested for all spectator entry lanes
- ☐ Segregation boundaries verified - home and away credential zones confirmed

Entry points, gates & doors

- ☐ Turnstile cycle test completed - mechanical and electronic function verified
- ☐ Test readers, turnstiles, supervised gates, barriers, intercoms, and critical door releases
- ☐ Emergency exit devices tested for free-egress function in all zones
- ☐ Door closers checked - all emergency exit doors self-closing correctly
- ☐ Accessible gate staffing confirmed and gate functions checked
- ☐ Confirm accessible ingress routes, staffing points, and exception-handling procedures

Vehicle & perimeter access

- ☐ Vehicle barrier system online and barrier arms responding correctly
- ☐ Confirm parking controls, approved vehicle lists, and protected emergency access routes

Monitoring, control room & systems integration

- ☐ Verify that CCTV, command positions, and access-event monitoring are online
- ☐ People-counting sensors calibrated and feeding live data to control room
- ☐ Control room access restricted to authorized personnel - access log cleared
- ☐ Communication tested between access control platform, surveillance, and operations

Operations planning & crowd management

- ☐ Confirm lane plans by stand, ticket class, segregation policy, and hospitality routing
- ☐ Review weather conditions and adjust staffing, queue management, and equipment readiness as required
- ☐ Align pre-event communications with all stakeholders

Emergency and safety preparedness

- ☐ Emergency evacuation zones confirmed in access system - release sequence programmed

Live event checklist

Live monitoring & control

- ☐ Live occupancy monitoring active across all zones
- ☐ Concourse flow monitored; hotspots addressed
- ☐ Track concourse density, queues, restroom pressure, and vomitory flow
- ☐ Continuous access-log archiving verified

Entry flow & queue management

- ☐ Monitor queue build-up by sector and redirect spectators early
- ☐ Correct wrong-gate arrivals before they reach the lane head

Access control integrity & exceptions

- ☐ Access-data anomalies flagged and investigated promptly
- ☐ Track failed scans, duplicates, accreditation mismatches, and tailgating

Segregation & restricted access enforcement

- ☐ Segregation boundaries maintained; violations escalated
- ☐ Protect restricted routes and maintain separation policies

Emergency readiness & safety

- ☐ Emergency exit hardware kept ready throughout the event
- ☐ Critical emergency routes kept clear and ready

Post-event checklist

Egress monitoring & crowd dispersal

- ☐ Egress flow monitored until venue is clear
- ☐ Monitor bowl egress, concourse clearance, and external dispersal rather than focusing only on door release
- ☐ Manage parking release, rideshare pressure, and crowd build-up at transport nodes

Access control reset & system transition

- ☐ Restore access zoning progressively as the venue transitions from event mode to reset mode
- ☐ All emergency exit devices confirmed closed and re-secured

Data management & reporting

- ☐ Access log exported and stored securely for required retention period
- ☐ Export and review access-event data, occupancy trends, and incident notes
- ☐ Post-event occupancy data reviewed against design assumptions

Incident review & documentation

- ☐ Incident log reviewed and any access-related events documented
- ☐ Record faults, unusual exceptions, and operational lessons for the next fixture
- ☐ Lessons identified and captured for next event briefing

Takeaway

The access log from every event is a data asset. Reviewing peak-entry rates, zone occupancy curves, and any access exceptions after each event builds a picture that allows the operation to improve continuously – reducing queues, improving credential accuracy, and identifying the hardware and zoning decisions that need adjustment.



How this helps stakeholders

- Owners gain a practical event-day tool.
- Security leaders gain a common checklist for control room and field teams.
- Owners gain evidence of disciplined operations and continuous improvement.

10 Conclusion: designing for the moment that matters



Stadium security protects more than a venue. It protects the experience people came for.

Every major stadium in the world was built to create something extraordinary – the roar of a crowd, the tension of a final minute, the memory of a moment shared between strangers who will remember it for the rest of their lives. Stadium security exists to protect that experience, and the people living it.

This playbook has argued that achieving that goal requires thinking about stadium security not as a checklist, not as a product category, and not as a compliance exercise – but as a design discipline. One that begins with the first line on the architect's drawing board and continues through commissioning, opening day, the hundredth event, and the unexpected emergency that, if the design is right, the venue will navigate without anyone ever knowing quite how close it came.

The three pillars – safety and compliance, security and access zoning, fan and staff experience - are not competing priorities. They are the same priority described from three different angles. A venue that is genuinely safe is also genuinely secure. A venue that is genuinely secure can also be genuinely welcoming. And a venue where fans feel welcome, and safe, and free to lose themselves in the occasion – that is the venue that fulfills its purpose to make every moment matter.



How can you create a safer, more seamless stadium experience?

dormakaba brings together access control systems, entrance solutions, door hardware, master key systems, and integrated security and access platforms under a single point of expertise for stadium and major venue projects.

From vehicle barriers at the approach road to emergency exit devices in the evacuation corridor, turnstiles, automatic doors, sensor barriers, access control, dormakaba provides the technology, the specification support, and the lifecycle service that major venue projects require.

Whether you are at feasibility stage, design development, or planning a retrofit of an existing venue, our team works with owners, architects, integrators, and operators to design access solutions that protect people, enable movement, and support the events that make stadiums matter.

"The right credential, in the right place, at the right time. Security that is invisible to the fan but unbreakable for the operator. A venue that handles the extraordinary with the same confidence it handles the ordinary. That is what great stadium security design delivers."

Our sustainability commitment

We are committed to fostering sustainable development along our entire value chain in line with our economic, environmental and social responsibilities toward current and future generations. Sustainability at product level is an important, future-oriented approach in the field of construction. In order to give quantified disclosures of a product's environmental impact through its entire life cycle, dormakaba provides Environmental Product Declarations (EPDs), based on holistic life cycle assessments.

www.dormakaba.com/sustainability

Our offering

Access Automation Solutions

Entrance Automation
Entrance Security



Access Control Solutions

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems



Access Hardware Solutions

Door Closers
Architectural Hardware
Mechanical Key Systems



Services

Technical Support
Installation and commissioning
Maintenance and repair



EN, 05/2026
Subject to technical modifications.

dormakaba.com

dormakaba
UK & Ireland Ltd
403B The Spirella
Bridge Road
Letchworth
SG6 4ET
info.gb@dormakaba.com
dormakaba.com